# **INFORMATION SECURITY BREACHES, INTERNAL CONTROLS**

# **AND RELATED LEGISLATION**

**By**

**Teresa K. Lang, PhD., CPA, CISA**

**Auburn University Montgomery**

**tlang@aum.edu**

**Rita C. Jones, PhD., CMA**

**Troy University**

**ritajones@troy.edu**

# **ABSTRACT**

In 2002, the passage of Sarbanes-Oxley (SOX) was supposed to protect the public by changing the reporting requirements in financial statement audits. Management and auditors were to attest to the existence and effectiveness of internal controls over financial data, and that would supposedly “fix” the problem. Recent disclosures of business practices at two companies who were victims of cybercrimes—Target and JPMorgan Chase—bring to light a lack of proper internal controls over the financial data they collect. This paper discusses information security, internal controls, and SOX, as well as concerns of why current internal control policies are not effective in securing information. Lastly, it is important to note the most recent legislation enacted in an attempt to improve information security.

# **INFORMATION SECURITY BREACHES, INTERNAL CONTROLS**

# **AND RELATED LEGISLATION**

**INTRODUCTION**

Target Corporation released to the general public in December 2013, that there had been an information security breach in their system. Hackers stole the payment card numbers of at least 70 million shoppers (Prah, 2014). As of February of 2016, the costs related to the data breach exceeded $290 million, with an expected offset by insurance recoveries of $90 million (Target-2015-Annual-Report). Further, if the government investigation had found Target guilty of noncompliance with industry-specific information security standards, the company could have been liable for fines ranging from $400 million to $1.1 billion (Jayakumar, 2014). Fortunately for Target, the Securities and Exchange Commission (SEC) concluded its investigation into the breach with a recommendation of no enforcement (Target Form 10-Q, 2015).

Several news outlets, including Bloomberg and the NY Times, reported that the Federal Bureau of Investigation (FBI) was investigating cybersecurity breaches of JPMorgan Chase and other banks during the summer of 2014. By October, it was confirmed by JPMorgan Chase that nearly 80 million households and 7 million small businesses were compromised during a data breach targeting their customers (Ro, 2014). In this regard, Senator Angus King (I-Maine) was quoted to say, “Congress must work to pass legislation that will improve our capabilities and protect us against more attacks like these. The next Pearl Harbor will be cyber, and shame on us if we’re not prepared for it” (Hattem, 2014).

As one way to take personal responsibility for this, a recent *Wall Street Journal* article proports individual investors should evaluate cybersecurity risks for themselves (Dipietro, 2014). Investors are advised to seek out and review how much a company invests in cybercrime prevention, including the number of employees and technology resources dedicated to cybersecurity efforts. Although this may be a move in the right direction, there are no guarantees of cybercrime prevention. For example, JP Morgan spent $250 million to secure their data, but evidence indicates the company’s breach most likely occurred because of something as basic as the failure to update a server (Goldstein, Perlroth, & Corkery, 2014).

In December of 2014, Sony reported that it was victim of a cyberattack that led to leaks of employees’ sensitive data, loss of other data, and the loss of control over films that had not yet been released (Steinberg, 2014). In a suit against the company, employees alleged that Sony was aware of the vulnerabilities of its system. The case was settled within a year, with Sony agreeing to pay $8 million; however, the company did not admit to any fault in the breach (Pettersson, 2015).

Though the Internal Revenue Service (IRS) has implemented a number of controls over its financial and tax processing systems, the United States Government Accountability Office (GAO) determined that there are still weaknesses in many areas leading to signficiant deficiencies in financial reportng for the department (U.S. Government Accountability Office, 2016). These weaknesses are noteworthy because of the consequent cost and the exposure of taxpayers to frauds. In filing season 2014 alone, the IRS estimates that it paid over $3 billion in fraudulent returns, but it prevented more than $22 billion in additional losses. The Consolidation Act of 2016 provides for nearly $300 million of funding—part of which is for cybersecurity (U.S. House of Representatives, 2015).

