2010

Cyber crime and telecommunications law

Robert Imhof

Follow this and additional works at: https://scholarworks.rit.edu/theses

Recommended Citation

This Thesis is brought to you for free and open access by RIT Scholar Works. It has been accepted for inclusion in Theses by an authorized administrator of RIT Scholar Works. For more information, please contact ritscholarworks@rit.edu.
Cyber Crime and Telecommunications Law

Researched by Robert Imhof
Thesis Committee: Charlie Border, Daryl Johnson, Tom Algoe

Defense Approved on May 10th, 2010
# Table of Contents

- **Introduction** ................................................................. 5
- **Literature Review** ............................................................. 8
- **Purpose Statement** ............................................................ 29
- **Methodology and Deliverables** ........................................... 29

## Telecommunications Laws

- The Computer Fraud and Abuse Act .................................... 32
- The Digital Millennium Copyright Act .................................... 38
- The Wiretap Act ................................................................. 46
- The Stored Communications Act .......................................... 50
- Identity Theft and Aggravated Identity Theft ............................ 54
- Access Device Fraud .......................................................... 56
- CAN-SPAM Act ................................................................. 60
- Wire Fraud ....................................................................... 62
- Communications Interference ............................................... 63

## Sociological Theories

- Differential Association ..................................................... 65
- Anomie and Strain Theories ................................................ 71
- Social Conflict Theory ...................................................... 77
- Rational Choice Theory .................................................... 82
- Social Learning Theory ..................................................... 86
- Social Control Theory ....................................................... 90
- Control Balance Theory ......................................................... 94

## Interviews

- Bradley Bartram ............................................................... 99
- Michael McCartney .......................................................... 124
- James Domres ............................................................... 139
- Martin Littlefield ............................................................ 152
- Mark Musone ............................................................... 163
Case Analysis

United States vs. Jeanson James Ancheta .............................................................. 188
United States vs. Scott Levine ................................................................................ 192
United States vs. Paul G. Ashley, Jonathan David Hall, Joshua James Schichtel
Richard Roby, Lee Graham Walker, and Jay Echouafni ...................................... 196
United States vs. Gary McKinnon ........................................................................ 201
United States vs. Kevin Mitnick ........................................................................... 205

Final Analysis ............................................................................................................ 208
Works Cited ................................................................................................................ 218
Special Thanks

I would like to thank my committee: Charlie Border, Daryl Johnson, and Tom Algoe for all your help and inspiration. I would also like to thank my interviewees: Brad Bartram, Mike McCartney, James Domres, Martin Littlefield, and Mark Musone for your time and efforts in helping to make my research a success.

I would also like to thank God and my parents for inspiring me to work hard and be the best I can be. I wouldn't have made it this far without your help.

Subject Category: Information Security
Key Words: Cyber Crime, Security, Sociology, Law, Hacker
Introduction

As the world becomes more dependent on technology and interconnected networks it changes the dynamic of how the world works. Before extensive computer systems and digital networks both public and private enterprise alike kept much of their confidential information in physical form such as in documents filed in cabinets. It was during this time that organizations and government institutions had to concern themselves primarily with physical security and internal classification schemes to make sure that this information didn’t become available to those who didn’t have the rights and who could also cause substantial harm with the information in question.

As our modern economy continues to shift towards a post-industrial economic base we begin to put much more emphasis on information and the providing of services. Much of this shift has lead to the increased dependency on digital systems to both store and process very large amounts of information. This shift has given rise to extremely large and important databases and storage area networks. Through the use of these technologies it allows an organization to store and process amounts of information that would have been seen as impractical just twenty years ago. This availability of information allows an enterprise to be more efficient and profitable because business analysis and intelligence personnel can now use tools and their own developed skills to pour quickly through information stored in storage area networks and data warehouses in order to find market trends and possible areas of future profitability.

The public sectors uses technology in just as important, and possibly more important, ways compared to the private industry. Federal and state databases that contain information on criminal DNA, fingerprints, open cases, evidence, and criminal histories allow investigators to
pour through large amounts of information quickly and efficiently in order to solve their cases as soon as they can.

All of this information from both private and public industry is a very attractive target for attackers. Because of the impressive amount of information that can be taken without even having to be physically on the scene makes for a target that is too enticing for some to ignore. The rate at which information systems are attacked and compromised skyrockets every year according to studies from both private interest groups such as the SANS Institute and through government agencies such as the FBI and their crime statistics.

The way in which most organizations have dealt with this problem has been to simply spend and implement technology, such as firewalls and intrusion detection systems, to keep the attackers out of their systems. Although this is a necessary step in order to institute best practices and fall into regulatory compliance from government acts such as Sarbanes-Oxley and HIPAA, it really doesn’t do a good enough job. If all that it took to keep an information system safe from intruders was technology than the solution to this growing problem would be simple. However as evidenced by the rising success of electronic attackers it shows that this isn’t the case.

What this research will do is to provide a more in-depth look at the attacker. This thesis does not propose or develop a new technology for combating the malicious user, rather it provides a look into who is actually looking to compromise the system. A famous quote by Sun Tzu is as follows: “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer defeat” (Tzu, ch.III).

This quote, although originally intended for use in military strategy, is also essential for the information security manager who is in charge of protecting their organizations vital
information assets. Many times people in these positions know the technology that they are in charge of, but rarely have a concept of who may attack their critical information assets.

Many times people will look at these attackers and infer that financial gain was their primary motivation. But is that really what motivates people in most cases? This thesis aims to provide research into the motivations behind the attacker. If the information security manager can understand who their enemy is and what their motivations may be, then they can create more effective security policies and baselines that would reduce the probability of successful exploits on their systems.

Because computer crime and the underlying criminology behind electronic attackers are very new there is a relative shortage of available research and literature on the subject which makes this research very important. I will be using my own developed methodology for this project which will be described in the section titled Methodology & Deliverables. This methodology will cover a number of different bases and provide for a complete view on what typically makes and motivates these attackers.

The deliverables from this research will be very useful in helping to develop strategies to combat cyber criminals. With the help of this research, organizations will be able to take a look at what their organization does and what may motivate somebody to attack them.
Literature Review

Although much has been written and researched concerning technological methods for securing an enterprise’s information system, very little has been researched about the people behind these attacks. Perhaps this is due to the relatively young field of information technology and as a result not enough consideration has been put into the electronic attackers and who typically fits this profile.

There has been some research into different kinds of hackers as shown in research by Holt and Kilger (2008). In this study they interviewed two populations of hackers. The first group are those interviewed from a hacker convention and were labeled as the wild group. The second group consisted of students that were enrolled in an information security course. The purpose of this study is to see if there are any significant differences between the two control groups and what may cause these differences.

Holt and Kilger (2008) gave a warning about their findings in this study when they state: “It should be noted here that there are significant barriers to entry for researchers attempting to study the hacker community … the privacy and secrecy inherent in the hacker community makes collecting data through social science methods such as personal interviews, field observations, and surveys a difficult task” (Holt, p.71). This means that although the findings of this study may be very interesting, they should be taken in the context of the secrecy surrounding the hacker subculture.

The first interesting finding of this study concerned the gender characteristic. According to this study, the control group had a higher percentage of females than the wild control group, yet the male sex had a higher percentage in the wild group. This is interesting as it shows how a
traditionally male dominated field is having an influx of females on the formal educational group. It should be noted that although the difference in the male sex between the wild and control group is relatively small, there is a large difference between the female wild and control groups.

This study also seems to dispel the myth that hackers are brilliant teenagers with too much time on their hands. Although the 18-24 age group was high for both groups, we find that there is a much larger percentage between the ages of 25-36. The average age of the control group (33 years) is older than that of the wild group (28 years).

The findings concerning the educational level of the two groups varies somewhat. While the control group had a higher percentage in the “some college” and “some grad work” categories, the wild group had a higher percentage in the “high school” and “college grad”. This may be explained by the fact that the control group was taken from an information security course and so we must then assume that they are still completing their college degree.

The wild group also significantly outperformed the control group in hours spent on the computer, number of computer languages known, and they were also younger on average when they had their first computer. What is surprising is that the control group had nearly equal percentages to the wild group when it came to the categories of “I do not trust the government” and “I should be able to look at any information regardless of the lack of official permission to do so”. This would seem to indicate that there isn’t a large gap in information ethics between the two groups.
According to Holt and Kilger (2008) they are able to hypothesize from their findings that:

“The level of perceived skill with computer technology is higher for the “in the wild” group versus the control group … The number of friends that an individual considers for hackers is larger for the “in the wild” group than in the control group … Individuals in the wild will spend more time in communication with others on-line than in the control group … Individuals in the control group will score lower on a legitimizing scales of unethical hacking activities, called the haxor scale, then the wild group … Individuals in the wild will score lower in terms of perceived knowledge of what is proper and improper on-line … Individuals in the “in the wild” group will have lower self control than those in the control group” (Holt, p.73).

The literature suggests that hackers in the “wild” have a higher perceived mastery than the control group and they generally compensate for their lack of support by further developing a mastery of the technology. “Perhaps the largest number of hacking friends is also a result of individuals in the wild looking for social support from within the subculture to compensate for a lack of normative support from traditional social institutions” (Holt, p.74).

The findings of this study by Holt and Kilger (2008) seems to suggest that the wild group have a greater interest in the underlying technologies as evidenced by the more time they spend on the computer as well as their greater perceived mastery of the technology. This study is a very important contribution to my research which differs in that my research aims to give a complete criminal profile based around criminology, case studies, and the experience of professionals who have experience with this subculture.
The findings from the previous study suggest that those in the hacker subculture are genuinely interested in their craft and pursue it both as a hobby and as a passion. The study by Sergey Bratus (2007) entitled “What Hackers Learn that the Rest of Us Don’t” is a study into what amounts to the intellectual pursuit of those who are involved in the hacker community. This study finds that there is a frustration in the hacker community about the traditional way that engineering design and development is handled. “The frustration such trends create is a driving force behind hacker culture, which eschews the path of least resistance and concentrates on fully understanding underlying standards and systems, complete with their border cases and vendor implementation differences” (Bratus, p.73).

This research also finds that hackers invest a lot of time into reading the documentation behind technologies in order to fully understand the underlying technical concepts. “Hackers insist on understanding the underlying API’s implementation and exploring it to confirm the documentation’s claims” (Bratus, p.73). Many times hackers are driven by their curiosity of the underlying technology question and the logic with which it has been engineered and begin to think about ways to alter the technology in new and often better ways. The result of this intellectual curiosity is that they will develop new ways for technologies to be implemented. “Hackers insist on tools that let them examine the full state of the system across interface layers and modify this state, bypassing the standard development API. If such tools do not exist, developing them becomes a top priority” (Bratus, p.73).

The research by Sergey Bratus (2007) finds that hackers have an intimate knowledge and drive to an intellectual pursuit of programming languages to understand exactly how these technologies work. This is what drives many in the hacker community to test and try to break or
alter applications in order to use them in ways that were not originally thought of by the original developers.

Sergey Bratus (2007) suggests that the drive to understand technology and its underlying concepts is an integral part of the hacker subculture and is something that is common among nearly all members of this growing culture. Although there is a perception of hackers in the popular media of being solitude opportunists who take advantage of those who are ignorant of the digital world, this research seems to indicate otherwise.

What has been strongly suggested in this research is the attitude and drive by those in the hacker culture to contribute to their craft. This research explains that the opportunity for hackers to communicate with others in their craft and talk about challenges met is a significant part of the culture. They are able to do this through Internet Relay Channels as well as certain Hacker publications and websites.

Sergey Bratus (2007) finds through his research that much of the integral technical information that hackers know is absent from many computer science curriculum's. This means that many who come to the information technology profession through the traditional academic path are not as well versed on technology and its underlying concepts as their hacker counterparts.

“The main obstacle toward developing a hacking approach was that students attitudes, apparently conditioned by their previous programming experience, were those of developers rather than testers, reverse engineers, or attackers. Developers are rewarded for sticking to tried and true recipes, generally learn to trust API and interface documentation, and so on. They intentionally confine themselves to working within narrowed computing environment models for better productivity
or compatibility, whereas, in reality such confines do not exist or can be bent by
the attacker … programmers are under pressure to produce working, easy to
understand code as soon as possible, leaving them no time to “question
everything”, explore less used library or protocol features, or puzzle out how
particular APIs are implemented (not to mention that proprietary software vendors
tend to discourage the latter activity, sometimes in an extremely heavy handed
manner).” (Bratus, p.75)

The research by Sergey Bratus (2007) explores a very important concept in the difference
of attitudes between those who are involved with the hacker subculture and those who take a
more mainstream view on technology. Many times people are heavily influenced by their
previous programming experience and how they were taught how to develop software. Research
by Duley and Maj (2002) argues for a non-traditional method of teaching students the concepts
of software development and its underlying complexities.

In their research, Duley and Maj (2002) suggest new and alternative ways for students to
learn how to develop code. It has been noted in the previous research mentioned here that
students do not understand the underlying complexities, rather they tend to have the goal of
trusting the underlying API, get the correct syntax and semantics, and just get their program to
work correctly. This research notes that the traditional method of programming is geared towards
a syntax approach where students are encouraged to get the programming correctly from a
semantic point of view. They are not usually taught about the underlying components of a
programming language.
The methodology that Duley and Maj (2002) used in gathering statistics of student knowledge at the conclusion of traditional programming courses came from twenty two Australian Universities. These students were tested by questions involving what they were taught in their traditional programming courses. What is disturbing is that only 13% of the students were taught about exception handling, 13% about data structures, and 0% about polymorphism.

The authors suggest a new way for university programming courses to teach programming languages in order for students to better understand the underlying technical concepts. This research suggests that students would better understand the technical components of programming if they learned from others. This is a concept that is widely adopted and used in the hacker community as hackers often communicate with each other through various forms of media.

“Many faculty members involved in teaching programming are drawn from fields like mathematics or electronics engineering … ‘Most of us teach what we were taught and teach it in the way we were taught it. Since nobody has yet graduated from a software engineering program (1998) we will have to teach unfamiliar material” (Duley, p.9). This makes it more imperative that students are interested in what they are learning and also learn from others.

The authors suggest that programming courses should break from tradition and teach programming on a concepts first basis. They believe that this method of teaching will encourage students to immerse themselves in the technologies being taught. Duley and Maj (2002) believe from their research that many traditional programming courses either shy away from difficult concepts and lower the bar or thoroughly explain the concepts but right before implementing the concepts and thus this overloads the student.
Duley and Maj (2002) believe that the traditional programming first concept “appears to be perpetuating the practice of concentration on syntax and semantics … This, according to the authors, appears to be teaching a language the wrong way round. We hold that students should be encouraged (driven) to clearly establish first the idea of what they are trying to do, to think through a problem and to understand how to think a problem through” (Duley, p.232).

The research from Duley and Maj (2002) seems to validate the research from Sergey Bratus (2007). It appears that while hackers are truly interested in their craft and strive to fully understand it, students are being taught programming in a methodical manner that seems to encourage syntax and semantics over the concepts that form the base of the technology that they are creating. This appears to put those who come to the field at a disadvantage when they are trying to develop secure software yet they do not fully understand the concepts over which the software is developed. It stands to reason that this causes programming errors which lead to vulnerabilities such as buffer overflow attacks.

Students and those who are in the same relative age bracket as students make up a rather significant part of the hacker community. R.A. Coldwell (1993) conducted a study into how students perceive computer crimes in his research titled “University Students’ Attitudes Towards Computer Crime: a Research Note”.

The purpose of this research by R.A. Coldwell (1993) was to determine if there is any significant differences in social views toward computer crime between students who are in machine concentrated majors such as computer science and engineering, and those students from people based disciplines such as healthcare and social work. The methodology that was used in this study involved a lecture based on non-professional practice in computing. After this lecture
students from both the machine and people based disciplines were asked a variety of questions concerning the ethical basis of hacking.

This study found that students from the machine based disciplines were far less likely to determine the ethical ramifications of hacking than their people based counterparts.

“Development of the young, computing-based disciplines has reaches an early, introverted, formalistic phase where they are sorting through their beliefs and testing limited hypotheses before they contemplate, fully, their social context … Computer Science has a fixation on methodology. It has not yet developed appropriate ethical standards nor has it developed an adequate code of practice” (Coldwell, p.11).

This research seems to suggest that the lack of discussion in many technical courses leads to the lack of understanding among computing students concerning hacking and its ethical standards. The result of this could be an explanation for the findings of Holt and Kilger (2008) when they were able to find little difference in the ethical beliefs of the control and wild groups. It stands to reason that it would be wise for higher education institutions to implement more extensive technological ethics courses into their standard curriculum's.

Most hackers are very smart and have at least some level of college training. Dr. Coldwell finds two fundamental problems which may have led to the rise of the hacker subculture. The college students “are being socialized into their disciplines by lecturers and tutors who have been educated throughout a strongly machine-related phase of the development of the subject areas. Secondly, and perhaps even more significantly, this socialization process follows undergraduate students earlier impact with childhood socialization when they may have developed anti-social attitudes and perhaps, pro machine withdrawal responses” (Coldwell, p.13).
The dictionary term for socialization is “a continuing process whereby an individual acquires a personal identity and learns the norms, values, behavior, and social skills appropriate for his or her social position”. This essentially refers to the way in which we learned right from wrong and how to be a contributing member of society.

It is important to understand from this study that although most contributing members of society find the act of hacking with malicious aforethought to be unethical, that is usually not the case for those who have the technical knowledge to do so. It should be noted however that those who are from a people oriented curriculum usually communicate well and as such it would usually make them excellent social engineers. Many times can be more successful at gaining unauthorized access than through electronic means.

Floyd, Harrington, and Hivale (2007) and their study titled “The Autotelic Propensity of Types of Hackers” is a study into what motivates hackers and what really drives their intellectual curiosity. The authors define autotelic behavior as a characteristic in people who often see challenges as an opportunity to do something new. “Autotelic behavior is a characteristic of individuals who see challenges as opportunities for action, when others see challenges as threats” (Floyd, p.1). This research seems to concur with the other studies in this literature review about the hacker mindset being driven by intellectual challenges.

This study hypothesizes that there are different hacker groups and these different groups are motivated in their actions for very different reasons. The first hacker group is generally motivated by curiosity and the intellectual pursuit while the other is motivated by crime. “Steven Branigan, a founding member of the New York Electronic Crimes Task Force, claims that those who get into computers first, and then start hacking, are motivated by curiosity whereas those
who have criminal tendencies to begin with and who later learn computer technology, figure out how to apply the technology to their trade” (Floyd, p.1).

Autotelic behavior, according to this study, is very commonly exhibited in those who engage in white hat hacking. These individuals, as this study suggests, believe that sharing information is a powerful advantage for their craft. By sharing information it allows them to inspire potential hackers to join their community while at the same time bragging about potential triumphs in their projects.

Although my research delves into what makes a hacker and why people become hackers in the first place, this research by Floyd, Harrington, and Hivale (2007) seems to suggest that hacking in and of itself can be a powerful motivator.

“Because hacking is seen as an enjoyable activity by those in the hacking community, these individuals seek the enjoyment of hacking again and again, and over time it becomes self-motivated. They become deeply immersed in the activity. Also, due to the high concentration and strong self-motivation, learning takes place very quickly. The learner is eager to find the necessary sources and tools and spends time on the acquisition of skills, even if some aspects are not exciting in themselves, as long as they contribute to the autotelic activity … It may be that the freedom to choose specific challenges matches with skill levels may be stifled in the corporate world”. (Floyd, p.2)

The findings of this research were supported by an unorthodox methodology by Floyd, Harrington, and Hivale (2007). In this study they enlisted the help of the hacker community
themselves as he was able to acquire communications from another hacker who was interested in this study. This hacker then sent out twenty volunteer surveys to which ten replied.

This survey asked a number of questions designed to judge the autotelic propensity of their actions. Floyd, Harrington, and Hivale (2007) were able to decipher from these results that those who hack for an autotelic purpose are generally doing it for good and intellectual curiosity, they are the white hat hackers. Those who hacked for personal gain or destructive purposes did not hack for autotelic purposes.

A purpose of my research into the hacker profile is so that information technology practitioners can understand who they are up against as they try to secure an enterprise from unauthorized breaches of confidentiality, integrity, and/or authentication. Floyd, Harrington, and Hivale (2007) believe that this study inspires “understanding of the different motivations (and) may lead to “thinking like a hacker” so that security controls can be developed that will thwart the variety of hacker types that they may encounter in their careers” (Floyd, p.4).

A common theme throughout the research so far has been that hackers are many times motivated by curiosity and the intellectual pursuit. This conclusion in most cases thus far has been based on sample groups and second hand accounts. The research by Roy Want (2008) titled “The Seeds of Inspiration” are based on his firsthand accounts of what motivates him to be a hacker. This research greatly enhances my own since this is based on first hand experiences and self described motivations rather than hypothesis based on second hand information provided by those who are in the hacking community.

Roy Want (2008) concurs with the research in Floyd, Harrington, and Hivale (2007) wherein he states that many times the act of hacking itself is exciting and motivation in and of itself. “The fun aspect of this approach was that I learned about a component’s physical behavior
by experimentation, sometimes breaking it but more often learning something unique. This is quite a different learning experience from sitting in an electrical engineering lecture and being presented with theory” (Want, p.1).

Although the author recites his experience with physical electrical devices from where he could alter and create new devices, this line of thinking aligns well with the hacker as many view them today in the digital world. Roy Want (2008) describes his enjoyment of being able to take an electronic device, open it, and alter it. This desire to experiment can explain why so many in the hacking community prefer to use electronic tools that are open source. When they are able to view and alter the source code for whatever reason they want it allows them the pleasure of creating something new and exciting that the original developers never intended it for.

The excitement that hackers many times get from taking a product and expanding it beyond its original purpose is a major motivation for hackers, according to Roy Want (2008). “First, it lets us take a device that performs one function and make a mental leap to another. Second, it can bring together many unrelated components and commercial products to be repurposed for a new design need. Finally, it lets us rapidly prototype ideas and then assess their value before taking a more resource-intensive next step” (Want, p.2). This study also states that science fiction has been a very important motivation for himself and many others in the hacking and scientific community.

Roy Want (2008) gives his own profile for what he is as a hacker. The literature so far has indicated that there are many different types of hackers and along with these types come different characteristics that make up their profile. Roy Want (2008) shows an autotelic motivation in his hacking as he purely enjoys the intellectual pursuit of being able to take one device, or a
combination of multiple devices, and creating new and exciting inventions. These are characteristics that are exhibited in many cases by white hat hackers.

The research thus far has shown that hackers tend to have a vested interest in modifying machinery to perform functions beyond their original design. This literature has not stated why they have this interest. Paradiso, Heidemann, and Zimmerman (2008) in their research titled “Hacking is Pervasive” try to give a view into why hackers put so much effort forth into their behavior.

The literature thus far has seemed to indicate that hackers participate in this activity because they thoroughly enjoy it. This seems to be a reasonable explanation, but it has yet to explain why they turn to illicit activities in their endeavors. The research by Paradiso, Heidemann, and Zimmerman (2008) also gives a view into why they prefer Linux and other open source tools in their activities rather than the closed source, shrink wrapped software products available through software vendors such as Microsoft.

This research suggests that these individuals, in addition to their desire to make new components, participate in hacking because nothing they currently have available suits their specific need. “In these cases, plenty of devices and software applications exist that relate to needs in the newer field, but nothing really fits well. This creates a need to customize – or hack. In many ways, pervasive computing fits this category, drawing inspiration, practitioners, and practices from HCI, distributed computing, wearable computing, sensor networks, and other fields – creating a fertile environment for hacking” (Paradiso, p.14).

The findings of this article seem to suggest that hacking is a subculture that is filled with people from a wide variety of backgrounds. Paradiso, Heidemann, and Zimmerman (2008), from their own background as hackers present their hypothesis for why people often find this
subculture enticing. The authors suggest that it is an activity that isn’t just performed for fun and creativity, rather it is something that is done out of necessity in certain cases to solve problems. “Hacking also becomes important when external pressures limit resources and shorten schedules. There might be insufficient time or budget to design a finished solution or develop a new system from the ground up … Hacking also serves inventors who build mockups and prototypes to flush out ideas before they’re developed enough to warrant formal production” (Paradiso, p.14).

These findings seem to explain why hacking attracts so many people from different backgrounds. It is used as a problem solving tool when no other formal or established tools serve the purpose for what they are trying to accomplish. They utilize their trade as a powerful problem solving tool. This is explained by the authors when they mention how hacking was used to solve problems in the problem ridden Apollo 13 mission. Innovative thinking and problem solving to use tools beyond their original purpose in order to create a solution to a dangerous problem was necessary in this event of American history. This study by Paradiso, Heidemann, and Zimmerman (2008) shows that there is really much more to the profile of a hacker than what is commonly portrayed in the mass media.

The purpose of my research in this field is to determine the character behind cyber criminals and to find out what causes them to engage in illegal activities. It seems that both white hat hackers and black hat hackers exhibit a strong understanding of technology and machinery while also having a drive to learn more about their chosen craft. This research by Paradiso, Heidemann, and Zimmerman (2008) further complicates the image that has been popularized in American culture. According to this research, hackers are people from very diverse backgrounds that many times use hacking as a means to solve numerous problems when no other solutions are available.
In their study, Paradiso, Heidemann, and Zimmerman (2008) have found that the community is very diverse with people from many different walks of life. This study however does not explain how large this population is or further explain why there are so many tools that exist, yet many hackers feel the need to either radically alter existing open source tools or create their own. The study by Hippel and Paradiso (2008) answer these questions.

The findings by Hippel and Paradiso (2008) come from qualitative research conducted by the authors. This research is based on empirical studies that they were able to incorporate into their own studies. The question of how large the hacker community is can be answered by this study.

According to Hippel and Paradiso (2008), between 10% and 40% of computer users modify the systems, tools, and applications that they use. Cultural perception leads us to believe that the hacker community is one of secrecy and relatively low numbers. However, this study has found that potentially almost half of users use hacking in one way or another to fill their needs.

The reason put forth in this study for these relatively high numbers is that, as hypothesized in Paradiso, Heidemann, and Zimmerman (2008), most ready to use closed source software products do not fully meet the needs of the end user. The question remains in this study that since there are so many software vendors in the world, why isn’t software being developed to take full advantage of the market and meet most of, if not all, of the demands of the end users?

Hippel and Paradiso (2008) answer this question when they write

“Mass producers tend to follow a strategy of developing products that are designed to meet the needs of a large market segment well enough to induce purchase – and capture significant profits – from many customers. When users’ needs are heterogeneous, this strategy of “a few sizes fit all” leaves many users}
somewhat dissatisfied – and some users seriously dissatisfied – with the commercial products on sale. When users are dissatisfied with what producers offer, they will often innovate for themselves” (Hippel, p.66).

These findings help to explanation the recent rise in popularity for the open source software community. Even if the code is proprietary, and illegal for resale, if it is open source so it allows the user to modify these programs to perfectly fit their needs. Hippel and Paradiso (2008) find that the rise in popularity of the web and open source software have changed the ability of users to innovate much quicker and in more radical ways.

This research has found that the reason why most software producers develop applications so broad is that it covers the needs of as many people as possible. Hackers develop and modify code in order to serve the purpose of a very specific situation. “One consequence of the information asymmetry between users and producers is that users tend to develop innovations that are functionally novel, requiring a great deal of user-need information and use-context information for their development” (Hippel, p.67).

This research also attempts to give an explanation for why the hacking community is so open about their developments and completed challenges while the business world of software tend to keep much more of their intellectual property under strict controls.

“Innovators often reveal their work freely because it might be the best or the only practical option available to them … They often find that others then improve or suggest improvement to the innovation, to mutual benefit. These users also might benefit from enhanced reputation, positive network effects due to increased diffusion of their work, or other factors” (Hippel, p.67).
This viewpoint that they take in their hard earned work differs greatly from those of the software industry who use legal means to hide their source code, mostly because they are afraid of theft and lost revenues. The software industry is motivated by market factors while the hacker community is motivated by other more intrinsic rewards. They offer support and ideas for innovation at a level which allows for hacker developed tools to be higher quality than they would otherwise be because of both budgetary restraints and the lack of a formal development team that is found in software development companies.

Much of this literature review thus far has been highly concentrated on the technological drive behind the individuals in this community. Cybenko, Giani, and Thompson (2002) and their study titled “Cognitive Hacking: A Battle for the Mind” give insight into the inner workings of the hackers mind. This study delves into many aspects of what makes a cyber criminal good at social engineering, or having the ability to trick others into divulging information that they are unauthorized to divulge.

The first case study in this research by Cybenko, Giani, and Thompson (2002) takes a look into a 23 year old hacker who was able to manipulate financial markets for his own gain with only limited and basic technological tools. He was able to post stock advice on an internet forum talking about how the company Emulex was under federal investigation and that their stock value was going to be hit. The result of this was that the hacker shorted his shares and made a lot of money when the stock plummeted from his fraudulent financial advice. “It had to do with manipulating perception and waiting for altered reality to produce actions that would complete the attack … This manipulation of perception – or cognitive hacking - is outside the domain of classical computer security, which focuses on the technology and network infrastructure” (Cybenko, p.50).
The case studies presented in this research by Cybenko, Giani, and Thompson (2002) adds complexity to the already complex hacker profile. Hackers are many times not only smart people who have the skill to manipulate and alter technology to fit their needs, they are also many times smart enough to understand the human element and manipulate human nature to fit their needs. The authors contend that there are two kinds of hacking. Covert which is where the attacker tries to conceal their actions and presence, and overt where the attacker makes their attacks noticeable. A covert hacker may gain unauthorized access to a financial institution’s information systems and install kernel level rootkits to give themselves a backdoor and a way to cover their presence. An overt hacker may attack this very same financial institution, but instead of covering their tracks they may deface their website in order to make some sort of statement. “Defacements are rarely motivated by anything other than self-aggrandizement” (Cybenko, p.52).

This research also suggests that mass market media have given hackers a competitive edge with which they can expand their attacks. If a hacker can twist reality in the digital world and sound authentic when divulging what is seen as reliable stock information then it is much more likely to be believed and broadcasted on the network news in some cases. The rush of modern news media to break stories has negatively affected the accuracy and given cyber criminals an advantage to make money.

Cybenko, Giani, and Thompson (2002) offer some advice for potential countermeasures to this ever increasing threat:

“As a new threat, cognitive hacking requires new countermeasures. Source authentication, information trajectory modeling, Ulam games, the Byzantine generals model, collaborative filtering, and linguistic analysis are relatively
mature technologies in the context of applications such as e-commerce. However, these measures are immature as applied to preventing misinformation and detecting user behavior. In applying information trajectory modeling, for example, how can we distinguish the stock price fluctuations that result from legitimate stock analysts’ reports from those caused by a cognitive attack?” (Cybenko, p.55-56).

The research into the mindset of the community typically involves a subject area that is far different from the traditional machine based courses offered in science, engineering, and information technology based majors. The study of the criminal mind is much more based in the sciences of criminology and psychology. My research, as well as that offered by Robert Willison (2004), will attempt to implement sociological and criminological theories associated with more classical delinquent behavior such as stealing and violent crimes to that of the new but quickly growing criminal sector involving computer and information crime.

This literature review would not be complete unless a discussion about the mindset and criminological theories behind this mindset were put forth. This is what Robert Willison (2004) has done in his study titled “Understanding the Offender/Environment Dynamic for Computer Crimes: Assessing the Feasibility of Applying Criminological Theory to the IS Security Context”.

In his research, Robert Willison has applied the criminological theories of routine activity, environmental criminology, and the rational choice perspective to computer crime. These theories, as well as other relevant criminological theories, will be explained in depth later in this research.
What Willison found in this research is that it is in fact possible to apply certain classical criminological theories to explain the motivations behind some of computer crime’s most notorious cases. He was able to do this in his research when he used these theories in a case study involving the collapse of Barings Bank.

Willison, through this case study, found that the important elements behind routine activity theory, environmental criminology, and rational choice perspective all were found in this case study of a crime involving financial and computer fraud. If information systems managers are able to understand the criminological theories behind what motivates and causes their criminal counterparts to attack their systems then it gives them the ability to implement better and more effective controls on their critical production environments. This would also allow them to implement more effective information security policies than if they did not understand the mindset behind the cyber criminal.

“Individual incidents of computer abuse would provide complementary findings for assessing the feasibility of applying the three theories to the IS security context. Routine Activity theory, in particular, may offer more fruitful findings when applies to less complex cases … prevention strategies based around the three theories could be examined and considered for the IS security field … complementary criminological concepts could be imported to reinforce the use of the theories, and help to develop more informed prevention strategies … One of the general deficiencies of IS security is the lack of theory both used and advocated by academics in the field. The position taken in this paper is that in order to understand computer crime and computer criminals the academic discipline, which can offer substantial insight into this area is criminology. Given
the multi-disciplined nature of criminology, drawing from psychology, sociology, law, social policy and economics, it can be sent o offer a voluminous body of knowledge which IS security academics can use” (Willison, p.9).

**Purpose Statement**

The purpose of this research is to profile the cyber criminal through criminology, legal case studies, and professional interviews.

**Methodology and Deliverables**

Studies into the cyber criminal are few because the field of computing is relatively new. My research expands on the established research by exploring the hacker profile through a different methodology.

I will include classical sociological theories into this research. This step will attempt to integrate traditional theories of crime to the context in which cyber criminals commit their crimes. These theories will give certain points of view and hypothesize why criminals commit crimes. This step is integral because it will educate the reader into reasons why these individuals may want to compromise their systems. This section of the research will incorporate seven criminological theories. It will define the theory, identify its creator, explain how it has been used in the classical context, and how this theory can help explain the behavior of cyber criminals.
The next part of this research will be to research United States telecommunications laws that exist at the federal level. This part is essential to know for the fourth part of my research which will be legal case studies into cyber crime cases. This research will cite numerous relevant statutes and build context around what is illegal in this country. The reader will not be able to understand the legal case studies if they do not understand the specific statutes that were violated in each case.

The fourth part of this project will be to research legal case studies involving violations of confidentiality, integrity, and authenticity. This will be researched through the United States Department of Justice Computer Crime & Intellectual Property Division as well as through Lexis Nexis. This part of the research builds a practical context around the criminological theories which were researched earlier. This will involve six cases where I will give the background and facts of the case, the specific statute which was violated, the outcome of the case (if resolved), and information that can explain why this act occurred based on evidence from the case itself as well as criminological theories that may apply based on the background of the criminal.

The fifth part will involve interviews with individuals who have dealt with cyber criminals in the past. Their different experiences give the reader a wide spectrum of different perspectives into what makes up the cyber criminal profile. The questions asked and the answers received will be documented in this research. The first interview is with Bradley Bartram who works as an Intelligence Analyst for the New York State Office of the Attorney General. Coming from a background of both Information Technology and Law Enforcement he was able to give good insight into what makes up the profile of different cyber criminals.

