WHAT TO DO BEFORE AND AFTER A CYBERSECURITY BREACH?

Written By:

Gurpreet Dhillon, Ph.D,
Virginia Commonwealth University,
Richmond, Virginia,
gdhillon@vcu.edu

KOGOD
SCHOOL *of* BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC

KOGOD CYBERSECURITY
GOVERNANCE CENTER

Previous publications in The Changing Faces of Cybersecurity Governance Series

March 2015

CYBERSECURITY GOVERNANCE: FIVE REASONS YOUR CYBERSECURITY GOVERNANCE STRATEGY MAY BE FLAWED AND HOW TO FIX IT

By Peter Iannone & Ayman Omar

March 2015

CYBERSECURITY ACT OF 2015 REVIEW: WHAT IT MEANS FOR CYBERSECURITY GOVERNANCE AND ENTERPRISE RISK MANAGEMENT

By Joseph J. Panetta & R. Andrew Schroth

September 2015

CYBERSECURITY REGULATION AND PRIVATE LITIGATION INVOLVING CORPORATIONS AND THEIR DIRECTORS AND OFFICERS: A LEGAL PERSPECTIVE

By Perry E. Wallace, Richard J. Schroth and William H. DeLone

September 2015

HOW CAN BOARDS AVOID CYBERSECURITY PAIN? A LEGAL PERSPECTIVE

By Perry E. Wallace, Richard J. Schroth and William H. DeLone

"We have been hacked!" These are the dreaded words no executive wants to hear. Yet this is exactly how the co-chairman of Sony Pictures Entertainment, Amy Pascal's, Monday morning started when the company discovered its entire computer system had been hacked by an organization called Guardians of Peace. This was one of the biggest attacks in 2014. Several others have followed in 2015 and 2016.

Over the past few years the size and magnitude of cybersecurity breaches have increased. The 2014 South Korean breach, where nearly 20 million (40% of the country's population) people were affected, epitomized the seriousness of the problem. More recently a cybersecurity breach was discovered in Ukrainian banks. Carbanak, a malware program, infected the bank's administrative computers. The breach resulted in banks of several countries, including the USA, Russia and Japan getting infected. The seriousness of the problem can be judged from the 2016 Internet Security Threat Report published by Symantec. Nearly half a billion personal records were stolen or lost in 2015 and on an average one new zero-day vulnerability was discovered each week. When a zero-day vulnerability is discovered, it gets added to the toolkit of cyber criminals.

An IBM study concluded that an average data breach costs about 3.52 to 3.79 million US dollars and it keeps rising every year[1]. It is not just the dollar expense that matters in breach situations. It is very likely that the breach damages the company's reputation, and some smaller unprepared organizations might never recover from a major disaster.

Cybersecurity breaches affect organizations in different ways. Reputational loss and decreased market value have often been cited as significant concerns. Loss of confidential data and compromising competitiveness of a firm can also cause havoc. There is no doubt that preventive mechanisms need to be put in place. However, when an IT security breach does occur, what should be the response strategy? How can the impact of a breach be minimized? What regulatory and compliance aspects should a company be cognizant of? What steps should be taken to avoid a potential attack?

Companies can defend themselves by conducting risk assessments, mitigating against risks that they cannot remove, preparing and implementing a breach response plan, and implementing best practices. Past events have shown that better prepared companies are able to survive an attack and continue their business operations. Experts recommend board of director's involvement in data protection; active participation from senior decision makers can reduce the cost of data breach. There are several other ways managers can prevent, reduce, and mitigate against data breaches.

Reasons for investing in cybersecurity

- Increased frequency
- Greater impact on business continuity
- Data breach costs have skyrocketed

Anthem

Another one bites the dust

On January 29, 2015, it was discovered that Anthem, Inc, one of the nation's leading health insurers, was the victim of a cyberattack whereby cyberattackers attempted to gain access to personally identifiable information about current and former Anthem members. The hackers began accessing the information in early December 2014 and, during a nearly 7 week window, perpetrators were able to gain access to nearly 80 million records[2]. Anthem has indicated that not only current members of Anthem were impacted. On its website[3], Anthem noted, "In addition, some members of other independent Blue Cross and Blue Shield plans who received healthcare services in any of the areas that Anthem serves may be impacted. In some instances, non-Anthem members and non-Blue Plan members may have been impacted if their employer offered Anthem and non-Anthem health plan options. Anthem is providing identity protection services to all individuals that are impacted." Although Anthem maintains that no credit card or financial information was accessed, the threat to individuals' finances remains. The hackers were able to gain access to names of individuals, health

care ID numbers, dates of birth, Social Security numbers, home addresses, email addresses, and employment information. With this data it is easy to create identities and impersonate someone in a variety of settings.

