Cyber Breach Coaching

GIAC (GCIH) Gold Certification

Author: Michael Hoehl, mmhoehl@gmail.com
Advisor: Stephen Northcutt

Accepted: December 29, 2014

Abstract

Data Breaches and Cyber Security are a new source of worry for the modern CEO. As demonstrated by several recent security breaches, how an organization handles a crisis plays a major role in whether the CEO (and CIO, COO, CPO, etc.) stays employed. Further, Corporate officers can be held personally liable if information security safeguards are not sustained in a commercially reasonably manner to prevent breaches from occurring. This paper proposes a new chapter to the CEO Survival Guide, and explores the current Cyber Breach Coaching options available to executives and organizations.

> "Data is more valuable than money. Once spent, money is gone, but data can be used and reused to produce more money." -- Deloitte 2010 Report

1. Introduction

Today, it is hard to find a business that is not in some way connected to the Internet and cyberspace. The expanding role of cyberspace has created new business opportunities for organizations that were simply not possible just a few years ago. Further, cyberspace is ubiquitous with no geographic boundaries. This opens the door to customers all around the globe.

Unfortunately, the same cyberspace used for lawful commerce and business automation provides a surface of attack for criminals. A growing number of individuals and groups are using cyberspace to unlawfully duplicate, distribute, or destroy confidential electronic information. The target data includes financial reports, employee salary, customer lists, passwords, trade secrets, marketing plans, identity information, and payment card numbers. This data has become a form of currency in some cases. Unfortunately, this currency is in an electronic format that a traditional safe or lock cannot adequately protect from theft. Physical and logical controls that had protected this data in the past can now be circumvented with just a few careless clicks on a website or a phishing email. The source of the threat might be half way around the world. Physical proximity is not required for cybercrime. Criminals have learned to use cyberspace to target businesses in countries of other jurisdictions, making law enforcement much harder. The lack of broad country accession to treaties like the Budapest Convention on Cybercrime has made extradition of cybercriminals almost impossible. According to Paul Day, this treaty condition is "allowing cybercriminals in those countries to plunder computers across the world with little fear of legal retribution" (Day, 2014).

In a 2014 study conducted by Corporate Board Member & FTI Consulting, Inc., nearly 500 corporate directors and general counsel were surveyed (FTI, 2014). Survey results showed managing Cyber Risk as a top concern. According to Thomas Brown, Senior Managing Director in the FTI Consulting Global Risk & Investigations Practice, "Cyber risk's pervasive nature presents an existential threat to the operation, reputation

and bottom line of virtually every company, regardless of industry. The priority that board members and general counsel place on cyber security and data protection not only reflects this reality, but is entirely in line with our experience assisting clients to address this threat."

The reason for this concern is there are several business direct and indirect losses associated with cybercrime and data loss. Direct losses include professional services fees (e.g., attorney fees, public relations services, temporary call center services, forensic experts, auditors, temporary IT staff augmentation, consumer credit monitoring, etc.), asset replacement (e.g., archiving tape replacement, Point-of-Sale hard drives, consumer credit card replacement, etc.), logistics (e.g., travel and living expenses for incident response teams, shipping expenses, consumer mailings, etc.), fines, business continuity expenses, and new security controls necessary to prevent future attacks of similar method (e.g., new firewalls for additional segmentation, new intrusion prevention technology, website coding changes, software updates, security patch deployment, etc.). Indirect losses can also be significant including drop in revenue, missed business opportunities, delayed project and product rollout, increased vendor service fees (e.g., credit card payment processing fees, future auditing services, etc.), security awareness and technology training, and additional recurring operational expenses to sustain new security controls. In the 2012 report "Measuring the Cost of CyberCrime" (Anderson, 2012), the hidden costs of cybercrime, including defense and indirect costs, exceed that of direct costs. Unfortunately, many of these direct and indirect expenses are unplanned and not in budget. These events can have a negative impact on an organization's cash flow and liquidity.

In addition to financial impact, cyber-breaches can cause broad collateral damage to members of a victim organization. First responders, forensic experts, IT staff, legal counsel, call centers, human resources, and management can be consumed by the commitment of time and effort associated with cyber-breach response. Further, a cyber-breach can cause major organizational shake-ups and impact the career of business leaders. History shows that CEO, CFO, and CIO are not immune to the fallout of a

cyber-breach incident. For these organizational leadership roles, the response to the cyber-breach is as important as the prevention efforts prior to the breach.