The second interview was with Mike McCartney who works for the New York State Office of the Attorney General as a Senior Investigator. His background is in Law Enforcement
and ended up investigating cyber crimes as his career progressed. The third interview is with James Domres who has a background in accounting and law enforcement and like Mr. McCartney began investigating cyber crimes as his career progressed. Mr. Domres is the Assistant Chief Investigator of the New York State Attorney General's Office.

The fourth interview is with Martin Littlefield who who works for the United States Attorney’s Office and prosecutes various cyber crimes in addition to his other cases. The final interview is with Mark Musone who was able to provide a perspective of cyber crime from private enterprise.

The final part of this research will involve analysis of my findings. This will essentially be a short recap of the findings documented previously in this research. The purpose of this part will be to include a section that an IT manager, corporate executive, professor, or other professionals can quickly read and understand the findings of my research. This part will include common patterns of black hat hackers that I was able to find through my case studies and will include the most relevant criminological theories.
Telecommunications Laws

This part of the research will focus on a number of very important laws pertaining to computer crimes and telecommunications. Some of these laws focus on certain industries and some may pertain to the private or public sector, but they are all important for information security and technology professionals to be aware of in their daily duties. In addition to serving as a short summary for these laws, this section also serves as an important precursor to part five of this report which will involve analysis for a number of selected legal case studies. While this section focuses on laws which are enforced in a criminal court it does not detail regulatory legislation such as the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, or the Sarbanes-Oxley Act. The laws detailed in this section are criminal statutes while the aforementioned acts are generally considered privacy regulations and are beyond the scope of this research.

The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act is perhaps the most significant legislature in the United States pertaining to cyber crime. This act, passed in the 1980’s, has been updated a number of times since it became law. The most recent update has come from the USA Patriot Act of 2002 which increased the penalties for those who were found guilty of breaking this law. This part will discuss the various sections of the law as well as the elements that must be met to charge an individual with a violation of said law.

A few key definitions need to be defined in order to understand the sections of this law. The phrase “protected computer” is used in various points. The definition comes through case
precedent as well as updates to the law, which has changed a number of times. The current definition of a protected computer according to 18 U.S.C. § 1030 (e)(2) essentially means any computer that is not designated for public use, such as a private accounting server. This is because although the law specifically makes mention of computers used by financial institutions and the Government it also states in 18 U.S.C. § 1030 (e)(2)(B) that it is any computer which “is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States”. Essentially through an understanding of networking and through case precedent we are able to see that nearly all communications through the internet travel across state lines and thus any computer that is able to communicate as such would be considered a protected computer.

The next important definition to understand is the distinction that this law makes in regards to the difference between acting in excess of authorization and without authorization. This law defines excess of authorization in 18 U.S.C. § 1030 (e)(6) to mean an act in which an individual who has legitimate access to a system escalates their privileges of the system to a level which was not originally intended for them. The term without authorization is not explicitly defined in the law, however through case precedent such as EF Cultural Travel BV vs. Explorica, Inc., the courts have found that it means individuals who access protected systems and do not have any legal or otherwise legitimate reason to do so. Essentially by these definitions we can conclude that an individual who exceeds their privileges tend to be insiders of an organization while those who act without authorization tend to be outsiders.

The first section of this act relates to the crime of illegally obtaining national security information as defined in 18 U.S.C. § 1030 (a)(1). The first element that must be met for a
violation of this section is for an individual to knowingly access a computer without or in excess of authorization. The definition of this element has been previously defined. The second element is that an individual must have obtained national security information. Generally national security information would be information designated as secret through executive order, legislation, or classified by a government agency. The third element that must be met for this crime is that the national security information itself must either damage the United States or benefit a foreign nation. For this element to be met the individual must have had reason to believe that the information would be damaging if it were to get into the hands of unauthorized personnel. The final element that must be met is that there needs to be willful communication, transmission, and/or retention of the information. The element could be proven if the offender transmitted the information to another country or even simply if they have the national security information still in their possession.

The second section of this act relates to compromising the confidentiality of information from a protected computer as defined in 18 U.S.C. § 1030 (a)(2). The first two elements of this offense are nearly identical to 18 U.S.C. § 1030 (a)(1) in that they require an individual to intentionally access a computer without, or in excess of, authorization. The only difference is that this requires an individual to be the one to actually access the information while 18 U.S.C. § 1030 (a)(1) could also charge an individual who receives the information. The third element that must be proven is that the offender obtains information from a financial institution, the United States Government, or any protected computer as defined previously. The financial institution section of this law also includes consumer reporting agencies.

The third section of this act relates to trespassing in a government computer as defined in 18 U.S.C. § 1030 (a)(3). The first two elements of this crime state that an offender must
intentionally access and do so without authorization. This law does not charge individuals who exceeded their authorization, rather it required offenders to have had no legitimate use on the system in the first place. The third element is that the computer in question must have been a non-public computer of the United States. This means that the computer must have a specific purpose for the internal use of a Government agency, such as a database server, and not simply one that provides a service to the general public such as a web server. The final element that must be met is that the offense must have affected the United States’ use of the computer. This element can be proven by anything as obvious as a denial of service attack or something a little less obvious such as an intrusion since an intrusion consumes bandwidth and may have compromised the integrity or sensitive information, although that does not need to be proven.

The fourth section of this act relates to accessing a protected computer to defraud and obtain value as defined in 18 U.S.C. § 1030 (a)(4). The first two elements of this crime state that an individual must knowingly access a protected computer without or in excess of authorization. This means that insiders of an organization can be charged if they violated this statute by means of escalating their system privileges. The third element of this statute states that the offender must have had the intent to defraud. This element can have different meanings in different courts, but generally it has come to mean thefts in which an offender uses a protected computer to wrongly obtain something of value from another individual. The fourth element states that the illegal access of a protected computer furthered the offenders intended fraud. An example of this would be if an offender attacked a protected computer and through the attack was able to steal credit card numbers which they then used to commit credit card fraud. The final element states that the offender must have obtained something of value. Many times this element could be easily proven if they obtained money, goods or services with a measurable value. The difficulty for the government would be proving the value of stolen information.
The fifth section of this act relates to damaging a computer or information as defined in 18 U.S.C. § 1030 (a)(5). To meet the elements of this crime an offender can take two different paths. The first path, as defined in 18 U.S.C. § 1030 (a)(5)(A)(i) requires that an individual knowingly cause the transmission of a command or program that intentionally causes damage to a protected computer without authorization. An offender would meet this element if they created malware which was sent to a protected computer and resulted in damage to the computer. The second path, as defined in 18 U.S.C. § 1030 (a)(5)(A)(ii) requires an offender to have intentionally accessed a protected computer and either purposefully cause or recklessly cause damage to the computer. This part of the statute would cover outsiders since no mention is given in the statute for individuals who act in excess of their given authorization. The final element of this crime must be met for both of the paths. This final element would be met if it resulted in losses of $5,000 or more in a single year. This element could be satisfied also with cumulative losses over a one year span and over multiple machines, it does not need to be a single loss from a single machine.

The final element can also be met if it affected the medical care of an individual, such as if the attacker locked out physician accounts in a hospital resulting in the physicians unable to access vital medical records for their patients. The final element may be met if it threatens public health / safety or if it damages systems used by the government for the administration of justice, national defense, or national security. The definition of what may constitute damage was defined previously and this element may be proven with an attack against most systems used by the United States Department of Defense or Department of Justice.

The sixth section of this act relates to the trafficking of passwords as defined in 18 U.S.C. § 1030 (a)(6). The first element of this crime is trafficking which is defined in 18 U.S.C. § 1029
as the transfer or control to transfer information, which in this case would be passwords. The
second element of this statute that must be met is that the information trafficked must be a
password. Passwords as defined in this statute might not just be passwords defined in the
traditional sense, but may also be user names and other instructions for access to a protected
computer. The third element is that the offender must have done so knowingly and with the intent
to defraud. This element was defined previously. The fourth element is that the passwords must
have affected interstate or foreign commerce. An example of this would be if an offender sold
and trafficked passwords across state lines for access to a financial server. The final element of
this statute is that the computer must have been used by or for the United States Government.

The seventh section of this act relates to the act of extortion in regards to damaging a
computer under 18 U.S.C. § 1030 (a)(7). An example of this crime would be if an offender
threatens to crack a system and delete a customer database unless they were paid not to. The first
element of this crime would be for an offender with intent to extort money or something of other
value which has a monetary value. For this element to be satisfied the offender does not
necessarily need to be successful or follow through on the threat, rather just the threat itself is
satisfactory to meet this element. The second element is to transmit communication in interstate
or foreign commerce which may or may not be electronic in nature. The final element is a threat
to cause damage to a protected computer, such as a denial of service attack against the web
servers of an e-commerce website.

This is a short and concise summary of the requirements for which an individual can be
charged with a crime under the Computer Fraud and Abuse Act. This statute is very important
and that is why I detailed the elements of each offense instead of just giving a summary of it.
Many cyber offenders are charged with being in violation of this statute because of its many
parts and different violations. Every information security and technology professional should have a solid understanding of this criminal statute because of its sweeping nature and importance.

The Digital Millennium Copyright Act

The Digital Millennium Copyright Act is a significant act in United States history that was signed into law by President Bill Clinton in 1998. Although controversial, this law enacted a number of measures and international treaties designed to protect the intellectual property rights for many individuals and organizations. This act amended a number of sections in Title 17 of the United States Code, most of which will be documented in the sections below.

The first part of this act is in relation to the intentional circumvention of copyright protection systems and the first section relates to the circumvention of technological measures as outlined in 17 U.S.C. § 1201 (a)(1). This section simply states that it is illegal for an individual to circumvent a technological measure that controls access to a protected work. As defined in the statute, when the law mentions circumventing technological measures it is defined as intentionally bypassing a technical control implemented by the works owner for the purpose of controlling access to their intellectual property. An example of this would be bypassing code that a record label implements for the purpose of combating piracy of their intellectual property.

The second section of this act pertains to the redistribution of intellectual property as outlined in 17 U.S.C. § 1201 (a)(2). The element of this subsection is that no individual should manufacture or traffic in any product or service whose sole purpose is the circumvention of technological controls access to a protected work. This makes it illegal for any individual to develop or sell programs or other tools which have the specific purpose of cracking intellectual
property protection controls. This element can also be satisfied if the product or service in question has only limited use outside of its purpose to break a technological control. This means that not only is it illegal to develop a tool with its only purpose to crack a technical control, but it is also illegal if the tool only has limited purposes outside of cracking the technical control. The third way in which this element can be met is if the offender markets a tool for the purpose of cracking a technical control of a protected work. This means that a tool may have other legitimate purposes; however it is illegal if an offender markets the tool for use in cracking the technical controls that are used for protected works.

This law was amended to make it illegal for an individual to circumvent access to an entire protected work, but it also makes it illegal to circumvent access to get a portion of a protected work under 17 U.S.C. § 1201 (b). This section is designed to make it illegal for the same three acts to occur in 17 U.S.C. § 1201 (a), such as developing and trafficking a tool with the sole purpose to circumvent a technical control of a protected work, but the lawmakers felt the need to include this subsection to close a potential loophole in a case where an offender circumvents a technical control not to obtain the entire protected work but rather just a part of it. An example of where this could be applied would be if an offender develops a tool that would circumvent a protected technical control for a music CD to get the first three songs rather than the music list for said CD. As in 17 U.S.C. § 1201 (a) this section makes it illegal to develop or traffic a tool with the sole purpose, limited purpose outside of, or marketed for the specific purpose of cracking a technical control for a protected work.

The statute as defined in 17 U.S.C. § 1201 (c) was implemented with the purpose of making sure that no other statues or rights are diminished by means of this statute. The first right specifically mentioned is that this statute will not increase or diminish liability for copyright
infringement. The second right defined makes sure to reinforce the right of individuals to
develop electronics and tools so long as they are not in violation of the previously mentioned
statute. The third right is that this act must not infringe on the free speech or right of press for
any individual or organization pertaining to consumer electronics and computing devices.

A major concern during the deliberation of this bill came from librarians of non-profit
institutions who believed that this act would diminish their ability to redistribute works under fair
use. This act under 17 U.S.C. § 1201 (d) provides for exceptions during these circumstances. The
section under 17 U.S.C. § 1201 (d)(1) states that a library will not be charged with violation of
the previously mentioned statutes if they gain access to an exploited protected work if their
purpose is to determine if they wish to obtain a legitimate copy of said work. This section
however makes note that the library may not keep the exploited protected work any longer than
they need to in order to make that decision and may not use it for any other purpose.
Organizations that qualify as a Library for purposes of the statute in this section are those which
are open to the public or institutions that serve a particular purpose for research. As defined in 17
U.S.C. § 1201 (d)(2) the previously mentioned exception may only be used if the Library can not
reasonably obtain another copy of the protected work that did not have its technical controls
exploited. Subsections 17 U.S.C. § 1201 (d)(3)&(4) reinforce the point that Libraries who violate
the law in developing or trafficking in tools designed to break technical controls are punishable
through civil remedies.

The next section of this law as defined in 17 U.S.C. § 1201 (e) addresses how Law
Enforcement, Intelligence, and other Government Agencies may or may not circumvent
established technical controls on protected works. What this section of the law states is that it is
legal for Law Enforcement or a Government Agency to test and investigate these controls if they
are legally authorized. This statute was designed to allow these agencies to perform information security activities on the products to identify and address potential vulnerabilities that could lead to government information systems becoming compromised.

The sixth section of this law as defined in 17 U.S.C. § 1201 (f) pertains to the actions which are, and are not, allowed in regards to reverse engineering. This subsection of the law is of particular interest to software engineers and malware analysts who may encounter this law on a daily basis during the duties of their job. The first element as listed in 17 U.S.C. § 1201 (f)(1) states that an individual may reverse engineer a technical control for a protected work if they obtained the right to use a copy of the program. This means that they would need to have received explicit consent to do so from the owner. The second element is that the Engineer’s sole purpose must be to analyze elements of the program to achieve interoperability of the program with other independently created programs. This means that the Engineer must be reverse engineering for the purpose of being able to make the program work in conjunction with the already established system.

The third element is that this process must not have already been conducted, readily available and it must not constitute copyright infringement. The term of interoperability is defined in the statute under 17 U.S.C. § 1201 (f)(4) as the ability of computer programs to exchange information and use the information that was exchanged. This statute under 17 U.S.C. § 1201 (f)(2) also makes it clear that this exception may only be used in the event that it does not cause copyright infringement.

Through the conditions set forth in the previous sections it leaves open the question of what the individual who reverse engineered the control defined previously may do with the information. The statute defined in 17 U.S.C. § 1201 (f)(3) states that this individual may share
the information that he reverse engineered for the sole purpose of being able to interoperate an independent program with other programs. This would be a case where an individual would reverse engineer a security control then share this information with another organization for the purpose of them also being able to interoperate the program.

The next section of this act relates to the activities that are, and are not, permitted for the purpose of encryption research. The section under 17 U.S.C. § 1201 (g)(1) defines encryption research as “activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products”. This means that the research may be done if the purpose is to discover vulnerabilities in the cryptographic control and further the research into better encryption algorithms. This section also defines encryption technology as the cryptographic algorithms and techniques used.

The statute under 17 U.S.C. § 1201 (g)(2) defines the various means through which an individual can perform encryption research on the various security controls that safeguard protected works. If the individual acts in good faith and has a legitimate copy of the work in question then they are allowed to perform research under four provisions. The first, as defined in 17 U.S.C. § 1201 (g)(2)(A) states that the person lawfully obtained the encrypted copy of the work. The second, as defined in 17 U.S.C. § 1201 (g)(2)(B) states that their actions are necessary to conduct encryption research. This means that the individual must be furthering the research in this area as defined previously. The third provision is that the researcher must have made a good faith effort to obtain authorization to conduct the research first. This means that the researcher must have taken proactive steps to obtain permission from the owner prior to their actions. The final provision is that their research must not constitute copyright infringement or violation of
any other criminal law including the Computer Fraud and Abuse Act, which was documented previously.

The statute also defines what may or may not be a factor in giving an exception to the circumstances as outlined in the previous paragraph. The statute under 17 U.S.C. § 1201 (g)(3) gives three factors that must be considered under the exception. The first factor as defined under 17 U.S.C. § 1201 (g)(3)(A) concerns the manner in which the information obtained under the research was communicated or published. This section takes into consideration whether the information was disseminated in order to further advancements in the field of cryptography or if it was done for the purpose of copyright infringement, violation of privacy, or breach of security. The second factor as outlined in 17 U.S.C. § 1201 (g)(3)(B) takes into account whether the researcher conducted their research as an employee of an organization, as a student, and whether they specifically trained in the field of cryptography. The third factor as outlined in 17 U.S.C. § 1201 (g)(3)(C) takes into account if the researcher notifies the owner of the protected work that their encryption technology was cracked and the time period in which they do so.

An exception is given in 17 U.S.C. § 1201 (g)(4) that allows individuals to develop technological tools to crack the encryption techniques only if they meet the exceptions that were outlined in the previous paragraph. The researcher is also allowed to share these tools with another individual under 17 U.S.C. § 1201 (g)(3)(4)(B) if the other person is assisting them in furthering the research or if it is used to verify their claims. There is an exception concerning minors and it is left to the discretion of the court in accordance to 17 U.S.C. § 1201 (h).

There are further exceptions allowed under the statute in 17 U.S.C. § 1201 (i) which pertain to personally identifiable information. This section allows for four exceptions in which an individual may circumvent a security control to a protected work. The first exception allows an
individual to circumvent a security control if the control is protecting a program whose purpose is to collect personally identifiable information from an individual based on their internet activities. An example of where this could be applied is that it allows an individual to circumvent a technical control to get to the information collected about them from a spyware program.

The second exception, as noted in 17 U.S.C. § 1201 (i)(1)(B) adds to the first and states that an exception also applies if the individual who had their data collected wasn’t notified that their personally identifiable information was collected, then that individual may circumvent the technical control. The third exception states that an individual may circumvent the control if the act itself has the purpose of identifying and disabling the program. This means that individuals may also circumvent a technical control if their purpose is to disable the program and prevent it from causing further damage.

The fourth exception also allows an individual to circumvent the technical control to gain access to the personally identifiable information collected about them. The section under 17 U.S.C. § 1201 (i)(2) states that the previously mentioned exceptions do not apply if the program in question is not collecting personally identifiable information.

The final section that will be covered pertains to security testing as defined under 17 U.S.C. § 1201 (j). The first part of the statute under this section defines security testing as accessing a computer system for the purpose of discovering and correcting vulnerabilities in the system with permission of the systems owner. The second part of this section as defined in 17 U.S.C. § 1201 (j)(2) states that it is not a crime to perform security testing as long as the act does not constitute copyright infringement or a violation of the Computer Fraud and Abuse Act. The third part of this section defines two factors which must be taken into consideration in deciding if the exception should be applied.
The first factor, as defined in 17 U.S.C. § 1201 (j)(3)(A) takes into account whether the information obtained from the security testing increased the security for the owner or user of the system and whether that information was shared with developers of the system. The second factor is to determine if the security testing violated copyright infringement or any other statute. As defined under 17 U.S.C. § 1201 (j)(4) it is not against the statute to develop or distribute any technology based means if it meets the requirements as set forth in the previously defined security testing. It is this provision that allows many tools such as Nmap and Nessus to be distributed and used. Although these tools could be used to crack technical controls for protected works their main and marketed use is for security testing.

There are other parts of The Digital Millennium Copyright Act which changed part of the United States Code but they are not covered here because they are beyond the scope of this research. In particular these parts would be 17 U.S.C. § 1201 (k), 17 U.S.C. § 1202, and the civil and criminal remedies defined in 17 U.S.C. § 1203 – 1205.

The Digital Millennium Copyright Act is an act which is very important for Information Security and Technology professionals to understand. This act makes it very clear what acts are and are not allowed when it comes to tampering with controls set on intellectual property. It is also important to understand the exceptions that are afforded under the various subsections of this law and defined in the previous paragraphs. It is important for organizations to structure their acceptable use policies in order to meet compliance with this act.
The Wiretap Act

The Wiretap Act is a very important law to understand from an Information Security and Technology perspective because it can affect how you monitor your systems. Although this law was originally designed to cover oral and telephone conversations, it now also covers electronic communications in addition to the previous two. This law is generally thought in the perspective of what law enforcement may do to intercept communications, but it also pertains to how an organization may draft their acceptable use policies and monitor communications. This section will cover the first part of The Wiretap Act which pertains to the protection of privacy for communications. The second part pertains to how law enforcement may access these communications and is beyond the scope of this research.

The first section of The Wiretap Act, as noted in 18 U.S.C. § 2511(1)(a) pertains to intercepting communications. This section makes it illegal for any individual to intercept or attempt to intercept any communication. The first element that must be satisfied is that the offender must have done so intentionally, which means deliberately and with a purpose. The second element is that the offender must have intercepted the communication in question. 18 U.S.C. § 2510 (4) defines an interception as acquiring the communication through any means, which could be electrical or mechanical. This also means that an offender who obtains information through electronic storage did not intercept any communications and would not meet this element. The third element that must be met is that the offender must have obtained possession of the contents in the communication. This essentially means that the offender must have been able to decipher the message sent. This element would be met if an offender intercepted an e-mail message and was able to see the content of the message.
The fourth element is that the communication must have been electronic, wired, or oral and affect interstate commerce. The section in 18 U.S.C. § 2510 (12) notes that any communication which is conducted over a wire, radio, or other electromagnetic means would fall under the electronic part. In United States v. Kopp the court ruled that a keystroke logger would not meet this element because it recorded communications within the victim’s computer and as a result did not affect interstate communications. The final element is that the communication must have been acquired through the means of an electrical or mechanical device. In many network crimes this could be the computer that the attacker used or a protocol analyzer such as Wireshark.

The second crime noted under this act is the disclosure of an intercepted communication under 18 U.S.C. § 2511 (1)(c). This would be the intentional disclosure of a communication that an individual knows was intercepted illegally. With that being noted, the first element for a violation of this statute would be intentional disclosure of the contents of the communication in question. If the information is already public knowledge then there would be no violation of this element. The second element is that the communication must have been illegally intercepted as described in the previous paragraphs. To be charged under this statute an individual does not necessarily need to be the individual who illegally intercepted the communication, but if they were otherwise involved such as purchasing the contents of the communication then that would also meet the requirements for this element. The final element is that the offender must have known, or have had reasonable cause to believe, that the communication was illegally intercepted.

The third section that is made illegal under this act pertains to the use of intercepted communications as noted under 18 U.S.C. § 2511 (1)(d). The first two elements of this crime are
identical to the previously mentioned crime of disclosing an intercepted communication under 18 U.S.C. § 2511 (1)(c). The communication must have been illegally intercepted and the offender must have known, or had reasonable belief to know, that the communication in question was illegally intercepted.

The third element for this crime pertains to the use of the intercepted communication. According to the courts decision in Peavy v. Harman, this element would be met only if the offender did more than just listen in on the intercepted communication. The offender must have used some “active employment of the contents of the intercepted communication for some purpose”. An example of where this communication could be applied in conjunction with identity theft would be if an individual performs a man-in-the-middle attack with a consumer and obtains their credit card number then sells that number. In this example the offender intercepted the communication illegally then used it for a purpose in conjunction with identity theft.

There are a number of exceptions for the three previously mentioned offenses under The Wiretap Act. The first exception, as noted under 18 U.S.C. § 2511 (2)(a)(i), pertains to telecommunications companies. This exception states that it is lawful for organizations such as internet service providers to intercept communications which are placed over their infrastructure for the purpose of combating fraud and theft of service. This exception can range from intercepting communications of an illegally hacked phone to locate its source to monitoring the traffic over its infrastructure in order to protect itself or prevent further damage. This exception however does not allow an organization to conduct unlimited monitoring and should tailor the monitoring to intercept only relevant communications.

Another issue that an organization must take into consideration under the previously mentioned exception is to make sure that they are not acting as an agent for the Government.
Organizations which act as an agent of the state may no longer be eligible for the exception and may be subject to possible civil ramifications. This exception also makes note that in some cases the organization may have no choice other than to overhear communications, such as a repairmen in the course of repairs, and would not be liable under the three noted criminal actions under this act.

The second exception noted under this act pertains if a party consents as noted under 18 U.S.C. § 2511 (2)(c)&(d). This exception states that interception of communications is not illegal if at least one individual participating in the communication gives their consent for the communication to be intercepted. If only one individual in the communication gives their consent then it must not be a law enforcement professional. The court has ruled in network communications that a service provider can not give consent because they transmit the communications rather than participating in them. If an organization wishes to have law enforcement get involved over monitoring communications which they are a part of then they must have given actual notice of consent rather than just implied.

The third exception pertains to what an organization can do if they suspect an individual is attacking their system as defined under 18 U.S.C. § 2511 (2)(i). This exception allows an individual or organization to allow law enforcement to monitor and intercept communications of an organization if: the owner of the system gives their implicit authorization to do so, the law enforcement agent is legally involved in the case and has reasonable belief that the attacker’s communications would be relevant to the case, and that the communications would be relevant to the investigation.

The individual who was authorized to intercept the communications must also make sure that they do not intercept communications other than those of the attacker. The individual
monitoring the communication may also be a private party if they are acting under the direction of law enforcement. However, if the private party was not acting under the direction of law enforcement then they are not covered under this exception. There are also a number of noted affirmative defenses afforded under this statute, with most applying to law enforcement.

As it has been shown in this section, The Wiretap Act applies to many more individuals than just law enforcement professionals. An organization that intercepts communications of its employees may be in violation of these statutes if care isn’t taken to institute notification of monitoring in their acceptable use policy that every user needs to sign. Organizations should also add banners and other forms of notification to their systems so that an individual can clearly see that the system is restricted and their communications within that system are monitored. Great care should be taken within organizations to make sure that they update their policies in order to be in compliance with this statute.

The Stored Communications Act

The Stored Communications Act was signed into law to address the issues for cases that are not covered under the previously mentioned Wiretap Act. This act is focused on protecting the confidentiality, integrity and availability of electronic communications that are currently in some form of electronic storage. This law was drafted with the purpose of protecting the privacy of e-mails and other electronic communications.

The first element that must be satisfied under 18 U.S.C. § 2701 is that the offender must have intentionally accessed the stored communication. The second element is that the offender must have done so without, or in excess of, authorization. The definition of this element is the
same as in 18 U.S.C. § 1030 which means that an offender who acts without authorization is typically an outsider to the organization in question. An individual who acts in excess of authorization typically does so as an insider of the organization and acts beyond the extent of their authorized privileges.

The third element that must be met is that it must have been a facility that provides an electronic communications service. According to its definition under 18 U.S.C. § 2510 (15) an electronic communications service is essentially any service that allows an individual to transmit communications to a third party. By this definition not only do internet service and telecommunications providers fall under this definition, but so would websites such as Hotmail or cloud computing organizations since they would provide an electronic communications service. The court has ruled in United States v. Steiger that a home computer or other end user device wouldn’t fall under this category since they do not provide a service to others.

The fourth element is that the actions of the offender must have affected authorized access to the communications which are being held in electronic storage. According to 18 U.S.C. § 2701 (a)(2) this means that the offender must have either obtained, altered, or prevented access to the communication in question. According to 18 U.S.C. § 2510 (17) electronic storage has a few different definitions. The first definition of electronic storage pertains to communications which are held in temporary and intermediate storage made in the course of communication, such as in random access memory and buffers. The second definition is storage by an organization for the purpose of backing up the data. An example of this would be if an offender was able to gain access to a victims e-mail before the victim had the opportunity to view it. The e-mail would be in temporary storage at the service provider’s e-mail servers and as a result would fulfill the requirements for this element. Although this is a very narrow definition of what
electronic storage is, as defined through statute, a relatively recent court decision ruled that the
definition of what constitutes electronic storage is broader than what is defined here and in the
statute. In Theofel v. Farey-Jones the court essentially ruled that all communications are in
electronic storage. This definition came about when the court ruled that previously accessed e-
mails fall under the previously mentioned backup clause.

This statute also makes provisions for a case in which the actions of the offender could
result in a felony charge. The section under 18 U.S.C. § 2701 (b)(1) states that violation of this
statute is a felony if, in addition to the previously mentioned elements, the offender’s acts are
“committed for purposes of commercial advantage, malicious destruction or damage, or private
commercial gain, or in furtherance of any criminal or tortuous act in violation of the Constitution
or laws of the United States or any State”. This means that it is a felony if the offender illegally
accessed stored communications for the purpose of making money or for any other malicious
purpose. This element of the statute was added through the Homeland Security Act of 2002.

There are a number exceptions afforded through the statute for violations of the
previously mentioned elements. The first exception as defined in 18 U.S.C. § 2701 (c)(1) is that
this law does not pertain to the person or entity providing the communications service. This
means that unlike in The Wiretap Act, a service provider may access the stored communications
without having to abide by a narrowly defined set of circumstances. The second exception
afforded under this statute is that the user of that service may use and authorize use of their
communications.

There are also a number of circumstances under this act which require the disclosure of
customer communications. The first circumstance as defined under 18 U.S.C. § 2703 (a) states
that an organization which has storage of the communications must hand over the
communications to a law enforcement agency if the agency has a court ordered warrant requiring the disclosure. Law Enforcement may also get the communications through another means as defined in 18 U.S.C. § 2703 (b)(1)(B). This section gives authority to Law Enforcement to obtain the records also through the use of a court ordered subpoena. The Law Enforcement agency may also obtain these records if they have the consent of the owner of the communications for disclosure.

The act allows for Law Enforcement to obtain certain information about the communications of an individual under 18 U.S.C. § 2703 (c)(1)(D) if the communications in question were used in conjunction with telemarketing fraud. The information that they are allowed to obtain is the name, address, place of business or residence, and the customer involved in the telemarketing. The information that the communications provider may supply to law enforcement in the event of a warrant or subpoena is detailed under 18 U.S.C. § 2703 (c)(2).

The section of particular note for information technology professionals working in an organization that provides a communications service is that under 18 U.S.C. § 2703 (g) the organization must first take all necessary steps to preserve the records and communications. The second part is that these records and communications must be kept for at least 90 days and may be held longer with a request from Law Enforcement.

As described previously, there are a number of circumstances in which an organization must divulge the communications and records of its customers. There are also a number of situations afforded under 18 U.S.C. § 2702 which makes disclosure voluntary and are based mostly around the customer consent clause which was mentioned previously. This statute also allows for an organization to divulge information to The Center for Missing and Exploited Children if a report was filed through the center.
The Stored Communications Act is very important for information security and technology professionals who work for a telecommunications and/or internet service provider. It defines what information can and can not be disclosed, to whom and under what circumstances. This act also defines what information must be retained in 18 U.S.C. § 2703 (c)(2) and database administrators must structure their databases to hold the information required through this act.

Identity Theft and Aggravated Identity Theft

With the popularity of e-commerce and internet banking continuing to increase every year it makes for an attractive target for people to steal identities. Through schemes such as phishing schemes, cyber criminals are able to get personally identifiable and financial information from e-commerce customers which makes identity theft a very lucrative and illegal endeavor. The following paragraphs will detail the relatively short but important identity theft statutes outlined in the federal United States Code.

The Identity Theft statute isn’t a separate section within the United States Code, rather it is a subsection of the Identification and Authentication Fraud statute listed under 18 U.S.C. § 1028. The section which specifically applies to identity theft is 18 U.S.C. § 1028 (a) (7). The first element of this section is that the offender must knowingly possess, use, or transfer the identification of another individual without having legal authority to do so. This means that the offender could meet this element if they have a large collection of identities such as in the case of compromising an e-commerce server and having a large collection of credit card numbers. They do not need to have necessarily used them yet to meet the possession requirement.
The second element of this section is that the offender must have intent to use the stolen identification to further a crime. This element may also be met if the offender in question was a co-conspirator or otherwise connected with the illegal activity. This crime could be a felony on the federal level or a violation of state and local laws. The definition for the victims identification in this statute is defined in 18 U.S.C. § 1028 (d)(7) as essentially being any information that could be used by itself, or in conjunction with other information, to identify a specific individual. For an organization this would constitute most of the information that they would hold in their customer databases such as names and social security numbers.

To be charged with identity theft as defined under 18 U.S.C. § 1028 (a)(7) a number of other circumstances must also be met which are defined under 18 U.S.C. § 1028 (c). The first circumstance that may be met to satisfy this requirement is that the identification in question must have been issued by or under the authority of the United States Government. An example of this would be the social security number of an individual. The second circumstance would be if the information in question was in possession of an individual with the purpose of defrauding the United States Government. An example of this would be if an offender had personally identifiable information about an individual that they obtained through identity theft which they later used to commit fraud against Medicare or other Government programs. The third circumstance would be if an offender possesses, uses, or transfers the information through either the mail or electronic means and affects interstate or foreign commerce.

Aggravated Identity Theft differs in a number of ways from the previously mentioned Identity Theft statute, which is why it has its own section as defined in 18 U.S.C. § 1028A. This statute defines a number of felony offenses that must be committed in conjunction with the illegal act as it is defined in this statute. The section defines these felonies in 18 U.S.C. § 1028A
(c) and are: theft of public money, falsely claiming to be a United States Citizen, false statements in connection with acquiring a firearm, fraud, mail fraud, wire fraud, bank fraud, violations pertaining to citizenship such as failing to leave after deportation, violations of passports or visas, violation of the Gramm-Leach-Bliley Act, or any violations of the Social Security Act.

For a violation of Aggravated Identity Theft the offender must, in addition to the previously defined felonies, commit identity theft by means of using, possessing, or transferring identification when they were not legally authorized to do so. This statute states in 18 U.S.C. § 1028A (a)(1) that if an individual meets these elements then in addition to the penalty for violating the original crime they will also be sentenced to an additional two years. Section 18 U.S.C. § 1028A (a)(2) includes a terrorism clause that increases the additional sentence from two years to five.

The need for information security and technology professionals to understand the Identity Theft statute is crucial. These professionals need to know what information would meet the requirements under this statute if stolen in additional to certain state specific notification requirements. Identity Theft is an ever increasing crime and if an organization falls victim then it could have severe legal and public ramifications, especially if best practices were not followed.

Access Device Fraud

Many of the cyber crime statutes mentioned in this research correlate closely with each other. The section in the United States Code pertaining to access device fraud would closely relate to offenses in which identity theft was conducted as described previously. The statute for access device fraud outline ten different offenses which an offender could violate and are listed under 18 U.S.C. § 1029.
The first offense as listed in 18 U.S.C. § 1029 (a)(1) states that it is illegal for any individual to knowingly traffic in a counterfeit access device. This statute describes a counterfeit access device as being any data, number, equipment or service that can be used to obtain something of value and which has been altered or forged. An example of this would be using authentication credentials of an individual, which the offender has no legal right to use, and using these credentials to gain access to a protected computer system. An offender could violate 18 U.S.C. § 1029 (a)(1) if they sold the authentication credentials to a third party.