Home Depot

Sheer embarrassment

In the case of Home Depot, in September 2014 the company announced its payment systems were breached which affected nearly 2,200 US and Canadian store locations in a cyberattack that may have started as far back as April 2014. Embarrassingly, Home Depot wasn't aware its payment systems were compromised until banks, and members of the law enforcement community notified the company months after the initial data breach. The Home Depot security breach actually lasted longer than the Target breach, spanning an estimated 4 months resulting in thieves stealing tens of millions of the customer's credit and debit card information. In the six months leading up to 2015, Home Depot processed approximately 750 million customer transactions that presented a treasure trove of information for hackers to focus on.

Sony

Simple blame attribution

Sony faced a cyberattack prior to the expected release of the movie *The Interview* where hackers released username and passwords for staging and production servers located globally, in addition to the usernames/passwords and RSA SecurID tokens of Sony employees. Sony was forced to "turn-off" its entire computer network infrastructure after it was also discovered the hackers posted information for all of Sony's routers, switches, and administrative usernames and passwords to log on to every server throughout the world. As a result of the Sony attack, an estimated 40% of large corporations now have plans to deal with and address aggressive cybersecurity business disruption attacks. The Sony attack, in which hackers also posted embarrassing work emails of the Sony Pictures executives, has led to more buy-in from C-suite and executive boards across all corporations.

Technicalities of a Breach

Now that the attack has happened and victims are reeling from the unsettling feeling that their personally identifiable information is out there somewhere, the real question is how did all this happen in the first place? To answer that question, we must first analyze the security policy that Anthem had in place at the time of their attack in early December 2014. At the time of the attack there were several media reports[4,5], accusing Anthem of inadequate policies for accessing confidential information. The insurer was also faulted for technical evaluation of software upgrades that verified authority of people or entities seeking access to confidential information. In addition to these accusations, the buzzword that surfaced after the attack seemed to be "encryption." Anthem was accused of storing nearly 80 million Social Security numbers without encrypting them. Some would argue that while encryption would make the data more secure, it may also render it less useful.

The root of the issue is not a solitary smoking gun. There are a variety of technical factors that contributed to the inevitability of this security breach, but first and foremost in creating a sound security policy is limiting access. As was mentioned above, Anthem did a very poor job of formulating sound policies for granting access to the various databases and failed to implement adequate measures to ensure unauthorized users who did not have a specific need to access the data were denied access to client data. The secondary issue is the part about encryption; without question, if the data was encrypted, the task of decrypting and making useful information out of the data would have been a significantly more difficult task for the hackers. But let's pretend for a moment that the benefit of using the data in its natural form outweighs the risk of leaving in unencrypted and readily available to hackers in the event of a breach, aren't there other ways of protecting the data? Certainly many companies employ a variety of additional safeguards to protect their data, of which Anthem employed very few. Among these additional safeguards are random passcodes generated on a keyfob that change over a brief period of time, the use of IP based access to remote servers, and the use of random IDs stored

in a separate, unlinked database to name a few. Anthem needs to take advantage of the veritable cornucopia of cutting edge security options to cover themselves from a technical vantage point or risk having disaster occur again.

Home Depot had similar issues and problems with their security policy. Once the attackers gained access to one of their vendor environments, they could use the login credentials of a third party vendor to then open the front door. Once on the network, it was easy for the hackers to exploit a known zero-day vulnerability in Windows. The vulnerability allowed the hackers to pivot from the vendor environment to the main Home Depot network. It was then possible to install memory scraping malware on the point of sales terminals. Eventually 56 million credit and debit card data was stolen. The Home Depot vulnerability could have been prevented. While the network environment did have the Symantec Endpoint Protection, the Network Threat Protection feature had not been turned on. While this may not guarantee security, it would have certainly made life more difficult for the hackers. Moreover, the policy seemed to be deficient in terms of a proper vulnerability management program.

Policy Considerations

There are a variety of technical and human factors that contribute to the inevitability of a breach. In a majority of the cases, fingers have been pointed to the technical inadequacy of the enterprise. In the case of Anthem, it was the lack of encryption. For Home Depot, it was the lack of technical controls to prevent malware from collecting customer data. At Target, there was a basic networking segmentation error.

Occasionally we hear issues related to policy violations. In the case of Anthem, the US Department of Health and Human Services may impose a fine of some $1.5 million because of HIPAA violations. In many instances efforts are made to ensure security policy compliance through rewards, punishment or some behavioral change amongst employees. Rarely do we question the efficacy of the policy. Was the policy created properly? Was it implemented adequately? Were various stakeholders involved? Were there any change management aspects that were considered? These are some fundamental issues that need consideration.

