5-2022

The Pentest Method for Business Intelligence

P. Soma Reddy

Justin Pelletier

The Pentest Method for Business Intelligence

P. Soma Reddy, J.M. Pelletier
Rochester Institute of Technology
Rochester, NY 14623
Email: jxpics@rit.edu

***Abstract*—Information transactions and data retention comprise critical inputs to Business Intelligence processes. However, despite ongoing data-driven Business Intelligence process improvements, many companies only discover they are vulnerable to a cyber-attack after a breach materializes the risk. In this study, we propose that compliance regimes such as the global Payment Card Industry Data Security Standard (PCI-DSS), the federal Gramm-Leach Bliley Act (GLBA), and the regional 23-NYCRR-500 standard provide externally-imposed risk discovery opportunities that should be part of managerial decision-making. This paper describes the penetration test (pentest) method relative to those regulatory regimes. We then consider the potential for the pentest method to yield predictive Business Intelligence data sources in five historical cases: the 2017 Equifax Breach, the 2014 J.P. Morgan Chase Breach, the 2012 Global Payments Breach, the 2010 Nasdaq Hack, and the 2009 Heartland Payments Breach. Our findings suggest that the pentest method–especially relative to PCI-DSS compliance–is a promising inclusion in Business Intelligence processes.**

***Index Terms*—business intelligence; penetration test; pentest; compliance; PCI-DSS; GLBA; 23-NYCRR-500**

I. Introduction

Information transactions and data retention comprise significant risk factors for all organizations. Cyber-physical systems, which process and store these data, continue to present "opportunities for an enhanced realtime steering and adaptation of [Business Intelligence] processes" [1]. Furthermore, cybersecurity is a growing application area for Business Intelligence (BI) process expansion [2]. The case for cybersecurity information as a component of critical business information is well established. We know that cybersecurity concerns impact customer trust and market growth. For example, a 2018 study found that information privacy concerns are significant sources of impedance on consumer and firm adoption of healthcare information exchanges [3]. In addition, investors demonstrate a preference for publicly traded companies that make proactive cybersecurity investment decisions and announcements [4]. This makes clear the necessity for the tools, infrastructure, and processes of BI to include the identification and analysis of cybersecurity risks. Despite this demonstrated need for proactive cyber information in BI, the community often discovers the business was at risk only after the report of a cyber breach. Therefore, we consider three regulatory regimes as BI discovery opportunities and conduct case studies of five historical cyberattacks to explore the potential for the penetration test (pentest) method to provide useful Business Intelligence.

II. Pentesting

Penetration Testing (pentesting) is a method that systematically evaluates risks to an enterprise's information systems. To do this, an organization intentionally invites skillful cybersecurity professionals to attack some portion of their information systems environment. In popular practice, these professionals are known as *pentesters*, *ethical hackers*, *red teamers*, and *white-hat hackers*.

The pentest method consists of five main phases: planning, scanning, execution, analysis, and output [5]. These phases are depicted in Figure 1.

During the **planning** phase, pentesters and organizational leadership decide on the type of pentest, attack scope and selection of threat models. The information available to the pentester and the techniques they will employ vary somewhat across the different types of pentest–such as white-box, black-box, and double-blind tests–as well as the systems under investigation [6].

Pentesters systematically enumerate vulnerabilities for all in-scope systems during the **scanning** phase. Of note, there is increasing evidence of attackers deploying automation systems to rapidly discover vulnerabilities [7], [8]. Those automation tools are also available to defenders and that availability suggests potential for BI systems integration.

In the **execution** phase, pentesters exploit those vulnerabilities to determine which of the potential avenues for attack present actual risks to the enterprise's information systems. Attack automation is also the subject of ongoing research [9].

The **analysis** phase considers the risks to the information systems relative to the organizational mission and potential for business impact. Analysis that considers how pentest results would integrate with the organizational risk register is consistent with recent cybersecurity auditing research recommendations [10].

Pentests conclude with the **output** phase, which generates and presents risk-prioritized recommendations for remediation usually in the form of a report and debrief between the pentesters and the organization's technical team. These reports include artifacts from the test to demonstrate proof of compromise, as well as references to improve defenses against the attacks that were successful [11].

Our practical experience conducting more than 100 pentests through the Eaton Cybersecurity SAFE Lab,[1] as well as over-

[1] https://www.rit.edu/cybersecurity/eaton-cybersecurity-safe-lab

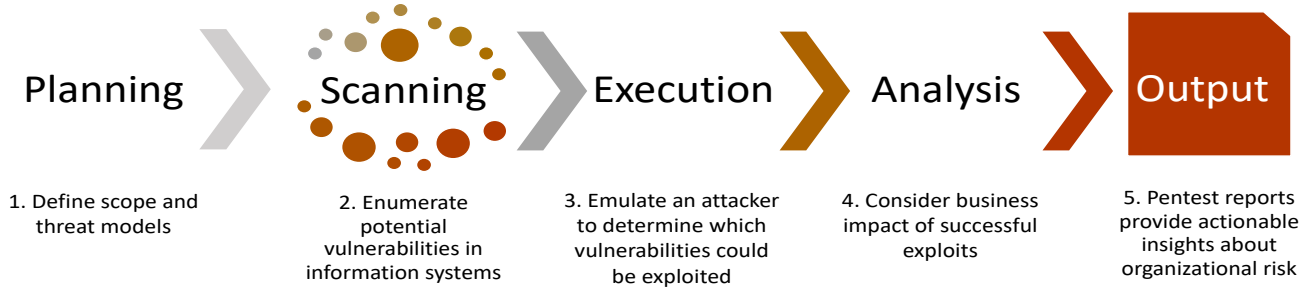

Fig. 1: Penetration tests (pentests) provide actionable insights that can inform decisions about risk.