The second offense would be if they trafficked the counterfeit access device with the purpose of committing fraud and obtained anything of value in return worth at least $1,000 during a one year period. An offender would be guilty of violating this offense if as a result of selling authentication credentials to a third party they were paid at least $1,000. The third offense states that an offender could be charged in violation of 18 U.S.C. § 1029 (a)(3) if they knowingly possess fifteen or more unauthorized access devices with the purpose to defraud. An offender could be charged with a violation of many of these sections if they have a collection of unauthorized access devices and sell them to third parties.

The fourth offense states in 18 U.S.C. § 1029 (a)(4) that it is illegal for an individual to produce, possess, or traffic in equipment to create access devices if their intent is to defraud. An offender could be charged with violating this section if they had equipment used to create credit cards from information that they obtained from a victim, perhaps through a phishing attack or some other violation of the identity theft statute. The fifth offense makes it illegal for any individual to receive payment in excess of $1,000 during a one year period from another individual who used an illegal access device which affected the transaction of another individual. An example of this would be if an offender sold an illegal access device to an individual and
received payment from the offender for use of the access device. If an offender bought authentication credentials illegally and used them to commit fraud then gave at least $1,000 back to the individual who sold them the credentials then both parties are liable under this offense.

The sixth offense is also closely related and states in 18 U.S.C. § 1029 (a)(6)(A)&(B) that it is illegal for any individual to solicit another individual and either offers or sells an illegal access device. This means that an offender doesn’t necessarily need to sell the authentication credentials, they can also be charged if they give it away for nothing.

The seventh offense states in 18 U.S.C. § 1029 (a)(7) that it is illegal for any individual to alter a telecommunications device and distribute or possess the device for the purpose of obtaining unauthorized use of a telecommunications service. An individual could be charged with violating this statute if they had satellite equipment for the purpose of getting satellite television and altered the access card used in the receiver for the purpose of getting channels that they are not authorized to view. An offender could also be charged with being in violation of this offense if they sold the equipment to another individual.

The eighth offense states in 18 U.S.C. § 1029 (a)(8) that it is illegal for any individual to produce, possess, or traffic in any scanning receiver. The statute defines a scanning receiver in 18 U.S.C. § 1029 (e)(8) as “a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument”. An example of this could be if an offender was able to gain access to a victim’s network and use Wireshark to record all communications across their network.

The ninth offense states that it is illegal for any individual to use or traffic a telecommunications device that they know has been altered for the purpose of gaining
Unauthorized access to a telecommunications service. An individual would be in violation of this section if they purchased a satellite receiver that they knew was purposefully altered to gain free access to channels. The final offense listed under 18 U.S.C. § 1029 states that it is illegal for an individual to use, or have another individual use, a credit card that they are not authorized to have. An individual would be charged with this statute if they used a credit card which was illegally obtained and used it to purchase goods or services. An example would be if an individual illegally obtained credit card information from a phishing attack and used the information to purchase a product from an e-commerce website.

There are a number of exceptions provided by this statute and described under 18 U.S.C. § 1029 (g). The first exception states that it is not illegal for an individual, agent for the individual, or an officer to violate one of the previously defined offenses if the purpose is to protect their property or legal rights. These individuals may not however use this exception to gain access to another telecommunications service provider without consent. Section 18 U.S.C. § 1029 (g)(2) also states that it is an affirmative defense for violations of the previously defined offenses if the individual was doing so for research and development purposes.

The issue concerning access to information and services of an organization, both electronic and physical, is vitally important for every information security and technology professional. The issue of access using counterfeit access devices can cause serious consequences for the confidentiality, integrity, and availability of organizational data assets. The statute concerning access device fraud and listed in 18 U.S.C. § 1029 is important to understand because it details exactly what is illegal and what the punishment for violations are. Many of the ten offenses which were described previously relate to each other and an offender may violate a
number of them with one criminal act. This statute is important to understand for the purposes of drafting information security policy and procedures.

**CAN-SPAM Act**

The proliferation and seemingly never ending traffic of unsolicited e-mail over the internet is constantly increasing and poses a problem both for organizations and individuals. The industry for these unsolicited e-mails, which is referred to as SPAM, is a very profitable business for individuals selling products for other organizations. Typically SPAM is sent in very large quantities and because of this the offenders of the CAN-SPAM Act need to have many systems to send out the sheer bulk of the e-mails and many offenders compromise systems to create a global botnet network for the purpose of distributing the SPAM. It is a major challenge for organizations to limit the traffic over their network to only legitimate communications. Because of these reasons it is important for information security and technology professionals to have a firm understanding of this act which is listed in 18 U.S.C. § 1037.

A couple of definitions need to be defined first before the offenses can be detailed. This statute defines commercial electronic communications as being any e-mail message with the primary purpose being the promotion or sale of a commercial product. The statute also defines what they mean by “multiple” in 18 U.S.C. § 1037 (d)(3) as being more than 100 messages in a 24 hour period, 1,000 during a 30 day period, or more than 10,000 during a one year period.

There are five offenses listed under 18 U.S.C. § 1037 and all of them have the necessary element that the act must affect interstate or foreign commerce. This element could be met by showing that the unsolicited e-mails consumed interstate bandwidth or if an individual bought a product that was being sold through the SPAM. The first offense is detailed under 18 U.S.C. §
1037 (a)(1) and states that it is illegal for any individual to illegally access a computer and send multiple commercial electronic communications from the computer. This makes it illegal for an individual to crack a protected computer and send unsolicited e-mails from said computer. An offender who violates this statute would also be in violation of the Computer Fraud and Abuse Act.

The second offense is listed in 18 U.S.C. § 1037 (a)(2) and states that it is illegal for an individual to use a protected computer to relay the commercial electronic communications with the intent to hide the origin of the communication from the receiver. This is an offense which could be used against offenders who use botnets to distribute the SPAM because a direct result of this is that the SPAM appears to come from the compromised computer which is a part of the botnet, not from the original offenders’ computer. The third offense states that it is illegal for an individual to intentionally falsify e-mail header information. An example of this would be for an offender to spoof the e-mail source information for the purpose of concealing the true source of the SPAM.

The fourth offense is listed in 18 U.S.C. § 1037 (a)(4) and states that it is illegal for any individual to create five or more online and/or e-mail accounts with a false identity, or at least two domain names, and send the unsolicited e-mails from any combination of these accounts or domain names. It is very easy for an individual to create false accounts through such services as Hotmail or Gmail and remain anonymous. These e-mail providers only keep the e-mails which are contained within the users’ inbox so law enforcement can not retrieve potentially illegal e-mails which were deleted by the offender. If an offender creates five e-mail accounts through Hotmail and uses these accounts to further their illegal SPAM scheme then they could be charged under this section.
The fifth section states in 18 U.S.C. § 1037 (a)(5) that it is illegal for any individual to “falsely represent oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses”. This offense makes it illegal for any individual to claim to be the registrant of at least five IP addresses and use these addresses to distribute SPAM.

SPAM is a major problem and will continue to be as long as it is profitable for an offender. Organizations and individuals at home must be sure they follow security best practices, such as applying patches, to make sure that their computers do not become part of a global botnet which distributes the SPAM. Individuals must also stop purchasing products sold though SPAM in order to take away the financial incentive for the distribution of these e-mails. Organizations should know this statute to understand what can be done if they find the identity of an individual, outside or inside of the organization who is engaging in this behavior.

**Wire Fraud**

The Wire Fraud statute is one which has been around for many years and has adapted to changes in the medium of communications. This statute is listed in the United States Code under 18 U.S.C. § 1343 and applies to crimes committed over different types of electronic medium such as telephone and network communications. Although this statute differs from the Computer Fraud and Abuse Act in a number of ways, a violation of this statute carries heavier penalties with a maximum sentence of thirty years in prison and/or a million dollar fine.

The first element of this statute is that the offender must have devised a scheme to defraud and obtain money or anything else of value under false pretenses. This element could tie
in closely with the identity theft statute if the offender sent out e-mails with the purpose of conducting a phishing scheme. The second element is that the offender must have sent the fraudulent communication over an electronic medium including network, radio, and telephone medium. A violation of these two elements carries a maximum sentence of twenty years and a fine.

A second provision has been added to this statute and states that if an individual violates the two elements and the fraud was used to defraud a charity in connection with a disaster declared by the President, then the offender could be punished by up to thirty years in prison and a million dollar fine. This second provision would also apply if the victim was a financial institution.

The Wire Fraud statute is a relatively short one but it is very important. This statute has been around for many years because of its flexibility to adapt to changing communications medium such as modern network infrastructure. The court ruled in United States v. Pirello that this statute is still applicable to individuals who use the internet and other network infrastructure to commit fraud. Organizations need to take this statute into consideration because of the penalties associated with it and potential civil liability on their end if their network was used as a medium for an individual to commit wire fraud.

Communications Interference

The final federal statute which will be covered in this research is Communications Interference as detailed in 18 U.S.C. § 1362. As with Wire Fraud, this statute has been around for a long time because it has adapted to changes in communications medium. This statute covers a number of different acts under which an individual may be charged with a crime. As with the
Wire Fraud statute, violations of 18 U.S.C. § 1362 carry a serious penalty of up to ten years in prison.

The first part of this statute makes it illegal for any individual to maliciously destroy any property such as the cable, system, or other means of communication which is operated or controlled by the United States. This first part would apply in both the event where an individual damages a physical communications line which is used by the United States Government or through damage to their systems which they use for communications. The second part of this statute makes it illegal for an individual to commit this crime if the property was for use by the United States Military. This part also makes it illegal for an individual to engage in this activity if the communications systems are not currently fully developed.

The third part makes it illegal for any individual to willfully interfere in the working or other use of the line. An example of this would be if an offender executed a denial of service attack on a Government system with the purpose of rendering its services useless. The fourth part follows closely behind the third in stating that it is illegal for any individual to willfully obstruct or delay communications transmissions over these lines. An example of this would be if an offender used a jamming device and blocked the wireless communications that the Government was using for communications. The final part also makes it illegal for any individual to conspire to commit any of the previously mentioned acts.

As with most of statutes covered in this section, the Communications Interference statute tends to overlap with a few others. Although all of the previous statutes applied to both private and public industry, this statute applies mostly to Government systems and systems used by defense contractors. This statute should be expanded to also include communications interference of systems used by private industry.
Sociological Theories

This section of the research will concentrate on outlining several sociological theories and their application towards computer crime. Very little research has been completed in this area. The analysis in this section will consist of describing each of the theories mentioned and my analysis of how they can apply towards computer crimes based on the interviews conducted in this research and through my own previous knowledge.

The advent of computer crime is relatively new which is why substantial research is lacking in this field of study. The theories described in this section are commonly used throughout the sociological field and were originally designed to help explain the reasoning and cause behind traditional crimes. Despite this, I believe that they can also be applied to help explain why many individuals are involved in modern crimes such as identity theft through electronic means, which was outlined previously in this research. Many crimes, such as wire fraud, are traditional crimes which are now perpetrated through a modern medium which is network infrastructure. This may be why traditional sociological theories can be applied towards modern crimes which were not possible when many of these theories were first developed.

Differential Association

The theory of Differential Association is one of the most known and respected in the fields of criminology and sociology. The creator of this theory, Edwin Sutherland, is considered in many circles to be the “Father of American Criminology” due to his important contributions to this field. This theory was first put forward by Sutherland in the second edition of his text book titled Criminology in 1934 and has remained unchanged since his last revision in 1947. The
interesting fact about this theory is that it was originally created by Sutherland to help explain white collar crimes. There had already been theories about deviant behavior however Sutherland felt that these theories did not accurately explain high crimes committed by individuals who, in many cases, are educated and make a decent living.

The basic idea behind Differential Association is that “Criminal behavior is learnable and learned in interaction with other deviant persons” (http://www.criminology.fsu.edu/crimtheory/sutherland.html). Simply stated, Sutherland proposes that people become criminals because they learn to be. It is through interactions with other people who engage in illegal activities that an individual learns the techniques, motive, and also develop a rationale for committing the crimes themselves. This theory can easily been seen when put into the context of crimes that we may deem to be traditional. This theory could help explain why normal law abiding individuals can turn into criminals depending on the circumstances that they may be put into. An individual may be a good person who through, perhaps no choice of theirs, is put into a poor socio-economic climate with an atmosphere of deviance. This atmosphere would be caused be people around them committing crimes, such as robberies or other types of felonies. Sutherland proposes that a law abiding individual would eventually learn the techniques of how to commit these illegal acts as well as their rationale to do so by seeing and becoming influenced by the individuals around them.

This theory is significant because it diverts from the sociological theories of its day which proposed that many biological factors are contributed to making an individual more susceptible to commit crimes. This theory puts an individual’s social environment into context as a means to explain why some individuals engage in criminal behavior. “The principle of differential association asserts that a person becomes delinquent because of an "excess" of definitions
favorable to violation of law over definitions unfavorable to violation of law”
(http://www.criminology.fsu.edu/crimtheory/sutherland.html). What this means is that an
individual will become a criminal because they are exposed to more favorable criminal
influences rather than more favorable legal influences. This can be seen in environments with
poor socio-economic conditions which may encourage negative views towards the law and
authority.

According to Edwin Sutherland and his text book Sociology there are nine contributing
factors which make up his theory of Differential Association. The first, which was previously
mentioned, is that criminal behavior is learned. This factor would propose that individuals are
inherently good and only turn towards deviant behavior as a result of learning the behavior. The
second factor ties in closely with the first and states that the criminal behavior is learned through
another individual during the process of their communication. According to Sutherland this
would mean that an individual is influenced to participate in criminal behavior through watching
and interacting with other individuals who are engaging in the criminal behavior.

The third factor of Differential Association is that individuals learn criminal behavior
while a part of an intimate group. This would be any group that has a significant influence over
them, such as their family or close friends. This factor makes a great deal of sense since the
process of socialization and growing up is heavily influenced by the groups of people that an
individual is a part of. Most families try to institute a positive influence on a member of their
own, however if a juvenile comes from a family that is broken and develops strong emotional
ties with friends engaged in deviant behavior then this is likely to also drive them into the same
deviant behavior, according to Sutherland.
The fourth factor of Differential Association has several parts to it. The first part is that when the criminal behavior is learned, an individual also learns the techniques for how to commit the crime itself. If an individual is influenced into learning robbery then they will also learn the techniques for committing the robbery. The second part is that they will learn the “specific direction of motives, drives, rationalizations, and attitudes” for committing a crime (http://www.d.umn.edu/~jhamlin1/sutherland.html). This means that an individual will be influenced into believing that the behavior, which they may have previously believed was wrong, into believing that it is right through rationalization of their actions. An individual from a disadvantaged background may rationalize robbery as taking from those who have wealth in order to make things fair.

The fifth factor states that an individual will be pushed into deviant behavior depending on their view of the legal code as being favorable or unfavorable. This states that an individual may be driven into deviant behavior if they see the laws as being tough and unfair. This would influence their rationalization for breaking the law since they view it as unfair.

The sixth factor states that a person becomes a criminal because of what they perceive as being an excess of reasons to violate the law rather than uphold it. This is a core component of Differential Association and it states that an individual will break a law if they see more reasons to break it than to stay in compliance with it. In their minds, an individual would take a look at a law and compare the rewards for both actions and make their decision based on the one which would benefit them the most. They may see robbery as having a financial benefit for them, but they would also see a prison term as a potential ramification and make their decision accordingly. It is when an individual views breaking a law as having a greater benefit for them than keeping it that results in deviant behavior.
The seventh factor states that Differential Association may vary in frequency, duration, priority, and intensity. This factor would be attributed to how strong their bond is with the individuals they interact with who commit the criminal behavior. If they interact on a daily basis and have strong emotional ties then they are likely to commit the deviant behavior more frequently than they otherwise would have.

The eighth factor states that the “process of learning criminal behavior by association with criminal and anti criminal patterns involves all of the mechanisms that are involved in any other learning” (http://www.d.umn.edu/~jhamlin1/sutherland.html). This means that individuals learn criminal actions, and legal actions, through the same way. An individual would learn behavior that is counter productive to society in the same way that they would learn behavior that is productive. This is why an individual would learn criminal behavior through their interactions with others.

The final factor of differential association states that while criminal behavior is an expression of general needs and values, it is not necessarily the fulfillment of these needs and values which causes deviant behavior since non-criminal behavior is an expression of these same needs and values. An example of this is the need for an individual to be accepted and loved. Sutherland argues in this factor that it would not necessarily be the fulfillment of being accepted and loved which leads an individual to deviant behavior since non-criminal behavior also can fulfill the requirement to be accepted and loved.

The theory of Differential Association can be applied towards computer crimes. The main premise behind this theory is that criminal behavior is learned through the social interactions with others. The profile of a traditional hacker, which may not always be applicable these days, is one who is a loner and very smart. Their social interactions may come through electronic
communications with other individuals who share similar technological interests. If they do not currently have any desire to commit malicious acts through electronic means, such as an act in violation of the Computer Fraud and Abuse Act, then they may become influenced through another individual with whom they share electronic communications. According to the seventh factor of Differential Association, the more time an individual would spend with members of these groups who are committing illegal acts it would also increase the frequency that they engage in deviant behavior.

This theory, which was developed to help explain white collar crime, fits in well with those who violate telecommunications statutes. From my experience I can state that a lot of hacking of systems occurs during college. Many of these individuals spend time with people who share similar interests. It is in these groups where the third factor of Differential Association can be applied which deals with learning deviant behavior as part of a close group. These groups may serve a well meaning purpose such as research or hacking of systems for fun, which would be legal if they owned the systems or if they had permission by the college as part of its lab infrastructure. However, being part of this group may lead a well intentioned individual to commit a crime if they are influenced by other members of their group which are doing so.

It is through these groups, or perhaps through IRC channels, that an individual would learn the techniques which would help them perfect their craft. It would also be through these means that they would develop a rationalization for illegal compromising systems. An example of this may be targeting a Microsoft or Apple operating system because they feel that all software should be open source. It would be through these social interactions that an individual would develop their attitude and feelings of rationalization for their deviant behavior.
There is a strong push from the open source community against Intellectual Property statutes which they view as overbearing and too powerful in the support of proprietary software manufacturers. Many individuals within this community believe that all software should be open and source code available to alter to fit their needs. It is this belief which could fulfill the fifth factor of Differential Association where the community would view the Intellectual Property statutes as being unfair and too powerful. This would also help fulfill the sixth factor if they believed that their deviant behavior was for the good of the open source community, such as if they reverse engineered proprietary software and published its source code.

In conclusion, Differential Association is a solid theory with a number of factors which could help to explain the cause behind why cyber crimes are increasing so quickly. As it has been documented through the interviews in this research, there is a wide spectrum of the different kind of offenders and motivations. Differential Association would apply best towards the stereotypical view of a malicious hacker that the public may have as a result of press coverage. This theory has remained valid for many years because of its nine factors and its ability to adapt to different kinds of statutory violations. This theory applies just as well to individuals who violate computer and telecommunications laws as it does for offenders of more traditional laws such as robbery.

Anomie and Strain Theories

Strain Theory is one of the most prominent theories in Criminology and it has been altered with different proposals from different individuals over the years. This section will detail the general concept of Strain Theory and Anomie as proposed in the works of Robert Merton, Emile Durkheim, and Robert Agnew. These changes are brought about in the field of
Criminology through changing concerns in political and economic matters. This theory is very important and plays an prominent role in many aspects of classical and modern Criminology.

The Strain Theory, much like Differential Association, attempts to put forth a general theory as to why some individuals divert into deviant behavior while others live a life which contributes to the progress of society. A big difference between these two theories is that while Differential Association was proposed for white collar crimes with potential applicability towards any crime, strain theory specifically focuses on those in society who are disadvantaged.

This theory depends heavily on what Durkheim defined as strain. Strain would be the drive of an underprivileged individual to achieve success, as defined by the society in which they are a part of, through any means they find necessary. Durkheim then further divided the concept of strain into two sections. The first section, called structural, is established at the societal level and concerns how an individual perceives their needs at this level. If an individual sees that their needs are not being met and that societies established structure to meet their need is not adequate, through regulation for example, then it will lead to strain and changes in their means and opportunities to meet such needs. The second section, called individual, states that the goal of meeting the societal needs may become so significant that the individual may no longer care about the means through which they accomplish their goal.

Structural strain can be seen in our daily lives, especially when the economy is not in great shape. A goal for an individual set at the societal level would, for example, be the need to be financially successful. In a mixed economy such as in the United States, individuals must choose their own path and work hard in this path for them to make money and purchase goods and services. This leads to the competitive nature of careers and employment. Many of those who are in underprivileged socioeconomic situations may perceive some individuals as having a
bigger advantage than they do at being financially successful and meeting this need. They may view the United States laws and regulations as being unfairly slanted to favor those from better socioeconomic standings. This would lead to strain on the part of the underprivileged individual and would cause them to find different paths to financial success, which could very well lead to illegal means to accomplish said goal. If they feel that they do not have a fair opportunity to go to college and earn a living through legitimate means then they will turn to crime such as robbery to fulfill their needs.

Individual strain can be summarized as being the strain that an individual would experience during which they no longer care about the means they use to accomplish their end goal. This ties in closely with structural strain and an individual may end up experiencing both types. Under this type of strain an individual would put so much importance into achieving their needs set defined by society, such as being financially successful, that they would use any means necessary to accomplish it.

While Durkheim used Anomie to explain deviant behavior in most societies, Merton used Strain Theory to apply specifically to deviant behavior as it is in the United States.

“The U.S., in fact, Merton sees as a polar example of a society in which success goals (often defined primarily in monetary terms) are emphasized for everyone in the culture, and people are criticized as being quitters if they scale back their goals. On the other hand, the culture is at best ambivalent in its norms about the appropriate means of being successful. Certainly hard work and ambition, in school and then in the economic marketplace, are the culturally approved means of success, but there's also an element of admiration for the robber baron and the rogue who breaks the rules about appropriate means but achieves success goals by
deviant means. In America, in other words, success is probably rated a lot more highly than virtue”

(http://www.d.umn.edu/~bmork/2306/Theories/BAManomie.htm)

What Merton is emphasizing is the approach taken through individual strain. He proposes that deviant behavior in the United States is caused because the society sets financial success as such an important goal and while it emphasizes hard work as the means through which an individual should accomplish the goal, it does not totally stigmatize illegal means. This can be seen through the American romantic vision of the mafia and individuals such as John Dillinger. This would only further influence an individual into deviant behavior to achieve financial success if they honestly believe that they can not do it through legitimate means and if they see the deviant path as being potentially okay.

This theory by Merton was also developed in a period during which American society was still very openly prejudice against minorities. His theory proposed that those individuals who are underprivileged may end up taking the honest and socially acceptable path to meet financial success and yet not end up as successful as those who are not in the same position. This would lead them to question why they would take the honest path when they could be more successful through deviant behavior. “Merton’s concept of anomie refers to a specific imbalance where cultural goals are overemphasized at the expense of institutionalized means”
(Featherstone, pg#478)

Robert Agnew is the latest to influence strain theory. His theory, proposed in the early 1990’s, tries to take the aspect of class and socio-economic status out of the central idea proposed by both Durkheim and Merton. His theory was proposed not to focus on an individuals
social class, but rather specifically on the direct strains that an individual experiences in meeting the norms and standards of society.

Agnew’s theory, unlike Mertons, focused on the strain an individual may experience when they do not meet the needs of society which are not financially based. Agnew measured strain through three different types. The first, failure to achieve positively valued stimuli, results from when an individual fails to achieve positively valued goals. Agnew states that money, status / respect and autonomy are positive goals which could be applied for this circumstance. “Another source of strain due to goal blockage is the disjunction between expectations and actual achievements. This disjunction rests on the outcome of an individual’s behavior. Strain is increased when the actual achievements of an individual are less than that which the individual had expected” (http://www.criminology.fsu.edu/crimtheory/agnew.htm). Strain occurs when everybody in society has the same goals, but one group is at a perceived disadvantage of achieving these goals. Individuals also turn to deviant behavior when the outcome of their behavior does not result in the expected result that they believe they earned.

Agnew’s second type of strain is the loss of positively valued stimuli. This could be if a relationship with a positively influenced individual becomes damaged, if they incur a financial loss through theft, or in any other way that they lose something positive in their life. “According to Agnew, the strain that is felt by the individual loss could lead the individual to delinquency as the individual attempts to prevent its loss, retrieve what was lost, or seek revenge on those who removed the positive stimuli” (http://www.criminology.fsu.edu/crimtheory/agnew.htm).

The final type of strain proposed by Agnew is the presentation of negative stimuli. “In a study by Hoffmann and Miller (1998:106), it was found that negative life events that include such things as parental unemployment, deaths in the family, and illness impose a strong impact
by increasing delinquent behavior in adolescents. This type of strain has also been applied
outside the realm of youths. In an interesting study on corporate corruption, Keane (1993:304)
found that corporations might violate regulations in order to escape from an adverse economic
situation” (http://www.criminology.fsu.edu/crimtheory/agnew.htm)

The theories of Anomie and Strain proposed by Durkheim, Merton, and Agnew can all be
applied to computer crimes. As it is stated in the interviews section of this research, cyber
criminals come from a very diverse background which can be difficult to group together. The
cyber criminal who would most likely fit into these theories would be those who are in high
school or college. They may see how they could put a lot of hard work into their studies and
development of talent, yet realize that it is unlikely that they could achieve the financial success
in other fields such as finance. As a result they may see crime as a means to achieve enormous
financial success despite it being through deviant behavior.

Strain Theory could also potentially explain the rise in cyber crimes coming from foreign
nations which are not nearly as well off as the United States. Since cyber crimes, especially those
violations listed under the Computer Fraud and Abuse Act, could be conducted from anywhere in
the world an individual may see it as a very profitable endeavor. The internet allows an
individual to instantly send communications anywhere in the world, but it also allows them to
commit crimes from anywhere in the world. An individual in a third world country could see
computer crime as a way to make large sums of illegitimate money.

Strain Theory and Anomie are very important and can be applied to computer crimes.
These theories can be applied very well to telecommunications crimes involved with identity
theft and other monetary crimes, as theorized by Robert Merton. These theories can also be
applied to cyber crimes which are not monetary in nature, as evidenced in the theories by Emile
Durkheim and Rob Agnew. These theories can traditionally be tied to the formation of organized crime and the strain individuals face when they want to meet the positive goals of society but are at a disadvantage or otherwise do not have the means to accomplish their goals. Organized crime now plays a very large role in cyber crimes and many of the individuals recruited by these criminal organizations could be influenced by Strain Theory.

**Social Conflict Theory**

Social Conflict Theory is perhaps the most controversial of the theories which will be documented in this research. This theory is documented extensively through the works of socialist theorists such as Karl Marx and refers to the struggles that individuals in lower socio-economic classes feel from those in higher classes. This theory is well documented in the field of criminology and sociology as it explains why crime is much more prevalent among those individuals who live below the average standard of living.

Karl Marx believed that the most important thing in an individual’s life is the work that they do and the results which they receive from it. He believed that it is through ones work that they receive the basic necessities needed for their survival, such as food and shelter. “Marx thought that the way the work is socially organized and the technology used in production will have a strong impact on every other aspect of society. He maintained that everything of value in society results from human labor. Thus, Marx saw working men and women as engaged in making society, in creating the conditions for their own existence” (http://web.grinnell.edu/courses/soc/s00/soc111-01/IntroTheories/Conflict.html).

Marx believed that conflict arises between two classes, one which has the bulk of capital and the other which only has their own labor and time as capital. The first class, defined as being
the bourgeoisie, is the small minority in society who own the bulk of the capital. The capital can be anything of value from being basic currency to property ownership. The second class is defined as being the proletariat. These individuals make up the vast majority of those in society, but own very little of the total capital. Marx defined these individuals as having only their own time and labor as capital which they then sell back to the bourgeoisie in return for employment. Marx theorizes that the bourgeoisie exploit the proletariat by not offering them fair wages and thus cause economic exploitation to occur.

It is because of this economic exploitation that there is conflict between these two classes. It comes down to the belief that those who have the capital use their capital to suppress those who only have their labor to offer. “Economic exploitation leads directly to political oppression, as owners make use of their economic power to gain control of the state and turn it into a servant of bourgeois economic interests. Police power, for instance, is used to enforce property rights and guarantee unfair contracts between capitalist and worker. Oppression also takes more subtle forms: religion serves capitalist interests by pacifying the population; intellectuals, paid directly or indirectly by capitalists, spend their careers justifying and rationalizing the existing social and economic arrangements” (http://web.grinnell.edu/courses/soc/s00/soc111-01/IntroTheories/Conflict.html).

The conflict arises from the political oppression that would occur by the bourgeoisie using their capital and influence to maintain control of their own power and interests. Those individuals who are part of the proletariat would end up feeling a sense of hopelessness to break out of their lower level of living and this would lead to conflict such as violence and political upheaval. The ideology and general perceptions of society are also controlled by the bourgeoisie since they have the political and financial power to influence these ideals. “Ideology and social
institutions, in turn, serve to reproduce and perpetuate the economic class structure. Thus, Marx viewed the exploitative economic arrangements of capitalism as the real foundation upon which the superstructure of social, political, and intellectual consciousness is built” (http://web.grinnell.edu/courses/soc/s00/soc111-01/IntroTheories/Conflict.html).

The simple premise of Marx’s theory is that crime is influenced by the social and economic forces of society, which are controlled by the bourgeoisie through their wielding influence. Those who are part of the proletariat would again feel that they are being suppressed because of their relatively small amount of power with which they could influence laws and social policy.

Marx however fails to take into account the affect of how the middle class affects social policy and law. In fact, at the time of this theory there really was no such group like the middle class. Conflict Theory simply boils down the conflict between those in society who have everything and those who have nothing. The Social Order of modern first world countries, such as the United States, includes a small upper class (bourgeoisie), a small lower class (proletariat), and a very large middle class. Marx fails to take into consideration the affect that since the middle class has the most individuals within it, it actually yields the most power to influence social change in a government that is ruled as a Republic, such as the United States. Since ruling officials are elected by the people of society it forces, in principle, the ruling party of Government to craft social policy towards the needs of the middle class. Even if there were no middle class, Social Conflict Theory is crafted towards a society which rules by the means in which a very small group of people can promote individuals into power. In America the proletariat can force those who are in power and promoted by the bourgeoisie to be forced out of office because they are not shaping social policy to meet their needs.
Although this theory is well documented in the field of Criminology, it isn’t widely accepted as a central sociological view about why certain individuals commit criminal acts while others do not. There are issues as to how this type of theory would be able to be implemented in many modern societies, especially those in modern America and Europe, and this has caused a good number of individuals within this profession to look towards other theories for explaining deviant behavior.

This theory however does potentially serve an important role in explaining why cyber and telecommunications crimes are on a sharp increase in certain parts of the world. There are still certain parts of the world, specifically in some Eastern European and Asian countries, where their society is representative of the bourgeoisie and proletariat portrayal theorized by Karl Marx. In certain countries, such as China, the vast majority of society is proletariat and very poor. Most of the people in China work very long hours in poor working conditions only to make very poor wages. It is because of this that they live in poor conditions while the very few in the Chinese Government are wealthy and make an extreme amount of wealth on the labor of what Marx would call the proletariat.

It is because of this that Social Conflict Theory could explain why China has seen a large spike in cyber crimes. Individuals in China may see themselves as the proletariat with very little power and even less hope of being able to change the social norms and ideals set forth by the Chinese bourgeoisie who hold high level Government positions. These individuals are the ones who set law and policy to keep themselves in power and remain control over the masses. If a large portion of the Chinese population has this viewpoint then it could explain why they would target foreign nations such as the United States or large financial institutions. They may see
cyber crime as a means through which they could accumulate wealth and potentially catapult themselves out of the low level proletariat life.

Social Conflict Theory also emphasizes the anger that the lower class has against the ruling class. This could explain why they would resort to deviant behavior through electronic means to strike back against those who have the capital. Although China was used as an example in this section it certainly isn’t the only nation that has this problem. Although far less common, this section could also be used to explain deviant behavior in the United States. If an individual in America is from the lower class, or perhaps from the Middle Class, then they may resort to cyber crime to accumulate wealth and strike back against the small upper class. This would be applicable if the individual in question believed that this would be the only way through which they could climb up the social ladder.

This theory can also be used to explain why individuals would target the upper class and financial institutions for means other than the accumulation of wealth. Those who are in the lower class may target the bourgeoisie for the simple reason of anger and revenge, or to inspire social change. Under this theory those who are in the lower class feel oppressed both socially and financially. If they want to change the social oppression they may cause denial of service or defacement of websites for the purpose of making a political and social statement.

Although Social Conflict Theory is controversial and not relatively accepted in the Sociological profession as being a universal criminological theory it can still be applied in certain circumstances. This theory would explain why cyber crimes are rising so rapidly in certain parts of the world. More research should be conducted in the potential connection between how this theory may apply to foreign cyber criminals. If we can understand the
connection then perhaps it could shape foreign policy to help reduce the amount of attacks on critical systems.

**Rational Choice Theory**

The Rational Choice Theory is one that does not place nearly as much importance of ones surroundings and relationships as other theories discussed in this research. This theory concentrates heavily on the individual who engages in deviant behavior and places a great emphasis on their line of thinking. This theory has gained a renewed interest in the field of sociology because of its ability to explain the behavior of those who engage in deviant behavior yet may not come from underprivileged backgrounds. This theory explains the rise of white collar crime and can also be well applied to explain the rising of cyber crimes.

The basic assumption made in this theory is that people by their very nature act in a reasonable and rational manner. This theory would state that that people think their situation through before making their decisions and realize the ramifications of their behavior before they actually make a decision. This assumption also states that the individual would consider all the means at their disposal to achieve their end goal before they actually engage in a course of action. This means that in order to be rational an individual may have two or three different methods to achieve their goal. If the goal is to make money a rational individual may be able to take an illegal path or a legal path to achieve that goal.

The rational individual would then need to conduct a cost – benefit analysis of their options before deciding on a course of action. For instance, the legal path to making money would not include incarceration as a cost, but it may be the more arduous path to the end goal.
The illegal path may be easier and may have the potential to make more money, but it also carries the risk of incarceration or possibly worse if things do not go right.

The core concept of Rational Choice Theory is based around what exactly makes up rational choice. These factors have been detailed through the works of Cesare Beccaria, Jeremy Bentham, and have been documented by Robert Keel (http://www.umsl.edu/~keelr/200/ratchoc.html).

The first factor that goes into rational choice is that the individual must be a rational person. This assumption was discussed previously. The second factor is that the individual must incorporate an ends/means calculation. This means that the individual must have thought about what they want exactly and the means that are available to them to accomplish that goal. As it was stated previously, there could be multiple means to accomplish a goal which could be legal or illegal. The third factor is that the person must have freely chosen their behavior based on their rational calculations. Again, this behavior may be legal or illegal in nature and would come from their conclusions derived from the second factor.

