Compliance as a Strategy for Business Success

portnox™

Introduction

With the increasing trends of Bring-Your-Own-Device (BYOD), remote workforces and the rapid growth of the Internet of Things (IoT), there are more devices on corporate networks than ever before. These trends, while great for innovation and productivity, have made securing corporate networks and their data extremely complex. Each of these devices are a potential point of entry for hackers to exploit in search of sensitive company and user information.

The latest count from the Identity Theft Resource Center (ITRC) indicates there have been 456 data breaches recorded this year through April 18 and that nearly 8 million records have been exposed since the beginning of the year. The total represents a 31% increase in the number of breaches to date compared with 2015[1]. Ensuring compliance and protecting sensitive data and intellectual property should be at the forefront of every security discussion.

Oftentimes organizations view compliance as a headache, but without it, they would not be able to successfully run their business, work with customers and partners, and if they are a SMB, it would prohibit them from working with large enterprises. The perception of compliance can often lead to security as an afterthought. But compliance has become so important that the discussions and decisions have shifted from security officers and IT manager titles to the C-Suite, underscoring the fact that compliance is a strategic decision for organizations. Those that include compliance in their overall security strategy from the start, rather than a siloed or reactionary approach, are in an even better position for business success.

[1] http://247wallst.com/technology-3/2017/04/20/data-breaches-on-track-to-reach-1500-in-2017/

State of Compliance in the US and EU

Protection of private information has become so important that both governments and organizations across industries have formalized data security rules associated with penalties for data exposure.

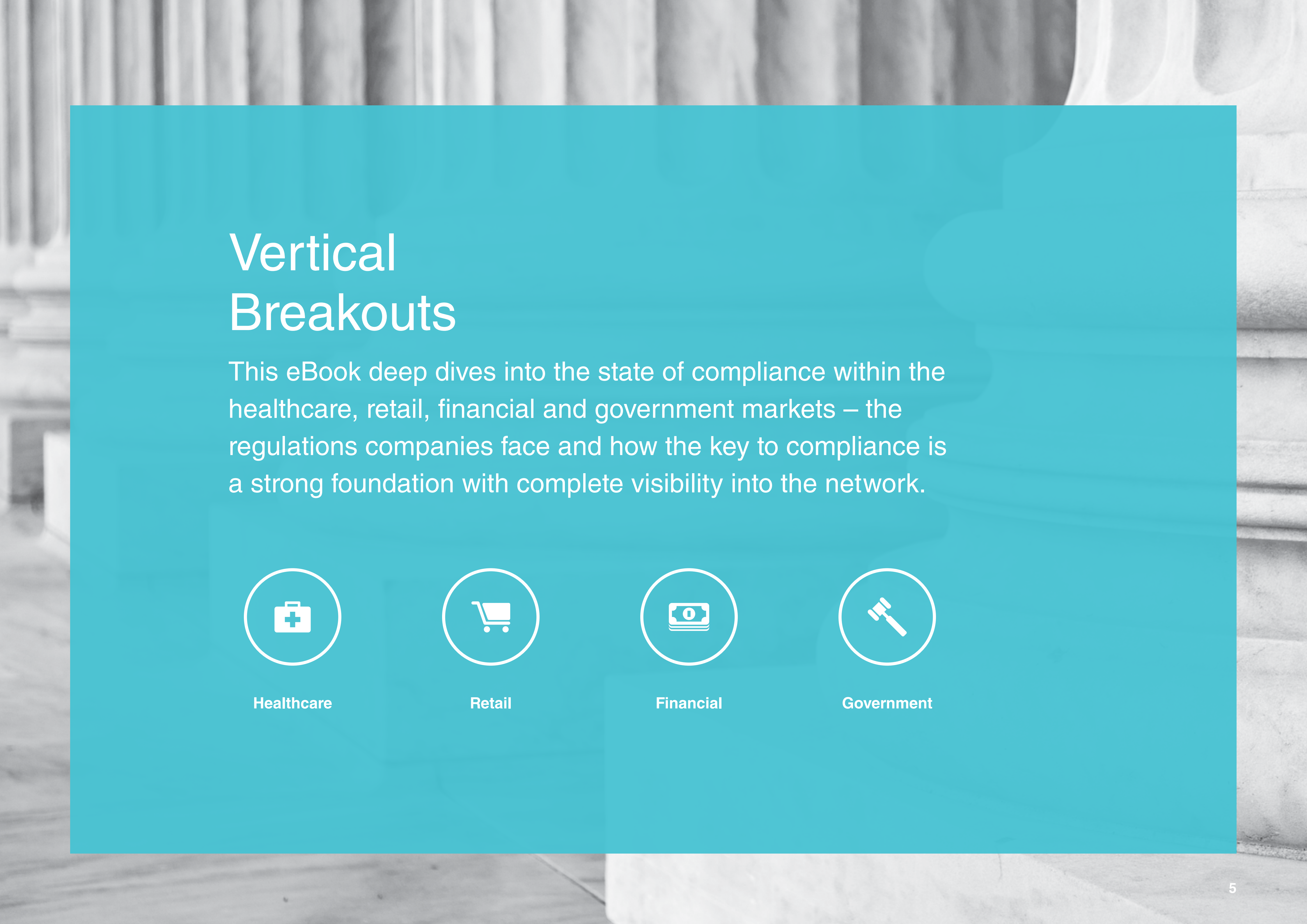
Within the United States, there are laws and industry agreements that require organizations to institute policies and procedures for identifying data exposure risks. These risks must be further classified based on their level of severity and the rules require instituting specific safeguards and controls to protect that data. If a breach occurs, companies are required to provide public reports of the data exposure and whether it was done accidentally or through malicious intent.

