https://doi.org/10.48009/2_iis_2016_208-214

Issues in Information Systems
Volume 17, Issue II, pp. 208-214, 2016

TRENDS AND PREVENTIVE STRATEGIES FOR MITIGATING CYBERSECURITY BREACHES IN ORGANIZATIONS

Marzie Astani, Winona State University, mastani@winona.edu
Kathryn J. Ready, Winona State University, kready@winona.edu

ABSTRACT

Cybersecurity breaches are a constant threat. According to the literature, malicious software attached to email accounts for the majority of computer breaches. There are various estimates about the cost of damage, but the most recent statistics estimate that the damage is in the range of billions of dollars. Yet, firms' budget allocations appear unaffected by the accelerated rate of computer security incidents. The continual increase in breaches constitutes a sense of urgency for organizations to take measures to safeguard their networks. This research discusses some recent cybersecurity breaches and summarizes some of the issues that organizations are faced with in securing their information resources. The objective of this study is to promote discussion in organizations about potential security weaknesses based on recent cyber-attacks, and serve as a resource for executives by incorporating suggestions by IT experts on ways to mitigate security deficiencies throughout the organization.

Keywords: Security Breach, Cybersecurity, Web Application Security, Organization Security Strategies

INTRODUCTION

Today's information driven organizations face fundamental challenge of making business-critical information available with maintaining integrity and security. This must be done in spite of increasing complexity of IT environment that includes traditional physical and virtualized infrastructure and most often cloud computing. Gartner predicts that information storage will grow from 40 percent to 60 percent annually (Data Growth Now, 2016) while new variants of malware, such polymorphic attacks that evade anti-virus software and intrusion vectors like web attack toolkits, grow exponentially – into the millions (IBM Corporation Software Group, 2013).

Application security breaches have been increasing in frequency and are becoming front-page news. These attacks have more serious consequences than ever before. Customers are the victims of these attacks and are demanding corporate accountability, and federal regulations. For example, the Health Insurance Portability and Accountability Act (HIPAA) in the United States requires organizations to disclose when a security breach occurs that is connected with sensitive, personally-identifiable data and personal health information. In addition to complying with federal regulations, organizations in many countries must adhere to rapidly-growing state and local regulations (IBM Corporation Software Group, 2013).

Historically, organizations have relied on perimeter defenses to keep their networks and data secure. Unfortunately, network firewalls and network vulnerability scanners cannot defend against application-level attacks. By design, web applications permit unknown users to interact with data and systems. This interaction passes through network defense mechanisms such as firewalls and intrusion detection systems, leaving business vulnerable to malicious attacks. Web applications have increasingly become high-value targets for hackers. Since so many websites contain vulnerabilities, hackers can leverage a relatively simple exploit to gain access to a wealth of sensitive information, such as credit card data, social security numbers and health records. Therefore, it's more important than ever to examine the organization's web application security, assess the vulnerabilities and take action to protect the business. Experts suggest several ways to protect organizations' information including: 1) Understanding Emerging Regulations and Requirements - As the number of web application security breaches has increased, regulatory and industry requirements have become more stringent. Standards in the Payment Card Industry (PCI) include Data Security Standards (DSS) – a framework that includes requirements for security management, policies, procedures, network architecture, software design and other protective measures. This includes directives for establishing and

maintaining web application security. These measures dictate that companies protect all web-facing applications against attacks by testing applications for security, reviewing application source code for vulnerabilities or installing an application-layer firewall in front of applications; 2) Establishing Proper Security Practices in the Company – In order to mitigate the growing threat of web application breaches, it's important to address three key areas of potential vulnerability in the organization: the people, processes, and technology (Internet Security Threat Report, 2016).

RECENT CYBERSECURITY BREACHES

A data breach occurs when sensitive information about an organization's employees, clients or its business is compromised for a variety of reasons, ranging from human error to fraud and theft. Whether by attack or as a result of accidental data breach, data commonly targeted by hackers includes employees' social security numbers, medical or financial records, customers' financial or account records, or competitive data used for corporate espionage purposes.