Unfortunately, these questions never get addressed. Security policies keep getting formulated and implemented in a top-down cookie-cutter manner. Organizational emphasis remains on punitive controls. And little attention is given to the content of the policy and how it is related. So, how can organizations ensure that a coherent and a secure strategic posture be developed?

- Security education, training, and awareness programs need to be established and monitored on an ongoing basis
- All constituents are given access to cybersecurity strategic goals, which helps in inculcating ownership and hence compliance
- Various stakeholders should be involved and encouraged to participate in cybersecurity decision-making, which helps with increased compliance.

Reputation and Responsiveness

Reputational damage is significant following a data breach, particularly if a company fails to respond promptly. Following the Anthem, Sony and Home Depot breaches various social media outlets criticized the companies their delayed or inadequate response regarding the breach. In terms of crisis management, a three-day delay is considered significant. Post-crisis communication and a response strategy are essential to ensure that the right message gets through. Transparency in how the breach is being handled has its added importance.

Another well publicized breach was that of JP Morgan, were hackers were able to steal confidential data for nearly 76 million US households. The author and a colleague stated collecting twitter data following the JP Morgan Chase breach in order to undertake a sentiment

analysis. Our objective was to assess how how individuals reacted to the breach. 39,416 tweets were collected during the month of October 2014[6]. Analysis of the results suggests that more than half of the tweets expressed negativity. Other significant findings included:

- When a data breach responsibility is attributed to a company, it results in negative emotions, which in turn translates to negative word of mouth and even severing relationships with the enterprise.
- If the negativity related to the breach is high, it results in a quicker spread of the negative word of mouth sentiment (in our case, Twitter posting exhibited a shorter re-tweet time latency).
- The initial security breach responsibility shapes the reputation of the firm. Hence, it is important to frame the message and security breach responsibility since it has a direct reputational impact.

Risk and Resilience

When a data breach occurs, post-crisis communication is perhaps the only opportunity that a company has to repair its reputation. Crisis situations can potentially have many negative consequences, ranging from losing customers, profitability, and market share to declining stock prices and job losses. A much less explored, but very important factor, is the impact of a crisis on organizational reputation. Corporate risk and resiliency planning are important for organizations to be able to bounce back from disruptions and thus retaining stakeholder confidence. Understanding and identifying potential adverse events in computerized networks is important for planning and implementing resilient mechanisms to defend, detect, and remediate from such threats. The risk reduces when organizations implement both resilient technical and socio-organizational mechanisms. There is a need to integrate risk and resilience mechanisms into the organizational culture to prevent security breaches. There are four key characteristics of any risk and resilience approach:

- The approach should provide a holistic framework, which assesses the systems and their interactions – from a system to the network; from the network to the organization and subsequently the societal impact
- The approach should emphasize capacity to manage the range of hazards.
- There need to be options for dealing with uncertainties, surprises, and any potential changes
- The focus should be on proactive management

Hence a system that effectively reduces risks is going to be more resilient to the security breaches. Risk reduction means a deflection of risk and risk sharing. Also an ability of an organization to prepare for the surprises and effectively responding to the breach incidents characterizes organizational resilience.

Governance

Well-considered governance is at the core of any successful cybersecurity program. Many important aspects require consideration - policy, best practices, ethics, legality, personnel, technical, compliance, auditing, and awareness. Weak governance is often considered to be the cause of organizational crisis. Over the past several decades, we have observed that in institutions where governance was poor or the structures of accountability and responsibility were not clear, they have been susceptible to cybersecurity breaches. For instance, the multi-billion dollar loss experienced by Société Générale because of violation of internal controls by Jérôme Kerviel. Similarly, the case of Barings Bank where Nick Leeson circumvented established controls. Société Générale and Barings Bank showcase a lack of governance as the prime reason for the security breaches. Key principles for a sound and robust security governance include:

- Senior leadership commitment to cyber security is essential for good security governance
- Cyber security is considered strategically with due consideration of risk management, policy, compliance and incident handling

- Clear lines of communication are established between strategic thinkers and operational staff.

Steps to avoid a potential attack

Managers can take steps today to avoid potential breaches and mitigate damage when breaches occur. There is a vast amount of data from many sources that purports to answer exactly how to prepare for the inevitability of a cyber attack. Because the nature and purpose of every attack is different and the composition of every business is different, there is no single prescription for prevention. However, by boiling down the data from multiple sources, we can derive a list of high-level practices that all organizations should adopt.