Between 2009 and 2011, Robert Giulietti, a United States Postal Service Employee, defrauded the federal government out of nearly a million dollars. According to the FBI (2014), Giulietti had the responsibility of reviewing and approving bids from contractors, certifying that the work was completed, and also authorizing payments to the contractors. This is a violation of the basic internal control of segregation of duties, which is covered in most accounting principles textbooks. Giulietti reportedly used his position to approve bids and authorize inflated payments for a company formed by his wife.

 According to a survey done by PricewaterhouseCoopers, detected information security breaches increased 38% from 2014 to 2015. Clearly, security crimes are continuing to increase despite increased allocation of resources in an effort to secure company information (PwC,CIO Magazine, CSO Magazine, 2014).

In response to the financial scandals created by Enron and WorldCom, Congress passed the Sarbanes-Oxley Act in July 2002. This Act was considered the most far-reaching reform since that enacted by Franklin Delano Roosevelt (Gupta & Nandkumar, 2007). The lack of reliable internal controls lead to an environment in which fraud was easliy perpetrated, and which resulted in investors losing huge sums. Sections 302 and 404 of the Act require firms to certify their financial statements and disclose significant control deficiences to the audit committee of the board of directors and the external auditors, and to disclose material control weaknesses to the SEC (U.S. House of Representatives, 2002).

Former Deptuy Chief Accountant of the SEC, Scott A. Taub, said in a speech shortly after the Act was passed, “we believe that the increased attention to internal controls on the part of management will reduce the potential for errors in the financial statements, including those due to fraud” (Taub, 2003). Further, former SEC Commissioner, Cynthia Glassman is quoted as saying, “this disclosure can be an important tool for investors in evaluating the reliability of a company’s financial reporting” (Glassman, 2005).

At the time SOX was created and adopted, it was heralded as the solution to corporate fraud. According to SOX, good corporate internal controls are essential to preventing and/or detecting fraud, which is exactly what the Treadway Commission concluded years earlier. Although internal controls have been considered critical for decades, and SOX intensified the emphasis to evaluate internal controls, corporate losses stemming from internal control weaknesses, including those related to data security, have increased.

Corporate internal controls to protect assets, such as company data, and ensure compliance with policies have clearly not prevented financial loss, and the number of firms affected is growing. The financial ramifications are significant. Since SOX involves internal controls, and management and auditors have to report on the effectiveness of internal controls, why are there so many data breaches? Are new laws being drafted? This paper investigates these questions.

# **BACKGROUND**

**Information Security**

Announcements about security breaches and the number of company records stolen or compromised seem like common occurrences. Most people have received, or know someone who has received, communication informing them their personal data has been lost or stolen.

Such a notice was sent by Target Corporation in their December 2013 notice informing millions of their unsuspecting customers that their payment card information had been compromised. Hackers gained access to Target’s point of sale (POS) system through a refrigeration vendor, Fazio Mechanical Services. The vendor’s system was infected by malware when an employee opened a phishing email. Fazio’s employees had not updated the anti-malware software, so the malware was not detected. Further, Target’s anti-malware signaled a problem, but Target employees failed to respond (Radichel, 2014).

The JPMorgan Chase data breach may have been avoided if a “simple security fix” had not been overlooked on one of their servers. JPMorgan, like many other companies, spends huge sums on computer security every year, only to have employee actions, or inactions, make the internal controls ineffective. In JPMorgan’s case, an employee’s stolen login credentials combined with the security team’s failure to upgrade a network server, left the bank open to intrusion (Goldstein, Perlroth, & Corkery, 2014).