In 2011, 855 data breaches occurred globally, compromising 174 million records, according to the 2012 *Data Breach Investigations Report*, conducted by Verizon's forensic analysis team in cooperation with international law enforcement agencies, including the Secret Service. Those breaches didn't exclusively target large organizations. Approximately 72 percent of exposed companies employed 100 or fewer individuals (Gunderson, 2013). While it may be a challenge, failure to secure sensitive data can be costly. The average cost of a data breach was $5.5 million in 2011, according to the *2011 Cost of Data Breach report*. Recovery costs following a breach typically stem from investigating the cause of the breach; notifying customers or employees affected; managing inquiries from those affected; public relations; legal defense; regulatory proceedings; fines and penalties; and credit or identity monitoring. In addition, organizations need to consider the innumerable types of hackers and tactics they use to confiscate data. The cyber risk and security assessment firm, NetDilligence cited statistics indicating that hackers and criminals were responsible for 32 percent of breaches; rogue employees cause 19 percent of breaches; and theft of mobile computer equipment like laptops and memory sticks carrying unencrypted data caused 33 percent of breaches (Gunderson, 2013).

In another cybersecurity breach in 2013, Advocate Health System announced that four computers were stolen from one of its Advocate Medical Group (AMG) administrative offices in Park Ridge, Ill. An international investigation was launched, which revealed that, while the computers did not contain patient medical records, they did house patient information – including names, addresses, dates of birth, and Social Security numbers. All four million patients were notified about the compromised information. This breach at Advocate Health is one of the largest Health Insurance Portability and Accountability Act (HIPAA) breaches reported and illustrates the importance of technology in health care and shows how easily a data breach can occur (Kieke, 2014). Experts such as J. Trevor Hughes, CIPP, president and CEO of the International Association of Privacy Professionals, emphasize training stating "we don't have enough laws, enough technology, enough understanding today to resolve all of the data risks that we are experiencing."

In 2015, nine individuals were charged by the United States Department of Justice (DOJ) with hacking into three separate newswires, stealing yet-to-be-published press releases, and passing this stolen information to approximately two dozen individuals who then traded on the bulletins before their public release. The Securities and Exchange Commission (SEC) has been investigating 32 individuals who are connected to this scheme, including the hackers as well as the individuals who allegedly traded on the stolen releases. According to the DOJ indictments, nine men have been charged with gaining unauthorized access to business newswire services Marketwired, PR Newswire, and Business Wire, from which it is believed they stole 150,000 confidential press releases prior to their public release. U.S. Attorney Paul J. Fishman, District of New Jersey announced that "the defendants were a well-organized group that allegedly robbed the newswire companies and their clients and cheated the securities markets and the investing public by engaging in an unprecedented hacking and trading scheme. They launched a series of sophisticated and relentless cyber-attacks against three major newswire companies, stole highly confidential information and used it to enrich themselves at the expense of public companies and their shareholders." Using proxy servers to mask their identities, two of the hackers posed as legitimate newswire employees and customers in order to conceal their intrusions, which may have included the installation of malware onto PR Newswire's servers and the theft of login

credentials from Business Wire. The hackers also made instructional videos showcasing their exploits as means to recruit traders. Following the completion of a successful hack, the two hackers passed their stolen information along to associates based in the United States, the Ukraine, Russia, Malta, Cyprus, and France via the creation of a secret web-based location. Those recipients then used the releases to place illicit trades in stocks and other trading options on a variety of companies, including Panera Bread, Boeing, Hewlett-Packard, and Oracle (Bisson, 2015).