The fourth factor is that the central element of the rational choice calculation must be based on the pleasure versus pain analysis. This analysis would take into account the potential benefit against the potential cost to achieve their desired result. This flows directly into the fifth factor which states that the choice an individual makes would be the one which directly points to the maximization of their pleasure. The individual will choose the path which gives them the best realization of their ultimate goal.

The sixth factor is that “Choice can be controlled through the perception and understanding of the potential pain or punishment that will follow an act judged to be in violation of the social good, the social contract” (http://www.umsl.edu/~keelr/200/ratchoc.html). This is
the concept that society uses to create laws that will influence the behavior of individuals in a
certain manner. If the individual believes, for example, that the potential punishment for robbery
is not worth the benefit they would achieve then the rational individual will not engage in the
behavior. The goal for legislation is to craft laws that carry a punishment which is appropriate
and fair, but also severe enough to influence the perception of a rational individual that the
potential cost is far worse than the benefit that they would receive.

The seventh factor states that it is the duty of the state to create and enforce laws which
preserve the common good. This creates what is known as the social contract or common
agreement between those in society who agree to the behavior which is acceptable and what is
not. An individual needs to know which behavior is acceptable before they can make the decision
on which of multiple means would be acceptable to society.

The final factor of rational choice is that the potential punishment for violation of the
social contract be swift, severe, and certain. This means that the offender must believe that if
they violate a law they will certainly be caught quickly and that the punishment will be severe.
The severe part goes back to the sixth factor and makes the point that the punishment for
violating a law must have the perception of being worse than the benefit they would receive.

There is an additional sociological theory which was created based upon the conclusions
formed from the Rational Choice Theory. The Routine Activities Theory however is different
because rather than focus on the individual committing the crime it focuses on factors
surrounding the crime itself. This theory has three major factors. The first is that there must be an
available and suitable target. This factor is obvious because if there is no potential victim than
there can not possibly be a potential crime. The second is that the offender must be motivated.
The motivation for an attacker could be that they perceive the benefits of their deviant behavior
outweighing the consequences if they are caught. The final factor is that there must be no authority figure there to prevent the crime from happening. Deviant behavior is much less likely to occur when there is a strong law enforcement presence in a neighborhood.

The Rational Choice Theory is one which many people believe. It has been around for a very long time, however the theory has a flaw by its very definition. This theory assumes that people act in a rational manner and think their decisions through before they decide on a course of action. This assumption is a very large one because we have seen that there are many circumstances in which people do not act in a rational manner. There are many cases where people react to a situation without fully thinking their course of action through, such as responding to emotionally charged events. Many times individuals act based upon their emotions and this will typically lead to irrational actions.

Rational Choice also states that people will not choose a course of action in which they perceive the consequences outweighing the benefit. There are cases in which people will choose a certain course of action regardless of how strict the consequences are because they perceive the benefit as being worth any risk. If this theory were to be combined with the theory of Social Conflict we can see where this may be the case. If an individual from the lower class feels oppressed by the ruling class than they may be determined to change things at any cost necessary and risk bringing any consequence upon themselves.

Rational Choice Theory applies very well to those who commit cyber crimes. Most of the cyber criminals are very talented and well educated, not necessarily formally, and have the ability to think rationally through their course of actions. Cyber criminals are able to selectively target and attack victims that they believe would give them the greatest amount of financial gain with the lowest chance of being caught. The most advanced cyber criminals are rarely caught.
because they have the intelligence to cover their tracks and move through proxy servers to stay undetected. For the individuals that this would apply to, they have the means to commit very large fraudulent schemes and remain undetected. It is because they have little chance of being caught that they perceive the large potential financial gain as outweighing the chance of being caught. Many times these individuals are only caught when they deviate from their formulated plan to evade detection and make a mistake.

In conclusion, Rational Choice Theory is a very reasonable theory to use to help explain the actions of cyber criminals. This theory does have its flaws and pitfalls; however its ability to explain the reasoning behind why rational and intelligent individuals commit crimes makes it very useful. This theory would apply best to cases in which the motive for the cyber criminal is financial. It would not apply very well for cases in which the attacker is motivated for other more intrinsic reasons such as revenge or for a political statement.

**Social Learning Theory**

Social Learning Theory is well respected within its field and used Edwin Sutherland’s theory of Differential Association as a base while expanding upon it and making changes. A number of different Sociologists have contributed to this theory as it has evolved over many years. This theory is also very important to field of Criminology and has served as the one of the most important theories upon which laws have been crafted in the United States.

The individual who first proposed the concept of this theory was Gabriel Tarde. His idea was to move away from the most prevalent theories of the day which focused on biological traits into the idea that individuals learn deviant behavior rather then being biological inherent. This
again works off of the work performed by Edwin Sutherland and his theory of Differential Association.

Social Learning Theory proposes that individuals learn deviant behavior from observing those around them. Tarde proposed that there were four main requirements upon which Social Learning occurs. The first is that the individual must have close contact with the person whom they are imitating. This could be a family member, a close friend, or a mentor. The second is that the individual must engage in imitation of their superiors. They must be influenced to the point where they are willing to see what an influential individual is doing and imitate it themselves. The third is that they must understand their behavior. They need to know what the behavior really is and the exact method of how to conduct the behavior. The final requirement is that the individual must be acting as a role model to the person who is learning this behavior.

An important point about this theory is that unlike some other theories applied in Criminology, this theory takes into account the fact that the behavior one learns can also be positive. The person who is close and acting as a role model could be a Mother or Father who is teaching their children the proper way to behave in society and contribute positively. However, the opposite affect may also be true where an individual is engaging in behavior which would generally be considered positive, but later turns to deviant behavior because they learned it from somebody who has an influential relationship with them.

Since this theory proposes that behavior, both positive and negative, is learned through the close interactions of others it is reasonable to think about what will happen if two influential individuals interact but engage in different types of behavior. A good example of this could be seen in the workplace. Perhaps there is a junior professional who is learning the job and thus needs to be paired with a more senior professional. If the junior professional is learning and
shows a hard working attitude but the senior professional knows the job and has a poor working attitude, then which individual will learn which kind of behavior? It is reasonable to expect the junior professional to adopt the poor working habit of the more senior professional, but this may not always be the case. The junior professional may be more influential in their work habits and thus the more senior level professional may learn their behavior rather than the other way around. If the senior level professional sees that his junior is being promoted quicker than he is then he may change his behavior to reap the positive rewards.

Perhaps the most important contributor to this theory is Albert Bandura. “Learning would be exceedingly laborious, not to mention hazardous, if people had to rely solely on the effects of their own actions to inform them what to do. Fortunately, most human behavior is learned observationally through modeling: from observing others one forms an idea of how new behaviors are performed, and on later occasions this coded information serves as a guide for action” (Bandura, p#22). Bandura reinforces the idea in this quote that deviant behavior isn’t something within oneself. Through the process of Socialization an individual learns the norms by which they should behave in society by learning from others, and the same concept would apply towards learning deviant behavior.

Bandura believed that individuals learn behavior through observational learning. The first part of this process is that the individual must pay attention to person whom they are learning the behavior from. The second part is that the observer must retain, or remember, all of the behavior that that they were observing. The third part involves motor repetition which involves the ability to replicate the behavior that the observer witnesses from their mentor. The final and perhaps most important part of observational learning is that the observer must have the motivation to
engage in the behavior that they learned from their mentor. If the observer has no reason to imitate the behavior learned then they will not engage in said behavior.

There are three principles of Bandura’s theory. The first is that “The highest level of observational learning is achieved by first organizing and rehearsing the modeled behavior symbolically and then enacting it overtly. Coding modeled behavior into words, labels or images results in better retention than simply observing” (http://tip.psychology.org/bandura.html). This means that an individual is more likely to retain the behavior that they learned if they are able to see it through images as well as practice it. The second principle is that individuals are more likely to engage in an observed behavior if its results are something they wish for. The final principle is that an individual will adopt the modeled behavior if they admire their mentor and the value itself has some type of functional value.

Social Learning Theory bases its concept on the observed behavior of others. When an individual becomes a cyber criminal, for either ethical or malicious purposes, they generally do not learn their craft from a text book. They learn through hands on use of the technology as well as learning from the exploits of their fellow criminals. In the interviews section of this research we see that many times hackers are motivated for more intrinsic rewards such as notoriety and bragging rights. These individuals are often willing to pass on their knowledge to fellow individuals who may not have their technical knowledge in order to act as a mentor. The individual with less experience would then view the more experienced person as being a mentor and a figure through whom they could perfect their craft. This type of behavior would fit perfectly within the theory as it is defined in this section.

The act of hacking is in many cases a solitary activity, however most of the time it is learned through group interactions. Students on a college campus may learn their craft by joining
student organizations where they could interact with fellow students who share the same interests
and have an eagerness to pass on what they know. Another preferred form of communication for
cyber criminals is through IRC channels. It is here that they can remain relatively anonymous.
Through IRC Channels they can use aliases instead of their real names and discuss their exploits.
Had they used their real name and other personal information to do this then it is very likely that
law enforcement would take an interest in them with potentially severe repercussions for the
hacker.

In conclusion, the theory of Social Learning serves an important factor in helping to
explain the motivations behind many cyber criminals. This theory has been well studied in the
field of Criminology and is well respected. Potential criticism of this theory comes from the fact
that it theorizes that deviant behavior is only learned. Although once dismissed in the
Sociological field, the concept of biological traits to explain deviant behavior is becoming
plausible. This theory states that deviant behavior must be learned from a mentor with influence,
but makes no mention for the affect that certain genes and family history traits have on potential
deviant behavior. This theory does however explain why individuals from a lower socio-
economic status emulate the behavior of those around them.

Social Control Theory

Social Control theory is another theory which tries to determine why individuals engage
in deviant behavior. Perhaps the most significant contributor to this theory is Travis Hirschi who
challenged a number of previously assumed factors and other sociological theories. As with other
behavioral theories this one ties in closely with interaction with other people; however there are
some key differences which will be noted in this section of the research.
This theory relies heavily on an individual’s internal code of ethics and morals. This theory proposes that if an individual has a strong sense of values which tie in closely with those of the community then they are much more likely to contribute to society rather than cause damage. “Control theories take the opposite approach from other theories in criminology. As their starting point, instead of asking what drives people to commit crime, they ask why most people not commit crime. Control theorists generally argue that there is no problem explaining why people commit crime since all human beings suffer from innate human weaknesses which make them unable to resist temptation” (http://www.apsu.edu/oconnort/crim/crimtheory13.htm).

A key factor to this theory is that the individual must have been socialized correctly in order for them to internalize the correct set of moral values. It is through these values and sense of right and wrong which would make an individual resist engaging in deviant behavior which would damage the community. Sociologists who focus on this theory would study an individual who has deviant behavior to determine what internal value is missing in them.

When an individual is going through the socialization process they have a number of influencing forces acting on their development as an individual. Two of the most important contributing influences of this theory come from family and religion. The influence that religion would have on developing the internal social bonds of an individual would be that of commitment, such as that to their faith and belief system. The value that family would contribute would be that of attachment, such as that to your siblings.

Although Travis Hirschi did not in fact invent this theory he has played an important role in its evolution. Hirschi proposed that there are four basic social bonds which when internalized in an individual prevents them from engaging in deviant behavior. The first bond, which has already been mentioned, is that of attachment. According to Hirschi this develops an individual’s
sense of affection and/or sensitivity for others and allows them to understand how their actions would affect others. The second bond is that of commitment which creates an individual’s sense of responsibility and investment in their community as well as conformity to its norms.

The third bond is that of involvement. There have been studies conducted that shows an individual is less likely to engage in deviant behavior if they are involved in different activities within their community. For instance, juveniles who participate in organized sports or after school clubs are much less likely to commit crime than those who do not. This gives them something to do with less time to engage in deviant behavior. The final social bond is belief, such as the extent of their belief that the laws are just and should be followed. The stronger an individual believes that they should obey the law the less likely it is that they will willingly break it. “Hirschi found a strong association between self-reported delinquency and agreement with the statement "It's OK to get around the law if you can get away with it", and this and related statements became measures of the belief component” (http://www.apsu.edu/oconnort/crim/crimtheory13.htm).

Hirschi later changed many of the factors in the previously mentioned theory in the 1990’s. During this time he collaborated with Linda Gottfredson to develop the theory of Low Self Control. This theory was developed to address changes in attitudes as well as to address some criticisms of his previously mentioned Social Control Theory. This theory greatly incorporates the importance of family bonds and its influence in the development of an individual.

Social Control theory proposes that every act of deviant behavior can be traced back to a certain trait within an individual. The certain traits of an individual may fall within three categories under this theory. The first would be a trait that indicates an individual’s low self
control. Traits which would fall under this category would be shortsightedness, poor judgment, or miscalculation of pain. The second would be a trait which would predict an involvement in deviant behavior. The traits under this category would be spontaneity, low intelligence, as well as high activity level and strength. The final category would be one which is the direct result of the socialization process. This could be being impulsive, insensitive, or having the need for instant gratification.

Social Control theory seems to tie in very closely with Social Learning theory. In Social Learning an individual learns deviant behavior from those who they hold a close bond with. Under this theory it is proposed that individuals learn acceptable behavior from those they would hold a close bond with, such as their family. The main issue which an individual may take issue with under this theory is the assumption that every individual is inclined to engage in deviant behavior but it is the social bonds and traits they learn which influences them to engage in behavior deemed to be acceptable to society. Those who subscribe to the theory of Social Learning would state that the deviant behavior is learned rather than inherent to every individual.

Social Control theory would apply well to individuals that engage in cyber crimes who have never developed a sense of ethics for what is considered acceptable in the field. This theory could be used to justify the need to incorporate ethics courses in the curriculum for computer science and information technology degree programs. As Social Control theory proposes that individuals must develop a sense of what is right to avoid deviant behavior, some individuals may learn the technology behind how systems work but may never understand the ethical issues associated with it. Every professional working in the field of information technology should subscribe to the code of ethics for a professional association such as that offered through the Institute for Electrical and Electronics Engineers or Association for Computing Machinery.
Social Control theory may also explain why crimes involving illegal peer-to-peer sharing of intellectual property and other violations of Digital Rights Management are increasing so quickly. Individuals of all ages participate in this crime and it could be because they were never socialized into believing that the behavior is wrong. If an individual’s internal sense of ethics does not find anything wrong with downloading illegally obtained music and movies then they will continue to engage in this behavior.

While Social Control theory is similar to some others documented in this research it does propose some very different elements for deviant behavior. The most important difference for this theory is that it doesn’t try to explain why people commit crimes; rather it tries to explain why people do not commit crimes. This theory puts a particular importance on how the socialization process influences individuals to engage in acceptable behavior. If an individual does engage in deviant behavior then this theory proposes that something went wrong in the socialization process and they are missing a trait which influences their behavior.

*Control Balance Theory*

The Control Balance Theory is the final theory which will be covered in this research. This theory is another control theory; however it is much lesser known than the previously documented Social Control Theory and expands upon the research conducted by Travis Hirschi. Control Balance Theory was proposed by Charles Tittle in his work titled “Control Balance: A General Theory of Deviance” (1995) and proposed a different opinion as to how controlling forces influence the behavior of individuals within society.

Charles Tittle proposes that individuals engage in deviant behavior when there is an imbalance of control in their lives. He proposes that an individual will react in different ways if
they either have too much control in their lives or if they do not have enough. This theory also
takes into account the factor of Social Control Theory which was documented previously in this
research and states that individuals are more likely to engage in deviant behavior if they feel a
weak obligation to uphold the social contract, which is following the laws.

Under Control Balance Theory individuals will react in three different ways if they have a
lack of control in their lives and it is called repressive deviance. The first way in which an
individual may react is to engage in predatory behavior. This would be the most dangerous way
an individual could react because it would cause the most damage to society. The crimes which
would be considered under this category would be acts of physical harm and/or theft of property.
Generally speaking behavior under this category would be considered on the felony level of the
United States Code.

The second manner in which an individual may react to a lack of control would be
defiance. This type of behavior is easily seen in juveniles as they generally have very little
control of their environment. The type of behavior an individual may engage in under this
category are far less dangerous than in the predatory category and would include things such as
rebellion, property damage, and other behavior typically defined under juvenile delinquency.

The final way an individual may react to a lack of control as proposed by Tittle is
submission. This way is less common and far more bizarre than either predatory or defiant
behavior. Under this theory, submission would be an individual allowing themselves to be
controlled, abused, exploited, and humiliated. This would happen if an individual has no control
and willingly allows themselves to remain in that situation. A classic example of this is when a
child is raised in an abusive household with little to no control. In many of these cases the
juvenile incorrectly goes through the socialization process and never truly develops correctly. In
this case an individual who grows in an abusive environment may not know any other type of living and as a result they allow themselves to be controlled and abused even after they can control their own environment and circumstances.

Individuals who have too much control would engage in one of three different ways than if they had a lack of control. The first way they may react would be exploitation. Individuals acting under this category have quite a bit of control over their environment and will do anything to make sure that they do not lose this control. An individual would manipulate circumstance and exploit individuals in order to maintain their own power and control. This can be seen in many cases where individuals engage in deviant behavior in both business and politics. People here generally have quite a bit of influence and power. They want to keep their power so they may do anything it takes to first get that power then make sure that they maintain it. This could explain why fraud and corruption are so prevalent among people in power.

The second way in which individuals may react when they have too much control is to plunder. This type of behavior could be considered the most dangerous of these three as it can result in violent behavior. History has shown how too much power and control corrupts people and changes them into people that they were not previously. History is littered with examples of where individuals with absolute power used their power for plunder and violence in order to keep or expand their own power. The classic quote that “absolute power corrupts absolutely” applies perfectly to this situation. The final behavior that individuals may engage in if they have too much control is decadence. This would essentially mean an individual is engaging in behavior which ends up causing their own physical and/or mental decline. A classic example of this would be drug use causing an individual to become an addict.
It should be noted that the six previously mentioned types of behavior are a result of what an individual perceives as an imbalance of control. Whether or not an individual actually has a lack or excess of control is irrelevant, what matters is how an individual perceives their own sense of control. This theory also notes that an individual with a control imbalance may not necessarily engage in deviant behavior, rather it is once an individual reaches their own tipping point of control imbalance that they begin to engage in deviant behavior. “The amount of control to which an individual is subject, relative to the amount of control he or she can exercise, determines the probability of deviance occurring as well as the type of deviance likely to occur” (Tittle, p.135).

Tittle describes the amount of control that an individual exercises to the amount they are subject to as the control ratio. This theory explains very well why cyber crimes are rising so quickly in certain parts of the world. In certain parts of the world people are still very much subject to tight Government control of their lives. However, what the internet has done is give them an opportunity to expand upon their own lack of power. For instance, a hacker in an oppressive nation may have internet access and see it as a medium through which they can improve their control ratio by increasing the amount of control they can exercise.

An individual in this example could engage in predatory behavior for instance by developing malicious software with the purpose of controlling other machines, such as a bot to create a botnet. If this individual could create a very large botnet under their direct control then they would be able to wield a tremendous amount of power. If their botnet is large enough they may be able to extort powerful organizations to give them what they want in exchange for not completely shutting down their communications infrastructure. The ability for an individual to
force a large organization to bend to their will or face the consequences would greatly increase their own sense of control.

Research conducted by Wood and Dunway (1997) argues that Control Balance Theory can be applied to sex offenders. As it is documented in the interviews section of this research, the internet is always becoming more and more popular as a medium through which sex offenders can engage in their deviant behavior. This research found that many sex offenders committed their acts because of their perceived lack of a perceived lack of control in their own lives.

In conclusion, Control Balance Theory presents a very plausible explanation as to why many individuals engage in cyber crime. There has already been some research conducted in the area of how Control Balance Theory can be applied to cyber crimes as evidenced by the 2008 work of Katherine Williams in her work titled “Using Tittle’s Control Balance Theory to Understand Computer Crime and Deviance”. Further research should be conducted to investigate the true extent of which this theory can be applied to cyber crimes.

All of the theories documented in this part of the research concentrate on behavioral and control sociological theories. This is because cyber crimes isn’t something that comes natural to individuals and as a result it is unlikely that biological theories could be applied to explain this. Telecommunications and electronics in general is an invention of man, it is not something that just comes naturally. Perhaps biological theories could explain why some people are sexual deviants but this would be outside the scope of this research. In the case of child pornography an individual is using electronic communications as a means to engage in their deviant behavior, it isn’t a cause in and of itself.
Interviews

This section of the research focuses on the experience of individuals who deal with cyber criminals on a daily basis. A standard list of questions were used in each interview however additional questions were asked depending on the answers which were given. The questions that I asked and their responses are documented in this section. Analysis of these interviews are listed in the final analysis section of this research.

Bradley Bartram – Intelligence Analyst
New York State Office of the Attorney General – Organized Crime Task Force

Imhof: Can you please tell me about your formal background?

Bartram: I actually transitioned into information technology back around 1995. Basically I had been working in project management and things like that at the time of a technical nature dealing with satellite technology and things like that. Also managing the installations of emerging satellite technology across the country and essentially I started transitioning more into information technology as I realized that I didn’t really want to be doing project management like that. So basically what wound up happening was that I made the transition and little by little I started managing more systems.

This lead to more responsibility and eventually into project management, which then as I began getting more and more into it I realized that I didn’t really want to manage information technology during that point in my career but I wanted to be more of a practitioner so I began getting more involved in day to day operations such as systems administration tasks, and
especially database administration tasks. There were a bunch of courses and formal training such as one, two, or three day training seminars that I went to. I did various things like that and just learning more and more about that and my experience just grew. Then in the backend of 2005 I decided to finish my degree which led me to the Economic Crime Investigation degree at Hilbert College where I finished and was hired here.

**Imhof:** What has been the extent of your experience with cyber criminals?

**Bartram:** I would say that my first real experience with it really back to around 1998 or 1999 which is when, not myself, but a colleague of mine had set up a system that he was using on the internet to communicate with some of our staff resources and things. What ended up happening was that it ended up getting compromised. Back in those days a firewall was more black magic then anything else. The biggest thing that may have happened was a misconfigured router or something like that or there may have been a proxy server up. Computer security was thought of as more of an afterthought and so what ended up happening was that the server was sitting out there with a bunch of open ports and became compromised. At that point when we realized that the system was compromised it led us down the path of trying to figure out who to call, which at that point was the FBI. They sent us a couple of special agents who talked with us about it but nothing ever happened. They did nothing with it or find information on it or anything like that.

All of this pre-dates really any type of technology with the Regional Computer Forensics Lab or anything like that. They were just a couple of guys sitting in an office somewhere with our computer and sent us on our way. After that really it became more of a passion for me to figure out why they got in. For me personally having a system compromised, even though it wasn’t my system, affected me. It bothered me to the extent this guy broke in and violated it and
I thought he would steal our personal data. In reality he didn’t, all he did was set up an IRC server to communicate with all of his buddies and that was pretty much the modus operandi of the day. However, at the same time it was like if a burglar broke into your house and they may not be looking for your personal stuff but it is on the floor anyway. It was at that point where I began pursuing information security more aggressively and went more into it to understand the why, how, and what was going on.

*Imhof:* What common patterns have you found, in your experience, between cyber criminals?

*Bartram:* From my experience I have seen two very basic types of cyber criminal. The first is going to be the stereotypical Hollywood portrayal of the super-hacker who gets in because they are after something specific that you possess. A perfect example would be somebody trying to get into VeriSign to compromise the root certificate where it is definitely something specific that they can target and approach with a goal in mind. This would more or less fall into the whole category of industrial espionage, intelligence gathering, or anything like that which you would see government to government or big business to big business. You see so little of this kind of hacking especially at the lowest levels. If you get into the Military or something you may see more of this.

At the same time the most often cases involve the crime of opportunity where you will have somebody that actually breaks in and says “this is the easiest system” or they are executing a port scan or something. Then the attacker may see that the system is vulnerable to an exploit they already have and they just try it. They then get in a set a toehold to compromise the system further. When I was actively working in systems administration in a corporate setting I would see mostly phishing scams, Metasploit, or attacking a web server through a hole in PHP or
something, escalate their privilege, throw in a hidden directory, start answering requests and compromise the sendmail installation or something like that. Sending spam or setting it up so that you received these hacked forms for phishing expeditions.

Those are the two that I really see and I tend to categorize them into one of those two categories. Generally speaking, 99.99% would fall under the crime of opportunity category. It is going to generally be somebody who has a little bit of knowledge, not an incredible amount, but enough to be dangerous. They may have a couple of tools but they aren’t going after anything in specific. They are going after a specific system because it is the path of least resistance. They know that they can get in and once they get in they can do whatever they need to whether it is using bandwidth or just poking around to see what you have or they may have a purpose in mind that they just need a system for.

*Imhof:* So, are many of these attacks perpetrated by script kiddies?

*Bartram:* I hesitate to use the term script kiddie because I think that it tends to be overused at times. You may have somebody that is a disgruntled systems administrator or something that is thinking about leaving, or has left, has a few beers and sits down thinking “hey, this is a great idea” and gets into a system that he knows he can get into and does something because he knows that he can do it. However, at the same time in the traditional sense when you start dealing with that whole continuum of knowledge the disgruntled administrator knows more then your average twelve year old kid with a couple of scripts that he downloaded from IRC. However, at the same time he is not the talented hacker who is getting in by busting through all of your firewalls and stuff. It is just the path of least resistance. It may have seemed like a good idea at the time, saw that he had a tool which happened to be where his limited knowledge is or whatever then got in
and may, or may not have, done something that was damaging to the company or the target to whatever extent however it isn’t like he is going after something specific.

He is not going after a CEO when he knows that he has all of his banking information on a specific computer and led their way in through multiple layers to get in. It is more like they throw back a few then see what they can do to damage their former employer or something to that extent. Script kiddies tend to be completely brute force while this guy has a little more finesse and a little more targeting but it is still pretty common.

Imhof: From your experience, have you seen more attacks from the inside or the outside?

Bartram: I have seen it mostly from the outside. When you talk about an attack I am using it more comparable with a negative connotation. I see a lot of stupidity from the inside. Information Security is that standard of making sure that the information is available, the essential information that the employee needs is available, and yes I have seen failures of that kind where somebody deletes the information and there is no backup of that directory or something and oh well I guess you are out of luck. In terms of an actual attack where somebody is trying to get in then it is usually from the outside. I could go through my Apache logs and see all of the attacks that we get hit with and again that would be a script kiddie.

Imhof: Do these patterns differ significantly with the different crimes?

Bartram: Surprisingly no, a lot of what I have seen between script kiddies and the traditional definition of a hacker and a child pornographer. If you take out of the equation from a child pornographer the people who are genuinely addicted or compelled to seek out and collect that
type of material then you are left with an element of people who are doing something because they know it’s wrong and they are testing the limits of how far they can go.

One of the interesting things that I really wasn’t expecting when I first started in some of the child porn cases was that we had actually come across a group that was communicated through completely encrypted channels and were a very secure group of child pornographers. We were able to be alerted because we intercepted a few plain text type of communications that showed what they were doing and we were able to view some of the images that they were sending and things like that. They were being discreet but they were not being completely anonymous. So we were able to see what they were doing and see who they were. We came across the back channel communications that they were using that was basically just a discussion group. They were not posting any pictures, all they would do is talk about it with their operations and things like that. Because it was a public forum we could just communicate and read what they were saying. The interesting part was that there was an interesting psychological profile that came out of this.

We were seeing a lot of guys, and I say guys because 99% of child pornographers are guys who are old and white, that were compulsive about it and were into the whole child pornography thing with genuine lust after children. However, there was also another group that was basically testing the limit of security to say that “I have something that I am not supposed to have”. This is a similar type of psychology for pirated music, movies or whatever. They just collect contraband information and whether they derived joy from it I don’t know. It was just one of those things that they talked about some of their security measures and some of the lengths that they went to were very in depth. This was interesting because you have the same type of things as you would with traditional hackers if you read about people from the golden age of
hacking with the 2600, Captain Crunch, Steve Wozniak, Steve Jobs and Bill Gates back when they were still young kids. It was a similar type of thing, they would first find out how it worked then test the limits. I think it goes back to that almost archetypal hacker mentality.

*Imhof:* Do you believe that malicious and ethical hackers have similar personalities, attributes and psychological drives?

*Bartram:* To an extent the whole ethical hacker thing comes down to definitions and where the limits of your definitions are at. The ethical hacker who is doing it for the betterment of mankind, research in computer security or something like that may not be their true motivations. With the malicious hackers you have to try and look at what their true motivations are. To actually just lump them in would match certain elements rather than they share their thought processes or whatever, but for the most part I don’t think that there is a lot of similarities. I think that there is definitely more behind their thought processes whether it is their ideology, money, recognition, fame or whatever. So, I mean once you get to that you can categorize them a little bit better into what their true motivations are.

*Imhof:* Many people believe that hackers are motivated solely by financial means, do you believe this to be true or are they motivated more by intrinsic means?

*Bartram:* I think you are going to find that the vast majority are going to have some type of financial aspect to it. If you look at the current trends where everything is happening right now you will see that in the last couple of years there has been a definite shift with people just hacking websites and defacing them or whatever. The trend has shifted more towards ideology
happening because people are hacking specific websites, putting up specific messages and things like that which are representative of their beliefs or whatever.

I think what really has happened is that now we are seeing more of this cottage industry of ideology hacking go by the waste side and big business infrastructure is taking over. If you start looking at the bigger trends that are happening like botnets or mass identity theft types of attacks or any of these big high profile incidents that are happening, when you boil it down it is really about money. At this point child pornography is big business. Most of what we caught in our last investigation had to do with child pornography in relation to somebody selling a service. They were not doing it just for a tit for tat trade, they were doing it and saying “come visit my website where you can get all of this stuff if you just pay me some money”. There is certainly a financial aspect to it and the trend is emerging where you are beginning to see a more organized crime aspect to it then with the individual ideology.

*Imhof: Do you believe this trend will continue into government sponsored hacking?*

*Bartram:* I don’t know how much the foreign governments are getting involved, but there is certainly a growing trend that there is almost like another branch of the armed services that is coming out and starting to emerge that is focused on defense of cyber assets as well as the offense of somebody else’s cyber assets. I think what happens is that the more we become online as a nation and the more personal thing we put into cyber space then the more you will see that continuing as a growing trend.

In general I think that mainstream security there is always going to be that danger that we are going to have to defend against that. Based on current trends what you are starting to see is that organizations are always becoming more complex and a dissection of modern malware
which are still commonly infecting Windows systems even with all the security upgrades and everything else, however valid they are from Microsoft’s point of view, we are starting to see a lot more sophistication and what the research suggests is happening is that the modern malware is starting to be developed in a much more in an illegal, yet corporate, structure.

We are starting to see this mix where illegal organizations are hiring legitimate and very talented regular software developers that are actually going to go out and develop a certain key component. Like for instance in a lot of the modern botnets that we are seeing have not only the spam setting but we are also seeing proxying, rootkits, disguise, and all of these various functions including network infrastructure with their own DNS services, web services, load balancing services, defense mechanisms, and things like that. They all have this individualized and decentralized infrastructure which the level of sophistication required to implement all of that requires more than just one guy or just a couple of people. It actually shows that somebody went through this whole project in house and starting saying develop A and Z to do B and C. There is just a level of sophistication where it shows there was organization, thought, and planning that went into the design and creation of this software as well as deployment.

We are also starting to see that after all of these systems are affected they are just staying silent and not doing anything, which baffles a lot of security researchers. But at the same time we are also seeing this whole emerging trend of other botnets are being sublet. People are getting different segments of it that are being sold off to the highest bidder. So, we are certainly seeing an emerging business aspect that is emerging out of it. The conventional wisdom is that the Eastern European, Russia, organized crime is behind it and we get a lot of that.
Imhof: Why do you believe that the rate of cyber crimes is increasing so quickly?

Bartram: I think because they’re easy. Again it is the path of least resistance. Cyber crime has such a low rate of conviction or even being caught. When you start dealing with a situation that, if you commit a crime that nobody knows about and you will gain from it, will you do it? The honest person says no, but then again what do they do when they’re left to their own devices. That has always been the psychological experiment. The internet is no different because cyber crime has such a low percentage of people being caught and if you cover your tracks it will most likely result in a dead end. As I have said a few times we tend to catch the stupid criminals, those that make the mistakes. The smart ones are those that cause us to run around in circles.

What is happening is because of the expenses that were eliminated by moving more and more of business infrastructure to virtual communication it makes for more potential targets. To give you an example, when I was in the corporate world we used to EDI, Electronic Data Interchange, which was carried along by a specified protocol, the EDI protocol, which I believe was programmed in COBOL or some other archaic language and we would pay $1 for each transaction and we were getting about 800 transactions per average day. On some days it would range to as high as 10,000 transactions. If you are paying that price then you can quickly understand the costs associated with it. As business keep moving further and further, all of a sudden as they became more and more online you didn’t need these expensive Frame Relay lines that were coming in, you didn’t need to string private networks between all of these organizations. So, the cost of doing business and acquiring those orders were reduced to basically just the cost of doing business that was part of your infrastructure.

It wasn’t something that you had to devote an actual line item that states that we are spending $750 million a year on just obtaining these orders. It was no longer a part of the cost of
goods sold. It was something you could attribute to operational expense or whatever. Now you have XML and all of these other data interchange formats that allow you to vary your costs. So as it happens it was just logical businesses want to save money so they are moving more and more data across the general pipe of the internet.

As with all businesses, or all organizations, some are going to be more secure then others and you are only as secure as your weakest link. You have the people that hold onto credit card data that is in excess of what you are supposed to in accordance to the PCI standards, then if you have a break in and the data gets compromised then you have just messed up your customers with results like TjMaxx or something losing millions of credit cards. When you leave your data on a laptop because it is no longer a situation where you need an infrastructure to run any of this. I mean, a laptop in this office may have a 250 GB hard drive in it which can store a lot of data, not just the operating system and more.

More of the trend is that more and more things, because of automation or whatever, telecommuting or anything like that causes more critical systems to be moved onto the open internet, or somewhat over the open internet. There are not so many divisions with the web server out front connected to the DMZ where it could communicate with all of the other servers it needed to but your customer database was on another completely private network which was very well isolated based on physical boundaries and things like that. These days that doesn’t happen, you may see because of the availability of space, resources, and everything else you may see both of these as instances on a virtual server.

As more of this happens there are more easy targets compromised. As security gets better the compromises get more ingenious. With the complexity of software somebody is going to make a mistake it’s just the nature of business. Whether you are in the government of private
business you are pretty much using the same software so you end up running into the same
problems. Part of the problem is that we are moving towards a much more wired society. People
are creatures that don’t think of isolation so much, it isn’t in our nature to say that we need to
isolate, put up walls, and create divisions between each piece of essential information. We want
to be open given the preponderance to be on Twitter, Facebook and MySpace. We want to tell
people what we are doing. It is in our nature to say we want to be more secure; however we also
do not want to be isolated.