Security experts have now had years to review and analyze the information security breaches noted above as well as the very highly-publicized breach at Sony. Most agree that the security practices employed at Sony were, at best, careless. Even more concerning, many organizations follow the same practices as Sony, so these experts believe there will be more losses due to preventable weaknesses related to information security (Riedel, 2015). Even with all the highly sophisticated technology, the biggest losses may have been avoided if strong system of internal controls (such as employee education, monitoring, policy compliance, and segregation of duties) had been followed.

 A nonprofit organization in California, Privacy Rights Clearinghouse (PRC), collects security breach information and makes this information available to the public. The PRC data is collected from government and verifiable media sources to help individuals protect their privacy. Although the database is not purported to report every data breach ever known, it is very enlightening about information security problems (PRC, 2016). The database includes both public (approximately 18% in 2016) and nonpublic (approximately 82% in 2016) breach information categorized by types of breach (See Table 1).

Table 1 – Breach by Type and Year

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Type ofBreach | Breaches Reported/Records Compromised2016 | Breaches Reported/Records Compromised2015 | Breaches Reported/Records Compromised2014 | Reported% Change2014-2015 | Reported%Change2015-2016 |
| HACK | 305/3,427,360 | 128/153,091,160 | 147/67,092,537 | -12.9% | 138.3% |
| INSD | 12/111,420 | 13/5,472 | 27/433,041 | -51.8% | -7.7% |
| PHYS | 42/533,663 | 19/6,180 | 16/20,358 | 18.8% | 121.1% |
| PORT | 51/6,155,748 | 44/116,998 | 39/80,520 | 12.8% | 15.9% |
| DISC | 123/819,121 | 57/6,098,166 | 49/175,004 | 16.3% | 115.9% |
| Total | 533/11,047,312 | 261/159,317,976 | 278/67,801,460 | -6.1% | 104.2% |
| (amended from data available from PRC website) |

In reference to Table 1, breach categories include: hacking or malware (HACK), insider compromises by employees or others with legitimate access (INSD), physical loss from paper documents that are lost, stolen or discarded (PHYS), portable devices such as laptops or USB drives lost, stolen or discarded (PORT), and unintentional disclosure (not from hacking or intentional) such as data posted publicly, mishandled, or sent in an email (DISC). As reflected in Table 1, hacking or malware is consistently the most common reason for information breaches and unintentional disclosures the second most common. These two reasons are also on the increase over the three year period included in the table, with unintentional disclosure increasing between 2014 and 2015, but jumping dramatically in 2016. In 2016 alone, if losses from unintentional disclosures and paper documents could be stopped, the number of breaches would decrease by 31% and documents compromised would decrease by 12.25%. If one includes physical loss of assets like laptops and other portable devices, the breaches decrease by 40.5% with 68% fewer documents compromised in 2016. So, if organizations protected assets (portable devices) and documents (lost, stolen or discarded) including protecting documents (posting, mishandling and emailing) using basic internal controls such as security of assets and documents, and segregation of duties, a large percent of documents may not have been compromised (Turner and Weickgenannt, 2013). According to SOX, companies are supposed to have strong internal controls. So, where is the disconnect?

**SOX and Internal Control Guidance**

The Sarbanes-Oxley Act became effective in July 2002 (United States House of Representatives, 2002). The Act applies only to publicly traded companies, is arranged into eleven ‘titles’ or sections, and creates the Public Company Accounting Oversight Board (PCAOB). In accordance with SOX Section 404, management is required to report on the scope and adequacy of the internal control structure and procedures for financial reporting, and the financial statement auditors must report on their assessment of the effectiveness of the internal control structure and procedures for financial reporting.

Internal controls are described and defined at various levels of the organization and by different authoritative entities. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. COSO is a joint initiative of the Institute of Management Accountants (IMA), American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Institute of Internal Auditors (IIA), and Financial Executives International (FEI). The COSO Internal Control-Integrated Framework is recognized worldwide as a respected methodology to design, implement and evaluate internal controls. This framework defines five components of internal control: 1) control environment, 2) risk assessment, 3) information and communication, 4) control activities, and 5) monitoring (COSO, 2016).