Unfortunately, there are several examples of cyber breaches that organizations were not adequately prepared for, and would have greatly benefited from Cyber Breach Coaching. According to Michael Bruemmer of Experian (Bruemmer, 2013), three of the most common mistakes include:

- No engagement with outside counsel — Enlisting an outside attorney is highly recommended. No single federal law or regulation governs the security of all types of sensitive personal information. As a result, determining which federal law, regulation or guidance is applicable depends, in part, on the entity or sector that collected the information and the type of information collected and regulated. Unless internal resources are knowledgeable with all current laws and legislations, it is best to engage legal counsel with expertise in data breaches to help navigate through this challenging landscape.
- No external agencies secured — All external partners should be in place prior to a data breach so they can be called upon immediately when a breach occurs. The process of selecting the right partner can take time as there are different levels of service and various solutions to consider. Furthermore, companies need to examine vendors' integrity and security standards before aligning the company brand with a particular vendor. Not having a forensic expert or resolution agency already identified will delay the data breach response process.
- No single decision maker — While there are several parties within an organization that should be on a data breach response team, every team needs a leader. Determine who will be the driver of the response plan and primary contact to all external partners. Also, outline a structure of internal reporting to ensure executives and everyone on the response team is up to date and on track during a data breach.

In many cases, an organization has only limited experience with responding to a cyber breach, so coaching in advance and during a cyber-attack is vital. For many

Author: Michael Hoehl, mmhoehl@gmail.com

organizations, these three common errors are not typically within the sphere of responsibility of IT to act on. These responsibilities fall on the shoulders of the CEO and business leaders. A Cyber Breach Coach is an expert in these three areas and can guide IT and top executives so they avoid these same mistakes.

Joseph V. Demarco states, "When a data breach occurs, there is a cascading series of decisions to make—irrevocable decisions which must be made quickly and with imperfect information. These decisions cannot be outsourced or delegated. It is essential, therefore, for every CEO to have an understanding of his or her company's technology organization, where its data resides, and how his company moves information around the company. Moreover, it is critical that a CEO think ahead of time about the series of recurring decisions he or she must make when responding to data spills or breaches" (Demarco, 2012). Ultimately, the CEO is responsible for the actions of an organization during a breach. So where does a CEO or CIO go for guidance for this seemingly inevitable crisis event? A new role known as a Cyber Breach Coach is emerging that provides vital insight to executives and businesses at risk of a cybercrime.

NOTE: This document is not intended to provide legal advice. No implied endorsement is intended for vendors mentioned in this document. The purpose of this document is general public education; it is not a substitute for legal or other professional advice. Do not rely exclusively on this document for guidance on data breach and risk management. Consult appropriate legal counsel for questions regarding business obligations and risk management for your organization.

2. Evolution of Cyber Breach Coaching

The concept of Cyber Breach Coach has evolved over time much like cyber risk. Initially, the title Cyber Breach Coach was simply a marketing spin on familiar privacy attorney services. A Cyber Breach Coach at a law firm would be engaged by a business only after a data breach was confirmed (e.g., Retail merchant credit card data theft) and government regulations mandated a coordinated and prompt notification of unauthorized access to consumer data. Breach notification is a key duty for an organization if a data

breach has occurred. New legislation has made fulfilling the breach notification duty complex. For the United States, privacy related law is governed at the state level. In other parts of the world, privacy is legislated at a federal and even multi-county level (e.g., European Union Data Protection Directive). As a result, determining what requires data breach notification, how this notification should occur, and timing of notification is challenging. "The regulatory duties and liability risks that companies now face take many forms, and go far beyond requiring a determination of whether and when a breach is sufficiently material to trigger (where applicable) SEC and state disclosure obligations. Companies also might face potential enforcement and private civil actions brought by, for example:

- FTC
- SEC
- State attorneys general
- U.S. Department of Justice
- Plaintiffs whose data is compromised (e.g., customers, clients, corporate partners, vendors, unrelated third-parties including affected banks, etc.)
- Shareholders