seeing the global Collegiate Penetration Testing Competion,[2] suggest that best practices in pentesting include:

1) sourcing pentests from a third-party organization,
2) including compliance managers in the scoping and output phases of the test, and
3) conducting pentests on a regular basis instead of as a one-time solution.

Ongoing cybersecurity research has demonstrated potential for applied artificial intelligence that will support or entirely automate pentest Planning, Scanning, and Execution [12], [13], [14]. This suggests that the pentest method can regularly inform Business Intelligence (BI) systems at scale. To consider this potential, we employ two sets of case studies to evaluate the *i.* regulatory mandate for pentest data, and *ii.* the potential impacts of those data if they had been included in BI systems prior to historical breaches.

III. Methodology for this Study

According to Ain, Vaia, DeLeone, and Waheed (2019), the case study is the most popular qualitative research method for Business Intelligence (BI) literature and comprises nearly 11% of all BI studies [15]. Accordingly, we perform a case study of three security standards that require pentesting. In Section IV, we analyze the value of the data required by those regulations. We also perform five historical breaches to determine what, if any, benefit pentesting may have had as a component of BI systems. We report these findings in Section V.

In selecting the cases for examination, we sought a conceptually representative sample to demonstrate the potential application of the pentest method as a data source in BI. We therefore followed the recommendations for *diverse sampling* in Seawright and Gerring's 2008 seminal work [16]. We chose three security standards that exemplify a range of legislative authorities–multinational, national, and state/regional–that require pentest data. We also chose five historical cases that exemplify a range of breach impacts to include compromise of personally identifying information, stock price declines, net income and market capitalization reductions, fees, fines, and elevation of geopolitical tensions.

The next two sections describe our findings and analysis of *i.* example security regulations and standards that mandate generation of pentest data, and *ii.* historical cases that could have included pentest data as a BI data source.

IV. Security Regulations and Standards

Regulatory compliance is a mechanism that can fuel data-driven Business Intelligence (BI). Previous research considers the role of big data BI for bank risk analysis [17], and current technical methods exist that translate compliance with regulations as additional dimensions of BI [18], [19]. Extending this research thrust, we describe here the scope, pentesting techniques, best practices, and recommendations for pentests relative to three cybersecurity regulations that require penetration testing: PCI-DSS, GLBA, and 23-NYCRR-500. There are other regulations that demand pentests, but we selected these three because they span the meta-regulatory (PCI-DSS), national (GLBA), and state (23-NYCRR-500) levels. Together, they illustrate the potential data that compliance regimes can make available to BI systems and processes. The remainder of this section is organized with a brief overview of each regulation, followed by a description of how much of the pentesting process is required by the regulation (**scope**), which **pentesting techniques** are generally most likely to generate useful insights to the BI processes, the **best practices** suggested by the regulation, and **recommendations** for incorporation of the pentest output to support BI processes.

Table I provides an outline of the three regulations described in this section.

A. PCI-DSS

Payment Card Industry Data Security Standard (PCI-DSS) is an international meta-regulation that has been introduced to protect customer's credit/debit card information. Even though

[2] For more information about the Collegiate Penetration Testing Competition, visit https://cp.tc/. Exemplar pentest reports are available at https://github.com/globalcptc/report_examples and exemplar presentations are available at https://youtube.com/playlist?list=PL16dKj3xTAakLEnX3xTydXsZiHC5Hpj4S

Sample regulations requiring pentests			
Regulation	Type	Scope	Reference
PCI-DSS	International meta-regulation	Applies to all industries, limited to cardholder data environment	[20]
GLBA	National regulation	Applies to U.S. financial industry	[21]
23-NYCRR-500	State regulation	Applies to New York State financial industry	[22]

TABLE I: Example compliance regimes at the international, national, and state levels that require pentests.

it has been active for over a decade, penetration testing has recently been incorporated into the compliance requirements for the standard. It is introduced in PCI DSS version 3.2 as PCI requirement 11.3.4.1. According to the new pentesting requirement, service providers are now required to perform segmentation testing every six months or upon any crucial change in the segmentation methods or controls.

Scope. The standards set forth in PCI-DSS require both internal and external testing to understand the scope of networks and validate the controls that are involved to isolate the cardholder data environment (CDE) from the external environment. Pentesters test the network, applications, and software of any systems that are connected to the CDE [23]. It involves all the pentesting steps with specific requirements for scanning, finding vulnerabilities, exploiting them, exfiltrating data and providing a report in the end.

Pentesting Techniques. In order to be in compliance with PCI-DSS, an organization must have a supporting environment such as domain controllers, firewalls, intrusion prevention systems, intrusion detection systems, patch management or other security controls be protecting the CDE [24]. Everything else interacting with the supporting environment and CDE should be strictly segmented through access controls, restrictions, authentication, and authorizations. This is intended to reduce the impact of a data breach by denying lateral movement if an attacker is able to establish a foothold.