The current trend shows that cyber criminals have turned the act of holding data for ransom into an efficient business while blurring the money trail enough to continue to collect from thousands of victims. Because of their success, criminals are increasingly using ransomware to infect computers. According to data from Intel's McAfee Labs, by the second quarter of 2015, ransomware attacks had grown more than tenfold compared to the same quarter a year earlier (Reisinger, 2014). Recent published cybercrime highlights include several notorious international hackers (Risk Management Framework, 2015). Below are some examples of international cybersecurity crimes/criminals:

- In 2002, Italian police, working together with the US Secret Services rounded up teens and young adults in several cities in Italy, accusing them of hacking NASA, as well as other government and banking sites.
- A US citizen, Albert Gonzales, was arrested in 2008 after stealing and selling millions of credit card numbers from a variety of US retailers.
- In 2010, Hungarian citizen Attila Nemeth compromised the network of the Marriott chain of hotels and attempted to use stolen data to extort the company into hiring him as a security consultant. He was arrested after flying to the US for a phony interview, pleaded guilty, and was sentenced to 30 months in prison. Hungary ranks fifth in countries categorized by malicious bot activity, according to Symantec.
- One Turkish hacking collective claims to have deleted roughly $670 billion in outstanding bills within a local utility company's database in 2014. Cybercrime causes economic harm in Turkey of up to 1.4 percent of the country's GDP.
- The Brazilian hacking underground market is known for its availability of robust training courses in areas like crypter programming and fraud to help budding criminals in their "careers."
- Russia-based bulletproof hosting services fuel the cybercrime economy worldwide. The Russian underground offers virtual private server (VPS) bulletproof hosting for as little as $20 per month.
- The Chinese group, Emissary Panda, also known as Threat Group 3390, is well-organized, sophisticated group notorious for attacking foreign embassies, defense contractors, energy concerns, and a wide variety of other organizations worldwide.
- The Icelandic government recently was behind 23% of malicious computer activity against systems in the US for its support of whaling activities. Iceland constitutes the highest source of cyberattacks when adjusted for population.
- Based in India, Operation Hangover cyberspying attacks continued for three years and snooped on targets like Porsche Holdings, Delta Airlines, The Chicago Mercantile Exchange, and a number of US law firms, according to Infosec Institute research.

Experts blame the increase in cybercrime incidents, in part, on security holes in the manufactured devices and software developed by software engineers that are coming to market before thorough testing and appropriate scrutiny of the products has been completed. In 2013, the U.S. government warned that Android devices are a major threat to personal and corporate security. Recent news reports indicate that the popular mobile app Snapchat has a flaw that can cause iPhones to crash and provide a gateway for denial-of-service attacks. There are several examples of vulnerabilities that currently exist with mobile devices and software applications (Reisinger, 2014). Additional reported security risk examples that are representative of concerns that all users face include:

- Ninety-two percent of the top 500 Android apps carry either a security or privacy risk, according to recent data from MetaIntell. But, it's not just Android; Snapchat, among several other apps, suffer from its own security issues on iOS. At this point, it appears apps – regardless of platform- aren't nearly as secure as one would expect.
- Reported in the Hackers last year in its annual security report, Sophos revealed that Android, not Windows, is the world's most targeted platform among hackers. That report came after it was revealed that an

increasing number of hackers were intentionally targeting iOS far more than all other mobile operating systems, save for Android. If the hackers are moving to mobile, both Android and iOS users along with all organizations and their employees should be concerned about increased security breaches.