*Imhof: Have hackers used social networking sites to gain information on targeted people?*

*Bartram:* I haven’t seen it personally in my experience yet, but that isn’t to say that it won’t
happen. One of the things that you need to look at, with Facebook for instance, you may end up
getting a survey request that asks for your perfect porn name or something which is one of these
innocuous things. What it requests is your mothers or fathers’ last name and your first pet’s name
or something like that then they put it together and that is what they have. The problem with that
is that it is asking a very indirect question, but you have essentially just given up your mother’s
maiden name which is a key component in identifying yourself for credit card purchases.

It doesn’t take that much to get a social security number from somebody and you are
giving up so much of your profile information including the street you live on and everything
else. Taken individually it doesn’t mean too much, but if a hacker compromises Facebook and
their database they will be able to find you and everything that you have ever posted. If you put
your information online they will be able to haul it over based on your postings and response to
the survey questions. With enough skill in analyzing the data and putting it back together again
they can gain an incredible amount of data on you. It is amazing how much data people willingly
give up on themselves just for the sake of being social.

*Imhof: From your experience, do many users use the same password across different systems?*

*Bartram:* I have seen it where the same password is used or a variation of it. Again, people don’t
like security. The security measures will only work to the point where they either stop being
enforced by management or it becomes onerous on the user. If it is too onerous and there is no
enforcement from management saying “if you don’t do this you will be fired” then it is of little
use, nobody hears you and nobody cares. This is definitely an avenue of attack. It is the same as
if somebody password cracked your website.

What I have seen are these multiple authentication tokens that are out, identify the picture
and phrase then enter your password if you think that everything is okay. After the first time or
two it just becomes routine. Are you really paying attention to what is going on? If yes then
proceed, but if not then people will probably think about it twice but just proceed anyway. People
do not tend to care too much about it. If you allow users to choose their own passwords then you
create a situation where they are going to also use it elsewhere. Once they use it elsewhere, if
that system is compromised then that is just one more available resource for the hacker.

If they can see a password then they can also see the psychology behind how they work.
What kind of password was this? Where did they derive it from? Is it their family or pet name? If
the hacker has access to their Facebook or other social networking profile then they may be able
to get that information as well. In this case we would be looking at a very directed attack, this
attacker would have a definite goal in mind and are looking at something specific. This would
not be an example with the path of least resistance.
Even with identity theft with credit card numbers the attackers are not going after the individuals one at a time, they could care less about your credit card specifically. What they are looking at is the path of least resistance which happens to be an example like TJMaxx. If they can get twenty million in one swoop without too much more effort. Why would they go after yours or mine individually when they can target an organization as get twenty million? The street value of an individual credit card number, valid or not, really isn’t that high so it all comes down to that motivational issue.

*Imhof: What kind of cyber crimes are increasing the fastest?*

*Bartram:* Definitely malware related crimes, that is pretty much the biggest thing you are going to see. If you are talking about individual perpetrators then it is hard to say. Depending on what statistics you look at and everything else it may be child pornography or it may be bank fraud. All of this is facilitated a lot by the malware that is coming out.

If you want to include in cyber crime, depending on your definition of cyber crime and how narrow or broad you want to be with it, if you include intellectual property violations then certainly it is peer to peer where you are downloading music and movies and whatever else is out there. If that is included then it is certainly the biggest, but after that I would certainly say malware, botnets, spam, or whatever else they want to do with this vast network of distributed computing. The federal government is very involved in child pornography cases, especially the United States Attorney’s Office because they prosecute it because it is a very easy crime to wrap your mind around.

Behind child pornography there is always a defined victim, which is the person depicted in that picture, and then there is the defined perpetrator which may be one or many. The
perpetrator may be the individual who took the picture, the individual who is distributing the picture, or the individual who obtained and possesses the picture. This also tends to be the focus of federal cyber law enforcement at this point. They have a number of agencies with a directed focus on investigating child pornography cases.

*Imhof:* What do you believe can be done to mitigate the rising crime rate?

*Bartram:* I think that what really needs to happen to mitigate this is to put more pressure on the software companies. Really the key to all of this comes down to the software companies and the consumer adoption. There is a push within the market, or in any market, where the consumers always want bigger, better, and best. This means they will always want faster operating systems, a lot more features and all of this other stuff. The problem is that the more you add, the more complex your code becomes.

We are in a system where we can’t just say that we aren’t supporting any of this stuff any longer and move on. So what happens is that we end up with all of this legacy code which is going to end up failing in new and unexpected ways since we can’t test for everything. Another problem is that software is developed for speed to market that is the prerogative. They want to get it out onto the market as fast as possible so they can sell it quicker, make more money and develop more software which causes a vicious cycle. The problem is that this process doesn’t rely too much on security. Security tends to be an afterthought within the operating systems or within the other software. It needs to be more out front and until it becomes more out front nothing is really going to happen about it.

The other thing that really needs to happen is that there needs to be more control over the internet itself. Not necessarily from a government standpoint, but there needs to be real serious
analytics and heuristics from the actual internet traffic itself. If somebody is doing something odd then it needs to be looked into. That is part of the problem with the internet carriers right now is that, going back to the 1996 Telecommunications Act as well as the DMCA, they look at they look at the incumbent carriers like Verizon or AT&T tend to have this attitude of being more hands off because they are afraid of losing their common carrier status. So, they don’t want to actually go in too far into a person’s content or whatever in order to monitor or protect their networks. They approach it in the same way that they approach their telephone service. We will connect anyone to anyone, what they do over that communication has nothing to do with us.

The problem is that with the internet a lot of this stuff can be prevented at the ISP level. We have had a problem with spam for decades and the ISP should know that if there is a home machine sending 5,000 e-mail messages an hour then it doesn’t take a rocket scientist to say that it isn’t right and we should probably do something about that such as rate limiting or something. They have the control and ability but they just don’t have the will to do it. That, in and of itself, would throw out a lot of cyber crime.

Since cyber crime is rising I think we need to further define what cyber crime is in light of modern society. Because if all of a sudden if the majority of people are committing crime then is it right to lock up the majority of the people or is it right to revise the laws that are being written or the societal values that result in that law. At that point we need to come to grips with that and think about what to change. Is it the law that needs to be changed or is it the behaviors. If we can not change the behaviors, then what is left? What can we control?

I think that ISP’s are really the front line. In a free and open economy ISP’s should be left to decide for themselves how to operate their business. However, at the same time though by the nature of how they provide a service, and not so much the reseller ISP’s, but rather the providers
of infrastructure who have been granted the limited monopolies such as the cable and telephone companies need to take more of a societal role because of what they have been given. I am not even looking at this from a copyright perspective for civil liability or anything like that. If people want to trade movies then that isn’t for me to say. Even with my job being what it is I don’t take a real firm stance on that because I really think that the market will work its way out by itself. In terms of other more criminal actions I think that there is a lot more that ISP’s can do to solve a lot of these problems in a non-invasive, but highly technical way.

*Imhof:* Do you believe that part of the increase in cyber crime rates can be attributed to the internet becoming a form of utility?

*Bartram:* Absolutely, I mean it is something that is so important to our modern society at this point. We have built it to be so important to us. At this point it would be almost like if we turned off the electric grid. If the power grid was gone then there would be a revolution in the streets. I am not really sure if the internet has gotten to that point yet, but it isn’t too far off. It is becoming ubiquitous and something that is everywhere, you can get it everywhere, and even in dial up it is one of those situations where somebody needs to take a role in it because the convoluted relationship between the federal and state governments, and even state governments themselves, makes for a big problem.

Never before in human history has one person had so much ability to fall under the jurisdiction of so many places at once. Even when you can just make a phone call you may fall under a state or federal law, maybe another country’s law or something. But, to have the level of interaction that occurs between all of these various jurisdictions, causes a serious problem. Because there is really nothing at this point that defines somebody as having clear authority.
Everyone says that they have clear authority but nobody is really practicing clear authority. It is one of those things where you may violate a federal hacking law, but a state may prosecute it because they don’t have a real good law on what was violated, but yet another state does. There is no uniform law to this.

What happened was that back in the 1930’s when all of a sudden communications and travel became closer together then the states got together and created the uniform commercial code. Basically this didn’t say “this is what it is”; it formed a model for how to conduct yourselves so that they were all on the same page. Basically what we need to do is re-evaluate the same thing, just with the internet. Everybody needs to get on the same page because when you go from jurisdiction to jurisdiction the laws are so wildly different. Then you end up with certain states that prosecute people more than in other states because their internet packet happened to run through in this particular instance. It is the Wild West and until we get a good grasp on that we will not be able to get a good grasp on cyber crime.

*Imhof: To what extent will most cyber criminals go to in order to be successful?*

*Bartram:* It depends on if you tickle their fancy or not. I have seen very lazy attackers to the point where they decided to launch an Internet Information Service, like an IIS server attack, against one of my Apache servers. We aren’t even talking about the same architecture here, they were running on two totally different operating systems and the hacker was just blindly doing that. They would sometimes hit a Sun box with a Linux exploit and we are talking about different things here. It just went down to the basic thought that they could care less about architecture. They would just fire out the exploit and eventually one of them was going to hit
something and get some kind of result from it. This would be the ultimate lazy attacker, that would pretty much be the slacker attacker.

As far as the dedicated attacker really getting in, I have done things that have really made an attacker angry where I have locked them out and they made attempts to get back in and it has gone back and forth like that. A lot of times that has happened, but this is more of a wounded pride thing. For the most part there are enough targets out there that they can attack. If you figure that every day more and more computers get added to the internet, why would they go after somebody difficult unless they really want to when there are so many other fish in the sea where they could just hit whoever.

Imhof: What sociological theories do you believe would apply to hackers the best?

Bartram: I would say that as a generality at this point with the way that the internet works that it is greed. Somebody wants to make money, whether they are making it and where they want to keep their money. They don’t want to buy something so they find a way to get it for free or they are trying to get somebody else’s money from them. It could be through a scam or just duping somebody into it like a con game. I think it really comes down to money and I think that is pretty much the biggest motivation. Somebody wants something, they have money and want more of it and this just happens to be the medium that they use.

Imhof: From a Law Enforcement viewpoint, what should IT Professionals know about cyber crime?

Bartram: I think on both sides, both from a law enforcement side as well as from a pure IT side, there is a definite disconnect. I have worked both sides of the fence and really what happens is
from an IT side there is a complacency that happens. You know, I have my firewall and active
directory set up right with strong passwords and whatever that I am set. I run anti-virus so I am
invulnerable; I am Superman of the network. I think really what happens is that they don’t quite
appreciate the sophistication of the modern attacker.

The rootkits and the disguise in the software that they are using to hide their tracks and
the vehicles they use to actually get into systems now are so sophisticated now that unless you
are doing some serious monitoring and analytics on the flow of your network with the actual
packets themselves then you will not even know it. You might be attacked and compromised and
you may not have any idea. It is something that really isn’t a failure with IT so much; I think it is
really a failure of law enforcement and government sources to really accurately identify these
threats. I think what it is, is having the right people articulate it the right way to other people.
Many times you have systems administrators in the corporate IT world hears the government
saying that they need to regulate more because they want more authority and visibility and they
are not saying why. They are not saying what is happening, what they are seeing, or the current
state of the research.

Both sides need to really communicate a lot better with each other because as a general
trend, most systems administrators that I have been in contact with during my time have had very
strong Libertarian leanings. They are distrustful of government intervention and authority or
anything like that. Whether that’s right or not is not for me to say, but it is one of those situations
where there is distrust on one side and secrecy on the other. That doesn’t work. We are in the
internet age and we need more communications. What also doesn’t help is that the government
tends to be years behind everybody else. The federal government is operating on ten year old
paradigms whereas the business community is moving however fast they need to in order to
compete, so they are two totally different things and the disconnect just continues to keep on growing.

*Imhof:* What should Information Technology and Information Security professionals know about cyber crimes concerning laws and regulations?

*Bartram:* I think that really everyone who deals with Information Technology, whether it is on the law enforcement or IT side, should have senior level positions at all levels require some type of certification. This would be similar to what the bar association does with lawyers. Something that proves competence but also proves a common bar bones level of information. One of the things I feel that is very important is understanding what law enforcement has to deal with in obtaining the information. They need to know what the fourth amendment is all about. Although it doesn’t apply on the private side, it is still something that is very important to understand. They need to know what the DCPA is and know the limits of it. They need to know the Privacy Protection Act.

They need to know The Computer Crimes Act and things like these that really tell from a practicing point what are the limits in terms of if there is a break in and first who do they call. From this point if you are managing a network, who do you call if you have a break in? My first instinct in 1999 was to call the FBI. Was the FBI appropriate? It could have been, they handle it. However, so does this office as well as all of these other offices. A bunch of local jurisdictions handle it. This goes back to the thing I was talking about with this whole mismatch over whose authority it is to handle it.

Really what it is that once law enforcement comes in, what steps can you take and what information can you provide given certain circumstances? Now if we subpoena somebody,
whether they are hostile or friendly, they are a witness to it and are defined by ECPA rules, PPA
rules, and things like that. When does a systems administrator cross that line between being a
systems administrator and watching their network and an agent of law enforcement? Where is
that line? I think this is something that both parties need to know between law enforcement and
the corporate IT staff. Also what would be helpful is know what is worth looking for. What are
they going to need to do? In the event of an attack and compromise, what are your first steps to
mitigate that loss?

How do you preserve the evidence that is there as the initial person that burst on the scene
as a first responder that is going to preserve the evidence in its state because they need to provide
it to law enforcement for their investigation. In homicide pretty much everybody knows that if
there is a dead body on the ground you don’t touch it. In IT it is different, somebody got into our
system so now what do we do? It is that disconnect in communications and both sides need to
work together. Also what to know from a third party is the civil aspect. In a criminal case it is
pretty clear cut, you can do XYZ but you can not do ABC. In a civil case what are you going to
do that opens you up to civil liability. In business and in personal it is a pretty big deal. If
somebody slaps a multi-million dollar lawsuit on you because you touched the wrong data you
will learn not to do that again.

I think that one of the things that has to happen is that it needs to be uniform. There needs
to be a common criteria for training among corporate IT or for somebody that carries the
moniker of an IT professional. It goes beyond vendor certifications and that type of technical and
practical type of thing. It goes more into what you need to know. If you are going to take up the
responsibilities of network engineer, systems administrator, systems engineer, or whatever it is
you need to know certain things. At that point whether you work in a corporate environment or
the government if you use the just following orders excuse it is an incomplete defense. It doesn’t work out; you can’t just say that the CTO, CIO, or CEO told me to because under the laws you can still be held responsible on both sides of that fence.

*Imhof: What do you believe is the best solution to educate users and organizations about the risks that they face?*

*Bartram:* I think that what really would need to happen is that you would need to stratify the business community not according to size, but according to their critical role within the infrastructure itself. You may have a small company that is a VOIP provider, is their data critical? How do you evaluate that? That is where you need to begin, you need to stratify them and determine who else is critical. At that point you can start prioritizing. For those that are the most critical you need to almost write a Sarbanes-Oxley type of law so that you can determine the audits that need to be performed because of this.

Because of your criticality to the infrastructure of the internet, the state, county, country, or whatever you need to perform these audits and you need to be up to spec on this. Someone needs to have general control. Whether you are looking at accounting, law, medicine, or anything that is of a critical nature in a critical industry or of a critical service there are standards bodies that basically define what the rules are that you operate under. There is GAAP in accounting, but there isn’t one for IT. There really isn’t a standards body that has any force to it. Everything within these organizations that define these standards rely on software developers and everyone else except for the end user. What you need is for someone to come along and say that you need to be certified to do this. You need to know what this is all about; you need someone to sign on a dotted line that they are liable for this if it fails.
When all of a sudden there was a problem in the financial sector and they instituted Sarbanes-Oxley they made the CEO and CFO sign the bottom of a financial statement indicating that it is accurate. Things changed, they were making sure that things were accurate. As soon as it came down that if it isn’t accurate they could go to jail it was able their attention at the right levels. I really think that the same thing needs to happen for companies that are a public or private organization on the IT side of things. At this point you will begin to see security improve.

_Imhof: Where do you see the future of cyber crimes heading towards?_

_Bartram:_ It will only increase. It is a big game, it is a back and forth between who gets the advantage. It will continue until something fundamental changes. Will it be anarchy? Probably not, there will always be some level of control to it. Will it be prison control? No, probably not. As long as there is ad-hoc wireless now that create networks you lose control of the overall infrastructure then you have just lost control of the network. There really isn’t anything stopping somebody from creating a new protocol and communicating on that protocol instead, whether it is wireless or over cables. The medium itself is just a method. It is going to be a constant back and forth. I don’t see anything happening any time soon that is going to put me out of a job.

_Imhof: What specific controls would be best for risk mitigation from these crimes?_

_Bartram:_ For individuals with their private computers at home, if we lived in a utopian society they would all be licensed before they were able to be hacked over the internet. In the real world there just needs to be more education about it. Unfortunately in our current state of technology and with the current way that things have shaped up, we are at a point where things are much more complex then just plugging into a wall and everything just works.
We are at a point where things still break quite a bit. With the internet you have a situation where there is a level of expertise that is required in our current usage but there is no failed consequence to doing it wrong. Therefore we have spyware, malware, and everything else that is under the sun. I think what will happen is that as we start putting everything into a simpler format for how to present, interact and move out data around the internet. We are starting to see this with smart phones, smaller notebook PC’s, iPod’s and devices that are specific purpose devices that are not all-in-one monolithic devices for doing everything. The personal computer is an example of this.

I think as the devices move to a more simple format the problem will eventually cure itself in some form because then you are exerting a level of control over what you are doing. You are not worrying so much about how it works; you are just interested that it works. I really think that this is when you will begin to see things change. When the average consumer doesn’t need to think so much about it because the average computer user is dangerous. They are going to do bad things and some of it will compromise their machines to make the internet worse, actually a lot of it will make the internet worse. As there is more of an aspect of control to it you are going to see only the best and brightest break out of those molds, then it is controllable.

From an organizational point of view, it really comes down to user education. Whether it is corporate or government you are already on a private network. You are at the mercy of the controls that your administrator implemented through policy. Really it comes down to education. A central theme in many of the security courses that I have taken is that you can implement all of these technical controls, but if you don’t educate users on the risk and why of what you’re doing and how to be secure then they wont be. They are going to do stupid things, things that will deliberately subvert you because it is the easier way to go.
Education is what really needs to happen. A side benefit of this is that if all of these users get security education they eventually need to go home and hopefully one or two things carry over. They may not access their computers from a smart card or a long key token or anything like that, but at the same time they may know not to click on something just because it is flashing. This might prevent one infection which may reduce the load of spam on the internet and that type of thing.

Michael McCartney – Senior Investigator
New York State Office of the Attorney General – Organized Crime Task Force

Imhof: Can you please tell me about your formal background?

McCartney: I went to Canisus College and graduated in 1990 with a bachelor’s degree in sociology and criminal justice. From there I began working in 1990 with the United States Attorney’s Office with the Western District of New York under the United States Department of Justice. I interned as a summer clerk then was offered in their asset forfeiture unit. The asset forfeiture laws allow the federal government to seize property, money, cars, boats, and houses from criminals then sell them to finance further law enforcement efforts.

I have an extensive financial investigations background trying to uncover hidden assets and locate and tie illegal activity into the proceeds of that illegal activity so that the government can take it legally. I did this work for about five years and after that I was offered a position at the New York Attorney General’s Office as a police officer to work in the Organized Crime Task Force in 1995. I was given an opportunity to attend the New York State Police Academy to become a certified New York State Police Officer and work here doing initially doing mostly
technical installation of wiretap equipment as well as bugs and tracking equipment in cars and homes. We have an entire technical unit that supports investigations by installing certain electronic surveillance equipment. I did this work for a long time, tapping phones and climbing telephone poles so that the police can listen to these phone calls from court ordered wiretaps.

In 1996 we fell into an investigation involving child pornography on the internet. Because I was technical and I knew my way around computers I was asked to assist and ultimately end up running one of the largest undercover child pornography investigations in the country from 1996 until around 2000. We ran operation Rip Cord which was an investigation into the trading and dissemination of online child pornography which was predominately of America Online. We had a number of undercover AOL accounts and we would log on and talk with other people who were suspected pedophiles and get them to send us pictures so we could investigate where they sent these pictures from and obtain probable cause to execute a search warrant at their house, seize their computer, arrest them and ultimate conduct a forensic investigation of their computer.

At the time there was no place to take a computer in 1995 or 1996. There was no lab where you can take a suspect computer and have them forensically examine it for evidence. The science didn’t exist or wasn’t mature enough and established in the crime labs like they are today. I was sent to a computer forensic school to learn how to do computer forensics. I was the first one from our agency to go and I came back to start the computer forensic unit for the New York State Attorney General’s Office. Now it is twenty-five people and four labs across the state level and I supervise this unit.

We also started the Regional Computer Forensic Lab where a number of Law Enforcement agencies can take the computers that they seize during the course of investigations
and submit them to the RCFL and they do not need to have the resources to purchase forensics equipment within their own department. It is expensive and time consuming, they need to stay proficient and be trained, certified, have equipment and all that stuff. It is a resource that is available for the Tonawanda Police Department, West Seneca Police Department, and other departments that couldn’t possibly afford to support a full time forensic endeavor.

Our agency does both of these things, we submit some evidence to the lab and we also have a number of people in the lab who work for me as a good gesture by our agency to support that lab. For some of our sensitive cases that we don’t want the RCFL to do, or if we need it completed quicker, we will conduct a forensic analysis in house.

*Imhof: What has been the extent of your experience with cyber criminals?*

*McCartney:* Pretty much all that I have done since 1995 is online computer crime. We have investigated cases in: child pornography exploitation investigations, online narcotics investigations, online stock fraud and financial fraud investigations, hackers breaking into systems, hackers stealing DirecTV signals by modifying the card that goes into the DirecTV satellite receivers, credit card fraud, and anything computer and high tech we do all of those investigations. Anything that is brick and mortar on the ground such as narcotics is handled by Pete and his unit. I do occasionally handle other non-technical cases, but these are typically handled by others in our department.
Imhof: How often do you handle cases involving hackers?

McCartney: Probably three or four a year. It isn’t to say that there aren’t more of these cases, but we get jurisdiction in a unique way. Most of the crime that occurs is typically investigated and prosecuted by a lower level judicial system. The police departments such as the Buffalo or Amherst Police investigate crimes and bring them to the Erie County District Attorney to prosecute.

Those crimes, regardless of the town, occurred in Erie County. Conversely, the Niagara Falls Department would investigate crimes that occur in their town and then bring the cases to the Niagara County District Attorney to prosecute. Where we get involved involves typically a bigger investigation which involves more than one county and it has to be something that affects generally the people in the State of New York as a whole rather then just one guy hacking into a single computer. We get involved at the State level with the State Attorney General. We get involved with cases that transgress multiple counties and multiple defendants.

Imhof: What common patterns have you found, in your experience, between cyber criminals?

McCartney: The most common thing is the way that they exploit systems to gain access. Sometimes it is the simplest way through such as a system that hasn’t disabled their guest account that allows them in through an open door. Then there is the more sophisticated attacker that attacks where they install key loggers and sniff traffic, break passwords, crack the encryption, or other things like this. They may install malware where they compromise the computer and open up a backdoor that gives them access.

Although there seems to be a common thread in a lot of these, their motivate is usually somehow related to their own self interest. In the last case we worked there was a guy that
worked for a company and was their IT guy that ended up getting fired. He left under very bad circumstances, but still held all of the keys to the castle. The company never disabled all of his accounts and he had knowledge of other user accounts. Because this individual was mad he went home and logged back into the system to destroy everything. In half of the cases there is some direct connection to somebody’s self interest and in the other half of the cases it is somebody who is hacking just because they can. It is like asking why somebody climbed Mount Everest, they will say because it was there. A hacker may hack a defense contractor because they want to see if they can. There really is no other connection other then just wanting to see if they can do it.

_Imhof: Many people believe that hackers are motivated solely by financial means, do you believe this to be true or are they motivated more by intrinsic means?_

_McCartney: It is certainly a contributing factor, but in most cases they do it because they want to see if they can and there is no monetary gain at all. I would say that even more than half and up to three quarters of the cases are driven by factors other then money in hacking cases. The fraud cases such as with credit card fraud are almost exclusively motivated by money. They are trying to get a credit card and get access to a credit card so that they can go buy things and get more money. In hacking cases, typically with the exception of the hackers that hack to gain access to credit card data to ultimately then have those credit cards to commit financial fraud, then hackers hack to destroy or gain access to systems don’t typically have a monetary motivation at all._

_Imhof: Why do you believe that the rate of cyber crimes is increasing so quickly?_

_McCartney: Availability, everybody is online. Every device that you buy and own now today is connected. Speeds have become quicker, access has become better and it is everywhere. Before
you used to have a dial up connection and it was slow and it wasn’t that great. Now with broadband, wireless and mobile computing it has a per capita ratio effect. It is opportunity, you are there and it is easy to be online. There are also a lot more ways to anatomized yourself online today.

There are companies, protocols, software, and other things that exist freely to make yourself almost completely anonymous on the internet and people take advantage of these services. Proxying and through computers that are untraceable as well as using encryption to conceal what you are transmitting all make the efforts of law enforcement retarded in the way of finding out who is actually responsible. Fortunately not everyone who commits these crimes uses sophisticated concealment protocols and software, and even those who do often times make mistakes and do not use it all the time.

It is cumbersome to always have to jump through a proxy to go and send e-mail or surf the web. As a result, sometimes they will say “I will just go quickly and check my e-mail” straight from their home or school. Often times with diligence we are able to find those mistakes among a batch of careful concealment activity. There are often one of two mistakes in there that will generally lead us to the suspect.

*Imhof:* What kinds of cyber crimes are increasing the fastest?

*McCartney:* Malware and financial fraud seems to be the big push right now and child pornography seems to be everywhere unfortunately. Child pornography and exploitation cases are always there and on the increase. The other crimes that are big are malware infestation for the purposes of concealing their identity so that they can go and commit financial fraud. Not so much rootkits, but more proxy-bot software applications that get installed on machines under the
radar from people and their malware and anti-virus detection software does not detect this software readily and it opens up their computer to be used by hackers.

This isn’t so much to get access to their computer, but to gain access to then use their connection and IP Address to then go somewhere else and do things which would cause their malicious activity to be traced back to the innocent user instead of them. Literally there are hundreds of millions of infected computers on the internet right now, home broadband computers and yours at home may be infected and you don’t even know it, and the hackers are using your Verizon DSL connection or your Time Warner cable connection. That is all, they are not reading your e-mail or trying to steal your TurboTax file. They are just simply using your connection to then go out and attack somebody, try to steal credit card information, or to do other things.

This is a major problem to the point where almost every time that we start an investigation the first jump back to the perpetrator is always to some innocent but infected computer. The reason that they are using them so frequently is because the person whose machine they are jumping through isn’t logging anything, it is just a home broadband Windows machine with no system monitoring or logging enabled. As a result, there is no way to find out who connected to them on the day and time that they went out and committed the crime, so it is very problematic.

Imhof: So then hackers generally use their malware for multi-purposes?

McCartney: That is exactly right, they may setup a botnet to conduct a denial of service attack against a competing organization by setting up a distributed network and sending SYN, SYN-ACK packets to a server or e-commerce website that would shut them down and all of the traffic is coming from everywhere. It is coming from all of the infected machines and not from them.
Imhof: What do you believe can be done to mitigate the rising crime rate?

McCartney: Better education and awareness for users that go out and purchase a machine but don’t subscribe to the anti-virus and network monitoring software. Basically after their sixty day trial which comes pre-installed on their machine they let it expire and don’t do anything. Explaining to them the importance of having a computer that is constantly updated and patched while running good anti-virus and anti-malware software to then prevent or minimize the effectiveness of these malware deployments of code that infects these machines and then allows for this large infrastructure of proxies. It is almost always the home user who either doesn’t have any anti-virus software running or running out of date definitions from an expired malware detection system.

Imhof: To what extent will most cyber criminals go to in order to be successful?

McCartney: It depends, some are motivated by the reputation of being successful and gaining access to certain systems. There are entire organizations of hackers that pride themselves on the ability to exploit other systems so it is almost like a notch in their belt or feather in their cap to have rooted a system. It is bragging rights so the motivation is reputation. The other motivation for a lot of them is financial.

There are huge infrastructures of financial fraud crime rings that operate on the internet where there are certain silos of criminal activity that make up a criminal bizarre. The hackers will go out and try to gain access to credit card data. They will hack into TJMaxx and compromise their credit card system and get all of their customer credit card information. Then there is the guys that sell the credit card validation system where before they can sell of use the information they need to check them to make sure that they are good. How do you check a credit card that
isn’t attached to a card? There are websites out there that are run by hackers which are run through proxy servers and are hard to find. These websites allow you to punch in your credit card number and they will actually tie into the legitimate credit card processing authentication system for Visa or MasterCard. Visa or MasterCard would then kick that back as if they were a legitimate merchant who needed pre-authorization on a sale like Hertz Rent-a-car. They check the cards and see if they have been reported lost, stolen, or compromised and get a pre-authorization code back indicating if the card is good.

Then there are the people who actually make the plastic. There is now a whole organization of people who now if you sell or give them for a fee credit card data they will then emboss it on a magnetic stripe, take the card and put whatever names and numbers you want on the front of it, and give you an actual piece of plastic with the stolen data on the magnetic stripe. Then there is another group of people who then take those cards, who are called money mules, who are hired by the people who bought and made the cards to actually go out to Wal-Mart or Home Depot with a stack of credit cards to actually buy stuff.

Then there is another group of people that take the stolen merchandise and sell it on eBay or ship it overseas to be sold for fees or things like that. So, there is almost like six distinct structures in which the crimes occur. Each section or faction of the criminal bizarre has a role but they all support the overall criminal enterprise. It is in many ways similar to traditional organized crime, you will have the Capo’s, soldiers, and everyone is running their own racket and doing their own thing.
Imhof: Do you see hacking going more towards organized crime and away from the individual hacker?

McCartney: I have seen a bigger move towards the organized crime structure. There is definitely a big shift towards the strength in the masses approach as opposed to the individual hacker doing his own thing for his own goods. A lot of the stuff that we are seeing with the form of the actual malware code that gets deployed is mostly Russian organized crime, Russian based. Programmers, Engineers and Hackers in Russia actually write most of the code that ends up infecting computers that makes them open up and become proxies.

They also use a lot of European, Romanian, and Eastern European influence to run a lot of money through off shore bank accounts once those money mules end up with a product. There is a very large European influence in a lot of what is going on. The biggest fear from a law enforcement perspective, especially at the state level, or even at the federal level which I am a member of the FBI task force is to question if any of these attacks are government sanctioned. Think about what a foreign nation, especially an enemy foreign nation, could do with 300,000 infected computers on the internet with broadband access. They could point it at our electrical grid and our water systems which are essentially run by computers and do certain things to our critical infrastructure that would not be very good.

Imhof: What role do you believe that Internet Service Providers serve in curtailing cyber crimes?

McCartney: Unfortunately they do not play a big enough role. They’re more concerned with their profit and running the business then they are concerned with security; let’s just say that security costs money. Any type of security, whether it is physical, computer, or network security
is expensive and they don’t for whatever reason want to spend too much money on those endeavors. While the technology exists to deploy detection systems to cut down on the number of computers that are being infected on their network they are not using it.

So, if I am Time Warner I could effectively through pattern and bandwidth analysis see that a normal user’s bandwidth usage is X then all of a sudden it is 5X then chances are that they are infected and criminals are using them to proxy through. Instead of taking a proactive approach to contacting a user or pushing out a virus detection system to a computer because they are chewing up the company bandwidth they just let it be. They do not do anything proactive to try and vet out the infected machines that are on their network. If Time Warner, Verizon, Cablevision, and Comcast were proactive in looking and trying to thwart some of this stuff then the hackers wouldn’t be as successful in infecting all of these machines and creating very large botnets.

*Imhof:* What sociological theories do you believe would apply to hackers the best?

*McCartney:* No theories really come to mind, they really cross all demographics really. They can be college professors that have a tremendous skill set down to the low socioeconomic people in Romania that have a low skill set and may be poor. So there really is no single demographic that is consistent in my experience with hackers. When it comes to child pornographers they are typically white males between the ages of 30 and 55, so it is an easier demographic to identify. They are typically not female but we have had a couple and they are typically not African American or other minorities.

However as I have said, hackers cross all demographics. Some are self taught and some are very educated, some are rich and others poor, some are professionals and others are laborers.
This is from my experience and because I operate at a certain level I am not seeing every hacker case, rather it is only the cases that we have an interest in but it is really all over the place.

Imhof: From a Law Enforcement viewpoint, what should IT Professionals know about cyber crime?

McCartney: The first thing that they should know is that they should be as fluent and as up to date as possible in information security. How to use protocols, systems patching, and system monitoring which are some of things we try to teach at a very entry level. To continue on in the information security arena and to be able to successfully guard whatever system they have been entrusted to guard then they need to be as good as they can be in all of the different exploits and other things that are happening out there.

Once they see or identify what has occurred on their networks then the first thing is to contact law enforcement if that is the policy that they have. The problem is that some corporations do not like to include law enforcement for a number of reasons. If they are a publicly traded company then they have shareholders to answer to then they will typically not reach out to law enforcement even if it is potentially the biggest law enforcement case in the world because they do not want to look to their shareholders like they can’t secure their data or their information so they would rather handle it in house.

This becomes problematic because if they don’t have the proper forensic skill sets or if they aren’t handling the data with the proper chain of custody thoughts and issues in mind then they run the risk of later when they do get to the point of involving law enforcement of having possibly contaminating the data in question. We see this a lot, we will see a referral to us some time after the incident only to find out that we can’t offer too much help because they have
stepped all over the data in their attempts to try and figure out what was going on. They didn’t think about the fact that by accessing the data they are changing data such as access, modified, and creation dates so it becomes harder for us to find out who committed the crime since important information is now missed.

*Imhof: What should Information Technology and Information Security professionals know about cyber crimes concerning laws and regulations?*

*McCartney: Well, there are many and in any corporate structure there are going to be lots of moving parts to this because you are typically going to have general counsel who works for the firm or company. You are also going to have senior management and compliance people who need to comply with certain regulatory oversight. There is a whole umbrella of regulatory requirements that companies need to follow and comply with in order to run their day to day business.

One that comes to mind is that if they are handling credit card transactions then they have to handle it in a certain way. It needs to be encrypted on their systems; they just can’t keep the CVV2 and credit card numbers in the same database. They need to be separate so if somebody hacks into a single database they do not have everything. They are not even supposed to keep the CVV2 number after the transaction has been processed, the authorization code has been received, and the transaction has been completed. They are supposed to discard it and not keep it at all. If an organization does suffer a breach and somebody does gain access to their system and accesses that stuff, then there are notification requirements and they can be fined and otherwise penalized for not notifying the right agencies, card holders, or other people that they are supposed to notify in a timely manner.
To lay out a litany of the laws that they need to know could take an entire weekend, but it is suffice to say that there are a lot of things that the corporation will probably bestow upon the information technology people and that is going to be their biggest headache is that they just want to keep the systems up and available. During this time they will be receiving pressure from legal and compliance people saying that they need to do things a certain way because there may be requirements that need to be met down the road.