In the EU, organizations are facing GDPR becoming law in May 2018 that will significantly affect how companies deal with information it holds on any EU citizen. Under GDPR, all companies and organizations will need to adopt strict procedures when it comes to collecting, protecting, and storing data. Like the US, if a breach does occur, GDPR requires companies to notify customers which data it holds within 72 hours of the breach.

Importance of Visibility to Achieve Compliance

Protecting sensitive data and intellectual property, while meeting security and industry compliance mandates such as SOX, HIPAA, PCI-DSS, and GLBA, has never been more important. However, there are still many companies that do not believe they will be penalized for not being compliant or that anything will happen to them if they do not comply with security regulations. Even if companies are not undergoing a compliance audit, they are still exposed to threats. While hackers may not be fining them in a regulated manner, the price their business can pay if they are breached, is by far higher. That is why companies should look at compliance as a business enabler.

To become compliant and run their business successfully, companies need visibility on what is happening on the network. In other words, what devices are connected to the network, when they connected, who has access to what data, and proof that mechanisms to secure private data are operational. Without visibility into what is on the network, it's impossible to ensure compliance.



Vertical Breakouts

This eBook deep dives into the state of compliance within the healthcare, retail, financial and government markets – the regulations companies face and how the key to compliance is a strong foundation with complete visibility into the network.

Healthcare

Retail

Financial

Government

HIPAA compliance is most often referred to HIPAA Title II, which includes:

- National Provider Identifier Standard
- Transactions and Code Sets Standards
- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Enforcement Rule

Healthcare

Since 2010, the number of attacks against healthcare providers has risen over 125%[2] and risk levels in the industry are now at the highest ever. In fact, just last year, cyber criminals hacked over half a million patient records and began selling them over the Dark Web for profit at approximately $365 per record.

That is about a third more costly than selling stolen financial records, so it is no wonder that this form of theft is growing at a dizzying speed. Part of the big issue is that hospitals, private clinics, vendors and insurance companies all share digital information, which of course creates the perfect conditions for cybercriminal activity.

Access to a health system's network means access to social security numbers, leverage in ransomware attacks, and loss of valuable information. Cybersecurity in healthcare is crucial, because the access to a healthcare system's information not only impacts the organization, but has the potential to impact each of their patients, considering the crown jewels of data are individual's personal health records. If a healthcare system is not compliant with security regulations, it's not just their own information at risk, it is also the information of their patients.

[2] http://resources.infosecinstitute.com/cybersecurity-in-the-healthcare-industry/#gref

Healthcare

Patient data can be accessed through various platforms, including EHRs, patient portals, diagnostic systems, and more. The Health Insurance Portability and Accountability Act (HIPAA) works to prevent this, by requiring privacy and security provisions over medical information, ultimately protecting patients.