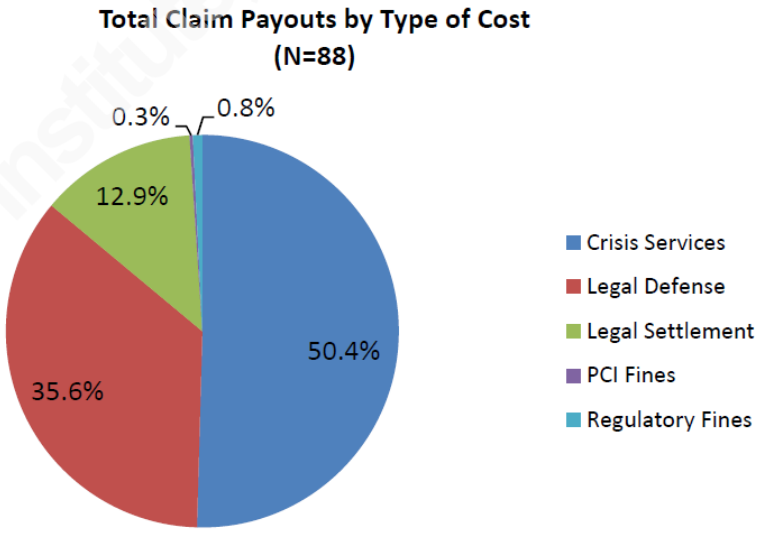
(Germano, 2014). Unfortunately, breach notification is just one of many legal considerations for victims of cybercrime.

As the frequency and scope of cyber breaches have increased year over year, a new insurance instrument was created for businesses. Cyber-breach insurance (also known as cyber liability insurance) products are now being offered for businesses that cannot underwrite the liability of a cyber-breach and wish to assign the financial risk. This insurance product first appeared in the late 1990s. According to Karl Pedersen, a senior vice president at global insurance broker Willis, "the market is maturing, with over 60 insurers now writing cyber coverage" (ABA, 2014). Insurance companies are now including with their insurance product offering a Cyber Breach Coach option. This offering benefits the insured as well as the insurer. The insured benefit from the guidance. The insurer benefits by improving threat response as well as reducing the actual payout necessary. Costs associated with State Attorney General litigation, fines, and notification mismanagement can be avoided by engaging a Cyber Breach Coach

early when an incident occurs. In some cases, the Cyber Breach Coach also guides the insured with the selection of professional service providers necessary for cyber-breach response. These professional service providers have pre-negotiated discount rates for the insurance company customers. This again helps to reduce the overall expense of the cyber-breach and cost absorbed by insurer. It is important to note that the entire loss associated with a cyber-breach is not necessarily covered by insurance. In some cases, the victim organization still has a significant financial burden to bear. For example, recent SEC filings by public stock traded retail companies suffering a breach in 2013 and 2014 reveal insurance covered less than half the total liability.

A study of actual cyber liability and data breach claim payouts by Mark Greisiger of NetDiligence in 2013 reveals the top costs are associated with Crisis Services and Legal Defense (please see Figure 1 below).

Figure 1: NetDiligence 2013 Cyber Liability & Data Breach Insurance Claims - A Study of Actual Claim Payouts



Cyber Breach Coach expertise includes Crisis Management and Legal Action. This expertise can help organizations improve execution of response and reduce cost of professional services. Considering a victim organization will still have a significant unplanned financial obligation as a result of the cyber-breach and the majority of the

claim payout is associated with crisis services and legal guidance that the Cyber Breach Coach is an expert with, the need for a Cyber Breach Coach is becoming more compelling for both insured and insurer.

While not all cyber-attacks require breach notification, recently several companies have elected to perform a breach notification even without any legislated or regulated obligation. Privacy Policy commitments and the desire to keep good faith with customers has compelled organizations to conduct breach notifications. This is a complex business decision. Further, not all organizations have a Chief Privacy Officer or an expert on all relevant privacy law. During projects or when data exchange with partner vendors is being considered, the Cyber Breach Coach expertise can be tapped. A Cyber Breach Coach can be engaged to explain data types eligible for privacy law consideration, precedent, and prior customer response (positive and negative) to elective notification.

As mentioned earlier, a cyber-breach event can have a career ending impact on a CEO or CIO. Board of Directors and Officers are also at risk of the possibility of a shareholder lawsuit alleging fiduciary duties and sufficient steps were not met to protect the company from a breach and its consequences. A survey by Corporate Board Member and FTI Consulting in 2014 revealed only a third of general counsel feel "very confident" in their company's ability to respond quickly to a security breach and determine whether confidential data had been compromised, and less than a quarter of directors felt the same (FTI, 2014). The Cyber Breach Coach can benchmark the organization with industry peers to qualify whether sufficient oversight and investment is in place. The Cyber Breach Coach serves as an outside, independent expert that works across the organization to answer the key question, "How do I know we are properly prepared for a cyber-breach?"