 The Securities and Exchange Commission guidance more specifically defines controls as:

 "...a specific set of policies, procedures, and activities designed to meet an objective. A control may exist within a designated function or activity in a process. A control’s impact...may be entity-wide or specific to an account balance, class of transactions or application. Controls have unique characteristics – for example, they can be: automated or manual; reconciliations; segregation of duties; review and approval authorizations; safeguarding and accountability of assets; preventing or detecting error or fraud. Controls within a process may consist of financial reporting controls and operational controls (that is, those designed to achieve operational objectives) (SEC, 2007).”

In accordance with SOX and guidance issued by the SEC, management is responsible for implementing, maintaining and reporting on Internal Control over Financial Reporting (ICFR). The internal control reports issued by JPMorgan Chase in 2013 (the year before the breach), 2014 (the year of the breach) and 2015 disclosed no weaknesses in internal controls by management or by the financial statement auditors. The same is true for Target and Sony.

Ultimately, any weaknesses in internal controls identified by management or by the financial statement auditor must be categorized as a control deficiency, a significant deficiency, or as a material weakness (SAS 112). At the same time, a material weakness in internal control over financial reporting may exist even when financial statements are not materially misstated. It appears that either the ICFR lacks full disclosure, and/or testing required by SOX, may not be very effective in preventing information security breaches.

For further consideration, be reminded that SOX only applies to publicly traded companies. Referring to the PRC database on data breaches, the authors estimate that approximately 18% of the 2016 breaches reported were related to publicly traded companies; therefore, about 82% relate to non-publicly traded companies, so large quantities of data collected and maintained by organizations are not subject to SOX internal control reviews. This would lead one to lean towards the successes associated with SOX; however, it is clear that current practices associated with the evaluation of internal controls still need to be improved for all companies. The key to changes of this type is probably linked to legislative changes.

**LAWS**

President Obama signed Executive Order 13636, *Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) – 21 Critical Infrastructure Security and Resilience* February 12, 2013 (Executive Order No.13636, 2013). Per this executive order the Executive Branch is to improve critical infrastructure cybersecurity by doing the following:

* Develop a technology-neutral, voluntary, cybersecurity framework
* Promote and incentivize the adoption of cybersecurity practices
* Increase the volume, timeliness and quality of cyber threat information sharing
* Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
* Explore the use of existing regulation to promote cyber security

On February 13, 2014, in response to this executive order, the National Institute of Standards and Technology (NIST), a non-regulatory agency of the United States Department of Commerce, issued Cybersecurity Framework 1.0. The framework is voluntary and is a product of collaborations between industry and government – “based on existing standards, guidelines, and practices for reducing cyber risks (NIST, 2014).”

The first paragraph of the executive summary of the Cybersecurity Framework reads as follows:

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation’s security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company’s bottom line. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate and to gain and maintain customers (NIST, Cyberframework, 2014).

Additionally, the Framework Core has four elements: 1) Functions, 2) Categories, 3) Subcategories, and 4) Informative References. The element, Categories, includes asset management, access control, and detection processes (internal controls). These elements are listed or implied in audit guidance AS 2201 (PCAOB, 2007), and discussed in most accounting information system courses taught in accounting programs across the country. The Framework is voluntary, but could be incorporated in part with standards already required by SOX for publicly traded companies.

 In an effort to extend the reach of Executive Order 13636, President Obama signed Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing,* in February of 2015. In part, its purpose is to facilitate voluntary collaboration and communication between nonprofit agencies, private companies, and other agencies in regards to cybersecurity risks, threats, and responses. To facilitate such communications, the order promoted the development of Information Sharing and Analysis Organizations.

The Cybersecurity Act of 2015 (“Cybersecurity Act”) presents the federal government’s first successful step toward creating a partnership between government and private industry to address cybersecurity issues. The consolidated Act was enacted as part of the FY2016 omnibus appropriations bill to ease passage through Congress. The Cybersecurity Act was signed into law on December 18, 2015.