The medical industry is struggling to uphold HIPAA regulations regarding privacy, security and enforcement. As the web of the medical industry connected devices continues to grow, a solution that is scalable across a wide range of institutions is a must. It is crucial that every institution sharing this data implements a solution that enables security teams to have complete visibility of all connected devices in real time, including switches, wireless controllers, VPN gateways and routers.

HIPAA compliance is most often referred to HIPAA Title II, which includes:

- **National Provider Identifier Standard**
- **Transactions and Code Sets Standards**
- **HIPAA Privacy Rule**
- **HIPAA Security Rule**
- **HIPAA Enforcement Rule**

Let’s dive into the HIPAA Security Rules

The HIPAA Security Rule, also known as the Security Standards for the Protection of Electronic Protected Health Information, ensures that all patient data stored or transferred electronically is secure, by means of both physical and electronic safeguards.

The HIPAA Security Rule applies to health plans, healthcare clearing houses and to any healthcare provider or system that transmits health data electronically. The rule is intended to ensure the confidentiality and integrity of all electronic protected health information (e-PHI), protect against any anticipated security threats and protect against misuse of information.[3]

The HIPAA Security Rule requires health systems to: [4]

- **Perform risk analysis and management by evaluating the likelihood of risk, and implementing electronic and physical security measures. This should be an ongoing process**
- **Deploy administrative safeguards including a security management program, security personnel, information access management, and implement workforce trainings to ensure staff are aware of proper security measures**
- **Implement physical safeguards including securing workstations and devices as well as limiting facility access**
- **Implement technical safeguards including access control, auditing of devices, and security measures over devices**
- **Take steps to remediate a breach if detected**

[3] https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/

[4] http://searchhealthit.techtarget.com/definition/HIPAA-Security-Rule

NAME: MR. PATIENT
AGE: 27 YEARS
DIAGNOSIS: BROKEN ARM
REASON OF ADMISSION: ACCIDENT
CARDIO: REGULAR BEATS, NO MURMURS
PULMONARY: CLAIR, NO RALES
ABDOMINAL: SOFT, NO ORGANOMEGALY
NEUROLOGICAL: NOTHING ABNORMAL DETECTED
XRAY:
BROKEN BONE
LAB FINDINGS:
WBC: 7.5G/L HB: 16.7G/DL
MCV 92 PLT: 201 G/L CRP: 0.1 MG/L
T: 37C
PULSE: 99/M

In 2015, a Florida-based cancer treatment center 21st Century Oncology was the victim of a data breach, resulting in the potential access of a database containing 2,213,597 patient medical records, including patient’s names, social security numbers, diagnoses, treatment, medical history and insurance information. At the time of the attack, 21st Century did not have adequate budget or IT staff to deploy an effective security infrastructure.

Retail

Cyber beaches in retail came to the forefront of the public eye in 2013 and 2014, with attacks on major stores including Target, Neiman Marcus, Michaels and Home Depot. Prior to this, the average shopper hardly thought twice about whether their credit card information was at risk when making a purchase.

Retailers are increasingly becoming the victim of cyberattacks, particularly with the growth of new payment technologies like Apple Pay and Level Up. Even without the vulnerabilities that these new systems bring, retailers can get hacked through credit card magnet strips, backdoors in point of sale systems, phishing attacks on network devices and more.

If a retailer falls victim to a cyberattack, they risk exposing their customer's personal payment information, and may even result in settling with customers for a considerable sum of money. Customer loyalty is also at risk, considering the increase of breaches getting in front of the public eye over recent years. Nineteen percent of customers said they would stop shopping at a retailer that experienced a cyberattack, even if the company remediated the hack.[5]

In order to protect against financial fraud, companies that accept credit-card payments must follow Payment Card Industry Data Security Standards (PCI DDS) regulations.

In 2013 between Thanksgiving and Christmas, Target was the victim of a cyberattack where hackers had access to the credit card information, names, mailing addresses, and phone numbers of over 40 million customers. Though the cause of the breach has not been confirmed, it's suspected that a phishing email may have been the cause, allowing the attacker to infiltrate Target's point-of-sale system.

Since the attack, Target has amped up security measures to avoid another breach. Looking back, it seems several points of PCI DDS compliance were not met, including protection of cardholder data, limited access to this data, and regular testing of the security system to ensure protection against attack.