- Executive buy-in
    - In order to create an optimal cybersecurity policy, support has to come from the top levels of the organization. Security must become a core part of the organizational culture.
- Fully understand your risk profile
    - By knowing your industry and its attack vectors, what is valuable to your organization and how to protect those assets, security personnel can effectively create, support and promote cyber security initiatives.
    - Identify and classify different cyberattack scenarios.
- Take threats seriously
    - Many organizations understand the full extent of the damage that can be done during an attack as well as the aftermath. However, many companies choose to ignore the possibility of such an attack happening to them, or they are willing to accept the risk of not taking adequate precautions due to cost or complexity.
- Policy Enforcement
    - Policies can be as simple as a strong password, but should ideally go well beyond passwords. Security policies should be documented and automated wherever possible to avoid human error or omission. Circling back to Executive Support, policies should be a part of the culture that everyone chooses to follow.
    - Keep things in simple terms that non-IT executives and users can understand.
- Training
    - Security awareness and policy enforcement is crucial in order to create a security culture within an organization. Awareness of policies, security and other, should be of paramount concern to all organizations.
    - There should be specialized training for those that deal with the most sensitive data in the company.
- Employee Screening
    - Not all possible employees possess the same moralities as the business owners and stakeholders. Employees should not only be screened to ensure that their skills meet the requirements of the positions but, more importantly, that their beliefs closely match those of the organization.
    - Remember that people are often the weakest link in a security chain
- Offline backup of critical data
    - Data is the lifeblood of an organization. Data loss is often as damaging, monetary and brand, to an organization as a data breach. Many organizations never fully recover from data loss events, some go out of business entirely. A copy of critical data in a secure offsite location is one small step that should not be overlooked.
- Invest intelligently in security
    - Information overload prevents many organizations from making intelligent

security decisions. There are a thousand vendors pitching a thousand variants of "best practice" security models. Create a plan based on the needs of the organization and implement policies and tools that augment the plan. Avoid tying your security policy to any vendor's software or hardware. There is no "one-size-fits-all" solution.

- One of the more direct methods for avoiding a security breach is to implement application whitelisting. Application whitelisting can prevent many forms of a breach where the spoofing of an application allows a virus or malware to traverse firewalls and scanners without detection.

- Keep systems updated
  - Another direct method for avoiding a breach is simply to apply security patches to software and hardware systems on a prompt and routine schedule. This may appear to most as a "no-brainer" but is often overlooked.

The detailed list above describes concepts that every organization should consider to improve their cyber security preparedness. These concepts can be tailored to fit the individual organization culture and data protection requirements. Regardless of the specifics, every organization should understand the company's security chain. The CEO must enable the Chief Compliance Officer (CCO), the Chief Privacy Officer (CPO), the Chief Information Officer (CIO) and so on, to ensure each understands their role before, during and after an attack. Working together, these individuals must create and own an enterprise-wide Incident (or Risk) Management Plan, a Data Management program, an Incident Response Plan and communication/reporting plans.
Once the above initiatives are in place, more detailed workflows, such as the Continuous Diagnostics and Mitigation (CDM) program from the Department of Homeland Security (DHS), can be adopted. This program utilizes commercial off-the-shelf (COTS) software and hardware to continually monitor for security related events as well as continuously improve upon processes and risk prioritization. A CDM-style framework, see figure 1, also provides a practical model that any organization can adopt and tailor to meet its specific cyber security requirements.

In this day and age managers have to be proactive in preventing an attack. No longer is the question asked if companies will be hacked but rather when they are hacked what will be the protocol. Being vigilant about even the smallest and seemingly insignificant changes can be extremely useful. To protect customers and employees from having their financial or private information stolen, both industry and governments have implemented regulations with the intent of securing against common cyber-attacks. To combat credit card fraud, the Payment Card Industry created the Data Security Standard that requires merchants who process credit cards to take specific measures that help protect against hacking attacks. The European Union, United Kingdom, United States, and Canada are among the governments that have also instituted privacy acts meant to regulate how businesses protect their customer and employee data from malicious hackers.
In addition to the fees and legal ramifications that can come as a result of failing to comply with the