- Communications has become a major target for hackers around the world. Several reports have recently indicated that SMS is among the top way for hackers to break into mobile devices and steal information. Hackers are successful by fooling mobile users into clicking on malicious links similar to phishing email.
- Data theft is a major concern for enterprises. But, the concern isn't necessarily about hackers; it's about employees. Fiberlink, an IBM-owned company, recently told Tech Republic that the enterprise's list of most-blacklisted apps was dominated by cloud-storage solutions like DropBox, Box and Google Drive. For organizations, one of the biggest threats is watching employees walk out of the office with the ability to take any sensitive data they want and put it on cloud storage.
- Another element of concern is a hardware element. Although much of the talk of mobile security centers on software, it's important to point out that smartphones and tablets are mobile. That means they can be easily stolen or used in malicious ways when outside the view of the IT staff. Hardware security is a huge issue in today's mobile-security landscape.
- Jailbreaking allows users more access to applications by being able to run unverified apps on devices. This results in potential security problems. In fact, the majority of security issues that affect Apple's iOS can only harm those products that are jailbroken and not locked down.
- Biometric Security is a major concern for enterprises. In the consumer market, biometric security, such as a fingerprint scanner or an eye scanner, can help secure devices, but for the IT side, it could result in major problems. If employees are using their personal devices in the office and they are securing them with their fingerprints or eye scanner, IT staff will have serious trouble gaining access to those devices and ensuring device security.

PREVENTING CYBERCRIME IN ORGANIZATIONS

While an exact roadmap for circumventing all data breaches might not exist, organizations can take some actions to help lessen the exposure of their information. First, companies must develop and implement an information security policy that takes into account hardware, software, user-identification codes and access controls. Then, IT departments or IT vendors should have a thorough operating structure in place that outlines responsibilities and access rights. Experts advise to deploy technology that can search for unauthorized software on the network. According to Larry Collins, vice president of E-Solutions for Zurich Services Corp., some behavioral analytics programs that audit whether employees are accessing inappropriate files, given their job duties need to be implemented. Further, he suggests all laptops, servers, cell phones, etc., should be encrypted to the highest standard (Gunderson, 2013).

Adding to the complexity, mobile technology has increased the risk for data breaches. Organizations should guard against information being stolen from these devices. Some experts suggest that companies should go beyond evaluating their own data security if using a third-party for services like accounting or data storage with cloud providers. They should review contracts to see how vendors protect clients' information, their policies if a breach occurs, and whether they carry cyber insurance. Many Property and Casualty policies won't cover data breaches. As a result, companies might consider investing in a separate cyber risk policy – either in the form of liability coverage or specialized liability insurance, like Error and Omissions or Security and Privacy policies. If third parties make claims against the organization, liability coverage helps pay for defense costs for regulatory proceedings, privacy breach costs, business interruption, digital asset loss and cyber extortion. Errors and Omissions, as well as Security and Privacy policies help cover management liability and employment practices. Data breaches are increasingly becoming problematic for businesses so experts advise that the leadership to be prepared whether the organization elects to invest in cyber insurance, implement technical data security controls, develop data security policies or do nothing (Gunderson, 2013). Additional suggestions for organizations to fight cybersecurity issues include the following (Harnish, 2016):

- Declare an Orange Alert – IT professionals are powerless if employees create security holes in the network system. The employees need to go through security awareness training to get them up to speed.

- Lock Down Phones – Conducting business on the same device used by one's children constitutes a major security risk. Noted security expert, David Stelzl, says, "a rogue program could hack into your phone and see your calendar, see you through a camera without you knowing it, and listen to you through the microphone." He recommends Check Point's Mobile Threat Prevention, which detects malicious apps, and Capsule, which helps create a secure mobile environment.
- Strengthen firewalls with intrusion prevention tools and consider adding DPI-SSL services, which pre-approve Internet traffic before it reaches you.
- Confer with Competitors – Your IT team should be sharing best practices with other members in your industry. One way is through Security Colony, a portal where firms can exchange ideas for a subscription fee of $2,000 a year.
- Avoid Hostage Situations – More hackers realize there's big money in taking over the computers of firms and demanding cash to set the data free. McAfee Labs reported a 165% increase in ransomware in one recent quarter. It is suggested to use a technology called OpenDNS, which will prevent users from stumbling onto hackers' sites where one might otherwise download malware. It filters the good sites from the bad.