3. Making the Case for Cyber Breach Coaching

The 2012 report "Measuring the Cost of Cybercrime" by Ross Anderson (et al.) advises, "…we should spend less in anticipation of cybercrime (on antivirus, firewalls,

etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail." Cyber-breach prevention (defense) is commonly associated with IT and Security. In many cases, organizations also assume that response to a cyber-breach is substantially an IT or Security function. Though they both serve a key role, a cyber-breach demands a planned response coordinated across many internal teams including Finance, Legal, HR, PR, IT, Commercial Operations, Customer Service, Finance, and Vendor Management--as well as external teams including law enforcement, state attorneys, regulators, vendors, media, and consumer advocacy groups. Leading all these teams during a crisis might not be the domain of responsibility for IT. Further, IT might be fully engaged in the technical demands of the incident handling that there is limited capability to perform other crucial duties. If a Security Manager or CIO identifies this gap, how do they make the case for enlisting a Cyber Breach Coach?

"First, you had better know your data, know how your data flows in and out of your organization, where data is stored when not in use, and who has potential access to it. Remember that there are different types of data driven by the business you are in, and understanding the sensitivity of that data is critical. Due to the nature of technology and expansiveness of data through your network, trying to protect all of your data at the same security level is futile. You must be able to identify and separate the non-sensitive data from the sensitive." (Angelo, 2014). Consider all locations of data, not just that residing within company owned assets. Many organizations have confidential data hosted remotely by vendors. These vendors might include cloud computing service organizations, franchisees, professional services providers, CRM services, data archiving providers, and call centers. The data classification and transportation evaluation will help confirm whether a Cyber Breach Coach is appropriate and where the services might provide greatest value.

Once this initial assessment of data sensitivity, flow, and touch points is complete, it is time to estimate the liability the organization has if the data safeguards fail. Initial qualitative considerations include reputational risk and loss of consumer trust. These are important considerations; however, these indirect losses tend to be highly debated when translated into quantitative values. During the first phases of evaluation, consider

focusing first on direct costs that occur when the sensitive data and associated IT systems are compromised. These costs could include the following:

- **professional services fees** - attorney fees, public relations services, temporary call center services, forensic experts, auditors, temporary IT staff augmentation, consumer credit monitoring, etc.;
- **asset replacement** - archive tape replacement, Point-of-Sale hard drives, consumer credit card replacement, etc.;
- **logistics** - travel and living expenses for incident response teams, shipping expenses, consumer mailings, etc.;
- **fines** - bank fees, state fines for late notification, etc.;
- **business continuity expenses** – this assumes information systems are temporarily unavailable while threat is contained, important assets are seized by regulators as part of investigation, or departments are inhibited from performing their duties during event.
- **new security controls** – changes necessary to prevent future attacks of similar method (e.g., new firewalls for additional segmentation, new intrusion prevention technology, website coding changes, security patch deployment software, etc.).

When exploring the financial costs, also gather duration and effort time estimates to perform each duty during a crisis. This will reveal how long it would take to put in place the people, process, and technology necessary to respond to the cyber-breach. Although the total direct cost might be palatable to Management (possibly with the help of insurance), the initial time estimate to perform all the necessary incident response activities might not be acceptable. In the past, this timing would have been compared to legislated and contractual obligations. This is no longer the case. The new breach notification standard is dictated by Social Networks and the Press. Now, businesses might have to prepare for public statements and incident handling far faster—even though regulators and investigators have already been properly engaged. A call from a

journalist formerly from the Washington Post might require a business to make a public statement and commitments the same day.

If determining these direct costs is a significant investment of time, an insurance broker is a great source for credible estimates associated with these liabilities. They offer benchmark data that will substantiate your estimates, too. Once these initial steps are completed, now there is enough quantitative information to assess risk and identify gaps. If the sum liability in time and money exceeds the organization's risk appetite, then a Cyber Breach Coach might be of value.

Socialize the role of the Cyber Breach Coach and map it to specific business risks. Ask "what if?" questions during conversations with organizational leaders. Examples of questions to stimulate thought include:

- What if the website or payment gateway was down during the forensic investigation, would a disaster recovery declaration be appropriate?
- What if the call center experienced a spike in call volume from customers wanting specifics about the breach, how could we provide temporary bench strength?
- What if journalist Brian Krebs called the CEO and stated that crime shop Rescator[dot]cc was auctioning off credit cards that appear to be from our POS system?
- What if new contracts, non-disclosure agreements, and master service agreements were necessary for key investigative service providers, how fast could this be turned around?
- What if requisitions and purchase orders were required today to secure the services of key first responders or to obtain replacement equipment for seized assets?
- What if 30 people needed office space, phones and network access in a confidential area for 30 days to conduct the investigation?
- What if the media or press called wanting a statement, is there a prepared scripted response for suspected cyber breach events? How would updates be handled?