Inhof: What do you believe is the best solution to educate users and organizations about the risks that they face?

McCartney: Who is doing it? Law Enforcement or Schools? There are a number of outreach programs that go on everyday and everybody is motivated by different reasons to participate. At the end of the day there could be public service announcements that are conducted by the governments at the city, county, state, and federal levels. Information could be disseminated to users by their internet service providers and provide PSA’s or other outreach educational opportunities.

We in Law Enforcement do it all the time and we are occasionally asked to conduct a parent-teacher outreach presentation in various different educational institutions. We go out and do this internet safety thing to talk about a lot of these things with the parents, teachers, and everybody else. There is just a whole magnitude of different ways to push this information out. Radio and television stations could broadcast more news stories on the threats and risks of not securing your home computer and those types of things. How do you prevent identity theft? Well, one of the ways is to make sure that your computer is secure. They could do more stories and news spots on these types of issues.
Imhof: Where do you see the future of cyber crimes heading towards?

McCartney: It is the end of the world, there is no slowdown in sight. As technology increases, the ability to encrypt and anonymize who and where you are, bandwidth increases, and mobile computing increases it will continue on its path. Everywhere you look around you see a coffee shop, airport, hotel and everywhere you go now has a hot spot and you can get online. I am online right now, this phone I have is online all the time.

These are also no long just phones, they are computers. So, as you saturate the amount of people that are on this communication facility then you increase risk of victims and increase risk of perpetrators exponentially just be sheer ratio of numbers. There is no end in sight, if you ever wanted to pick a career to get involved in it would be information security on the defensive side or law enforcement investigations of high tech crimes on the offensive side.

Imhof: What specific controls would be best for risk mitigation from these crimes?

McCartney: From an organizational viewpoint it is good information security policy. It is all about making sure that your systems are all updated, patched, and hardened. Make sure that you are aware of all the vulnerabilities and threats that your system may be susceptible to. Make sure that you’re conducting vulnerability assessments on a regular basis and actually doing log review on a regular basis. The organization must also act on the results of the security audits. A lot of people say that they will perform an audit, however nobody really does anything with it. From a corporate perspective it is just traditional and thorough information security policy.

For the individual it is hard because you can purchase a laptop for $300, a desktop for $500 and network them all in your house. When I first started this career in 1995 we would go into a house and find one computer. Today when we go into a house on a search warrant we will
find four or five computers. The entire house is networked; there is wireless access point, a
computer in the office, a computer in all of the bedrooms, the family room, a laptop out in the
car, and that is just the way it is now. They are building houses now with CAT 5 connectivity in
the walls. There is a phone jack, power outlet, and a CAT 5 connection.

James Domres – Assistant Chief Investigator
New York State Office of the Attorney General – Organized Crime Task Force

Imhof: Could you please explain your formal background?

Domres: I went to Canisius College where I earned my Accounting degree where my thought at
the time was to become an accountant. As I was working in Accounting as an intern I realized
that it wasn’t what I wanted to do. I saw an opportunity to join the FBI as an accountant. I
graduated then moved to Washington, D.C. to take a job with the FBI doing any kind of paper
work. Within a couple months all of the accountants that were doing that kind of stuff moved
into other jobs. They moved me into the Inspections Staff and was responsible for auditing field
offices and operations. I would travel and audit operations such as time and attendance, petty
cash funds, as well as undercover operations.

From my time there my plan was to become a special agent. However, because of a hiring
freeze that came on I sought an opportunity and got a job in the New Jersey Division of Criminal
Justice which is the investigative branch of their Attorney General’s Office. I worked in the
Medicaid Fraud unit there. I also investigated nursing home fraud and those types of things, but I
would also move on to environmental fraud and any type of white collar crimes. I did that for
two years then there was an opening with the New York State Organized Crime Task Force
which was then an independent agency in the state of New York.
The Rackets Study found that people from different disciplines made a very strong investigative team. We would have an attorney, someone with a police background, someone with an analytical background, then somebody with an accounting background. The three non-attorneys were investigators, but they came from different disciplines. The idea was then to identify organized crime problems in the area you were assigned and investigate them with all the tools available. While I was there they also created the Enterprise Corruption Statute.

We investigated crimes from misuse of funds on the transit here in Buffalo, misuse of funds for off track betting, kickbacks for renovations, and things like that. Finally we moved into investigating a large scale Cocaine distribution ring. We started with an undercover investigation in Ellicottville, New York and on the ski slopes. I was fortunate enough to be the undercover investigator and for six months they paid me to ski, party, and buy drugs. From our wiretaps we found it to be involved with a mob controlled Cocaine distribution ring located here in Buffalo. We ended up arresting and convicting an associate member of the local mob, plus sixteen or seventeen other people. We seized $1.3 million in cash. From that it spun into an investigation into another ring that moved in to take their place. Once the cocaine distribution job is created and taken out there is a void created and somebody else jumps in to take it over. This new group was importing right from Columbia and bringing in 400 kilograms at a time into New York. We investigated that and it took years. We then investigated other organized crime cases with some in Niagara Falls.

There was a point, probably around 1993, where because of budget restrictions they decided to close the Buffalo office. There were going to work everything out of Albany and White Plains. A lot of the staff went to other places but I stayed and was eventually transferred to Albany. The cloned cell phones were becoming a major problem for Law Enforcement.
Criminals were using cloned cell phones which allowed them to take a number in use, put it into a phone, and have both individuals use the same number. Basically they could commit crimes using another person’s cell phone without actually having physical possession of it. They would both operate with the way the network was designed. It was a huge problem.

What we were seeing was that the Colombians in New York would import the drugs and deal only with the Dominicans. They did this because most of the time the Dominicans were illegal aliens. They were already complicit just by being here. The Dominicans were ruthless and could live in all types of conditions. The distribution network for the Cocaine would involve the cloned phones and coming up the thruway to make their deliveries. So, another guy and I developed technology and a concept where instead of trying to follow the person we would track the actual telephone technology. If you get a new cell phone you will still call the same people. So, we began to analyze telephone traffic by who was called as opposed to who was calling, which was the traditional way.

We then became involved with the National Center for Drug Control Policy. They had some grant money and programmers. We worked with the programmers to develop a program to analyze this telephone traffic. We then went to the telephone companies to help them with their cloned phone problems by putting this technology on their switch. This program would gather all traffic, look at any two numbers that were calling five or more of the other same numbers then put off into a pool which would then be sent into our analytical program and spun around to try and group cell phones. We could actually analyze the cell phone traffic real time. It got to the point where it was good enough to see them coming down the thruway.

So for example the Dominican in New York may get his cloned cell phone and begin calling the people that he is going to supply. We named the program Gladis after Gladys Kravitz
in Bewitched who was the nosy neighbor. They then sent us to this international symposium and they featured this program. Now the big question was what does it mean? We couldn’t tell them that so I think we came up with the Global Law Enforcement Analytical Drug Investigations Service so we came up with a name for it. In the mean time this is when they closed the office. A lot of people ended up moving to the Syracuse Police Department or the Onondaga District Attorney’s Office and set up in a location at the center of the state.

We ended up setting up at a barn next to the Onondaga reservoir. In Law Enforcement in those days any time that you worked a wiretap you had to get what you could for free. So, the county had this barn that was there and it even had dirt floors, so we called the place DIRT. Well, once again what does it stand for? The first thought was Dominican Interdiction Response Team but that doesn’t work because you can’t single out a certain group. We ended up calling it the Drug Interdiction Response Team. If you go there today, 18 years later, it is still there. There is an actual organization that handles drug trafficking coming up from the city. We put Gladis in that location and worked on it from there.

At that point Dennis Vacco was elected Attorney General and with a new Governor they changed the structure of the Attorney General’s Office. The director of the Organized Crime Task Force was appointed by Mario Cuomo and Robert Abrams, both Democrats. It is a joint appointment so the only way it could change is if the party changes. When Vacco and Pataki are elected we have two Republicans and he brings the Organized Crime Task Force under the Attorney General’s Office. So at that point I moved into this Office and I believe that was in 1995.

Based upon DIRT information I began a wiretap in North Buffalo and it was successful. We actually ran drug cases out of there as OCTF, but this time as part of the Attorney General’s
Office. A new administration came in, different people were hired, and they decided that in addition to drugs we would look into the problem of pedophilia on the internet. So, Mike McCartney begins working on that and all of a sudden he is the guy. I wrote all of the search warrants and wiretap stuff.

When the office closed we didn’t have any Attorney’s so I had to write it all. They then saw that I had computer experience with Gladis and had the aptitude. I had written the search warrants so they asked if I would help out with the child porn stuff. So, this was sort of my introduction to computer crimes. We would get referrals from AOL and in the early days there were reluctant to give it to us but we forced their hand and said that they were in possession of child porn. AOL would then provide us leads and we would then go out and execute search warrants, sometimes many at a time. We would go out to an area and execute search warrants as a group and make arrests. What we found was that we had a bunch of computers and nobody to do the analysis. First year Mike McCartney went to IACIS (International Association of Computer Investigative Specialists) and the second year I went. We became certified into doing computer forensics so we could actually do something. We had a few guys here who were certified, but nobody else locally could do it. The FBI took care of themselves and didn’t really care about anybody else.

We started doing that and all of a sudden everybody else is calling us to do a computer forensics examination. At this point we determined that we really need some sort of a lab to do this because you can’t do both. You can’t go out and do the investigations then come back and do the analysis. In a perfect world you could, but the reality is that you are either investigating or analyzing. You are doing half of each instead of being great at one. So, this is when we got together with Marty Littlefield and created the Forensics Lab. The Attorney General’s part of the
first lab was funding. There was a grant that came out that would give you three times whatever you found to fund the lab. Well, we came up with $19,000 and it gave us an actual budget. The only budget we needed was for expendable supplies. Customs provided the space and a number of agencies provided workers as part of the lab.

The FBI sees this as a wonderful thing. They get the Regional Computer Forensics Lab and eventually fund the thing. At that point I petitioned that we should have somebody there. This is how I ran into the computer age. Aptitude and the real computer expert is the person in the room who knows how to move the mouse better then the other guy, so I was that guy. When I sat down and mapped out my career I didn’t exactly see this path. However, when I began accounting I knew that I wanted something different. In Law Enforcement the opportunity is there for a variety of jobs and I haven’t been doing the same job forever. I didn’t put on the uniform and drive patrol for my 33 years. I have done a wide variety of different things. I have worked with a variety of different task forces such as the labor task force, drug task force, anti-terrorism task force and I was involved with the Lackawanna Six investigation. There have been a lot of big cases that I have been able to work on.

*Imhof:* What common patterns have you found among cyber criminals?

*Domres:* If you look at pedophiles and hackers they live in two totally different worlds. From what I have found Pedophiles really want to tell you that they did something wrong. They want to confess because it is like a cleansing of their soul. There have been times where I have actually had to throw the Jesus card, tell them about God and get down and pray for forgiveness in order to get them to the next level. I like to say that I think it would help, but my goal was to
get them into the system so that John Q Public knows where they are. You don’t want them to move next door.

On the other side, the major hackers who have done the original phishing schemes want to tell you because they’re proud of what they did. Both sets sort of want to let you know. One because it is bragging and a kind of macho thing and the other because they want to bear their soul. The other common pattern in 99% of these people is that they have been white males. We have had very few cases to the contrary.

There are also organizational tendencies in many of the cases. In most cases people do not go out on their own, there is some interaction with other people. They need to learn from somebody so they join a board or a group like the Shadow Crew which is an American based credit card and identity theft group. It was a forum for different types of fraud. You could learn about different things and they actually had a ranking within the group. All of these people are underground now because they realized that if you do stuff on a website then anybody can read it. There is still an organizational aspect and people commit crimes for financial gain or pleasure. Avoid pain and obtain pleasure and the financial gain creates pleasure. Even with the pedophiles we had a case with Pedophile University where they would trade among themselves and talk about it. There is certainly an inner-working. Not necessarily the Godfather hierarchy of the old days but there certainly is organized crime there. For pedophilia the pleasure is within the confines and for financial gain it is a little broader.
Imhof: Many people believe that hackers are motivated solely by financial means, do you believe this to be true or are they motivated more by intrinsic means?

Domres: No, for some it is the old thing of letting others know that you were there. Some criminals take pleasure in doing that. IRC Channels have traffic full of people bragging about what they accomplished.

Imhof: Why do you believe that cyber crimes are increasing at such a rapid pace?

Domres: I believe a lot of it is from the availability of the internet and the availability to remain anonymous. In the old days if you wanted to be a pedophile and I keep going back to this because it is the basic cyber crime, and you wanted to look at pictures of little kids you had to go to the adult store and talk them into giving you the magazine that was under the counter. All that stuff is available online now and back then you didn’t have the ability to remain anonymous. When you turn a computer on and you are in your room all by yourself you have the ability to trade all by yourself. You can commit a crime without ever leaving the house. To go down the road and rob a bank it takes much more guts then doing it online.

Think about how much money you can make on the internet. We have arrested people who were running illegal pharmaceutical sales on the internet and making hundreds of thousands, or millions, of dollars. If you are going to rob a bank, first of all you need to get away and there are cameras. Second of all how much money are you really going to get? If you get $5,000 then you stole a lot. The other side you see is that the pharmaceutical sales guys that we went after with this large scale internet pharmacy case only got probation. The judges in local courts see rape, murder, and robbery then see a guy selling pills on the internet and don’t really care. They may say don’t do it again and get out of here. He may be making millions of dollars
and those pills could be responsible for overdose deaths, but how do we find out? How do you know? You can’t go to the 600,000 customers they have and ask them if anybody in their house has overdosed. How do you prove he bought it on the internet, and if so how do you know if it was from the guy you just arrested? How do you prove that?

A problem too has been that the laws themselves were created in the day when the guys in wigs robbed a chicken from the guy next door. The laws are not antiquated and they are not cyber laws. It took time to get at least some of this stuff in. The Computer Trespass law is an example. If it isn’t posted that individuals should not trespass then it isn’t trespassing. The took the computer trespass law and said as long as it is posted that you can’t go on that computer then the statute would apply. Where do you post it? If there is a sign next to my computer does that count? They have since changed that, but you used to have to give notification that you can’t trespass on your computer. Who does that?

*Imhof: What do you believe can be done to mitigate the rising crime rate?*

*Domres:* The best thing to do would be to eliminate the internet, but I am kidding of course. It is a resource and jurisdiction thing really. I think you really need to rework the entire framework of how the criminal justice system is set up. It is a far fetched idea but if you look at American law enforcement at all levels there are a lot of agencies that do the same thing. If you have a hacking case the question arises of where the jurisdiction lies and every agency is working towards a better press release because it gets you better funding and whatever is needed. I hate to say Big Brother but it is almost like there needs to be one agency that would be responsible for cyber crime. It would be really controversial but really there are too many cooks in the pot. Fortunately
with the world of cyber crime it is a target rich environment. There is stuff there all over the place.

There are jurisdictional problems all the time. It is really strange because the FBI is set up like there are sixty two different FBI’s in New York State. They work based upon districts so Buffalo FBI is responsible for seventeen counties. New York Attorney General’s Office has sixty two counties so my jurisdiction is actually more then theirs. If something occurs in Onondaga County then the Buffalo FBI won’t be involved in it and they would need to sell their case to the Albany FBI who may take a look at it. It is almost dysfunctional how the whole thing is set up. We are pretty good about collaborating among cyber criminals but a lot of that is through organizations like HTCIA, IACIS, and different boards that we are in. However we have had issues in the past. In the drug case we did have some issues because the DEA had something similar that crossed over at some point at they were closed lipped about what they were doing. We ended up doing a search warrant and taking a server in Rochester that they were working on. This occurs in most types of crimes, the coordination is critical.

*Imhof:* What do you believe individuals can do to mitigate damage done to themselves and/or their organization?

*Domres:* Security is key so know your network, patch your systems, and just adhere to best practices. They need to stay on top of it. The other thing they need to do, and corporate America doesn’t do this enough, is report. If you have a system at a major corporation and you have a leak or hacked then many times they will keep it quiet because they don’t want it to affect stock prices. That doesn’t help the investigators or the company next door who may end up suffering the same problem.
If there was a mandatory reporting of all these breaches then things would be better. If you lived in a neighborhood and you see somebody break into your neighbors house then you are alert. If you see him walking down the street and you don’t tell anybody then can the police enforce anything? No, there needs to be some way that they be corporate citizens and let law enforcement know by reporting it. There are some reporting standards that people are required to do. Identity Theft things, if you are a corporation and you lose a persons identity of some sort by a hacker or whatever then you are required to report it to the state. This is the case in many states, so at least identity wise we are protecting the consumer. For other things a lot of that just goes under the table and nobody ever knows.

_Imhof:_ Do you think that mandatory reporting for all cyber crimes would overwhelm Law Enforcement?

_Domres:_ It clearly would overwhelm Law Enforcement, however Law Enforcement is reactive. We would need to find a way just like back with the cell phone thing where we could analyze that information. We would then use that to go after the bigger fish. We can always catch the criminals on the low end, but with the big guys if we had some sort of mandatory reporting and an analytical interface of that then yes it should work. Even the best of criminals end up making mistakes.

_Imhof:_ To what extent will most cyber criminals go to be successful?

_Domres:_ Most will go very far to get what they want. As for a percentage I don’t think I could put a number on it, but for the cases we have worked I have had a few that we just couldn’t get with the information that we had. A lot of it is how far do we run everything into the ground and
how long do we go, like that thing we worked here and you can’t talk about. You cover every
lead and every option then keep on going. If they are good with the information we get then they
could be gone forever.

*Imhof:* What role do you believe ISP’s serve in curtailing cyber crime?

*Domres:* I think as far as child pornography goes they could do content filtering and shut down
the trading of child porn online. Record retention is huge, especially chat retention. They are the
information holders so if they kept more logs, connectivity logs, and database chat sessions then
it would go a long way to help Law Enforcement.

*Imhof:* What should IT Professionals know about cyber crimes?

*Domres:* I think the biggest thing is that they need to go out and join organizations and attend
meetings where there are Law Enforcement professionals. I think there is a big distrust between
the two sides. IT professionals are typically concerned with their particular systems while Law
Enforcement needs to look at the big picture and I think some type of coordination between the
two sides would be huge.

As far as laws go there really isn’t anything that jumps out at me. They should know their
systems and enable logging with good log retention as a basic measure. If you do get hacked the
biggest thing is the information you can give about what has happened. Anything they know
about the law can help, but laws change. I think that is why there needs to be some type of
integration between cyber investigators and IT professionals. Some sort of organization where
they can sit and discuss issues with each other.
The other thing it would create is that if one side had an issue and needed the help of the other then connections have been made. This is really like community policing, if we could get out to the IT people then there would be better trust among the two sides.

*Imhof: What would be the best solution to educate users and organizations about the risks they face?*

*Domres:* I would say that it could be handled at the ISP level. If Verizon required it on their wireless access points, such as making encryption standard and only making it work on their access points, then they can institute security. If they forced it then I think everybody’s home systems would be secured. Are there still ways to hack it? Of course, and it still would be expensive which is why it will never happen unless government mandates it. There will be open wireless access points forever or at least in my lifetime.

*Imhof: Where do you see the future of cyber crimes heading towards?*

*Domres:* I think it is pretty wide open now. Hopefully it doesn’t become over regulated because the internet is a great place and we all use it, but there is a lot of junk on it too. I think that generations to come will become less vulnerable then the current generation because many people my age just don’t get it because they didn’t grow up with it. I think that we are making great strides to curtail it. It will always be there and it isn’t going to go away but I think we can find better ways to investigate it and handle some of the issues. If we can deal with the encryption problems that are occurring then we will be okay. With that being said the vulnerabilities of the infrastructure are huge.
The cyber crimes are already an organized function. You will see Russian Organized Crime anywhere that there is money to be made. I think that National Security is the key. When somebody finally figures out how to take down a country then that is going to be a widely used warfare strategy. The ability is there and it is just a matter of time, the biggest thing is national security. The other stuff is monetary and law enforcement is reactive, we will solve it a little at a time. We need to keep the traffic lights up, the power on and the water flowing.

**Martin Littlefield** – Acting First Assistant United States Attorney
*United States Attorney’s Office – Western District of New York*

*Imhof: Can you please tell me about your formal background?*

*Littlefield: I have been an Assistant United States Attorney for twenty seven years and I have been doing work related to computers both in the practical sense and in the course of criminal investigations for the last ten to fifteen years.*

*Imhof: What has been the extent of your experience with cyber criminals?*

*Littlefield: We are in a different position in the Western District of New York then if we were in Silicon Valley or if we were working out of a major area where there is more hacking or headquarters for business that would be targets for hackers. I think I can speak for offices like this size in a region like ours in that the majority of the cases that we see will involve the transmission and sale of child pornography. For hacking we get reports of hacking with people playing a prank or a disgruntled employee rather then a major assault on an organization. Again,
in this district we don’t see many cases with a major assault on a financial institution or many cases of that nature.

*Imhof:* What common patterns have you found, in your experience, between cyber criminals?

*Littlefield:* Again, distinguishing between different types of crimes is not the same. I would say that after child pornography the other major type of cyber crime that we see is fraud related cyber activity meaning people posting things on EBay or other areas where transactions occur to sell products or scams of that nature where the Internet is used as a vehicle to commit it. So the patterns you would see involving child pornography would involve the adolescent group who are curious and the predator group who are attempting to snare children or very young adults.

In the fraud area you see a pattern which could be a phishing scam designed to lure people in and get their credit card numbers and other financial information on a mass scale. To go to hacking again the pattern we see predominately in a district like ours is an emphasis on the cases we may prosecute is on a less serious offense. What we see a lot in the area of hacking involves foreign sources, places like in Eastern Europe, Russia, Africa where within those regions there is an inability to get all the way back. Not that the foreign countries are not cooperating, it’s just the nature of working through geographical limitations where as you know that the internet has no geographical limitations. It is changing and the geographical and political respect that we need to show other nations it can be very difficult to work in cooperation to gather evidence and identify somebody in a foreign country.
Imhof: Is it much more difficult to extradite people for these types of crimes?

Littlefield: No, I don’t think there is any more difficulty. We have treaties with foreign nations that define the crimes with which people can be extradited. As long as one of those crimes have been violated there is still a level of proof that must be satisfied for a foreign government that we have actual evidence of the crime and that the person in their country is responsible for, or a good reason to believe, that they were involved.

The two real criteria is: one, is it a crime defined in the treaty between the United States and that government and if there is an agreement to extradite the suspect for that type of crime, Fraud is generally one of those crimes. Two, do we have sufficient evidence to satisfy that country that they should take their citizen and jail them to have them brought to the United States.

Imhof: We have seen that the internet makes commerce easier, do you believe that it also makes crimes easier to commit?

Littlefield: Absolutely, and many crimes are committed because the internet speeds everything up. When this happens you have more people with access to each other. The increase in commerce and the rise in defrauding commerce run parallel.

Imhof: Many people believe that hackers are motivated solely by financial means, do you believe this to be true or are they motivated more by intrinsic means?

Littlefield: That is really two questions. If you are talking about people who are trying to steal things such as credit cards and things like that I would say that their primary motivation is financial. If you are talking about hacking it could be to embarrass the organization, show off or
whatever. The motivation could be simply “I am the baddest guy in the West”, I am the best at this and showing off. This is common among a lot of kids who show off for their friends. Other times the conduct is malicious to shut down the financial institution and to cause that kind of problem it is another type of crime. In this case it could be a foreign government, an individual angry with a particular company, mad about capitalism or somebody trying to put themselves in a better position then others. I would caution to speak about motives, plus in this district we don’t run into that type of conduct too often on a large scale.

Imhof: From your experience, what type of backgrounds do these criminals typically have?

Littlefield: In general I would say that the demographics are much more inclined to be younger then older. However, we have seen people in their 30’s and 40’s with credit card fraud using the internet to trade and obtain financial information to commit fraud. I would say that younger people are more adapt at this simply from the nature of growing up with it, but there are a fair number of people in their 30’s and 40’s that we see undertaking fraud scheme using the internet.

Imhof: Why do you believe that the rate of cyber crimes are rising at such a rapid pace?

Littlefield: It depends on what you define as a cyber crime. If it is traditional fraud and the internet is being used then there really isn’t an increase it is just another means. Instead of using the mails and the telephone they are using the internet. So, if that is now included in the definition of a cyber crime then all you have done is moved it over. If there has been an increase in the occurrences of fraud then it could be because of the pace at which we are working at.
You can reach people quicker, there is more commerce going over the internet and as a result there are more opportunities for individuals to commit crimes. I think the better aspect is that when you saw fraud it used to be all over the mails and telephones including telemarketing and now it’s all over the computer using internet communications. With hacking there are more places to attack and more people to cheat with a means to commit the act over the internet. The increase is likely due to the explosion in usage of telecommunications over the last fifteen or twenty years.

Imhof: From your experience, what kinds of crimes have been increasing the fastest?

Littlefield: The most common has been child pornography. There has been an explosion in the transmission of child porn and the exploitation of children using the internet. This is the crime that has been increasing the most. But there has also been increasing in hacking going on. Some of it is just kids playing around and trying to show how good they are, it is like they are on a playground with one kid trying to kick the ball further then the other one. It is wrongful conduct but it isn’t necessarily of the same ilk as somebody who is trying to shut down an entire business for some malicious purpose.

It is still just as criminal because the statute doesn’t break it down into if it was intentional or reckless. From the perspective of this district it hasn’t been as predominant as if you look at it national statistics where you would see an increase in hacking cases. We are limited to the Western District of New York.
Imhof: What do you believe would be best for individuals and organizations to mitigate damage to themselves?

Littlefield: There are things that they could do which may end up being cost prohibitive. They can install better security, more watchful in the patterns of the network, and things of that sort. I also think that there is a learning curve in starting to learn what seems to be an expensive avenue in prevention software or hardware setup. You know, in the long run it may be more cost effective and I think that financial interests are learning that.

There is still the cost of business and like anything else. What they could do is just to simply to have a technical solution in cases with hacking where they need to make an extensive analysis in the risk they are willing to take by not having XYZ security measures. I don’t have the technical skill to say what controls are necessary. What I do know is like with anything else you can ramp it up and make it so layered where people will no longer go to a website and do their business for another organization because of the difficulty involved with the new security measures. To get the information and keep the organization secure, I think it is a trade-off that needs to be made by the financial interests.

Imhof: What role has social engineering played in successful hacking?

Littlefield: This is the beauty of phishing schemes, that’s a type of social engineering attack by sending people fake information to scare them as opposed to being nice to them. This is obviously one technique opposed to a technical brute force where a teaspoon of honey is better then two cups of vinegar. If they can fool people by being nice to them then that is great for the attacker, but if that doesn’t work then they will scare them by getting a URL that looks like the
authentic one. So yes, social engineering can be a big part of it. It is as different as having the technical skill to build a faster getaway car for robbing a bank.

You know, if you can tweak the engine to make it faster does it make it a better robbery then somebody who can finesse their way into robbing a bank without many people knowing what happened. They could drive away slowly and nobody knows that they just stuck them up. They may have had weapons with them but they didn’t need to show them. It is just different ways of committing the conduct.

Imhof: To what extent will most cyber criminals go to in order to be successful?

Littlefield: They will go as far as they think they can to get away with it. They will go as far as they can and it is like any other criminal conduct if they are successful they become greedy. It is like betting and gambling where if you win a little they keep going on. Smart people quit but they aren’t smart enough to quit because they think they will keep winning so very often this is how criminals get caught. When they are ahead in the game they should quit because they will be exposed when they eventually make mistakes.

Imhof: What role do you believe that Internet Service Providers serve in curtailting cyber crimes?

Littlefield: Well again that is a tough question. When you say curtail they can filter out child porn because there is known hashed values that are associated with known child pornography images. How do they stop something large scale and how are they supposed to police what is going on in their public building and electronic infrastructure? How much are they seeing? The sheer volume
that travels through would require filters and setting the parameters of the filters to define what and what not to look for.

I think they could be effective in recognizing large scale mailing that is going on and if it isn’t from a known entity then they can put a hold on it and look at it to determine what is going on. They can use mechanisms that are to their benefit to protect their consumers. I think it just depends on what you are looking to stop. If you ask any ISP “do you want to stop crimes?” they will respond with a yes. Okay, now how do you go about doing this. I think there is a different case when known criminal activity is occurring and the ISP knowingly allows it to occur then they have criminal exposure themselves by allowing it to happen.

*Imhof:* Are you trying to strike a balance between privacy of communications and trying to stop malicious activity from occurring?

*Littlefield:* That is their call. There is a difference between the government intruding and private business having the right to intrude to ensure that their business isn’t being used to facilitate improper purposes. But, when the Government gets in the middle of it then that is where you run into all kinds of legal issues in terms of privacy protection, Fifth Amendment protection, and all sort of issues regarding how far the Government can or should go. Private businesses have the right to regulate itself between the contractual relationship between themselves and their customers depending on the agreement that is signed. Like I said, if they are themselves liable if they allow a crime to occur that they knew what was going on. The question is what do they know and how do they know and what is reasonable for them to have known.
Imhof: *What sociological theories do you believe that pertain to cyber criminals?*

Littlefield: No, because I mean there is a whole range of offenders from kids trying to be smart or show off to people in foreign governments to people who are trying to make quick money or citizens in foreign countries to people here who are just trying to make a quick and easy buck. Again, if you are talking hackers as opposed to fraud then there could be any number of reasons why anybody would want to send a bot out to shut down entire systems. To answer that question is to answer your question. To define the people that are doing that and you have the answer to your question. It may be because of political reasons in some cases.

Imhof: *What should Information Technology and Information Security professionals know about cyber crimes? Which laws and regulations?*

Littlefield: Well, I have always compared 18 USC 1030 to the burglary statute. 1030 is designed to address entry into protected systems. If they are just entering the system and not doing anything then it isn’t a major crime. It is like somebody walking in your house without permission but they don’t do anything or intend to do anything. They are just walking in for some reason. It would be the equivalent of criminal trespassing misdemeanor crime. When you enter somebody’s house and steal things out of it then it becomes a burglary. If you enter then shoot somebody it is a burglary, trespassing and a shooting. If you go into somebody’s house and spray paint the walls and do damage to it then it is a burglary and also malicious damage. So those are all more serious crimes.

There is a whole series of statutes with 18 USC 1030 being the base. There are all sorts of previously used states such as the Wire Fraud statute, the Electronic Communications Privacy Acts, and other older statutes that have been updated to account for the change in
communications. Unlawful use and obtaining these communications such as for credit card and identity theft in 1028 1029 of Title 18 can be all part of it. Those are all still older crimes. Hacking is just a more sophisticated method of burglary except we are all in a whole different world of access and speeds a million times faster then what we were operating at before. We are talking about being able to flash information as opposed to going in and carrying out a television set from somebody’s house which is much more difficult and time consuming to do.

With the internet you could attack many institutions at the same time by sending out spam and if you are lucky with two or three of them then it is quick money at almost instantaneous speeds. There is a whole array of traditional criminal conduct. 18 USC 1030 is just another tool that addresses cyber related issues but it is no less lawful when you compare what is happening in the real work compared to what is happening in the virtual world.

*Imhof:* Do you believe people are more susceptible to fall for phishing schemes that are electronic as opposed to through traditional media?

*Littlefield:* The more legitimate it looks the bigger the chance is that the person will fall for it. Traditional phishing schemes used the mail where through the internet they use the bank logo with a hyperlink that appears genuine and wants the victim to click on it. It is like setting up a phone bank in a building and making the storefront look like a real legitimate bank and being able to get away with it if you can do it in the real world. Most people want to trust information and if it appears legitimate they will generally trust it.
Imhof: *What do you believe is the best solution to educate users and organizations about the risks that they face?*

Littlefield: It is one thing to have malicious code that installs a back door for unauthorized access from a disgruntled employee that allows that to happen or to educate people about what is out there and do it themselves. I don’t know what you can do to educate against that except if your systems manager isn’t catching it. The best way is to let the employees know about what is going on, what is bad, alerts as to the kind of activity that is going out there. Make it as public as you can to educate as many people as possible. Preventing internal hacking involves good supervision of your people to monitor disgruntled employees. Vigilance, paying attention to it, systems administrator to watch over things and have good personnel management.

Imhof: *Where do you see the future of cyber crimes heading towards?*

Littlefield: It is the nature of communications that it will integrate more and more things in our lives into the virtual world. This could be most of the things we do, so many things have changed in the past fifteen years in how we purchase goods and services. Much of this is done over the internet. Quicker medium means more rapid changing of dollars within the economy. It just makes absolute sense that all it will do is get bigger and bigger, faster and faster, and the criminal side will grow at an equal if not faster rate.
**Mark Musone** – Chief Technology Officer  
*Shatter I.T.* – Buffalo, New York

*Imhof:* Can you please tell me about your formal background?

*Musone:* I graduated from the University at Buffalo with a degree in Electrical Engineering and a minor in Computer Science. A lot of my background is in Electrical Engineering with a lot of focus in computer systems. An example is that I had to design a CPU from scratch which helped me build an understanding of how computers and software work. Once you build a computer from scratch you know everything you need to know about it and everything else is just an add on from there.

I also started, but didn’t complete, my masters in digital signal and image analysis. I concentrated more on the computer sub part of Electrical Engineering. From there I worked at the University at Buffalo in their department called CEDAR, which is the Center of Excellence in Document Analysis and Recognition, where they still do work in OCR (Optical Character Recognition) and were really inventive of OCR technology. They started with the United States Postal Service. In fact, every letter that you mail out gets scanned by CEDAR computers and tries to recognize the addresses and puts it into a format that the systems can understand. For instance if a person puts in the wrong zip code or if the address is out of order then the system's intelligence built in will help to correct the mistakes. It isn’t just a dumb OCR system converting it into computer format.

I was in charge of the systems there and was essentially the main systems administrator. Over there we had mission critical needs because the Postal Service uses this and the systems couldn’t ever go down. A lot of the stuff that I focus on in business has been mission critical, high performance, and high reliability type of systems. From CEDAR I moved to help start a few
internet companies and one of them was called Afterfive Technologies. Right when the web was essentially first invested we were one of the very few web development companies and web hosting companies here in Buffalo, this was around 1994. One of our claims to fame was that we were extremely reliable. Again, this goes back to my background in high reliability systems.

We were lucky that we were able to keep the systems at such a speed, always up, and always reliable. I was asked what certifications that I have and the truth is that I really don’t have any. This is because I was essentially there investing this stuff as it happened. Do I have a certification in CISSP? No, but I actually do CISSP training and training for other certifications where I would just need to get around to actually taking the test and getting the formal certification.