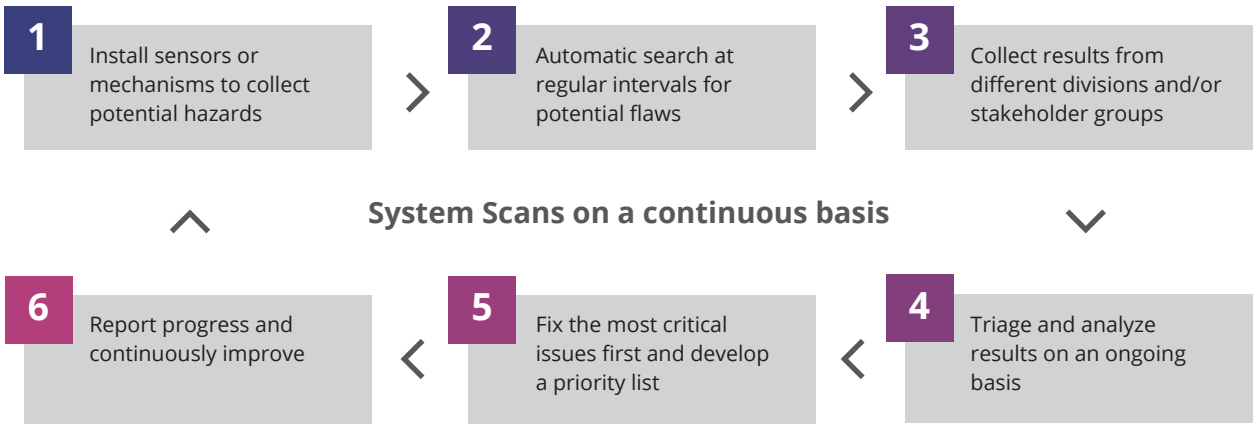

Figure 1, Continuous Diagnosis and Mitigation Framework

different regulations, hacking attacks can also damage a company's reputation or brand to the point that they lose customers and revenue. A company who is in the news because they have been hacked is sure to lose the trust of even their most loyal customers. The same happens with web sites that are identified as containing spam or malicious scripts. Once this is known, most visitors will stay away. A company's brand, once damaged, may never be restored to its former status. Despite the restoration of services at Sony Pictures after the breach earlier this year, the Sony brand continues to fall under scrutiny. While monetary losses from the breach were significant, losses because of a damaged brand will continue to plague Sony for years.

How to respond when a breach occurs

As discussed above, managers and organizations should take preventative steps to avoid the risk of a breach occurring. After spending time planning, spending money, and training employees, someone still manages to break through the organization's security measures? What do you do now?! Once a breach has been discovered, the organization should take the following immediate steps to limit the breach.

Step 1: Survey the damage

Following the discovery of the breach the designated information security team members need to perform an internal investigation to determine the impact on critical business functions. This deep investigation will allow the company to identify the attacker, discover unknown security vulnerabilities, and determine what improvements need to be made to the company's computer systems.

Step 2: Attempt to limit additional damage

The organization should take steps to keep an attack from spreading. Some preventative strategies include:

- Re-routing network traffic
- Filtering or blocking traffic
- Isolating all or parts of the compromised network

Step 3: Record the details

The information security team should keep a written log of what actions were taken to respond to the breach. The information that should be collected include:

- Affected systems
- Compromised accounts
- Disrupted services
- Data and network affected by the incident
- Amount and type of damage done to the systems

Step 4: Engage law enforcement

A major breach should always be reported to law enforcement. The law enforcement agencies that should be contacted are:

- The Federal Bureau of Investigation (FBI)
- The U.S. Secret Service (USSS)
- The U.S. Immigration and Customs Enforcement (ICE)
- The District Attorney
- State and Local law enforcement

Many companies wait until after a security breach before contacting law enforcement, but ideally the response team should meet with law enforcement before an incident occurs. The preliminary

discussions would help an organization know when to report an incident, how to report an incident, what evidence to collect and how to collect it. Once the incident is reported, the law enforcement agency may contact the media and ensure that sensitive information is not disclosed.

Step 5: Notify those affected

If a breach puts an individual's information at risk, they need to be notified. This quick response can help them to take immediate steps to protect themselves. However, if law enforcement is involved, they should direct the company as to whether or not the notification should be delayed to make sure that the investigation is not compromised. The individuals are usually notified via letter, phone, email, or in person. To avoid further unauthorized disclosure, the notification should not include unnecessary personal information.

Step 6: Learn from the breach

Since cybersecurity breaches are becoming a way of life, it is important to develop organizational processes to learn from breaches. This enables better incident handling, should a company be effected by a breach in the future. Some learning issues include:

- Document all mistakes
- Assess how the mistakes could have been avoided
- Ensure training programs incorporate lessons learnt

The above responses to an event in progress should not be a surprise. These reactions should be rehearsed components of an organization's Cyber Incident Response Plan. Keep the plan up to date. Without a plan, confusion ensues and costly mistakes will likely be made. Working a plan will show to law enforcement and the public that your intentions are good and will likely reduce fallout. Ensure the plan calls out Key Assets. Have those resources at the ready. Identify tools and processes that will be used and followed. Knowing your industry and what is valuable to your organization (or what is valuable to someone looking to exploit your resources) will allow you to understand the attacker's intent and allow for proper assessment of the threat and proper plan execution. Have a post-attack plan to ensure effective triage after the event. Use this plan to prioritize the efforts required to recover from a cyberattack, understand the extent of the damage, and minimize further damage. Close gaps in the environment and work the plan in such a way that it prevents causing more harm. Once again, document everything. Thorough documentation fosters credibility for your organization, prevents repeats of mistakes, and produces confidence throughout the organization. Figure 2 summarizes the response process for a cyber security breach.