[5] http://www.prnewswire.com/news-releases/cyber-attacks-could-cost-retailers-one-fifth-of-their-shoppers-kpmg-study-300316520.html

Let’s Dive into the PCI DSS Security Standard Regulations

The PCI DSS Security Standard is aimed at building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks and maintaining an information security policy.

To meet these goals, PCI DSS requires[6]:

- ✓ **Do not use vendor-supplied defaults for system passwords and other security parameters**
- ✓ **Install and maintain a firewall configuration to protect cardholder data**
- ✓ **Protect stored cardholder data**
- ✓ **Encrypt transmission of cardholder data across open, public networks**
- ✓ **Use and regularly update antivirus software or programs**
- ✓ **Develop and maintain secure systems and applications**
- ✓ **Restrict access to cardholder data by business need to know**
- ✓ **Assign a unique ID to each person with computer access**
- ✓ **Restrict physical access to cardholder data**
- ✓ **Track and monitor all access to network resources and cardholder data**
- ✓ **Regularly test security systems and processes**
- ✓ **Maintain a policy that addresses information security for all personnel**

[6] https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

Financial

Compliance functions are struggling to keep pace with today's customers demand for digital services such as online banking, online advice and the online purchase of insurance products. While it is driving an increase in online business volume across financial services, it is putting stress on control frameworks and giving rise to new risks related to cybersecurity and data privacy, making compliance risk one of the most significant ongoing concerns for financial institution executives.

In addition to addressing general cybersecurity concerns, financial institutions must also minimize the risk of a data breach that could compromise customer financial or personally identifiable information. The standards financial institutions adopt for housing sensitive data must comply with privacy regulations, as well as with traditional federal and state privacy statutes that require privacy notices and restrict sharing customer information for marketing purposes.

Traditionally, financial institutions have met strict security requirements through security best practices and traditional security products such as firewalls, data loss prevention and anti-virus software. However, considering today's growing threat climate and the long list of breaches at prominent financial institutions, traditional thinking needs to change.

Today, new approaches are being considered to raise security, and enhance accountability and visibility. To meet the challenges of data security and regulatory compliance – protecting sensitive data and avoiding fines and penalties – organizations need to see, control and automate their networks.

But before companies can become compliant, they need to be familiar with the regulations. There are many US regulatory and industry standards such as GLBA and SOX, as well as a long list of SEC requirements where relevant, that financial institutions need to be aware of.

Let's Dive into GLBA

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. Financial institutions must give their customers - and in some cases their consumers - a "clear and conspicuous" written notice describing their privacy policies and practices.[7]

It is particularly important to ensure that customers' nonpublic personal information, or NPPI, remains secure. GLBA requires financial institutions to:

- ✓ **Securely store NPPI**
- ✓ **Advise customers of information-sharing practices**
- ✓ **Provide certain opt-out rights to customers**

The regulations implementing the GLBA require a range of disclosures in privacy notices. Financial institutions must provide certain disclosures when they collect data, and then on an annual basis for ongoing customers.