After Afterfive we went from not just hosting websites but actually into the web development piece. Now we were programming to perform actions on a web user’s request. This was back when we had to write programs in C then eventually PERL and now we have languages like PHP. From Afterfive I went to help start a company called Synacor which used to be called Check.com where we did web based e-mail. We were pretty much going head to head against Hotmail because we essentially came out at the same time. We offered free web based e-mail and at that time nobody was offering this besides Hotmail and maybe a handful of others. We were inventing a lot of our commonly used technologies right there.

I was also one of the core developers of PHP and helped develop a lot of the e-mail functionality such as the IMAP, FTP, and about another half dozen PHP modules that I developed. I have always been involved with open source to the point where it helps other people but it also helps us. For instance, over at Check.com we needed to do web based e-mail so we needed a programming language that could handle e-mail pretty well. For the requirement we
would go and write a PHP module that would help us handle e-mail then also offer it for the rest of the PHP community. Back then we had about 20 million e-mail users that we had on the system. Back then this number of people was pretty much unprecedented.

For the entries in our database we were using MySQL and at the time it was the most entries that anybody had ever put into MySQL so we were using leading edge technology and working with the MySQL developers to help modify the database to be able to handle such a high number of rows and things like that. Going back to Afterfive, because we were doing web development and web hosting we would occasionally get the security alerts and the security / hacking attempts. For Check.com since we had 20 million users we were actually one of the top three most trafficked sites on the internet and we would receive a lot of security attacks and we would work with the Authorities quite a bit back then.

Whether it was hacking, identity theft, or other illegal activities occurring it happened that there was a number of people using our free web based e-mail system who committed these crimes. It was less of people attacking our systems and more of people using our systems to further their illegal activity. There was one case where we helped the authorities find a missing girl that was in Disney Land and we were able to track her because she had logged into her e-mail account.

Since we are not providing hosting here at Shatter I.T. for mission critical systems we work with the authorities on occasion. We have the standard attempts and I was actually working with the FBI a couple of weeks ago to help track down an international identity theft ring. For formal systems experience through the years in things that I have led in different jobs has really been leading edge technology and helped develop parts of the internet as it was becoming the internet that we use today.
Imhof: What has been the extent of your experience with cyber criminals and intrusions?

Musone: Being a hosting provider here, Check.com, and at Afterfive has given a lot of real work experience because we get attacked all of the time. We get about 10,000 security attempts a day on about 300 or so servers. At UB, and most universities, are havens for hackers and have pretty much given up. Between the attacks that are internal and external it becomes too much. The systems from the outside have to generally be pretty open because of the nature of being a University.

One of the other things that I also do is consulting for the government agencies. Some of the work I will do for them includes security, auditing, and helping them with the processes and technologies to help prevent network intrusions. Because it is federal, often times they will get directives from the other federal agencies with requirements to increase monitoring for a number of different aspects on the network. I do a lot of penetration testing, security audits, and other security work for the federal government in addition to all of the stuff here and in the past.

Imhof: What common patterns have you found, in your experience, between cyber criminals?

Musone: What I have seen is three different types of criminals. You have your lower level offender who just wants to cause mischief and just want to hack for the sake of hacking. Then you have your underground hackers, or internet hackers, who hack systems for wares. They may want to get them or just find a place to host them such as movies, music, and other things like that. Then you have your true financially oriented hackers who are trying to steal credit card numbers, facilitate identity theft, or making money directly or indirectly through spamming.

The most recent large organized crime thing that we have dealt with was an international identity theft ring. You can tell they were organized because they were jumping through five
different proxy systems all across the world and we finally nailed them down to somewhere in Asia. This ring most likely had at least some sort of organization, but whether it was organized crime or not is difficult to say from my end. I would say that a lot of the financially oriented attacks are seemingly having an organized crime aspect to it.

From the federal government side there have been directives for increased surveillance that seems to have an emphasis on organized crime. Do I see organized crime more? Yes, but that is in comparison from not seeing it at all a few years ago. From what I have seen it hasn’t yet reached a level where we could say for example that 90% of hacks are some sort of organized crime. What we have seen is that 80% of our 10,000 attempts a day are the script kiddies that launch attacks just to see what can be done more often then not. Then about 15% are people that are trying to go in for wares and about 5% are trying to get in for true financial and other malicious intent.

*Imhof:* Why do you believe that cyber crimes are increasing at such a rapid pace?

*Musone:* A large part is because it is so easy. I think that there are essentially three reasons why cyber crimes are rising at a very rapid pace. The first being that it is so easy because there is software out there like Metasploit that any script kiddie can get to attack a system and take their chances to see that a person or organization is running an unpatched system, which is fairly high. What contributes to this is the availability of all these scripts, and the ease to run them.

The second thing is the ubiquitous nature of all these systems and there are thousands of computer systems now. This makes it easy to pick and find a target that is not patched simply because there are so many of them out there. There is also a very large financial benefit, whether it is through spam or leaving movies. People can actually get something for themselves out of it
now, while back then people would hack into machines just to hack them and there really wasn’t a financial motivation or benefit for them.

I relate a lot of this stuff to crimes in the physical world. The internet is akin to everybody having storefronts and never locking the front doors. It is very easy for somebody to go into a store and steal something because the doors and never locked and there are so many stores to choose from. They literally have their pick of the litter. The biggest security hole is people. I believe that people use technology the wrong way.

Technology should be used as a tool, not as a solution. A lot of people rely on technology to do their jobs and provide the overall solution rather then using it as a tool to make their lives easier. We do a lot of monitoring for computer systems and we use tools to let us know about alerts a little bit quicker and more reliably what is going on with the systems. Our claim to fame here at Shatter is that we are the only one in the region who has 24/7 on site network operators. To me you can’t beat that no matter what technology you have because nothing is better then a human. I have seen data centers where they have eight levels of security but nothing is better then having somebody use the technology as tools in addition to their own level of vigilance. You could have the best systems and monitoring technology in the world, but if there is a problem you need to have somebody there and being vigilant.

In the past with things that I have done I have prided myself on being able to go into a system and in a matter of two commands being able to tell if the system has been hacked or not. It is primarily because of vigilance. I can’t tell you how important it is for people to know their systems. If people know their systems and know what is normal and what is not then you would be amazed at how you can go into your system and literally do an ls command and subconsciously know that they system just isn’t responding in the way that it normally does.
For instance, you may be able to recognize that when you do the `ls` command it takes \( \frac{1}{4} \) of a second less time but now it is taking a little bit longer. Your gut feelings many times are more valid then your analytical feelings because these feelings are essentially your subconscious noticing something that is different and not normal, but your mind just can’t place the logic to it. It is like your peripheral vision where you can know that something is going on without actually looking at it. Your instincts are more valid, especially when you are talking about security, then your normal logic. Your logical mind will find reasons why that `ls` command took \( \frac{1}{4} \) of a second longer but it is your instinct that notices these very hard to define elements that brings it to the surface.

Another example is that you will get colored output which may be different because the machine was rooted and the hacker installed the wrong library.

*Imhof: How do you detect kernel level rootkits?*

*Musone:* Normally way before that point you already know that the system has been compromised. Then it is the forensics piece of knowing that the system has been hacked; now you need to go into more detail to find out exactly what went on and boot off of a different disk and use separate commands or use a jump drive and just put the commands on there. One of the benefits of running an older type of Linux system is that the script kiddies are typically usually all of the newer stuff. So, they will go and root a machine and change all of the binaries but these newer binaries are expecting a different shared library. As a result you may execute an `ls` command and the system experiences a segmentation fault and this will tell you everything.
If you have a core system command and it causes a segmentation fault or if the ls command returns different coloring then it is because they swapped out the commands for different binaries.

From what I have seen, vigilance is key when it comes to security. You can have the best Intrusion Detection System in the world, but if you are solely relying on this technology to safeguard your system then you’re nuts. You are certainly going to get hacked if that is the line of thinking that you have. To me it is all about vigilance. Vigilance and security really go hand in hand with each other so when you know how much disk space you have and you know what is normal for your CPU load and bandwidth utilization, then the split second that the system defers from this then you should be aware that there is a potential problem happening. If you know how your system normally acts then you can notice and stop actions that are not normal and may be harmful. Even an Intrusion Prevention System that drops connections will not tell you if somebody was actually successful in their attacks.

I don’t care very much if somebody is attempting, what I care about is if somebody was able to get in. Neither IDS and IPS technologies will tell you that. I recently changed some of my mindset about how in many ways people would put their IDS in front of their firewall. Now the mindset has been completely changed where if there are a bunch of attempts and the firewall is blocking them then who cares? You know that people will be knocking at your door, why do you have it in front of your firewall? Now the mindset is to stick the IDS behind the firewall because you only really care about people that are getting through. Again this will only tell you if there was an attempt, not if somebody was successful or not.

The attacker will typically get in then install and run some type of software that will make the system run in a manner that is not normal. If they are running some software then the CPU
and bandwidth utilization will typically be different. It all comes down to knowing your system, knowing what is normal, and then being able to make an informed decision.

*Imhof: Do the patterns differ significantly depending on the type of crime?*

*Musone:* Just like in the physical world, if you have someone serious on getting in for a financial or other truly malicious benefit and if the place is a Brinks shop then there is going to be a lot of planning, scoping the systems, performing ping tests and things like that so when you get broken into the organization will have some record. You may not know it at the time, but you will be looking at the video tapes and you may see a guy taking a photo of the building and he actually went to the teller a month before and opened an account or tried to make a deposit. The patterns differently differ in the sense that if somebody is intent on doing something malicious they will do their homework. If they tried hacking into my company’s website you will see that maybe a month before they accessed the website and they went in as a normal web user to poke around without doing anything malicious to do their homework.

The script kiddies typically will not know or care what they are doing. They may have a set of IP addresses and just get their scripts and run them to see what happens. They are a lot more ignorant in what they do. Because of that, they are more haphazard and may do something like formatting the entire machine by accident. This is where I see the patterns differ, just like in the real world where you have the street thug that just wants to throw a brick through the window just to be mischievous, are they going to cause a ton of damage? No, but they aren’t doing much homework either.
Imhof: Many people believe that hackers are motivated solely by financial means, do you believe this to be true?

Musone: No, mischief and their own personal benefit which may not necessarily be financial. A lot of times they want a system to store and trade movies and other things like that. I would say that some of the more serious crimes over the internet are for financial means. The crimes that truly cause harm, investigating, and effort are the cases where there would typically be a financial benefit for the attacker.

From what I have seen, the criminals who have a different motive work differently in the sense that if they are protesters against a company they will not care if the machine goes down. If all else fails when they are trying to hack into a machine and if they can’t get into a machine, then they will try to shut the machine down. They don’t care what damage they do to the machine because the machine being up or down doesn’t necessarily hurt them. Whereas the hackers with a financial motivation want the machine to stay up so they are going to cause much less actual, physical harm to the machine. If they knock the machine out then they wont be making money. It is certainly different MO’s (modus operandi) and different objectives.

Imhof: From your experience, what kind of cyber crimes are increasing the fastest?

Musone: I would say Identity Theft. That has certainly become a very big problem. It has been happening much more often because it is very lucrative to do. In a sense this cyber crime is ideal because there is a good chance that nobody is ever going to be able to catch you. In the real world there is a much greater chance that somebody is going to be able to catch you.

If somebody came up to you and said that you could make $10,000 a month and not get caught there would be a lot of people interested in that. It is very easy because of large databases
and once they break into a system they may have 10 million credit card numbers. This is certainly a big issue because a very small amount of work can result in a huge windfall for these criminals. So, I think a lot more people are trying to get into it. Obviously they are not going to be as skilled as organized people, but it is still very easy to do. Any user can send an e-mail to trick people into giving money for a nonexistent yet sick relative. A lot of people are heading towards identity theft because of that, all they really want is a social security number or bank number and from there you are golden. This is why I believe that identity theft crimes are increasing the fastest.

*Imhof: What do you believe can be done to mitigate the rising crime rate?*

*Musone:* There are a couple of problems. Number one is that we are still in the thought that it is ten years ago when the internet was becoming big and we are still in the wild west of the internet and it is a serious problem. Every user on the internet has a revolver in their pocket and a lot of people have no idea how to use it. A lot of people just go around shooting wildly. It is very hard to protect yourself when everyone around you has a gun.

As far as mitigating the rising crime rate we need to wrap our minds around this Wild West mentality. A lot of what comes from this mentality is because things are always changing so rapidly. We don’t have time to fix or secure the old stuff let alone the new stuff. It is all about getting it out as quick as you can with really no thought to the consequences or the security piece. Ideally if things were a little bit more civilized and things were not so rapid then it would certainly help. People aren’t even putting patches out anymore because by the time they are ready for the patch there is a new version of the software out anyway. So, the company may
never put a patch out for the old version because they tell people to go out and buy the new version.

The attacks are typically the same thing over and over again. One of the best things that has happened with the internet is that now you can do everything over the web. You can do your banking, web based e-mail, web based administration for your servers where you don’t need to go in and manually configure files. One of the worst things that have come about with the internet is that you can do everything over the web. Everything runs over port 80 and it is the worst thing in the world. Years ago every individual service would run on its own port. SMTP would run on port 25, SSH on port 22, Telnet on port 23, and now these days you can transfer files over the web on port 80. A few years ago if you wanted to transfer a file you would use FTP and port 20 and 21. Those were the ports, if you wanted to stop somebody from uploading files you would block off the FTP ports at the firewall.

Right now because of this firewalls are somewhat useless because nearly everything can be done over port 80 and it is the worst thing in the world. What can be ideally done to mitigate is to someway go back stop tunneling everything over port 80. One of the best things that could be done is to have separate services again use their own separate ports. Whether it is well defined web services, web ports with well defined services, but again it is more of a pipe dream then anything else. I doubt the industry will go this way, but this is one of the biggest factors that hurts any possible mitigation because everything can be done over port 80.

People these days will actually do reverse shells by hacking into a machine using whatever exploit and then do a reverse shell back out. So, now if you close off all of your firewall ports people will still be connected. That remote machine is actually making an outbound connection to the hackers machine and now the hacker has full rein.
Mitigating the rising crime rate is a problem because things are just going so rapidly and there is no control. The ideal thing would be to roll back time ten years and do things in a more intelligent and engineered way. One of the problems with IT, and especially software development, is there are no standards and at best certifications. Anybody can read the book and study up to take an exam or course to get a certification. It really gives a low confidence as to how qualified the person really is at doing the job.

I would like to see licensing for technology professionals. Electrical Engineers need to be licensed to do stuff and licensing is very different from certifications. Certifications are a one time only thing where you take a test and get certified. You are literally judged on the test. For licensing you actually need to be on the job working under somebody who already is licensed. You can’t blindly go and take a test; you actually need to work in the industry for a number of years under the supervision of somebody who already is licensed. There is no such thing like this in technology where you could see how it is actually done in the real world. The CISSP exam comes close, but this is one in comparison to the thousands of certifications out there. Also with licensing you are required to go through additional training every year. With licensing you will have people who actually know security and how to program properly.

Also what is needed to mitigate the rising crime rate is vigilance. The first thing that most neighborhoods do when they have a rising crime rate is to establish the neighborhood watch program and they are vigilant. Once your neighbors and everyone is watching they see what is going on and they communicate back and forth. They know what is normal for the street and can tell if things have changed.
Imhof: What do you believe individuals and organizations can do to mitigate damage done to themselves and/or their organization?

Musone: The vigilance piece again. It is amazing when you know your systems how you can type in one command and know that something is not normal, this machine isn’t acting right. They need to understand their systems. There are the usual suspects also, make sure your systems are patched, don’t use default passwords, and I would have to assume that this is all being done regardless. I think it is all about knowing your systems and being vigilant. You will know the split second that there is a problem and something is not normal.

What suppliers and vendors can do is by default secure their stuff and we are seeing that. I have Verizon FiOS and it came with a Wi-Fi wireless access point and by default it had WEP enabled. This is not just using the MAC address as the WEP key or anything, and I was very pleasantly surprised by that. A few years ago if you received an access point it would have the security turned off. Now there are certainly a lot of vendors and suppliers who are by default turning the security on. Most people will say forget it and plug in their wireless access point and that’s it. If the instructions tell them to go in and type in a WEP key they will and just forget it. Most people will go with the default; whether that default is manually putting the WEP key into the AP then they will do it. It is just a matter of changing the default from no security to security enabled.

You get this in the physical world too. I read a lot of financial forums on the web and I can’t tell you how many people post on the forums saying how they just noticed they were charged by some fraudulent company for the past eighteen months. You need to be vigilant and read your credit card statement every month to make sure that they are the correct charges and this doesn’t take a lot of work.
Imhof: To what extent will most cyber criminals go to in order to be successful?

Musone: Most cyber criminals will go to whatever extent it takes to be successful. To be successful it typically entails two things. Many people think it is one and it is for financial gain, but not really. It is financial gain and not being caught. To them even if there is no financial gain but they won’t be caught then they will typically consider themselves to have been successful.

This is the same thing with your wares guy and script kiddie. They don’t want to get caught and that is a measure of success, which is very scary. If they are not getting caught then it may mean very bad things for you or whoever they are attacking. I conducted a presentation with a few local groups on computer forensics from a corporate point of view.

What I have noticed in dealing with the authorities and conducting some computer forensics work is that most people in the IT world talks about security and changes their default passwords, but people have no idea what to do when they have been hacked. This presentation was all about what to do when you have been hacked. Most people have no idea because they have never experienced it. It is like if their car is broken into they will panic or go into shock and wonder what to do next. Not doing certain things is just as important and doing certain things.

This was also on your standard forensics stuff that actual IT people just don’t know. When you have been hacked do not think that you have just been hacked, chances are that you have already been hacked for weeks and maybe months. Just because you know right now it doesn’t mean that you need to do something immediately. You may have been hacked for months now, what is another day? The hacker doesn’t know that you know, so doing something immediately may not be in the company’s best interest. Going and doing something may cause more harm because a lot of people that have never experienced it will log into their machine and
try to find out more information. They will look around the directory and every command that they type in invalidates the evidence.

If you have been hacked the first thing you should do is image the server and you only work off of that image. It is your standard forensics stuff but a lot of people don’t know that. One of the things I talk about at the end is that there needs to be a time where you pull the plug on the hacker. Planning and doing that properly is absolutely critical because if a hacker knows that you know then they are going to do something either out of anger or fear. If the hacker knows that you are aware of them then they will do what they feel needs to be done in order to not be caught. A hacker has no problem going into a machine and formatting that entire hard drive.

To what extent will most cyber criminals go to be successful? Well, they will format your hard drive if they need to. They will delete your entire database, because they won’t get caught if they do that. That is more of a concern then how much they will hack into the system in order to get some data. A company losing would be if the data gets out or lost. It is harmful either way for the company.

A company needs to be careful with backups though because a lot of people if they get hacked the first thing they will do is turn off the machine and restart it from backups. Well, you just restored your hacked version on your machine. Again, most of the time when you realize that you have been hacked and see that they have installed some backdoor software, you will go in and uninstall that backdoor software. The first rule is that once you have been hacked you can never go back to that machine again; you need to rebuild it from scratch. What that hacker installed to get them a backdoor is not the original way that the hacker got in.

You may delete their backdoor Trojan software, but it still reverts back to the way it was when the hacker first got in. What does the hacker then do? They will do their SQL Injection and
go back in the same exact way. That is where the rule comes from where if you have been hacked then the plug gets pulled and they can’t go back without rebuilding the system from scratch. Backups are really good for getting your data, but you need to be cognizant that there isn’t a single piece of data on the hacked system that can be trusted.

The only thing that you can bring over is the actual data on the old system. But you still need to look quite a bit at that old data to make sure that none of that has been compromised. Many hackers will perform a SQL Injection then add to the data set to give themselves Administrator privilege to that web based system. You may find this out and delete a Trojan that they installed but they don’t care, they will do the SQL Injection again and put the Trojan or other back door back in. If you don’t review the data sets then there is a good chance you will miss the fact that he still has Administrator credentials. They are in some ways like cockroaches, you may see one way they got in but in reality they may have ten other ways.

*Imhof:* What role do you believe ISP’s serve in curtailing cyber crimes?

*Musone:* There are a couple of pieces to cyber crimes and we want to walk a fine line between freedoms, privacy, and it is a very difficult problem. To me there are different levels of cyber crime. There is your hacking stuff and wares stuff, is it a crime? Absolutely, but is it life threatening? No, and then you have your identity theft and true financial crimes. Then you also have your harmful to people crimes that may be life threatening such as your child pornography crimes. I do believe that those are the three basic levels of cyber crimes and we need to be careful not to just throw a net over the entire thing.

ISP’s are trying to weigh that balance of privacy and helping law enforcement. There is helping law enforcement, refusing to help law enforcement, and there is proactively helping law
enforcement. Typically how it works is that if Law Enforcement gives me a subpoena they will get what they want and people will willingly comply with that court order. It will protect me as a company because I need to make sure that if I give out one bit of data that I shouldn’t have with our litigious society it may put my company out of business because I gave them a last name when technically I should not have. A lot of ISP’s walk this line because they don’t want to be sued by anybody that they give information about.

I am very comfortable giving information to law enforcement if they have a court order because I am pretty much protected and at the same time helping law enforcement.

I believe that ISP’s need to comply with court orders such as subpoenas or search warrants. I also believe in the harm to people category where ISP’s should be ready, willing, and able to do whatever it takes to help law enforcement even without a subpoena. A lot of times time is of the essence, but these days you can get a subpoena very quickly. When time is truly of the essence and people’s lives are in danger then I am willing to take that risk and I believe that ISP’s should go up and beyond to comply with law enforcement to the best of their ability.

Then there are the other cyber crimes which involve the financial stuff. In these cases I believe that Law Enforcement needs a court order and this is a lot harder. There was just a law passed in Sweden or The Netherlands which says ISP’s are only allowed to keep data for three months. After three months they need to delete any logs of IP Addresses and things like that. I think there certainly needs to be a compromise because I do not want to, nor can I, store all of that data because it is just too much.

It is too much to manage, too much to deal with, and there is a lot of liability because if I get hacked into and someone steals my records then all of a sudden I am being sued by one of my customers because the hacker was able to get some of their personally identifiable
information. This is a lot more of a grey area because a lot of these lower type of crimes, especially like your DMCA stuff, which I get notices for all the time, and whether it is a customer or their users will lead to a lot of these little crimes being abused through litigation and the laws. These laws are being abused by certain companies to make life very difficult for the ISP’s. I think that the ISP role should be very akin to the old Telco role.

The old telephone companies had the same problems for the most part. To what extent are they responsible and what role should they play? It should be the same type of thing whether it is wiretapping and recording communications, to if somebody tries selling something fraudulent or committing identity theft over the telephone. Should the phone company be responsible for that? I personally don’t think so. Should the phone company be able to comply with a court order demanding that they produce phone records? Yes, if some companies are continually abusing subpoenas or things like that to make life difficult for the telecommunications companies then that isn’t fair either. I think there certainly needs to be that compromise. None of this is black and white because everything is still panning out.

*Imhof:* What should law enforcement professionals know about cyber crimes and attacks?

*Musone:* There are a couple of levels to that, a lot of your local Police departments do not even know where to begin with these kind of cases. This is even to the point where if somebody was hacked the Police department really wouldn’t know what to do. The local Police often times have more pressing issues to attend to. The good thing about cyber crimes is that if they are financial then it is much less of a crime then physical harm to people. However, law enforcement agencies should at least have some idea of where to send people and what actions they could possibly take.
If somebody goes into a store and steals a candy bar then the Police are all over that guy. However, if a Hacker gets into a server and steals $10,000 worth of credit cards and things like that then it tends to be relatively low on their priority list. A lot of times Law Enforcement professionals do not really understand the tangible and financial affects of the hacking. The general rule of thumb is that law enforcement agencies will usually not even take cases if the financial loss is less than $10,000. This is about the tipping point where the FBI will begin looking into it where you could demonstrate losses of $10,000 or more. This really isn’t fair when it’s compared to the guy stealing a candy bar.

A lot of Law Enforcement professionals have a focus on the big picture stuff such as a million credit card numbers being stolen, or child pornography and this stuff is certainly more important. Anything less then that tends to fall by the waste side. I think a lot of Law Enforcement professionals on that side don’t really know or understand the true impact that these cyber criminals have on companies.

*Imhof:* Many times the technology of law enforcement lags behind that of hackers or other cyber criminals, what do you believe could be done to help fix this situation?

*Musone:* It is a game of catch up. It is the same thing in the physical world where Law Enforcement is always complaining that the criminals have better weapons then they do. It is a problem and there is certainly significant training that needs to be done on the Law Enforcement. My fear is that a lot of them are people that like technology and received on the job training. My understanding of a lot of the forensic software out there that Law Enforcement uses is your typical sector editor type of software. This would be where somebody is manually going through bit by bit and there is a lot of manual work involved.
I think that more intelligent technology is needed. Most of that computer forensics software is your typical grunt work type of forensics software going through it bit by bit. Technology can be made pretty smart so the ability for tools to be there which allows Law Enforcement to much more intelligently look through data rather then go through it bit by bit would be very helpful. From what I understand they have their standard check list that tells them to look for certain files and note the modification, creation, and access dates. They need to have smarter technology that does things like correlation for you. As an example, when you go through the logs and create a timeline of a hack that happened and at this one point in time you notice that a hacker came in from a specific IP Address. The computer may have been hacked the entire time but what you can do is take that IP address and start from the beginning to see any lines anywhere for where that IP Address ever hit the system. You could then get the IP Address of the hacker from when he was using it at home to innocently view the company’s website.

Now you have to take that instance of somebody directly accessing that website or file and feed it back through the entire system from the beginning. There is a constant feedback loop and I am not sure if a lot of the forensics tools have the technology to perform this correlation and feedback. There is certainly a lot of technology that will help automate stuff and a lot of times I think they are simply using tools to physically go in there and allow them to see a lot of the details that they normally couldn’t see. They don’t have the ability to perform that correlation in an automated fashion.

*Imhof: What would be the best solution to educate users and organizations the risks they face?*

*Musone:* Developers code very ignorantly and they don’t even know how the stuff works that they’re developing. They don’t understand the HTTP protocol even though they are doing web
development. They don’t understand what a SQL Injection is and there is certainly a lot of education necessary for an in-depth understand of the stuff that they do. Developers need to understand what they are doing and the technology that they are working with. Anybody that does web development and database querying need to understand what a SQL Injection is. I think we need to start at that base.

Organizations need to understand a lot of this basic stuff too. Nobody has really come around to educate them from what I have seen. People are truly interested because it is like a whole new world opened up to them. People are just very ignorant and we need to get them out of that ignorance. They need to understand what is out there and how to do the basics.

It needs to be more than public service announcements and it needs to be an educational type of event. There is the Homeland Security conference in a couple of months and there are events that are focused around security for people that are selling their wares but it isn’t really educating people. I like the idea of actually having security training through security workshops and I think that it would be very good. This coupled with public service announcements would make things better. The media certainly needs to be involved but there needs to be free classes on how to program securely or whatever we want to call it. I think it should be sponsored by a lot of these companies. MySQL should be able to sponsor a course on MySQL security. Not many books on software development talk about security and that is a problem. If they do talk about it then it is typically as a side section.

There was a workshop on how to program securely and there were more people there then I had ever seen before because people are truly interested in this stuff. One thing that I needed to make clear to them through this workshop was that all it was on was programming securely, nobody mentioned anything about an IDS. You could program the most secure stuff in
the world but if you are leaving the Telnet port open there will be serious problems. There is two completely different factions, there is the coding and development piece then there is the networking and operating systems security piece. We need to be wise to both of them because they definitely work together.

One of the things that I have been calling for is increased security supplied from the vendors. MySQL has a flag called “I am a Dummy” because people in the past have done: “delete * from table” and it ends up deleting the entire database. Now MySQL has it in default where you couldn’t execute that command on a database without a proper where clause. This makes it so that you will not be deleting every single row. By default technologies should do things a little more securely. PHP has made it very easy for people to develop web pages; it has been the best thing about PHP. The worst thing about PHP was that it made it very easy to develop web pages. Some people have no idea what they are doing, they don’t understand validating data. I have been using a framework in PHP called Symphony which is a web programming framework.

I have been a very big proponent of this framework because it allows you to program easier. The nice thing is that it does all of that validation for you so you don’t have to do it. You can not get a SQL Injection in Symphony because it uses what is called Parametrized MySQL queries. Instead of doing it all as one string it will do each individually so you won’t get it as one string. The nice thing about this and other frameworks is that it does the validation for you which is nice especially when you have a language like PHP which attracts people that are very naive and unskilled in doing this development. We aren’t saying that they shouldn’t or need to do it, but at least it covers a lot of the bases.
Even if you do program it securely in six months there will be another exploit out and you will need to go back to your code to do all of those patches. By using this framework all you would have to do is update it and the framework will take care of it. You are outsourcing all of that validation to other people and that is what they focus on then you meld it into your actual code. This is a very good solution that I have seen lately.

Imhof: Where do you see the future of cyber crimes heading towards?

Musone: Identity theft is everywhere and it is increasing as well as data breaches for financial means. It is so easy and there are so many targets out there.

Imhof: What controls are best for risk mitigation from these crimes?

Musone: Solid programming standards, having vendors by default enable security on their products and vigilance. There are some nice controls that can be instituted for risk mitigation versus actual attack mitigation. For risk mitigation a lot of people will put in honeypots or database entries that should never be queried upon. If you have a database of credit card numbers you could put in a special credit card number such as all 9’s and the IDS is tuned to look for that and send an alert if it ever comes across the wire.

There are credit card and user accounts and you could put something in your data warehouse that you know in a normal condition should never appear. You then go and watch for this data because if it comes across the wire then you know that somebody has breached your data. There are a lot of ways that do not necessarily have to be highly technical such as sticking some data in it and watching for it. There are two things, reduce the affect it may have on you
and the risk that it has on the data. It is necessary to follow best practices obviously. The best way for a company to reduce its risk is to stay vigilant.

*Imhof:* What changes to the current laws and regulations would you like to see concerning cyber crimes?

*Musone:* I think that it is fairly rare for people to be punished for cyber crimes. It is viewed as the whole victimless type of thing. The punishments and the number of arrests should certainly be increased significantly. There needs to be a higher level of fear for the criminals over what happens if they get caught so that they don’t even try doing it. It is one thing to knock on the door but it is another thing to get in and trespass. I think essentially there needs to be a trespassing piece and if you trespass then the punishment should be much higher. For the internet the crime should be punishable just like trespassing. You could arrest somebody for coming into your house whether or not you took something.

I think number one there needs to be more of a trespassing law and make people think twice but also set a line. Basically say that if you gain access to that system and that system houses financial information then it’s a big difference. Just like it is a big difference between breaking into a bank versus breaking into somebody’s house.

Most of the script kiddies don’t know what they are breaking into so I would think that they would think twice before performing a generic Nmap scans or run some scripts against an unknown system. If there are credit card numbers stored there then you are in big trouble. Even if there is no financial harm but rather just financial data stored there such as personally identifiable information or other information that could be used for identity theft then there needs to be some serious repercussions and it will make people think twice.
Case Analysis

The fourth part of my research will involve analysis from a number of documented cases involving computer crimes. This section will involve analyzing the facts surrounding the case, the specific laws which were broken, and analysis of why this offense ended up taking place. The specific case law will involve different statues including violations of the Computer Fraud and Abuse Act as well as Economic Espionage.

*United States vs. Jeanson James Ancheta*

In this case the defendant, Jeanson James Ancheta, is accused of setting up a criminal business venture for the sole purpose of creating large scale botnets which he could then use to sell groups of bots to buyers for the purpose of executing denial of service attacks. He would sell up to 10,000 bots at once to waiting buyers. This case is especially important as it is the first time in American history that the government was able to prosecute a botnet distributor.

Ancheta is technically talented and used his skills very well. He was able to create malware which he then sent to his targets for the purpose of infecting their computers. Ancheta also set up an IRC Channel for selling and communicating with his bots. Once the worm was installed on the computer of his victims it would report to the IRC Channel which he was controlling, scan other computers for the same vulnerability, and leave open a backdoor on the machine for future unauthorized access. Ancheta also incorporated a function into this worm which would give him the option of using the infected machine as a proxy. He would also consult with potential buyers about the number of bots they would need in order to successfully carry out their planned attack.
Ancheta also offered a number of other services to his prospective buyers. One of these options was to provide them with the executable program containing the worm which they could then use to spread to other vulnerable machines and increase the size of their botnet. He would offer an option to create an additional IRC Channel on his server which the purchaser could then use for control and communication of their purchased botnet. Ancheta used PayPal as a means for financial transactions and would disguise the purchases as web hosting services.

The customers of Ancheta used his services for a number of purposes. A purchaser only identified as “Circa” bought 10,000 bots from him for the purpose of using them as proxies for mailing SPAM. A purchaser named KiD purchased the worm from Ancheta to increase his already existing botnet. Ancheta also conducted denial of service attacks, in one instance at the request of a purchaser named zxpL.

In August 2004 Ancheta entered into a business arrangement with a buyer named Daytona. Daytona bought 250 bots from Ancheta as well as the worm. He also provided instructions to Daytona about how to use the bots. He then referred a friend to Ancheta for the purpose of purchasing more bots. There were also a number of additional cases where Ancheta provided individuals with bots for reasons of denial of service attacks or SPAM distribution.

In the second count of the indictment Ancheta was charged with purposefully sending malware and causing the damage of an organization exceeding $5,000 in value. This was caused when he performed a denial of service attack for zxpL against King Pao Electronic Co., Ltd and Sanyo Electric Software Co., Ltd.

Ancheta co-conspired with an individual identified only as “SoBe”. These two individuals set up the IRC Servers and Channels to control the infected bots. They became affiliates of advertising companies and would modify the ad-ware they received to install the
worm without permission on the computers of individuals and expand their global botnet. When
the victim clicked on one of their advertisements it would direct them back to one of their ad-
ware servers which would then install the malware onto their computer. Ancheta and SoBe
would then receive payment from the advertising company for the number of clicks that victims
had on their ads. To avoid detection by law enforcement they would vary the download times of
the malware to make it appear as if it were legitimate web traffic.

The fifth count that was charged against Ancheta was because his malware caused the
infection of United States Government computers, namely a computer at the China Lake Naval
Air Facility and at the Defense Information Security Agency. His malware caused these
computers to attempt to join his IRC Channel. This count charges that as a result of this action
Ancheta caused damage affecting the computer system used by the government for national
security, defense, and justice.

Ancheta was charged with the following offenses:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 U.S.C. § 371</td>
<td>Conspiracy</td>
</tr>
<tr>
<td>18 U.S.C. § (a)(4)</td>
<td>Accessing Protected Computers to Commit Fraud</td>
</tr>
</tbody>
</table>
Ancheta was found guilty and sentenced to five years in prison for his offenses. He earned $3,000 for his botnet services and over $100,000 for his ad revenue services. The majority of this revenue as well as other assets he obtained as proceeds of his illegal activity were confiscated by the Government. He must pay $15,000 in restitution to the Federal Government for damage to their systems.