How to respond to a breach

A six step process

Figure 2, How to respond to a breach

Best practices: How to be prepared for an intrusion

Companies should use good judgment in avoiding, preparing for and managing security events (even presumed events). History shows us a mixed bag of responses by major organizations. In Target's case, during the 2013 attack where payment card readers were infected, much evidence points to negligence by the retail giant. The retailer's FireEye malware detection product was found to be perfectly functional. In fact, the software found the same malware infection on consecutive attacks. There is an assumption based on these facts that Target either did not know how to read the data that the monitoring tools were reporting or that they intentionally neglected to report the breach. The net effect of either ignorance or negligence was huge brand damage to the retailer and sales numbers dropped for some time. Having an adequate response plan along with notifying law enforcement and victims in a timely manner could have reduced the fallout for Target. In contrast, Anthem's response to the January 2015 breach was swift and thorough. Anthem found the breach themselves, reported it immediately to federal law enforcement and set up a website and hotline for impacted customers. Anthem further offered its customers identity protection services. Contrasting the Anthem and Target attacks: Anthem appeared to be poorly prepared for a breach, as the stolen data should have been encrypted, yet their response was almost textbook; Target had the appropriate monitoring in place, yet they either did not understand the reports or neglected to act on them appropriately. Despite Anthem's quick and forthright response, brand damage was still done due to their perceived lack of focus on cybersecurity. The 2014 Sony Pictures hack, however, was a different beast. The data breach affected mostly current and previous employees, not customers. It was a rapid and focused attack on Sony Pictures bent on inflicting brand damage to the company. Sony has eluded scrutiny in their preparation and response to the attack due to the assumption that the hack was conducted by North Korean operatives and was sensationalized as an act of cyberterrorism. Sony did offer its employees identity protection services in response to the personal data loss.

Must Do's

- Organizations must put the proper resources in place to ensure that any form of cybersecurity breach is dealt with swiftly and efficiently.
- There should be an effective Incident Response Plan.
- Thoroughly check all monitoring systems for accuracy to ensure a comprehensive understanding of the threat.
- Engage in continuous monitoring of their networks after a breach for any abnormal activity and make sure intruders have been inhibited thoroughly.
- It is important to perform a post-incident review to identify planning shortfalls as well as the success in execution of the incident response plan.
- Be sure to engage with Law Enforcement, and any other remediation support entity, soon after the threat assessment is made to allow for containment of the breach and to inform any future victims.
- Documentation is paramount. Thorough documentation from the onset of the breach through the clean-up must be a priority to ensure continual improvement of the Incident Response Plan.
- It is critical to the success of a business to integrate cybersecurity into its strategic objectives and to ensure that cyber security roles are defined in its organizational structure.

Some best practices for being prepared for a cybersecurity breach are:

The Chief Information Security Officer Role

The Chief Information Security Officer's role is essential for large organizations. This position must be integrated into the organizational structure in such a way that it is included in all strategic planning discussions at the executive level. The inclusion ensures that information security is included in high-level strategic planning and that C-level executives are considering risk assessment along with other strategic planning objectives, including investments and business development. The CISO role will be able to assist in identifying an Information Security structure, and building policies and procedures that protect an organization's most important assets.

Business Continuity Plan with Cybersecurity Integration

As global cyberattacks increase, organizations must plan around this imminent danger. When we look at the broad impact of the cyberattack on Sony, it is apparent that organizations need to invest in business continuity plans with cybersecurity as a focal point. Many organizations are already doing this. However an astonishing four in 10 companies have no formal security strategy[7]. In another survey it was found that 83 percent of small and medium sized businesses have no formal cybersecurity plan. It goes without saying therefore that cybersecurity plans are important and need to be instituted. Plans can include a broad spectrum of responses, ranging from network auditing and segmentation to coordinating the release of information to media. Organizations must evaluate existing business continuity plans and ensure that information security strategy is included.

Shift from Remediation to Prevention

Many large organizations have sophisticated network security mechanisms. These include security-oriented network designs, network intrusion prevention systems, and the most traditional systems like enterprise antivirus, firewall, group policy, and patch deployment. These systems have been effective for preventing most attacks, and are somewhat effective for helping to identify where a breach may have occurred, but are not sophisticated enough for more advanced attacks, which are often the most damaging.