PCI-DSS version 3.2 introduces another important requirement: vulnerability scanning (requirement 11.2). Scanning is generally automated and provides minimal information about potential vulnerabilities [25]. Performing penetration testing on the information gained from a vulnerability scan provides a proof of that the vulnerability is exploitable and eliminates false positives. It also helps to understand the real-world security attacks and risks involved.

Best Practices. Before considering the system provider to be PCI-DSS compliant, organizations must address all the vulnerabilities found by either remediating them or applying required security controls. By discussing the risk, impact and probability of the exploit, the report incorporates risk calculators such as common vulnerability scoring system. Few additional low risk findings can be remediated through changing the infrastructure or applying code changes. The report should include other documentation to be submitted to Quality Security Assessor (QSA). It is the QSA's decision to certify a company as PCI-DSS compliant, after they have come to the belief that there are necessary defenses to protect against the security risks.

Recommendations. PCI-DSS should be considered the minimum degree of security for credit and debit card transactions. It only deals with networks, systems, and applications that deal with payment information and nothing else. Hence it is necessary to focus on different gray areas such as malicious HTTP beaconing, malicious software, and business email compromise that could be used as a staging ground for an attack against the CDE. The specificity provided by a comprehensive pentest output could extend the utility of PCI-DSS compliance audits for BI purposes. Furthermore, nearly every company and industry accepts payment cards and is therefore within the scope of PCI-DSS. This ubiquity, combined with the requirement for pentests at least every six months, make PCI-DSS related pentest outputs particularly promising for widespread inclusion in BI systems.

B. GLBA

The Gramm-Leach-Bliley Act (GLBA) is required for financial organizations to protect the customer's privacy. One of the important requirements of GLBA is to perform regular risk assessment of customer information. Assessment under GLBA includes discovering the threats, analyzing the likelihood of those vulnerabilities being exploited, and enabling defense mechanisms to protect against them [26]. It is also necessary to provide a report to the higher authorities on a regular basis.

Scope. When performing penetration testing to be compliant for GLBA, the actions undertaken are similar to any other penetration testing [27]. Testing also includes social engineering attacks to expose the existing technical-personnel gaps. Through testing under GLBA, organizations can identify how closely the architecture and configuration accord with vendor guidelines.

Pentesting Techniques. The risk assessment process includes various steps that are taken from the Federal Financial Institutions Examination Council (FFIEC) information technology examination handbook. The FFIEC advises multilayered security to protect the data. Before performing risk assessments, penetesters must obtain the list of assets such as software, hardware, applications and data. Maintaining this asset inventory will help classify the devices and analyze the risk. Once the assets are classified, threats related to them can be gathered. Threats may include insider attacks, vulnerabilities, failure to patch the systems, or anything resulting in valuable information being exposed to attacks from hackers. Through gathering all the information required, pentests examin the organization's network, applications, software, and hardware.

Best Practices. The goal of risk assessment under GLBA is to understand the assets available in the environment and to

identify the vulnerabilities associated with those assets. This emphasizes the planning and scanning phases of pentests under GLBA. A pentester should validate a full enumeration of assets and vulnerabilities, and then test and analyse the risks that might affect the security of the environment. This will help to define security controls and improve the security posture of the organization.

Recommendations. GLBA supports previously developed security controls and improves them by requiring penetration testing [28]. Through the pentest report, an organization can regularly evaluate the risks presented by new technologies added to the organization's asset list. GLBA also advises that organizations provide physical security to protect the hardware that supports the electronic data, which could be useful support to conventional loss protection information.

C. 23-NYCRR-500

New York Department of Financial Services CyberSecurity Regulation-500 (23-NYCRR-500) is a set of regulations and minimum standards introduced by state of New York in 2017. That set of regulations is intended to protect financial companies from security breaches. It applies to any organization that deals with finance, mortgage or banking in New York state. In order to be considered compliant, organizations are required to perform risk assessment and review their security posture which includes all their software, hardware, web applications, and any other internet connected electronic device.

Scope. The cybersecurity program required by 23-NYCRR-500 must maintain information systems' confidentiality, integrity and availability. The scope of testing must include an assessment of internal and external security risks that may affect the confidential information stored in the systems.

Pentesting Techniques. 23-NYCRR-500 includes monitoring and testing the environment on a scheduled timeline. Risk assessments mandated by 23-NYCRR-500 are designed to support the organization's security program. Risk assessments under 23-NYCRR-500 include regular penetration testing and vulnerability management of all assets. Further, 23-NYCRR-500 suggests annual testing and bi-annual vulnerability analysis. This will provide valuable risk information about the organization's information systems, and requires prioritized risks according to the severity of the potential compromise and the criticality of the information system to the organization [22].

Best Practices. 23-NYCRR-500 focuses on protecting the nonpublic information of the financial organizations in New York State. It is necessary to assess all the assets that have contact with the confidential data. The pentest report helps the organization develop and refine its security policy. Data governance, access controls, system and network security, monitoring, customer data privacy, and incident response should be implemented throughout the organization's governance and policies in response to the specific prioritized risks described in the pentest report.