Ancheta is well educated in the technology involved with this case. He was able to take a piece of malware that was engineered by another individual and then totally re-engineer it to serve his own purpose. He also realized that there is a profitable illegal market for botnets as it can serve a variety of different purposes besides just denial of service attacks.

This case reinforced what was shown in the interviews section of this research that cyber criminals are beginning to become more organized. In this case Ancheta conspired with a fellow individual to help set up and maintain the IRC Channels through which he sold, communicated with, and controlled his bots. Although it may have only been two people this shows that many cyber crimes are not being perpetrated by individuals acting alone. There is a lot of planning and execution that must occur in order to be successful. This makes it very difficult to implement the lone wolf act.

The chat communications between Ancheta and a few of his buyers show that he took great pride in his work. He was more than willing to talk about his work as well as instruct people about how to use the malware that he developed. He would receive comments about how efficient his malware was which only seemed to drive him further.
According to what could be proven by the prosecution he made $3,000 selling bots while he was able to make over $100,000 through his advertising revenue. This would lead one to question why he would risk the serious prison time that he eventually received over a few thousand dollars when he could have kept making more money legitimately. Was this really a case where an individual was motivated just by the money he could potentially earn? I do not believe this to be so. This scheme provided a means for him to show off his technological skill while also making some money at his venture. Had Ancheta been solely motivated by financial means then he could have used his vast botnet to distribute SPAM rather than selling it to others and making far less money than he otherwise could have.

United States vs. Scott Levine

Organization within cyber crime have been increasing rapidly. The days where individuals acted on their own seem to be over in most cases. In this case the defendant, Scott Levine, led an organization which engaged in serious data theft. His organization not only engaged in data theft but also in violations of the Computer Fraud and Abuse Act and other serious cyber crime statutes.

The organization led by Scott Levine was known as Snipermail.com. Snipermail would be a distributor for companies wishing to advertise over the internet. They would perform the task of actually distributing the advertisements to various customers via e-mail. Snipermail claimed that their list of e-mail addresses were obtained from an opt-in process where the individuals would specifically state that they would like to be included in their customer list. The customer would specify various areas of interest that they have and Snipermail would send them e-mail specifically pertaining to their interest. They did not always stick to this claim and would
often send e-mail to their general customer list which likely would not match the customers’
specified interest. They would also sell lists of e-mail addresses to various companies depending
on what business that organization engaged in as well as the specific interest of the customers.

The Acxiom Corporation is one of the largest companies in the world which keeps a
repository of personal and financial information for its customers who freely provide this data.
They use an FTP server to allow its customers to upload their information and for its business
partners to download this information. The information provided through each account is
accessible through the FTP server by providing a valid username and password. By providing
these authentication credentials an individual may only see the information available under the
specific account.

Levine and various other co-conspirators at Snipermail did not want to become a
legitimate business partner with Acxiom yet they still wanted the valuable data kept within the
Acxiom FTP servers. Rather than becoming a partner with them legitimately they would instead
impersonate a partner of Acxiom in order to gain access to the protected data. By engaging in
this behavior Levine and Snipermail would gain unauthorized access to a computer system and
use the stolen information for their own financial gain.

After accessing the Acxiom FTP server by using stolen authentication credentials
Snipermail would then download the valuable customer data and incorporate it into their own
customer database. Snipermail would then sell this customer data in conjunction with the stolen
customer data from Acxiom to their own business partners. Snipermail would also download
encrypted files off of the Acxiom FTP server which contained passwords. After decrypting these
files Snipermail would then use these newly acquired authentication credentials to gain further
access to protected Acxiom information. Scott Levine and his co-conspirators were charged with
140 counts of illegally accessing a protected computer and obtaining data with a value exceeding $5,000.

Levine and his co-conspirators would run Snipermail as a legitimate organization. They would recruit new employees and distribute funds and bonuses for performance compensation. They would even offer certain individuals favorable immigration and visa arrangements to join their organization. As it was noted in the interview section of this research, cyber crimes are beginning to become far more organized than they were in the past. Some of these organized crime schemes, such as that perpetrated by Snipermail, are hiring legitimate professionals to further their illegal schemes.

Once it became known to Snipermail that they were the target of a law enforcement investigation they proceeded in an attempt to destroy evidence. They attempted to destroy documentation of their scheme as well as hide digital evidence. They stored hard drives containing the stolen information from Acxiom under stairwells which were eventually discovered by law enforcement. They would then replace these hard drives with recently purchased sets in order to conceal the digital evidence residing on them.

Levine was charged with the following offenses:

| 18 U.S.C. § 1030 (a)(2)(C)                  | Intentionally Access a Computer Without, or in Excess of Authority and Obtain Information |
Scott Levine was found guilty by a trial of his peers on August 20th, 2005 in Little Rock, Arkansas. As a result he was sentenced to eight years in prison. The sentencing judge stated that the sentence reflects the seriousness of his crimes because the direct result was theft of data worth millions of dollars to Acxiom. Levine and his co-conspirators stole over a billion records of personally identifiable information from Acxiom.

This case is one where the perpetrator, Scott Levine, and his co-conspirators clearly were motivated by financial means. Snipermail was an organization which actually performed a legitimate business function. The organization performed a vital function for many companies by distributing advertisements to potential customers based upon their business functions and interests. Clearly Levine and company were not satisfied with the size of Snipermail so they decided to get greedy.

The first thing they did was to discontinue supplying their business partners with e-mail addresses based only on the interests of their customers. For instance, if their business partner was a hunting equipment manufacturer they originally would only supply them with the e-mail addresses of customers interested in hunting. Levine and company eventually just gave the hunting equipment manufacturer e-mail addresses of any customer regardless of their specified
interests. The second act they committed which demonstrated their greed was the illegal scheme documented in this section.

The organization and structure of this illegal scheme is what really makes this case interesting. This was not just a single individual distributing mass lists of e-mail addresses for the purposes of SPAM. Scott Levine may have run Snipermail, but he had a large staff and a number of co-conspirators. His co-conspirators included software engineers, database administrators and systems analysts. They were legitimate professionals employed to further an illegal scheme. The illegal scheme was perpetrated in order to further increase the profits of their already established and legitimate business function.

This case is one which clearly shows the trend of where cyber crimes are heading. Organized crime with multiple layers of perpetrators and co-conspirators are now becoming the norm rather than the exception in these types of cases. The illegal scheme documented in this section involved theft of billions of records which were worth millions of dollars. Schemes of this size will involve more than one individual making organization even more important. Snipermail had multiple co-conspirators involving different talents and abilities. The combination of these different abilities will make these organized crime structures far more dangerous than a single individual.

Operation Cyber Slam was an effort by law enforcement to investigate and shut down an organization engaging in an illegal botnet scheme. The investigation was launched based upon a number of online companies suffering distributed denial of service attacks. These attacks were
severe involving large scale botnets and causing nearly two million dollars in damage and lost revenue between the victim organizations. This case involves organization and different layers of responsibilities into an effort at disrupting the business operations for three organizations.

Weakness.com is an online company which sells digital video recorders such as TIVO and is based in Los Angeles, California. Weakness earns nearly all of its $3 million in annual revenue from its e-commerce operations. Since so much of its revenue is dependent on the successful running of its website the company suffered substantial damage when it fell victim to a large scale botnet attack on October 6th, 2003. The website was unavailable for twelve hours while it was victim to a large scale and very successful SYN-FLOOD attack. This attack was so large that the hosting company for Weakness, Lexiconn, had to drop them as a customer because the denial of service attack was affecting other customers on their servers. Weakness then hired Rackspace.com to host their website. Despite being larger then Lexiconn with more bandwidth the website for Weakness was still being shut down for a period of about two weeks.

The attack on Weakness was very sophisticated as it had the ability to evolve. Weakness and Rackspace implemented countermeasures to defeat the SYN-FLOOD attack so the perpetrators changed the attack to an HTTP-FLOOD attack which involved using HTTP GET commands to retrieve large image files and invoke search operations from the Weakness web servers. This method was even more effective in shutting down the web operations for Weakness, however Rackspace was eventually able to implement an effective countermeasure against the HTTP-FLOOD and the attacks against Weakness were eventually stopped. Weakness estimated their losses to be around $200,000 from this attack.

A business competitor of Weakness is RapidSatellite.com and they also fell victim to a distributed denial of service attack. RapidSatellite upgrades the digital video recorder systems for
their customers. Recently they had a business partnership with Orbit Communications Corp, which was owned by Jay Echouafni, fall through. This company is a subsidiary of WebClick Concepts and generates the vast majority of their revenue.

RapidSatellite fell victim to the same SYN-FLOOD attack that Weakness experienced. RapidSatellite then changed their web hosting company to Speedera to try and mitigate the damage caused by the denial of service attack. Although Speedera had more bandwidth available it did not do much to mitigate the attacks because the botnet changed its target from the web servers to the RapidSatellite DNS servers which quickly became overwhelmed. Since RapidSatellite shared the Speedera DNS servers with other clients, such as the United States Department of Homeland Security, other clients for Speedera also suffered service loss as a result of this attack. RapidSatellite was again forced to migrate to a new web hosting company, this time Akamai, with even larger available bandwidth. RapidSatellite estimated their losses to be around $300,000 from this attack.

After close analysis of a compromised computer, Law Enforcement was able to determine that a bot named “W32.HLLW.Gaobot” was responsible for controlling the traffic for the botnet in question. Analysis of the logs for Weakness determined that a computer performed reconnaissance on their servers to determine what files and functions would be most effective in a denial of service attack. As a result of tracing this IP address Law Enforcement were able to determine that it came from a computer owned by Unixon.net. Further analysis determined that the user who perpetrated the attack from within the organization was Lee Walker. After an interview with Walker and search of his apartment in the United Kingdom, Law Enforcement discovered that Walker had been paid by an individual named Paul Ashley to conduct a denial of
service attack against both Weakness and RapidSatellite. The bot was specifically developed for Walker by another individual to use as he saw fit.

Paul Ashley owned Creative Internet Techniques which is a web hosting company that also ran its own IRC network called FOONET. Ashley’s organization would perform web hosting responsibilities as a legitimate business would but the company also engaged in illegal activity. Ashley would pay individuals to investigate security issues on behalf of his clients and issue denial of service attacks against the perpetrators. Ashley would also instruct denial of service attacks to be carried out against hackers who attacked FOONET itself. The botnets responsible for the attacks on both Weakness and RapidSatellite communicated through the IRC servers in FOONET.

Ashley had also contacted and instructed Joshua James Schichtel and Jonathan David Hall, both well known for their expertise in the development of botnets, to use their botnets to carry out an attack against both Weakness and RapidSatellite. Although Ashley had orchestrated the actual planning and execution of the denial of service attacks he was not the individual who made the original request for it.

Jay Echouafni was the individual who made the request that these denial of service attacks be carried out and had hired Ashley to carry out the request. Echouafni had bought Creative Internet Techniques prior to these attacks from Ashley then hired him as a network administrator. After becoming owner of Creative Internet Techniques, Echouafni instructed Hall to carry out a denial of service attack against another one of his competitors named Expert Satellite which resulted in another $400,000 loss in revenue for the organization. Richard Roby was another individual who had a large botnet, consisting of about 15,000 infected machines, and
also developed the bot Agobot which was used to execute a number of denial of service attacks used by Creative Internet Techniques.

The defendants were charged with being in violation of the following offenses:

<table>
<thead>
<tr>
<th>18 U.S.C. § 371</th>
<th>Conspiracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 U.S.C. § 1030 (a)(5)(A)(1)</td>
<td>Transmission of a program with intentional cause to damage a protected computer</td>
</tr>
</tbody>
</table>

Echouafni fled the country after search warrants were executed and he learned that an investigation was being conducted on him and his organization. The charges against Ashley, Hall, Schichtel and Roby were dropped. Charges are still pending against British citizen Walker and a federal arrest warrant is in effect for Echouafni.

This is a case that showed how organized cyber crime can be. There was a well defined organizational structure here with Echouafni in charge. He would tell Ashley what he wanted done and who should be targeted. Ashley would then contact and instruct other individuals to carry out the denial of service attacks against the targets specified by Echouafni. This was certainly not a case where a single botnet owner attempted to commit extortion against a large organization.

The primary motivation for Echouafni in this case was not to make more money. His primary motivation in this case was to get revenge against his competitors for a couple different reasons. The first was that Weakness had a pop-up advertisement come when he accessed the
website for his organization. It is documented in the indictment that he became infuriated at this and soon after contacted Ashley to conduct a denial of service attack against them.

The same motivation was evident for Echouafni with RapidSatellite. They had a business agreement that fell through and Echouafni became infuriated over it. Creative Internet Techniques was a legitimate web hosting organization that decided to wander into activity that is illegal. Originally they would conduct denial of service attacks against people who were hacking their clients. This is illegal and what this organization ended up doing is using their FOONET system to launch denial of service attacks against anybody willing to pay to have it done. According to reports these denial of service attacks were not one time incidents from the FOONET IRC system. This means that denial of service attacks for profit may have been conducted by Creative Internet Techniques for some time. By the time Echouafni was in charge of FOONET he just wanted to cause damage to all of his competitors. He attacked Expert Satellite with a denial of service attack for no reason other then they were his competition.

*United States vs. Gary McKinnon*

This is perhaps the strangest case which will be covered in my research. The United States vs. Gary McKinnon involves an unusual combination of compromising United States government computer systems, political debate, Pink Floyd, and secret UFO information. Unlike most of the other cases covered in this research this case does not extensively involve the compromise of computer systems used by individuals or private enterprise.

In 2002 Gary McKinnon was an unemployed Systems Administrator living in the United Kingdom. During February of 2002 McKinnon compromised numerous computer systems used by various branches of the United States Department of Defense. In addition to compromising
computers used by the Department of Defense in Fort Meade, Maryland and the United States
Air Force in Crystal City, Virginia, McKinnon compromised computers used by the United
States Army in the following locations:

- Fort Myer, Virginia
- Alexandria, Virginia
- Fort A.P. Hill, Virginia
- Fort Irwin, California
- The Pentagon
- Fort Meade, Maryland
- Rosslyn, Virginia
- Fort McNair, Washington DC
- Fort Belvoir, Virginia
- Arlington, Virginia
- Fort Polk, Louisiana
- Hinton, West Virginia
- Fort Benning, Georgia
- Great Lakes, Michigan

McKinnon was able to compromise computers used by the United States Navy in the following
locations:

- Groton, Connecticut
- Crystal City, Virginia
- Pearl Harbor, Hawaii
- Patuxent River, Maryland
- Bethesda, Maryland
- Wayne, Pennsylvania

McKinnon was able to compromise computers used by NASA in the following locations:

- Hampton, Virginia
- Greenbelt, Maryland
- Moffett Field, California
- Houston, Texas
- Huntsville, Alabama
- Herndon, Virginia

In addition to the locations mentioned previously and through various branches of the
armed forces, he was also able to compromise a computer used by Tobin International in
Houston, Texas; the University of Tennessee in Knoxville, Tennessee; Frontline Solutions in
Wayne, Pennsylvania; Louisiana Technical College in LaFourche, Louisiana; Martin Township
Library in Colfax, Illinois; and Bethlehem Public Library in Bethlehem, Pennsylvania.
McKinnon would follow the same pattern in all of the systems that he compromised. After gaining unauthorized access to these systems he would give himself administrator privileges which would allow him to install any software he wished and perform any action he wanted. He would install RemotelyAnywhere which is a remote desktop application. This would allow him to remotely control the compromised system. He would then obtain authentication credentials for other accounts, install other hacking tools, and finally delete critical system files and user accounts.

McKinnon was charged with the following offenses:


McKinnon has been fighting extradition to the United States for these offenses committed in 2002 with appeals to England’s Supreme Court. As of this writing in October 2009 he has been denied his appeals and still awaits extradition.

The United States have taken the actions committed by McKinnon very seriously because they ended up crippling some of the computers used by the United States Navy to track the location of war ships. This attack also took place shortly after the September 11th attacks which raises the suspicion of terrorism on the part of McKinnon from the perspective of the United States Government.
McKinnon has offered a bizarre explanation for his actions. According to him he compromised these computers for the purpose of searching for information he believed the United States were holding about UFO’s and alien anti-gravity propulsion systems. He believed that the government had this information and were withholding it from the general public as part of a large scale conspiracy theory.

McKinnon was diagnosed with Asperger Syndrome which is a form of autism. This raised the question of whether the United Kingdom should extradite a man with a known mental illness. This revelation brought about pleas from some in the mental health community, his family, and Pink Floyd member David Gilmour to reject the extradition request based upon his mental state.

The issue that arises here if McKinnon were to be taken at his word is why he decided to cause damage to the systems he compromised if he was only trying to get information from them. If he was only trying to find information on UFO’s then why did he go about deleting critical system files and user accounts? Could his mental state have affected the perception of how his actions would affect the systems he compromised?

This case is especially interesting because it highlighted that a single individual can still cause a lot of damage. McKinnon was able to compromise and damage sensitive Government computer systems to the amount of seven hundred thousand dollars working by himself. This is a case where he wasn’t motivated by financial gain or revenge, rather he was motivated to find information he felt the government was holding on alien technology and activity. While this case is far outside the norm in the manner of the damage done to government systems as well as the perpetrators motivations it does show that every hacking case is unique. There does not appear to be a financial motivation for McKinnon in this case.
United States vs. Kevin Mitnick

Kevin Mitnick is well known in the hacker community for his famous exploits. Mitnick is considered by many to be one of the most dangerous and successful hackers because of the success he has had in compromising very large institutions with relatively little effort. The varying methods through which Mitnick achieved his goals is as impressive as the organizations he was able to compromise. Mitnick is the author of a few books and has started his own Information Security consulting company since his release from prison.

Mitnick was able to use a variety of different attacks to achieve his end goal. While he is technically adept and was successful using technical attacks to compromise systems, he would usually resort to this as a last step. In his book “The Art of Deception”, he described the strategy he used in order to be successful. Mitnick primarily used Social Engineering attacks before he would resort to more technical attacks. By using Social Engineering, Mitnick would prey on the human element of security.

Social Engineering is a form of attack where an individual talks their way into getting what they want. People generally want to help others in distress and Mitnick would often take advantage of this. Often he would pretend to be an employee of the target organization claiming to have lost his authentication credentials. He would then claim that he needed to get onto the system to complete a project and if he didn’t then his job could be in danger. This would play to the human element of pity and worked with great success.

Mitnick was also famous for using intimidation is his Social Engineering attacks. He would impersonate an employee from the target organization but this time he would act as if he were a high ranking officer. By pretending to be an officer of the organization it gave him credibility and authority. He could use this to threaten the employment of an individual within
the organization to give him access to the system. Believing that people are always the weakest
link for the information security of an organization he was able overcome significant technical
barriers put in place for many of these organizations.

The United States Government alleged that Mitnick broke into the systems of Motorola,
Novell, Fujitsu, Sun Microsystems, University of Southern California, and Nokia in order to
steal source code for various projects they were working on. These were the organizations that
the Government had evidence of Mitnick’s wrong doings. It is believed that Mitnick had actually
compromised many more systems, but this can not be proven.

Mitnick was charged with the following offenses:

18 U.S.C. § 2511 (1)(a) Interception and Disclosure of Electronic Communications

18 U.S.C. § 1030 (a)(5)

18 U.S.C. § 1343 (2)(a) Wire Fraud
18 U.S.C. § 1343 (2)(b)

Kevin Mitnick plead guilty and served twenty-two months in a federal prison in 1995.
Following his release form prison he continued to hack cell phone codes and served another year
in prison. Following his release from prison he had to agree never to use the internet again
despite also using various other medium to commit his crimes.
Mitnick claims that he didn’t commit these crimes for any financial benefit. He claims that all of his actions were for his own intellectual pursuit. He was curious about what these organizations were developing and wanted to see their source code. Mitnick also appears to have engaged in this behavior to satisfy his own ego. He targeted high level organizations because of the challenge that it posed to him.

Mitnick claims that he never caused any damage to these organizations as this wasn’t his motive. Mitnick was thrilled by the challenge as well as his own curiosity. He is also very well informed about the manner in which people behave and react to certain situations. He has shown that even if an organization implements high dollar security technology they can still be vulnerable. The human element must be mitigated through policy and procedure which is well thought out and planned.

Mitnick is a traditional hacker which has was defined in the literature review section of this research. Mitnick as well as his friends and family claim that his actions were purely based on curiosity and his own intellectual pursuit. He was motivated by the challenge which was put in front of him and he handled it well. Mitnick could have made a lot of money and caused a lot of damage to his compromised systems if that were his goal.
Final Analysis

Through the various sections of this research it has become evident that while cyber crimes are generally unpredictable there are some common trends and patterns that are appearing. Through the interviews we are able to see cyber crimes defined in a number of different classes. Within these classes a number of different motivations appear. The interviews with Bradley Bartram, Mike McCartney, James Domres, Mark Musone and Martin Littlefield show us some common trends but they also differ in a few areas. The difference in opinion comes from the difference in their individual experiences. Sometimes motivators for cyber criminals can be unpredictable as seen in the Case Analysis section of this research.

According to the interviews and case analysis sections of this research, organization between cyber crimes have quickly become very common. There are entire criminal enterprises that specialize in all different types of crime from extortion and denial of service attacks to child pornography or large scale identity theft. There are criminal organizations that hire legitimate information technology professionals to do things such as building malicious software to infect vulnerable computers and build large scale botnets.

Cyber attacks are constantly on the rise from foreign sources. All five interviews mention the ever increasing threat of cyber attacks against critical network infrastructure of both public and private enterprise. There have been many news reports out recently about this ever increasing threat. Law Enforcement and the Military have seen attacks from foreign sources increasing at an alarming rate. As of February 2010 there have been numerous reports of cyber attacks originating from within China, Russia and other Eastern European countries. This is cause for major concern since there are a lot of critical functions within the United States that
depend heavily on information systems. An example of this would be the Supervisory Control and Data Acquisition, or SCADA, system.

The SCADA system handles critical functions within the United States such as electrical and water control. There have been documented cases of hackers gaining access to this system from within China. The importance of reliable and secure information systems have changed the way in which modern warfare will be fought. If one country can hack into the others electrical system and shut it down then it gives them a distinct advantage. According to the interview with Mr. Bartram it is because of this that new branches within the United States Military are forming with the sole purpose of protecting their own cyber assets and attacking those of other nations if needed.

Wall Street relies heavily on instant financial data and real time transactions. This means that the financial institution relies heavily on its own information systems. A foreign nation could cause serious disruption to the economic stability of another nation if they could gain unauthorized access to its vital financial information systems.

Individuals who hack systems seem to mostly be divided into two well defined classes according to Mr. Bartram, Mr. McCartney and Mr. Musone. The first class is the dedicated hacker that we think of in the traditional sense. This individual is very dedicated to their craft, are technically savvy, spend a lot of time researching their targets, and are generally after something very specific. The second class would be individuals who would be considered script kiddies. Generally these individuals are about causing havoc, don't extensively research their targets, and will typically launch scripts developed from individuals in the first class. Sometimes these individuals will blindly launch scripts and just hope that one is successful. An example of this is noted in the interview with Mr. Musone where he mentions how he has seen malicious code
developed for use against Windows launched against a Linux machine. According to Mr. McCartney, 99.99% of attackers are opportunistic and will take the easiest way in.

The motivations of cyber criminals are varied and determined based on a number of different factors. Crimes such as large, organized identity theft rings are almost always motivated by financial gain. This is not always the case as evidenced by the United States vs. Jay Echouafni. In this case his primary motivation was revenge against competitors. He wanted to get them back for advertising in a pop-up add on his website and another for breaking a contract.

Most cyber crimes originate from the outside. Typically it will involve someone who is using a tool to scan a wide range of IP addresses to find open ports and unpatched machines. They would then launch a previously developed exploit to take over this machine. Despite this, many attacks still originate from the inside. Typically this will involve someone within an IT department who has privileges and root access to certain machines. He typically wouldn't be the super hacker, but he will know enough to cause serious damage. If they are disgruntled for any reason they can make the parent organization pay through damages or extortion. They are not after anything in particular, rather this would be their path of least resistance.

While there are some organizations developed from the beginning just for the purpose of furthering an illegal scheme, the more likely scenario is that there is a legitimate company that wanders into illegal activity. An example of this is the United States vs. Scott Levine. In this case Levine ran his company Snipermail like a legitimate organization. Snipermail provided a legitimate purpose but Levine became greedy and used Snipermail as a front to perpetrate large scale data theft. Snipermail used multiple individuals to gain unauthorized access to gain customer date from a competitor. He had a large staff and co-conspirators who also helped him to destroy evidence when his illegal scheme was discovered. Snipermail had legitimate information
technology professionals perform illegal actions. This is a case where financial gain was a clear motivation.

According to all five individuals interviewed, financial motivation does not tend to be the primary motivation for criminals who are acting on their own. Mr. McCartney noted that 75% of the cases involving individuals don't have a financial motivation. Most of the time in these circumstances the individual is motivated by making a political statement, revenge, curiosity or boosting their ego. This is seen in the communication between cyber criminals through IRC channels where they boast about their exploits and offer advice to those who are less talented. These individuals get a boost to their ego and can foster a mentor relationship with those who admire their talents. These individuals know that their actions are wrong but they want to test the limits of how far they can actually go. Although this would be a common trait for both malicious and ethical hackers they are doing it for different reasons.

The ethical hacker is doing it to genuinely improve the security for an organization or to better technology in general. The malicious hacker would test the limits in order to cause havoc or feed their ego by being able to say that they were able to do it. Mr. McCartney noted that talented hackers are half motivated by self interest and half motivated because they view it as a challenge for them.

Hackers who do not commit these crimes for financial gain can cause a lot of damage because they do not necessarily care if they are caught or not. If a group of individuals deface a website for political and ideology means then they obviously want their actions to be noticed. If these same people compromised the system of a bank for financial gain then they would want to remain anonymous within their system for as long as possible. Being caught means that the victim is aware of the compromise and will begin working on securing their system and kicking
them out. If they are no longer in the system then they will no longer be able to collect vital financial information. Hackers may also take over a system to use its resources such as file space to store illegal content or its bandwidth to control and launch denial of service attacks from.

If 75% of the individual hacking cases are not based on a financial motive then there are still 25% of the cases which are. One of these cases is the United States vs. Jeanson James Ancheta. In this case Ancheta sold large scale botnets and offered malware that clients could use to build their own. He would also instruct the clients on how to use the malware and what machines are most vulnerable. He charged for his services which accounted for around $3,000 in botnet sales. The interesting part of this case was that he also earned over $100,000 for his ad revenue services. This would lead one to ask why he would risk serious prison time for a few thousand dollars? This may be explained by the fact that the $3,000 number is what the government could prove. It is very likely that he made much more than that because his botnets and malware worked well.

There are certain cases where the motive for a cyber criminal is either unknown or strange. In the United States vs. Gary McKinnon he didn't have a financial motivation. His motivation is strange but still ideological. He hacked vital government systems in order to find information on UFO's and anti-gravity propulsion systems. He believed that the United States Government was holding this information and he wanted to find it. Through his actions however he ended up crippling some United States information systems, specifically one which was used by the United States Navy to track war ships.

As stated in the interview with Mr. Littlefield, the internet is being used as a vehicle through which many traditional crimes are now being perpetrated. Instead of criminals holding up banks with shotguns and hostages they are hacking financial institutions and getting away
with much more money than they ever could have in person. They may break into an e-commerce website and steal many thousands of credit card numbers. This has a far higher payoff than stealing an individual's wallet. Mr. McCartney and Mr. Domres noted that cyber crimes are increasing so quickly because everyone is connected to the internet through various devices. Things also happen in real time which makes the internet a very attractive means to commit crimes through. There are also technologies, such as proxy servers, which allow an attacker to remain anonymous while they commit their crimes.

An interesting point brought up in most of the interviews was that hacking is generally considered to be pretty easy. Criminals see cyber crime as being easy to perpetrate. There is a low chance of them getting caught and an even lower chance of being convicted. Many people do not patch their machines or follow information security best practices. This has led to the success of script kiddies. These individuals do not have extensive technical skill but they know enough to launch a previously developed script against an unpatched or otherwise vulnerable machine. Mr. Musone noted that there are many similar and unpatched systems which allow script kiddies to be successful. Similarly, people who are ignorant of information security best practices are highly vulnerable to social engineering attacks.

While there may have been a general consensus on some issues between those interviewed for this research there were still some differences in opinion. The issue which seems to have caused the biggest difference in opinion was about what cyber crime they viewed as increasing with the most frequency. Mr. Bartram and Mr. McCartney believed that cyber crimes involving malware are increasing the fastest. They tie this back in with the increase in organization with cyber criminals. Mr. Bartram noted that large scale botnets are being created that have their own infrastructure services. These botnets are expansive, sophisticated and run by
multiple people. An example of this is the United States vs. Paul G. Ashley, Jonathan David Hall, Joshua James Schichtel, Richard Roby, Lee Graham Walker, and Jay Echouafni as documented in the case analysis section of this research. This case involved multiple botnets as well as multiple layers of personnel involved in this illegal scheme.

Mr. Musone believes that cyber crimes involving identity theft are increasing the fastest. This is easy to see with the increase in organization within cyber crime and the large amount of money which can be made with identity theft.

A common trend in this research has been the belief that crimes involving child pornography and exploitation are common and increasing quickly. Mr. Littlefield believes that these crimes are increasing the fastest. Mr. Bartram made an interesting point in his interview about these criminals when he stated that they are essentially broken up into two groups. The first group tend to be older white males who genuinely lust after these unfortunate children. The second group tend to be people who have these pictures and videos for the purpose of testing the limits by having something that they shouldn't. The second group would usually be those who traffic in child pornography for the purpose of financial gain. Many of the people who would fall into the second group of criminals trafficking in child pornography use the same technologies that hackers use. These people, for example, would use proxies to mask their source and encryption both during the transactions and with the content itself.

Mr. Domres brought up an interesting point in his interview when he stated that pedophiles and hackers live in different worlds. According to him pedophiles want to confess their misdeeds to cleanse their souls while hackers want to brag about their accomplishments as they are proud of what they were able to accomplish. This fits in with the behavior noted earlier in this research which stated how hackers like to brag about their accomplishments and form a
mentor relationship with those who are also interested in the craft, but who may not currently have the same skill set.

Cyber Criminals will generally go as far as they think they can get away with and not get caught. Many times these people are caught because they made a mistake and ended up leaving a trail right to themselves. Mr. Musone noted that these people would use elusiveness as a metric for success.

It should be noted in the literature review section of this research that cyber criminals are traditionally male dominated. Many people who are hackers do not necessarily do it with malicious aforethought. Many of these individuals are frustrated over the traditional way of engineering where everything is proprietary and closed source. They have a genuine curiosity, and sometimes a need, to alter technology to perform a function that is outside of its original means. Their curiosity drives them to explore technology in depth and fully understand the underlying technical concepts. For these people hacking serves not only as a problem solving tool but it is also fun and exciting for them. For those who feel that hacking is enjoyable it also gives them an intrinsic reward. According to Mr. Littlefield these individuals tend to be younger.

A reason why these individuals go from ethical hacking and modifying technology for beneficial reasons is the lack of formal ethics training in technology based college programs. Many cyber criminals are well educated in technology but may not fully understand the true impact of their actions. They view their actions as being very solitary and mechanical rather than its widespread affect on people and events that they did not previously think of.

While many cyber criminals think in very solitary and mechanical means it doesn't mean that they don't understand how to manipulate people to get what they want. As documented in the
United States vs. Kevin Mitnick, there are some cyber criminals who are very convincing and able to manipulate human perception. Mitnick had both technical and social skills. His reasoning when hacking into a system was to manipulate the weakest link in the security chain, people themselves, to gain access rather than trying for a long period of time to launch technical attacks against sophisticated technical controls. He was able to prey off of the natural human desire to be helpful and off of pity to gain access to systems which may have taken him weeks or months to crack through technical means. According to Mitnick he looked at is as a challenge and used hacking as his own intellectual pursuit.

Many of the problems caused by cyber criminals can be avoided through mitigation measures. The most important of these measures would be increasing pressure on software companies to develop software that is properly beta tested and not rushed to market. The motivation for a financial company to rush a product to market is clear from a financial viewpoint, but it causes problems through exploits such as buffer overflow attacks that can be avoided through proper parameter checking. ISP's can also be doing traffic flow analysis. If they see a home network sending out 10,000 e-mails a minute then it is highly unlikely that it is legitimate.

The laws in the United States are outdated to handle the wave of sophisticated modern cyber crime. There is apathy in the judicial system about these offenses and viewed as a victimless crime when there is substantial damage caused. There needs to be better communication between the private and public sector about threats and exploits. The Government needs to better inform private industry about emerging threats and private industry needs to notify the Government when their systems have been exploited. Many organizations, despite Federal statute and best practices, continue to ignore education and information security
best practices. When the employees of an organization are ignorant of best practices through a lack of education it gives the attacker an advantage and greatly increased their chances of success.

This research has shown that cyber crimes are all increasing and becoming more dangerous. While some crimes such as child exploitation affect only a few individuals other cyber crimes can affect entire nations. Cyber Warfare is becoming a very real threat to all countries and will play a very large role in modern warfare. Although it hasn't been proven there are many individuals who suspect that Russia used Cyber Warfare against Georgia in their 2008 conflict. Most of Georgia's information systems were subject to large scale denial of service attacks during this conflict and were shut down. This is a very real threat since so many critical functions of society depend heavily on information systems.

All five individuals interviewed for this research agreed that Cyber Crimes are only going to increase. There is no foreseeable slowdown in the future for these crimes. Mr. Musone used the analogy that the internet is like a street with many businesses having unlocked doors. Information Security isn't where it needs to be and criminals are able to exploit these weaknesses for their own financial gain. Military involvement will become even more pronounced as modern warfare will be targeted at the critical information systems that countries depend on. Everyone is connected all the time and rely very heavily on internet communications. Users depend heavily on technology in their daily lives which increases the target pool for attackers. E-commerce has become very popular in the past decade and will only increase in popularity. Identity theft and fraud are very lucrative for organized crime and has led to substantial involvement in recent years which will become more serious in upcoming years.
Works Cited


Sutherland, Donald. (1934). Criminology. New York: J.P. Lippincott


Abstract

Cyber crime is a new and emerging area of concern for technology professionals, business leaders, and heads of government. This research takes a look at the individuals behind these crimes in order to develop a profile and determine emerging trends. Classical Sociological theory is detailed and its ability to apply to modern cyber crime is explained. Interviews were conducted with five professionals in the field in order to gain a wide range of differing experiences and emerging trends. The most important cyber crime laws in the United States Code were broken down into their elements and explained in a way that technology and business professionals, without a legal background, can understand. Seven case studies were then conducted to find the facts of the crime, the statutes which were violated, the outcome, and analysis. The research concludes with a final analysis section which outlines the findings of this research.