For an organization to move ahead of the threat of cyberattacks, it must go beyond traditional security systems, and shift focus to more preventative solutions. Organizations must invest in tools that bring the organization to the front of cybersecurity, with a focus on prevention. Below are some examples of preventative tools and techniques that organizations can invest in:

- **Threat Detection.** Organizations should focus on investigating and learning about breach attempts. An effective detection and response system should be implemented.
- **Network Traffic Inspection.** Network traffic inspection is essential for anticipating cyberattacks. A good network engineer should be asked to perform network traffic analysis as a daily routine.
- **Network Segmentation.** Many organizations are segmenting business units from the network level, using VLAN technology. This type of segmentation ensures that in the event of a cyberattack, problem areas are isolated as they are investigated.
- **Penetration Testing.** Penetration testing should be performed on a continual basis, to ensure that network security is maintained at the highest level. In addition to network penetration testing, social penetration testing should occur, to ensure that employees are trained on safe business communications practices.

Auditing and Monitoring

As cybersecurity risks increase, it is important to ensure the organization's workforce is using information systems safely and securely. All too often, business units find themselves creating their solutions when IT is not involved, which leads to a significant security risk. An example would be the use of cloud storage services like Dropbox, which end-users can very easily install and setup for sharing and storing business information. With

the appropriate computer usage policies in place and the right governance structure, an effective CIO should be able to ensure that end users are complying with the right policies and procedures.

Even with perfectly functioning IT governance, it is important to check in with business units to ensure they are following policies and procedures. The best approach to ensuring security best practices is to perform continual IT assessments. Assessments, when supported by the organization, allow IT to review how individual business units are using technology to perform business functions. This assessment produces a report that allows the CISO to see overall compliance with security policy and identifies risks that can be mitigated. Logins should be tracked and reviewed for any activity outside of what is expected. Systems that don't automatically log activity should have such logs created. Programs that employees download and websites they visit should be reviewed for potential risks. Let employees know tracking mechanisms are in place to ensure cybersecurity. This will discourage them from engaging in non-work related internet activities that can be risky. Informing employees informs the workforce that not only is monitoring most essential, but employee awareness of the practice is very important as well.

Focus on Employees

While an organization can put in place state-of-the-art security infrastructure, with a security focused organizational structure, these root level improvements cannot prevent employees from causing harm. Research over the years suggests that employees are at the root of most cyberbreaches. Employees are most capable of an error—sending a confidential email to the wrong email address, forgetting to protect a sensitive document, or having their business-connected mobile device stolen. While IT policies can be implemented to prevent most of these occurrences, employees may not always follow the policy, and will inadvertently put the business at risk.

The best way to mitigate this risk is to put in place a security training program for the workforce. Many organizations already do this for various compliance requirements, like HIPAA. The objective is to provide the workforce with best practices for various processes and systems. Employees need to know how to recognize phishing attempts via phone, email, and other methods. Require strong passwords and enforce penalties up to and including termination for sharing them. Educate employees on how to recognize suspicious websites. Share stories of current security attacks in the news to explain how those companies were compromised and how the incident is affecting the business. Most employees are loyal to their company. They will gladly work to ensure its success if they are informed, understand how important their role is in cybersecurity, and feel as if they are part of the solution.

In some cases, a disgruntled employee may be at the root of a cyberattack. Disgruntled employees are capable of significant long-term damage to an organization. Below are a few solutions to mitigate this risk:

- Implement clear access rules to ensure employees have access to only the information they require.
- Put in place auditing process for access granted to business resources, including a reporting/review process.
- Ensure termination processes include functions for disabling access to business systems.

Pay Attention to Personal Devices

In today's age, personal devices are a given risk. They have allowed companies to augment performance and throughput by giving access to systems outside of standard business hours and locations. But allowing access to secure systems via these devices can be extremely risky. Personal devices can range anywhere from cell phone devices to mini thumb drives. Within today's society, cell phones are considered dependencies with the mass majority of the corporate workforce. Making actual phone calls from these devices is probably in the low percentile of true usage needs, vs. the email and social media components. Connecting these devices to Wi-Fi based networks is an automatic "necessity" for most users. The logic

for this ranges from the financial impact of cutting cost on the monthly utilization bill to speeding up the use of a cell phone application. Most organizations have “guest” Wi-Fi connections within their infrastructure, and these are not always secured to prevent potential spam infestations, major or minor. Controlling these connections with protocols that require users to register for usage is a good way to track these devices down when they cause risk.