Cybersecurity was the subject at the heart of the CIO Network conference in February 2016. Some of the recommendations that were made by the Task Forces' Priorities team in this conference were published in the Wall Street Journal (13, 2016). They concluded that CIOs need a data culture, where firms treat data as a product, whether it be internal or external. Data policies and the data should be regarded as a corporate asset. CIOs need to find ways to deliver data analytics to the business in a timely manner and within the firm's everyday decisions, understand the source of data, including the technology or devices that generate and deliver it and help business partners understand the importance of data quality and how it impacts decision making. Some of the top recommendations related to cyber security were as follows:

- All entities, from private sector to government, should share threat indicators as quickly and as widely as possible in an automated way, free of cost and consequences.
- Deterrence should be heightened by increasing consequences for hackers trying to attack systems.
- Create a common language and independently validate standards for all constituencies to assess security.
- Create an entity that investigates and analyzes incidents for the purpose of sharing lessons learned and developing best practices for security.

Still other cybersecurity experts have proposed the integration and increased use of advanced cloud services, such as Google Cloud Platform, Amazon Web Services and Microsoft's Azure, to prevent potential attacks by monitoring online behavior (Burg, 2016). The advantage to this approach is that the cloud software is independent of specific hardware platforms, thereby reducing the points of vulnerability and permitting the organization to more readily keep up with ongoing technological changes. By the time a cyberattack is detected in an organization, current security systems have already been compromised or failed, resulting in IT professionals and executives dealing with the accompanying fall-out. When using a cloud based system, security technologies are combined into an analytics platform across several computer hardware systems and can more quickly respond to cyber-threats by immediately incorporating operational data into the analytics platform, analyzing it with the accumulated security technology information, and quickly moving the threatened applications and data into a new network beyond the reach of the attacker (Burg, 2016).

CONCERNS AND CONSTRAINTS

Security breaches are a worldwide concern and continue to be a major area of emphasis in IT Departments and organizations as cyber threats continue to escalate. In an online information security survey conducted by Ernst & Young between June and September 2015, sixty-seven CIOs and other executives in information security operating across 67 countries responded about information security issues they faced in their organizations (Concerns and Constraints, 2016). The CIO executive respondents indicated that criminal syndicates (59%) pose the most likely source of attack, followed by the company employees (56%), Hacktivists (54%), lone-wolf hackers (43%), external

contractors working on site (36%), and state-sponsored attackers (35%). Priorities for the next 12 months concerning security challenges as indicated by the CIO executive respondents are shown in Table 1. Over one half of the respondents indicated that data leakage/data loss prevention and business continuity disaster recovery resilience were high priorities. Other areas of high or medium concerns by 85% or more of the respondents included identity and access management, security awareness and training, incident response capabilities and security operations (antivirus, patching, and encryption).

Table 1. The Importance of Security Matters for Organizations

Priority	High	Medium	Low
Data leakage/data loss prevention	56%	33%	11%
Business continuity disaster recovery resilience	55%	33%	12%
Identity and access management	47%	41%	12%
Security awareness and training	44%	45%	11%
Incident response capabilities	44%	44%	12%
Security operations (antivirus, patching, encryption)	41%	44%	15%

Despite these reported security concerns of IT executives in their organizations, they are confronted with many obstacles and challenges in developing plans to deal with these issues. Over 60% of the IT executive respondents indicated that budget constraints are a major challenge in dealing with information security issues. Lack of skilled resources was listed as a major challenge by 57% of the respondents, followed by a lack of executive awareness of support (32%). Other major challenges included lack of quality tools for managing information security (28%), governance issues (28%) and 23% fragmentation of compliance/regulation (Concerns and Constraints, 2016).