Recommendations. With the impact of security breaches heavily focusing on financial organizations, 23-NYCRR-500 provides a strong baseline to develop a security program. It suggests testing to better secure applications, control access privileges, perform risk assessments, and prepare an incident response plan. These components would further extend the value of pentest outputs to support organizational BI.

V. Historical Cases

There are several historical cases that demonstrate the potential application of the pentest outputs for better-informed business decisions. In this section, we consider five diverse breaches that might have been prevented by the incorporation of pentest data in the organization's Business Intelligence (BI) processes. In Table II, we summarize the cases, including the business risk intelligence that a pentest might have informed and the breach impacts that could have been avoided.

A. Equifax

Equifax is one of the largest data analytics companies that monitors credit scores and helps individuals and organizations make decisions. In September 2017, they encountered a security breach that leaked the sensitive data of over 148 million American citizens. This leak included names, credit card numbers, addresses, Date of Birth, Social Security Numbers and driver's license numbers [52]. Though there were larger security breaches in the past, the sensitivity of the data that Equifax held and the business impacts make it an appropriate case for consideration.

Breach Description. The security breach on Equifax was due to a vulnerability on the Apache struts (CVE-2017-5638)[3] installed on an automated consumer information system. Struts is a Java Web Application framework maintained by Apache. The vulnerability was never patched, though the internal security team ran scans to discover the vulnerability. On July 29th, 2017 suspicious network traffic had been discovered and two days later led to a distributed denial of service attack on web applications. Through hiring forensic investigators from Mandiant, it came into light that more than 145 million customers data had been exfiltrated by attackers. Further investigation revealed that the breach also impacted international customers from Canada and the UK. Equifax was one of the largest security breaches happened at the time. The report demonstrated that attackers were in the environment for weeks or months, and performed various actions that might have been detected or prevented. One of the requirements of PCI-DSS is File Integrity Monitoring. Daily monitoring may have helped to catch the suspicious behaviour happening in the environment even though it was happening stealthily. If Equifax was GLBA compliant, the organization would have had to perform risk assessment on a daily basis and through that, the Apache Struts vulnerability probably would have been discovered and patched, along with all the expired secure

[3] https://nvd.nist.gov/vuln/detail/cve-2017-5638

Historical Case	Year	Compliance Standard	Testing Target	Description of Business Risk Intelligence	Breach Impact	Reference
Equifax	2017	GLBA, 23-NYCRR-500	Web Application, Network	Use of expired SSL Certificates while transmitting CDE data. Data was sniffed from the network by attackers.	Net income down 27%, market capitalization dropped $5.3billion, paid $127million in legal fees	[29], [30], [31], [21], [26], [27], [28]
JP Morgan Chase	2014	GLBA, PCI-DSS, 23-NYCRR-500	Network	Failure to develop and maintain secure systems. Attackers exploited a known vulnerability (Hearbleed).	Lost personally identifying information for 76 million households and 7 million small businesses, increased cyber expenditures by $250million	[32], [33], [34], [35], [36], [37]
Global Payments	2012	PCI-DSS	Network	Failed to continuously monitor network logs. Attackers were active on the network for 13 months.	Lost at least 1.5 million credit card numbers, paid $60million in remediation fees and $36million in fines	[38], [39], [40], [41], [42]
NASDAQ	2010	GLBA, PCI-DSS, 23-NYCRR-500	Web Application	Failure to implement a firewall or store critical data behind a firewall. Attackers accessed the *Directors Desk* application remotely.	Geopolitical incident caused systemic concern about entire U.S. financial industry; malware reportedly built by Russian spy agency	[43], [31], [44], [45], [46]
Heartland Payment Systems	2009	PCI-DSS	Web Application	Failed to restrict card holder data to a "need to know" basis as per PCI-DSS.	Stocks down 78%, paid $170million in fines, and lost ability to process MasterCard and Visa payments	[47], [48], [49], [50], [51]

TABLE II: Five historical cases where pentest outputs as a Business Intelligence data source could have informed better business decisions.

sockets layer (SSL) certificates that contributed to the breach [53].

Breach Impact. The Equifax security breach could have been prevented through taking basic security steps such as patching, renewing security certificates, and implementing accurate security controls. It impacted both the company and customers involved in it. Equifax net income fell by 27%, market capitalization dropped by $5.3billion, and the organization paid $127million in legal fees [29]. In addition, many customers encountered credit card frauds [54].

Findings. An external pentest would almost certailny have caught misconfigurations and vulnerabilities in the environment [52]:

1. Once the Apache struts vulnerability was exploited, attackers uploaded 30 web shells across the network. Through scanning the network, a pentester would have recognized all the outdated versions running in the environment, and made a list of vulnerable services. The Apache struts vulnerability was well known and commonly exploited back then and as it was not patched, pentesters could have exploited it and reported it.
2. More than 320 of SSL certificates belonging to Equifax were expired by that time. Basic risk assessment or network penetration testing would have helped the organization realize their controls were insufficient to secure the network traffic.
3. Attackers sent more than 9000 queries to 48 databases and successfully exfiltrated unencrypted personal information of customers. Web application pentesting involves finding exploitable features in the available applications. Attackers were able to query more than 48 databases, by performing a sql-injection attack, which pentesters might have found first and the organization could have fixed.
4. Attackers later transferred the exfiltrated data through Equifax's Automated Consumer Interview System and the suspicious network was not detected due to expiration of a security certificate. The certificate had been expired for over 19 months. Pentesting outputs would have helped to realize the basic misconfigurations that went unnoticed within the organization.