Conclusion

Data breaches can happen to a wide range of organizations. Most likely, the attacker aims towards bigger corporations that have a lot at stake. However, instigators may also target smaller organizations with malicious attacks. Statistics show us that the cost of an attack is high and is increasing yearly. It is up to the company’s management to adopt a cybersecurity policy and data breach response plan. Managers should evaluate their system and sensitivity to a potential data breach. They also need to keep in mind that the attacks do not just come from outside intruders. They can come from outside as well and employees are either knowingly or unknowingly contributing to an attack. Sony’s data breach constitutes a great example that an employee generated data breach can go unnoticed for months and the outcome to the company may be grave. If a breach does occur, a good security response strategy should help mitigate the impact. A good plan should have response actions listed and responsibilities assigned to team members. It should detail contingencies and prepare for business continuity. Every minute a company is not functioning the revenue stream is impacted and overall financial health is in jeopardy.
Managers have access to the best industry accepted practices that allow them to reduce infrastructure weaknesses and defend the company against potential attacks. Following best practices can also reduce the impact if an attack does occur to aid in normalizing company operations more quickly. Managers cannot prevent cyber attacks, and due to the expanding technology, they are increasing in occurrence and cost every year. The best practice for any size company is to develop security measures and a response plan if a breach occurs.

END NOTES

[1] 2015 Cost of Data Breach Study: Global Analysis. Ponemon Institute, May 2015.

[2] Hummer, C. (2015) Anthem says at least 8.8 million non-customers could be victims in data hack. Technology, Reuters. Feb 24, 2015.

[3] Following the breach, Anthem developed a dedicated website to share facts related to the breach (http://www.anthemfacts.com)

[4] Murphy, T (2015). Hackers infiltrate insurer Anthem, access customer details. Richmond Times Dispatch. February 5.

[5] Fox News: http://www.ktvu.com/business/4155658-story. Accessed June, 15, 2016.

[6] The research reported here is from: Chowdhuri, R. and Dhillon, G. (2015). Dynamics of Data Breaches in Online Social Networks: Understanding Threats to Organizational Information Security Reputation. Proceedings of the International Conference on Information Systems. Dallas, December 13-16, 2015.

[7] O'Dwyer, P. (2016). Firms 'lack cyber security plan'. Irish Examiner. May 4.

THIS PUBLICATION IS SPONSORED BY

A.T. Kearney

Discovery Communications

Raytheon

FINRA

protiviti

Kogod School of Business
American University • Washington, DC

CYBERSECURITY GOVERNANCE CENTER ADVISORY COMMITTEE

Ben Beeson,
Cybersecurity Practice Leader, Lockton (Insurance Brokerage)

John Brady,
Chief Information Security Officer, FINRA

Steve Cooper,
CIO, US Department of Commerce

Jim Dinegar,
CEO, Greater Washington Board of Trade

Renee Forney,
Deputy CIO of Enterprise Operations, US Department of Energy

John Gambale,
Head of Professional Liability, AIG

Bruce Hoffmeister,
Global CIO, Marriott International

John Honeycutt,
CTO, Discovery Communications

Gary LaBranche,
President & CEO, Association of Corporate Growth (ACG)

Scott Laliberte,
Managing Director, IS Security and IT Audit Services, Protiviti

Israel Martinez,
President & CEO, Axon Global Services

Jim Messina,
The Messina Group, former White House Deputy Chief of Staff

Hitesh Sheth,
President & CEO, Vectra Networks

Howard Steinman,
Partner, AT Kearney

Dr. David Swartz,
Vice President & Chief Information Officer, American University

Ralph Szygenda,
former CIO, General Motors and Senior Fellow, Kogod Cybersecurity Governance Center

Stuart Tryon,
Special Agent in Charge, U.S. Secret Service, Criminal Investigative Division

Leif Ulstrup,
CEO, Primehook Technology, LLC, former VP & GM Business Services for the Computer Sciences Corporation and Kogod Executive in Residence

David S. Wajsgras,
President, Intelligence, Information and Services, Raytheon

AFFILIATED CYBERSECURITY LEADERS

Donna Dodson,
Chief Cybersecurity Officer, NIST Liaison to KCGC

KOGOD CYBERSECURITY GOVERNANCE CENTER FACULTY MEMBERS

Dr. Erran Carmel,
Dean Kogod School of Business

Dr. Parthiban David,
Faculty Research Director, Kogod Cybersecurity Governance Center (KCGC)

Dr. William DeLone,
Executive Director, KCGC

Dr. Gwanhoo Lee,
Research Associate, KCGC

Rebekah Lewis,
JD, Associate Director, KCGC

Dr. Rich Schroth,
Executive Director, KCGC; Managing Director of the Newport Board Group Cyber Practice; NACD Board Leadership Fellow & Kogod Executive-In-Residence