CONCLUSION

Developing and implementing an efficient and effective security strategy and policy permits organizations to take a more proactive stance in safeguarding their resources and assets while developing standards on how to interact with others in a global marketplace. When an organization fails to adopt effective security strategies, the potential for financial burdens they may be faced with significantly increases. Network vulnerabilities reduce efficiency and leave the organization's resources and assets unprotected and compromise the integrity of information systems and resources. In order to strengthen an organization's information system, an effective computer security plan and policy must be in place. One increasingly popular way to go about this is to partner with a managed security services provider. In a survey published in early 2016 (Frenel, 2016), the results show that the number of respondents who either already partner or plan to partner with a managed security services provider climbed to 86%, from 78% last year. Pressure to select the latest security technologies jumped from 67% to 74% but resources to implement them fell from 71% to 69%. Job loss continues to be the third-highest fear following a breach, having grown from 8% to 11%. Reputation and financial damage are the first two fears. Respondents who wish to quadruple their staff due to the increased needs they face have risen from 24% to 29% for 2014 and 2015, respectively.

To mitigate cyber security breach some companies will likely look to encryption to increase their data security, especially, when the information travels outside the firewall. Over the past 10 years, encryption use has doubled. According to responses obtained from the Thales e-Security's survey, most respondents encrypt data for three main reasons: compliance, to address specific threats and to reduce the scope of audits. The healthcare and retail sectors are leading the charge to encryption, according to an annual survey sponsored by Thales e-Security – unsurprising since both industries have been hard hit by breaches. The survey, also, showed that 34% of the respondents indicated they used encryption extensively. According to the same survey, 61% of the respondents stated that employee and other HR data were the most important data that companies were trying to protect. Credit card data was the second most important type to protect. Companies are most concerned with managing internal mishaps. Eighty-seven percent said they are concerned with "employee mistake, system or process malfunction." This was followed by hackers or malicious insiders (47%), and government eavesdropping (19%).

As intruders and hackers become increasingly sophisticated in their approaches, more integrated processes overall may be needed to fend off potential security threats. A cloud-based analytics system is able to monitor customer, employee and introducer activity simultaneously, thereby benefiting individual users, and at the same time information can be shared among companies and governments about identities of attackers and the threats they pose resulting in mitigating potential damage (Burg, 2016). The use of a cloud-based system is an integrated approach that should be considered in conjunction with all cyber-security strategies in an organization to most effectively deal with potential threats. Systematic strategies that incorporate the continual monitoring of an organization's data and data processes to fend off any potential cyber threat is key to financially protecting organizations from increasingly sophisticated cyber-attackers and serves as a major competitive advantage in any industry.

REFERENCES

Bisson, D. (2015). *STATE OF SECURITY.* Retrieved from http://www.tripwire.com

Burg, D. & Archer, T. (2016). Safety in the cloud. Strategy+Business, Retrieved from http://www.strategy-business.com/article/Safety-in-the-Cloud

Concerns and Constraints. (2016). *The Wall Street Journal*

Data Growth Now. (n.d.). Report 273073. Retrieved from http://www.cioinsight.com 10/c/a/Latest-News

Frenel, K. Why security pros are always under pressure. Retrieved from http://www.Cioinsight.com/security

Gunderson Hunt, K. (2013). Firewall under fire: Could a cybercrime send you up in flames? Retrieved from *irem.org/jpm*

Harnish, Verne. (2016). Immediate Ways to Fight Cybercrime. *Fortune*.

Internet Security Threat Report: http://www.symantec.com/business/threatreport/topic

Kieke, R. L. (2014). Recent data breach stresses the importance of effective privacy efforts. *Journal of Health Care Compliance.*

Protect People, Processes and Technology from Web Application Threats. (2013). *IBM Corporation Software Group*, Route 100, Somers, NY 10589.

Risk Management Framework. (2015). NSIT SP 800-37. Retrieved from http://www.Tripwire.com

Reisinger, D. (2014). Mobile security issues that should worry you. Retrieved from http://www.eweek.com/mobile/10

The Task Forces' Priorities. (2016). *The Wall Street Journal*.