[7] https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm#obligations

Financial

Let’s Dive into SOX

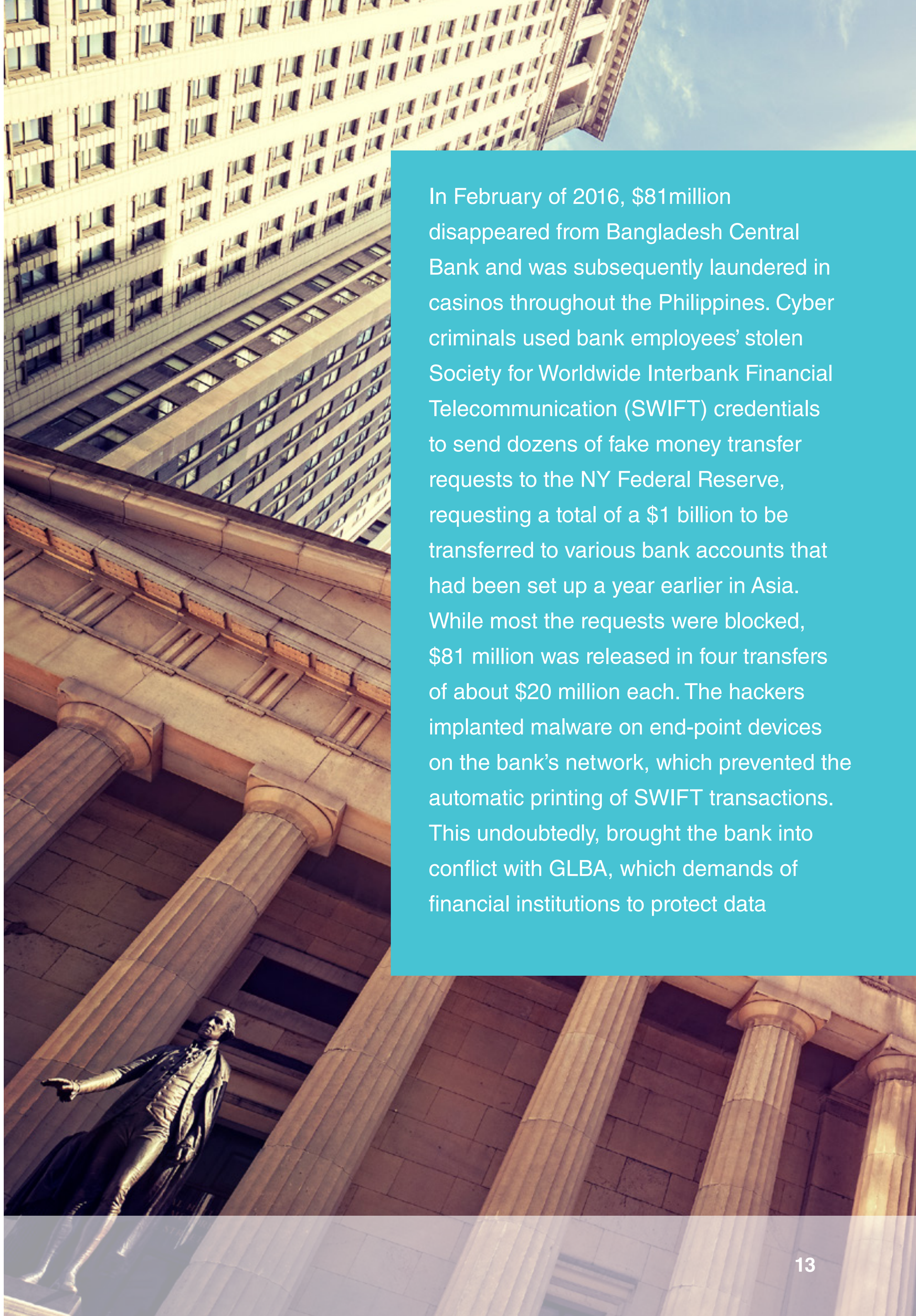
The Sarbanes-Oxley Act (SOX), or the Corporate and Auditing Accountability and Responsibility Act, holds publicly-traded companies and their upper management responsible for maintaining internal controls over financial systems.

In fact, CEOs and CFOs must certify the accuracy of their financial reports and could be held criminally liable for any inaccuracies. This means that upper management could be held liable for exposure of financial data they own, regardless of whether the exposure was their fault or the fault of a third party.

SOX has four major compliance requirements[8]:

- **Management is accountable for establishing and maintaining internal controls and procedures that enable accurate financial reporting, and assessing this posture every fiscal year in an internal control report**
- **Public accounting firms that prepare or issue yearly audits must attest to, and report on, this yearly assessment by management**
- **List all deficiencies in internal controls and information, as well as report any fraud involving internal employees**
- **Detail significant changes in internal controls, or factors that could have a negative impact on internal controls**

Any financial information needs to be safeguarded, and its integrity assured. Specific internal security controls need to be identified that protect this data, auditing must take place, and this security posture re-assessed every year – including any changes or deficiencies because of changing conditions.