B. JP Morgan Chase

A cyberattack on JP Morgan Chase left open more than 76 million user accounts [35]. Along with that they also compromised 7 million small business accounts. Similar to other security breaches, information comprised of addresses, email ids, usernames and passwords. Attack affected the users who use web and mobile apps of Chase and JP Morgan [36].

Breach Description. The attack happened in 2014, and was one of the largest security breaches at the time. The resulting investigation disclosed that Heartbleed was one of the vulnerabilities that allowed attackers to get into the environment. Reports reveal that the company did not enable two-factor authentication on one of the network servers. Attackers had been in the environment since June but discovered this misconfiguration in July [37]. Attackers created a roadmap to

the available applications and vulnerabilities linked to each. Attackers then escalated their privileges to gain administrative rights to many servers in the environment.

Breach Impact. The company had to swap all of its software and application with new licensing deals. Reconstructing their security controls to protect against attacks in the future cost JP Morgan Chase around $250 million [32], [34].

Findings. JP Morgan Chase must comply with PCI-DSS, GLBA, and 23-NYCRR-500, among other regulations. The breach investigation report revealed that the Heartbleed vulnerability probably provided an initial foothold. Attackers then moved laterally through the network. The Heartbleed vulnerability is associated versions of secure sockets layer (SSL) encryption that were outdated at the time of the attack. A pentest would have discovered outdated implementations of SSL and recommended update to prevent the exploit [33].

C. Global Payments

Initial reports about the Global Payments security breach revealed a spillage of nearly 1.5 million consumers' information such as credit card numbers, names, addresses and driver's license numbers. As the investigation proceeded, it was revealed that the damage was far more extensive than originally suspected. Attackers stole more than 10 million credit and debit cards over a period of one month in January and February of 2012.

Breach Description. Investigation revealed that the database that stores the private information of the customers had been breached. Reports said that track 1 and track 2 data had been stolen. Track 1 data contained credit card information such as primary account number, name, service code, expiration data. Track 2 data contains payment card verification value (CVV) codes but omits usernames. This means that track 1 data allows attackers to counterfeit the new cards, and attackers can use track 2 data for fraud. According to the attackers, they had full criminal control over the company's network [39]. Though the company had been performing end-to-end encryption, it was not enough to protect against external attackers. Hackers had been sitting on the network for over 13 months and gathering more than 24 million transactions before they were caught. As a company that provides payment solutions, Global Payments should have been compliant with PCI-DSS [38]. After the security breach, the company informed the public that they hired a Qualified Security Assessor to perform a PCI-DSS review on all the information systems.

Breach Impact. Global Payments hired a security assessor to perform independent review against their environment for PCI-DSS compliance. They paid $60 million for the security investigation, incentives, identity protection insurance and remediations for the breach. They paid another $35.9 million under fraud loses and other fines imposed by credit card networks. Along with that, payment processors Visa and Mastercard removed Global Payments Inc., from their list of approved service providers [41].

Findings. The breach report concluded that attackers were on the network for over 13 months gathering information [40]. If the company had previously performed network penetration testing to analyze the risk of network traffic sniffing or a man-in-the-middle attack, they would have understood the shortcomings of their network security and how security controls might have prevented data exfiltration from the environment. Pentesting probably also would have revealed the potential for lateral movement and privilege escalation, which could have helped to mitigate the impact of the breach.

D. NASDAQ

NASDAQ is one of the largest stock exchange organizations in United States. Interestingly, hackers breached into the network but did not attack the trading platform. Instead, the attackers targeted insider information. There was no evidence that attackers exfiltrated any customer data. Reports claim that to achieve their goal, hackers exploited a web application that is used for insider communication, called the "Director's Desk" [44]. NSA and top firms were involved in the investigation of the attack and the organization ultimately reported that the trading platform was completely inaccessible from internet facing applications like Director's Desk [55].

Breach Description. During routine monitoring, NASDAQ reportedly discovered malware acting as a command and control servers on the Directors Desk's network. According to the investigations, it is probable that attackers exploited the Director's Desk product to gain a foothold on the network. Another assumption is that attackers got control over the network through a phishing email clicked by an executive [45]. Through this, they were able to access confidential documents and communications between directors. NASDAQ is the second largest American stock exchange company. NASDAQ handles 19% of stock tradings compared to New York stock exchange's 27%. It deals with incredible amounts of confidential data on everyday basis. Such an amount of confidential data would almost certainly be covered by both GLBA and 23-NYCRR-500 today.

Breach Impacts. Security breaches have had a long term affect on the stocks. The compromise of the Directors Desk communication platform between executives may have spilled critical data such as reports, financial documentation, and planning documents for more than 10,000 board members from many Fortune 500 companies [46]. This security breach, and the assessed attribution to Russian spy services, became a geopolitical concern about the stability of U.S. financial markets [47].