**DISCUSSION AND CONCLUSION**

With the passage of time, the risks businesses face are changing and expanding, yet the need for basic internal controls appears to be unmet. Although the importance of internal controls was a primary focus of the development and passage of SOX in 2002, as well as the Treadway Commission twenty years before, neither has been especially effective in preventing information security breaches. Upon the adoption of SOX, it was believed that requiring management to review, evaluate, and report on internal controls, and also requiring financial statement auditors to attest to managements’ assertions would end preventable corporate losses and decrease fraud. To some extent, this may be true for publically traded companies, but fifteen years later, significant weaknesses exist related to safeguarding assets, segregation of duties, and data monitoring.

Perhaps the financial statement audit function currently in place can be amended to help, but more is required. In response to the attack on JPMorgan Chase in which nearly 80 million household accounts were affected, members of Congress agree there is a need to do something, but they have yet to advance any mandatory cybersecurity legislation for private or public companies. Other than Executive Orders 13636 and 13691 in 2015, little else has been done by the Congress.

In the end, it will probably take a combined effort to effect any real change in information security/cybersecurity such as:

* legislation to require companies and others entrusted with data to protect it,
* expansion or reformulation of mandatory audit requirements for financial and information systems to monitor and provide feedback about security efforts,
* meaningful, consistently applied consequences for noncompliance,
* education for individuals to help them understand the threats,
* a way for individuals to fight back when victimized.

 The problem of information security is large, but as pointed out in this paper, truly mandating basic internal controls for both public and private companies could significantly decrease the losses.

**REFERENCES**

COSO. (2016). *Committee of Sponsoring Organizations of the Treadway Commission.*

 Retrieved February 18, 2017, from https://www.coso.org/Pages/default.aspx

Cybersecurity Legislation. <http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx>

Dipietro, B. (2014, August 21). *The Investor Approach to Assessing Cybersecurity.* Retrieved October 15, 2014, from The Wall Street Journal: <http://blogs.wsj.com/riskandcompliance/2014/08/21/the-investor-approach-to-assessing-cybersecurity/>

Executive Order No., 13636. (2013, February 12). *National Archives.* Retrieved October 14, 2014, from Federal Register: <http://www.archives.gov/federal-register/executive-orders/2013.html>

Executive Order No. 13691. (2015, February 20). *National Archives.* Retrieved September 8,

2016, from Federal Register: <https://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf>

Federal Bureau of Investigation. (2014). Former USPS facilities project manager pleads guilty to

bribery, fraud, and tax charges. Retrieved September 7, 2016, from the Federal Bureau of Investigation: <https://archives.fbi.gov/archives/newhaven/press-releases/2014/former-usps-facilities-project-manager-pleads-guilty-to-bribery-fraud-and-tax-charges>

Glassman, C. A. (2005, February 22). Speech by SEC Commissioner.

Goldstein, M., Perlroth, N., & Corkery, M. (2014, December 22). *Neglected server provided entry for JPMorgan hackers.* Retrieved September 1, 2016, from The New York Times:

 http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-

 identified/

Gupta, P. P., & Nandkumar, N. (2007). Information Content of Control Deficiency Disclosures Under the Sarbanes-Oxley Act: An Empirical Investigation. *International Journal of Disclosure and Governance*, 3-23.