In February of 2016, $81million disappeared from Bangladesh Central Bank and was subsequently laundered in casinos throughout the Philippines. Cyber criminals used bank employees’ stolen Society for Worldwide Interbank Financial Telecommunication (SWIFT) credentials to send dozens of fake money transfer requests to the NY Federal Reserve, requesting a total of a $1 billion to be transferred to various bank accounts that had been set up a year earlier in Asia. While most the requests were blocked, $81 million was released in four transfers of about $20 million each. The hackers implanted malware on end-point devices on the bank’s network, which prevented the automatic printing of SWIFT transactions. This undoubtedly, brought the bank into conflict with GLBA, which demands of financial institutions to protect data

[8] https://www.vormetric.com/compliance/sarbanes-oxley

Government

All businesses, regardless of industry, must comply with laws passed by legislative bodies and regulations. These laws and regulations can come from all levels of government – federal, state and local. Some of these laws and regulations apply regardless of the nature of the business and if a business is engaged with more than one state or local jurisdiction, they must comply with the applicable laws and regulations within all locations

When companies work with government agencies – either domestically or internationally – they must understand the nuances and differences between each law and regulation that pertains to that country or business. Even if they are not subject to a specific regulation, they are bound to the same rules and regulations in which they do business. Beyond organizations conducting business with government agencies, they themselves are subject to security and compliance risks.

The security challenge for government agencies is twofold: Threats can come externally or from within. Data leakage and network instability can have disastrous consequences, regardless of origin. Therefore, security must be implemented to block entry of unauthorized users and prohibit the exit of confidential data. Many threats are due to user laxity, negligence or worse.

Users may unknowingly open doors to external threats by using unauthorized or unpatched software that allows hackers entry onto the system. Employees may routinely transfer sensitive data onto removable devices (such as USB flash drives) and leave the building, only to discover later that the device has been lost or stolen. If the data has not been encrypted, the consequences are more serious.

Government

That is why it is important for all organizations, including government agencies, to be able to discover and continuously monitor devices on the corporate network that may be subject to compliance. Device discovery is the first step to understanding where potential hackers may enter to obtain information. The device could be a smartphone, laptop, PC, network equipment, etc., that could show false compliance. Meaning that an organization may think they are compliant, but without knowing where the devices are located and by whom they are accessed, you cannot truly tell whether the device and information is safe.

In one case, John Podesta, chairman of the Hillary Clinton campaign received a phishing email, which was in fact correctly identified as such by an aide. The problem was that the aid accidently made a note calling the email legitimate instead of illegitimate, leading Podesta to open the email. This single mistake, placed over 60,000 highly sensitive emails in the hands of the Kremlin, which went on to distribute the information to websites like WikiLeaks.

Even after the FBI sent a special agent to warn to the DNC of the phishing emails, their IT did not respond to the warnings because computer logs did not reveal any intrusion. Podesta should not have required an aid to manually mark the email as illegitimate.

Compliance Done Right Starts at the CORE

Compliance is a business enabler – without it, business growth may suffer. If companies are not compliant, they could lose out on future growth and opportunities to work with a well-established customer or partner. Understanding compliance and regulatory policies is only the first step. Organizations need a strong security technology partner that enables CISOs and IT departments to see and profile all network devices, remediate any security issues and automate actions that have traditionally been conducted manually.

Portnox's compliance strategy will help companies in the following four segmentations:

- **Seeing all devices on the corporate network in real time. Understanding how mobile, BYOD and IoT devices affects and transforms not only the organization, but the industry and implementing the right processes and tools to control them.**
- **Tracking any network related device or program in real time via our centrally secured platform providing full visibility.**
- **Addressing cloud security is paramount, because everything today is going through the cloud. It is important to strictly control access to the network and applications even based on the geographical locations of users.**
- **Ensure that your business is compliant with governmental regulation like SOX, PCI DSS, HIPPA, FINRA, FISMA, GLBA among others. Strict compliance will provide legitimacy with clients and partners.**

Without full network visibility, it is impossible to control devices or maintain compliance standards. The challenge for many is how to maintain a level of security (even large companies struggle to attain compliance) often with limited resources and budgets. Portnox's advanced technology – available both on-premise and in the cloud – gives network operators the tools they need to see and control, any device, any time, any place. With these tools, Portnox makes compliance a more straightforward and smooth process, setting your business up for success.

About Portnox

Portnox protects the network from vulnerabilities that result from mobile, BYOD and IoT devices and the use of authorized and unauthorized devices, giving full visibility into devices within the network as the foundation. On top of that, Portnox offerings delivers control, prevention, enforcement and management of activities for any user, any device, any network, anywhere

Contact Us

Americas: usinfo@portnox.com | 1.855.476.7866 • Europe: dotell@portnox.com | (44) 1273.256325

www.portnox.com

portnox™