Findings. It is clear that the Directors Desk application played a key role in this security breach. It is considered one of the most important assets of NASDAQ, as it is a communication application for executive members that work with NASDAQ. There had been reports that attackers were able to exploit this web application either due to a sql-injection attack or through session hijacking [44]. Network penetration testing and web application penetests would have helped to avoid such incidents.

E. Heartland Payment Systems

On May 8th, 2009, Heartland Payment Systems (HPS) suffered a security breach revealing data about their payroll customers. Though the accurate details about the customer data that was compromised was never released, it is believed that HPS was making more than 100 million transactions per month [49]. Attackers created malicious software (malware) that was active for four months on the network, observing and collecting personally identifiable information (PII) of customers.

Breach Description. Though HPS quickly found and attempted to mitigate the malware, it continued to be active for almost four months. During this period of time, the malware laterally moved from the corporate network to payment processing network, while HPS believed the malware to be mitigated. Though it was approved as PCI compliant, and their internal investigations revealed no evidence of malware according to HPS, they later discovered that the malware was still persistent on their systems. Reports revealed that databases containing PII had not been properly encrypted, which exacerbated the breach. Organizations such as Heartland Payment Systems that process payments are required to be compliant with PCI-DSS. One of the requirements of PCI-DSS is to continuously monitor the network and test the information systems and processes. Through following the guidelines required to be compliant, HPA was responsible for monitoring the logs and evaluating the security on daily basis [50].

Breach Impact. Stocks plummeted 78% after the security breach. They were removed as the service providers from MasterCard and Visa. In addition, HPS paid $170 million in fines [47].

Findings. Investigations revealed that attackers made their initial foothold through a sql-injection attack, then uploaded malicious software for persistence. Performing web application testing on the publicly facing and internal web applications would help to find and remediate susceptibility to attacks such as sql-injection, cross site scripting, extensible markup language (XML) external entity attacks [48].

VI. Conclusions and Discussion

Penetration testing techniques will vary based on each organization's requirements and the technology in use. Similarly, it is reasonable that Business Intelligence (BI) data sources are tuned to the needs of the organization. In aggregate, our examination of five historical case studies relative to three compliance regimes suggests that the pentest method is likely to provide useful business risk intelligence. Given the breach impacts in each of the historical cases, it seems clear that pentest outputs should inform business decisions about security program investments. We also found that pentest reports required by the Payment Card Industry Data Security Standard (PCI-DSS) are probably an especially useful data source for systemic inclusion because PCI-DSS is ubiquitous and demands frequent tests.

A. Limitations

We did not consider a fully representative sample of breaches, and those breaches we did consider are subject to availability bias. Because of this, our study does not conclusively describe the potential for pentest outputs to inform prevention of breaches of all types as a forward-looking indicator.

Also, we did not consider a fully representative sample of regulations that demand pentests, and those standards and regulations we did consider are mostly specific to the United States. It is useful to remember, too, that many prominent standards and regulations may interpret the process for and requirements of pentests in a way that leads to limited testing in practice. This could create false confidence and, if substandard pentest outputs are integrated in BI systems, it could dampen other important signals of risk.

B. Future Work

The ongoing integration of pentest outputs into BI systems–especially amid automation advances in the planning, scanning, and execution phases–is likely to yield promising opportunities for future work. More specifically, we recommend a proof of concept BI system that integrates automated pentest phase outputs relative to other BI data sources. This recommendation is consistent with Liang and Liu's 2018 findings that the horizons of BI and big data research include security and privacy applications [56]. Such a system could simultaneously support the automation of pentest analysis and the validation of regulatory compliance.

VII. Acknowledgements

This research was funded in part by ongoing activities in the Eaton Cybersecurity SAFE lab at Rochester Institute of Technology's ESL Global Cybersecurity Institute. J.M. Pelletier would also like to acknowledge the support he has received from the *Ordo Praedicatorum*.

References

[1] H. Baars, C. Felden, P. Gluchowski, A. Hilbert, H.-G. Kemper, and S. Olbrich, "Shaping the next incarnation of business intelligence," *Business & Information Systems Engineering*, vol. 6, no. 1, pp. 11–16, 2014.

[2] S. M. Tisdale, "Cybersecurity: Challenges from a systems, complexity, knowledge management and business intelligence perspective." *Issues in Information Systems*, vol. 16, no. 3, 2015.

[3] P. Esmaeilzadeh, "The effects of public concern for information privacy on the adoption of health information exchanges (hies) by healthcare entities," *Health communication*, 2018.

[4] S. Chai, M. Kim, and H. R. Rao, "Firms' information security investment decisions: Stock market evidence of investors' behavior," *Decision Support Systems*, vol. 50, no. 4, pp. 651–661, 2011.

[5] D. Garg and N. Bansal, "A systematic review on penetration testing," in *2021 2nd Global Conference for Advancement in Technology (GCAT)*. IEEE, 2021, pp. 1–4.

[6] P. Vats, M. Mandot, and A. Gosain, "A comprehensive literature review of penetration testing & its applications," in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*. IEEE, 2020, pp. 674–680.

[7] B. S. Meyers, S. F. Almassari, B. N. Keller, and A. Meneely, "Examining penetration tester behavior in the collegiate penetration testing competition," *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 31, no. 3, pp. 1–25, 2022.