Hattem, J. (2014, October 3). *Lawmakers push cyber law after JPMorgan hack.* Retrieved October 15, 2014, from The Hill: <http://thehill.com/policy/technology/219675-lawmakers-push-cyber-law-after-jpmorgan-hack>

Jayakumar, A. (2014, February 26). *Data breach hits Target's profits, but that's only the tip of the iceberg.* Retrieved July 26, 2014, from The Washington Post: <http://www.washingtonpost.com/business/economy/data-breach-hits-targets-profits-but-thats-only-the-tip-of-the-iceberg/2014/02/26/159f6846-9d60-11e3-9ba6-800d1192d08b_story.html>

NIST. (2014, February 12). *Cyberframework.* Retrieved October 14, 2014, from NIST: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Pettersson, E. (2015, October 20). *Sony to pay as much as $8 million to settle data-breach case*. Retrieved September 5, 2016, from Bloomberg: <http://www.bloomberg.com/news/articles/2015-10-20/sony-to-pay-as-much-as-8-million-to-settle-data-breach-claims>

PCAOB. (2007). *AS 2201*. Retrieved September 8, 2016, from PCAOB: <https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx>

Prah, P. M. (2014, February 10). *Target's data breach highlights state role in privacy.* Retrieved July 24, 2014, from USA Today: <http://www.usatoday.com/story/news/nation/2014/01/16/target-data-breach-states-privacy/4509749/>

PRC. (2016). *Privacy Rights Clearinghouse*. Data Retrieved February 20, 2017 from https://www.privacyrights.org/data-breaches.

PwC,CIO Magazine, CSO Magazine. (2014, September). Defending Yesterday. *Key findings from The Global State of Information Security Survey 2014*. US: PwC.

Radichel, T. (2014, August 5). Case Study: Critical Controls that Could Have Prevented Target

Breach. Retrieved February 20, 2017 from SANS Institute InfoSec Reading Room: <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412>

Riedel, D. (2015, January 26). *Could the Sony breach have been prevented?* Retrieved February

21, 2017 from SC Magazine: <https://www.scmagazine.com/could-the-sony-breach-have-been-prevented/article/535761/>

Ro, S. (2014, October 2). *JPMorgan reveals gigantic data breach possibly affecting 76*

 *million households.* Retrieved September 1, 2016, fromBusiness Insider:

 <http://www.businessinsider.com/jp-morgan-data-breach-2014-10>

SAS 112. *SAS 112 Categories of Control Deficiencies.* Retrieved February 19, 2017, from Blink University of California San Diego: http://blink.ucsd.edu/finance/accountability/controls/sas-112/categories.html

SEC. (2007, June 27). *Security and Exchange Commission*. Retrieved October 12, 2014, from 17 CFR Part 241: <http://www.sec.gov/rules/interp/2007/33-8810.pdf>

Steinberg, J. (2014, December 11). *Massive security breach at Sony—Here’s what you need to*

*know.* Retrieved on September 5, 2016, from Forbes: <http://www.forbes.com/sites/josephsteinberg/2014/12/11/massive-security-breach-at-sony-heres-what-you-need-to-know/#6f954a8de9a5>

Target-2015-Annual-Report. Retrieved September 18, 2016 from https://corporate.

target.com/\_media/TargetCorp/annualreports/2015/pdfs/Target-2015-Annual-Report.pdf

Target Form 10-Q. (2015, August 15). Retrieved September 19, 2016, from https://www.sec.gov/

Archives/edgar/data/27419/000002741915000029/tgt-20150801x10xq.htm#s

8CBAB43D6ED514585F45B9780D1FD409.

Taub, S. A. (2003, May 29). Speech by the SEC Staff: The SEC's Internal Control Report Rules and Thoughts on Sarbanes-Oxley Act.

Turner, L. & Weickgenannt, A. (2013) *Accounting Information Systems: The Processes and Controls,* 2EHoboken, NJ. John Wiley and Sons.

U.S. Government Accountability Office. (2016, April 12). Information security: IRS needs to

 further improve controls over taxpayer data and continue to combat identity theft refund

 fraud*,* (GAO-16-589T).

U.S. House of Representatives, C.o. (2002, July 30). Sarbanes-Oxley Act of 2002*. Public Law No. 107-204.* Washington, D. C.: Government Printing Office.

United States House of Representatives, C.o. (2015, December 18). Consolidated Appropriations

 Act of 2016. Public Law No. 114-113*.*