[8] N. Munaiah, A. Rahman, J. Pelletier, L. Williams, and A. Meneely, "Characterizing attacker behavior in a cybersecurity penetration testing competition," in *2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*. IEEE, 2019, pp. 1–6.

[9] S. Y. Enoch, Z. Huang, C. Y. Moon, D. Lee, M. K. Ahn, and D. S. Kim, "Harmer: Cyber-attacks automation and evaluation," *IEEE Access*, vol. 8, pp. 129 397–129 414, 2020.

[10] O. M. Al-Matari, I. M. Helal, S. A. Mazen, and S. Elhennawy, "Integrated framework for cybersecurity auditing," *Information Security Journal: A Global Perspective*, vol. 30, no. 4, pp. 189–204, 2021.

[11] H. M. Z. Al Shebli and B. D. Beheshti, "A study on penetration testing process and tools," in *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, 2018, pp. 1–7.

[12] V. Casola, A. D. Benedictis, M. Rak, and U. Villano, "A methodology for automated penetration testing of cloud applications," *International Journal of Grid and Utility Computing*, vol. 11, no. 2, pp. 267–277, 2020.

[13] D. R. McKinnel, T. Dargahi, A. Dehghantanha, and K.-K. R. Choo, "A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment," *Computers & Electrical Engineering*, vol. 75, pp. 175–188, 2019.

[14] V. Casola, A. De Benedictis, M. Rak, and U. Villano, "Towards automated penetration testing for cloud applications," in *2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. IEEE, 2018, pp. 24–29.

[15] N. Ain, G. Vaia, W. H. DeLone, and M. Waheed, "Two decades of research on business intelligence system adoption, utilization and success–a systematic literature review," *Decision Support Systems*, vol. 125, p. 113113, 2019.

[16] J. Seawright and J. Gerring, "Case selection techniques in case study research: A menu of qualitative and quantitative options," *Political research quarterly*, vol. 61, no. 2, pp. 294–308, 2008.

[17] N. Rahman and S. Iverson, "Big data business intelligence in bank risk analysis," *International Journal of Business Intelligence Research (IJBIR)*, vol. 6, no. 2, pp. 55–77, 2015.

[18] O. Akhigbe, D. Amyot, and G. Richards, "A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance," *Requirements Engineering*, vol. 24, no. 4, pp. 459–481, 2019.

[19] O. Badreddin, G. Mussbacher, D. Amyot, S. A. Behnam, R. Rashidi-Tabrizi, E. Braun, M. Alhaj, and G. Richards, "Regulation-based dimensional modeling for regulatory intelligence," in *2013 6th International Workshop on Requirements Engineering and Law (RELAW)*. IEEE, 2013, pp. 1–10.

[20] P. security standards council, "Securing the Future of Payments Together," Accessed: May 15, 2019. [Online]. Available: https://www.pcisecuritystandards.org/n

[21] J. D. Groot, "What is GLBA Compliance? Understanding the Data Protection Requirements of the Gramm-Leach-Bliley Act in 2019," Accessed: May 20, 2019. [Online]. Available: digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act

[22] "What is the 23 NYCRR 500 Regulation," Accessed: May 16, 2019. [Online]. Available: www.cspi.com/what-is-23-nycrr-500-blog/

[23] "5 Things You Should Know about PCI DSS Penetration Testing," Accessed: May 18, 2019. [Online]. Available: www.tripwire.com/state-of-security/regulatory-compliance/pci/5-things-know-pci-dss-penetration-testing/

[24] C. Horton, "New 3.2 Requirements For Penetration Testing And Segmentation: What You Don't Know," Accessed: May 16, 2019. [Online]. Available: www.securitymetrics.com/blog/new-32-requirements-penetration-testing-and-segmentation-what-you-dont-know

[25] J. Kersten, "Overdue on New PCI Penetration Testing Requirements? What You Need to Know About PCI Requirement 11.3.4.1," Accessed: May 19, 2019. [Online]. Available: kirkpatrickprice.com/blog/new-pci-requirement-11-3-4-1-new-penetration-testing-requirements/

[26] B. Hickey, "How to Comply with the GLBA Act — 10 Steps," Accessed: May 16, 2019. [Online]. Available: resources.infosecinstitute.com/how-to-comply-with-the-glba-act-10-steps-2/#gref

[27] "GLBA Compliance ," Accessed: May 17, 2019. [Online]. Available: www.csiweb.com/industries-we-serve/financial-institutions/regulatory-compliance/federal-regulations/glba-compliancel

[28] K. Bong, "Conducting an electronic information risk assessment for Gramm-Leach-Bliley Act compliance." Accessed: May 16, 2019. [Online]. Available: www.sans.org/reading-room/whitepapers/auditing/conducting-electronic-information-risk-assessment-gramm-leach-bliley-act-compliance-1053

[29] R. A. Spinello, "Corporate data breaches: A moral and legal analysis," *Journal of Information Ethics*, vol. 30, no. 1, pp. 12–32, 2021.

[30] D. Kolevski, K. Michael, R. Abbas, and M. Freeman, "Cloud computing data breaches: A review of us regulation and data breach notification literature," in *2021 IEEE International Symposium on Technology and Society (ISTAS)*. IEEE, 2021, pp. 1–7.

[31] E. J. Hyla, "Corporate cybersecurity: The international threat to private networks and how regulations can mitigate it," *Vand. J. Ent. & Tech. L.*, vol. 21, p. 309, 2018.

[32] S. Dongre, S. Mishra, C. Romanowski, and M. Buddhadev, "Quantifying the costs of data breaches," in *International Conference on Critical Infrastructure Protection*. Springer, 2019, pp. 3–16.

[33] I. Agrafiotis, J. R. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, no. 1, p. tyy006, 2018.

[34] A. A. Hall and C. S. Wright, "Data security: A review of major security breaches between 2014 and 2018," *Federation of Business Disciplines Journal*, vol. 6, pp. 50–63, 2018.

[35] "JPMorgan Chase Hacking Affects 76 Million Households," Accessed: May 21, 2019. [Online]. Available: dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?mtrref=undefined&gwh=7DCD608D54C726A9B8AE10C60D692091&gwt=pay

[36] J. Roman, "Chase Breach Affects 76 Million Households," Accessed: May 16, 2019. [Online]. Available: www.bankinfosecurity.com/chase-breach-affects-76-million-households-a-7395

[37] "Neglected Server Provided Entry for JPMorgan Hackers," Accessed: May 20, 2019. [Online]. Available: dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/?mtrref=undefined&gwh=A501573D2A5C52FD75E8CA3D53EFEFD4&gwt=pay

[38] D. DeMille, "Global Payments Security Breach," Accessed: May 18, 2019. [Online]. Available: www.asecurelife.com/online-security/global-payments-security-breach/

[39] "Global Payments Data Breach Exposes 1.5M Consumers' Card Info," Accessed: May 16, 2019. [Online]. Available: risnews.com/global-payments-data-breach-exposes-15m-consumers-card-info

[40] "Global Payments: Breach Contained, But Damage Done," Accessed: May 20, 2019. [Online]. Available: www.esecurityplanet.com/hackers/global-payments-breach-contained-but-damage-done.html

[41] M. Lemieux, "Cyber crime, governance and liabilities in the banking and payment industries," *Banking & Finance Law Review*, vol. 31, no. 1, p. 113, 2015.

[42] J. Black, "Developments in data security breach liability," *The Business Lawyer*, vol. 69, no. 1, pp. 199–207, 2013.

[43] N. Sangani, "Cybersecurity and its impact on the financial services industry," *NY Business Law Journal*, p. 48, 2017.

[44] T. T. Joe SaluzziSal Arnuk, "The Security Breach At NASDAQ Was Really Scary Because Of What It Reveals About The Way Our Stock Exchange Works," Accessed: May 21, 2019. [Online]. Available: www.businessinsider.com/hackers-at-the-nasdaq-2011-2

[45] T. Kitten, "NASDAQ Breach: You Should be Concerned," Accessed: May 16, 2019. [Online]. Available: www.bankinfosecurity.com/blogs/nasdaq-breach-you-should-be-concerned-p-877

[46] K. Zetter, "NSA TO INVESTIGATE NASDAQ HACK," Accessed: May 20, 2019. [Online]. Available: www.wired.com/2011/03/nsa-investigates-nasdaq-hack/

[47] F. Quader and V. P. Janeja, "Insights into organizational security readiness: Lessons learned from cyber-attack case studies," *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 638–659, 2021.

[48] "A Famous Data Security Breach PCI Case Study: Four Years Later," Accessed: May 16, 2019. [Online]. Available: www.secureworks.com/blog/general-pci-compliance-data-security-case-study-heartland

[49] "Heartland Payment Systems Suffers Data Breach," Accessed: May 20, 2019. [Online]. Available: www.forbes.com/sites/davelewis/2015/05/31/heartland-payment-systems-suffers-data-breach/#2cb6f4a8744a

[50] T. Martin-Vague, "Lessons from the Heartland Payment Systems data breach, redux," Accessed: May 16, 2019. [Online]. Available: www.csoonline.com/article/2935814/lessons-from-the-heartland-payment-systems-data-breach-redux.html

[51] "Heartland Payment Systems Suffers Data Breach," Accessed: May 20, 2019. [Online]. Available: www.forbes.com/sites/davelewis/2015/05/31/heartland-payment-systems-suffers-data-breach/#2cb6f4a8744a
[52] "Equifax Data Breach," Accessed: May 16, 2019. [Online]. Available: epic.org/privacy/data-breach/equifax/
[53] "The Congressional Report on Equifax Hack," Accessed: May 16, 2019. [Online]. Available: www.sans.org/security-awareness-training/blog/just-released-congressional-report-equifax-hack
[54] Z. Whittaker, "Equifax breach was 'entirely preventable' had it used basic security measures, says House report," Accessed: May 18, 2019. [Online]. Available: techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/
[55] T. Team, "Nasdaq breach points to growing security needs," Apr 2011. [Online]. Available: https://www.nasdaq.com/articles/nasdaq-breach-points-growing-security-needs-2011-04-05
[56] T.-P. Liang and Y.-H. Liu, "Research landscape of business intelligence and big data analytics: A bibliometrics study," *Expert Systems with Applications*, vol. 111, pp. 2–10, 2018.