- What if the data was not regulated but still related to the customer (e.g., name, phone number, mailing address and email address), but confidentiality commitments were made in privacy policy posted on website? Would notification still be business appropriate?
- What if the Call Center and Commercial Operations team wanted a scripted response that could be shared with inquiring customers and vendor partners?

This approach will provide them insight into common events that occur as a result of a cyber-breach and can be helpful clarifying business leaders' expectation of involvement. The output of these conversations will help the development of an initial RACI (Responsible, Accountable, Consult, Inform) matrix to determine roles and responsibilities.

When socializing the role and need for a Cyber Breach Coach to organizational leaders, consider approaching the trusted advisors of the CEO and CIO. This includes Legal, Audit, Finance, Public Relations, and Human Resources. Nothing will put the brakes on faster than recommending a "vital" service that no one has heard of before. Be prepared to speak to recent and relevant cyber-breach events that could happen to the organization and the positive, proactive impact a Cyber Breach Coach would provide. A brief slide presentation can be helpful at this point. The presentation should clearly reveal the purpose of a Cyber Breach Coach and how the investment will save time, save money, and reduce risk. Be sure to clearly distinguish the Cyber Breach Coach from familiar duties performed by Audit, BCP, and IT.

4. Cyber Breach Coaching Options

For organizations with a cyber-liability policy in place, chances are a Cyber Breach Coach is included (though not necessarily free). In some case, the services are offered by the insurer as a proactive effort to identify and reduce risk. The coverage might include a finite number of hours each year for phone calls and additional on-site services available for a discounted hourly rate. In many cases, the Cyber Breach Coach

is not an employee of the insurance company. A vendor partner (e.g., law firm) might be presented to the insured for this proactive service. Careful review of the insurance policy is advised. The insurance company might require the use of specific vendors for Cyber Breach Coaching cost coverage pre and post event. In addition to insurance providers, organizations should consider approaching their current vendor partners that offer legal services. Public Relations firms can also be a source of recommendations for finding Cyber Breach Coach candidates.

As the demand for the Cyber Breach Coaching has grown beyond that of a privacy attorney, more than just law firms are offering this service. These firms many times have their roots in forensic investigation and have expanded their services to include Cyber Breach Coaching. Typically, they offer supplemental services such as PCI Forensic Investigator (PFI), Penetration Testing, Policy Review, Standard Operating Procedure (SOP) development, General IT Risk Assessment, and Security Awareness Training.

Crisis/Incident Management software vendors (e.g., CO3 Systems) and Business Continuity Management software vendors (e.g., RSA/Archer) are maturing to serve as a Cyber Breach Coach “in the box”. The software products are intended to facilitate rapid, prepared response to crisis events. Default scripts are also offered so that organizations do not have to start from scratch creating a prepared response to cyber breach events. Many of these software products are available as a cloud offering. These software and cloud options can be used at the same time as a Cyber Breach Coach (even sold by the Cyber Breach Coach) to expand scope or reduce total cost of services.

5. Coaching Integration with Computer Security Incident Response Plan

According to Michael Bruemmer, vice president at Experian. "Being properly prepared doesn't stop with having a response plan. Organizations need to practice the plan and ensure it will result in smooth execution that mitigates the negative consequences of a data breach" (Bruemmer, 2013). Many organizations perform mock security incidents

to test and improve their computer security incident response. These simulations are similar to those done for disaster recovery or business continuity in which a fictitious event is planned so the appropriate teams get practice responding to the cyber crisis. Initially, these mock security events can be technical and scope of participation primarily IT staff (System, Network, and Security teams). But as mentioned earlier, an actual cyber-breach requires a coordinated response from many teams in addition to IT.

To be effective in preparing for a cyber-breach, an organization can employ a Cyber Breach Coach to orchestrate the mock incident with other teams such as Legal, Public Relations, Internal Corporate Communications, Human Resources, and Executive Leadership. The Cyber Breach Coach can assist with expanding in scope IT first responder and standard operating procedures to include the integration points with the peer departments. Lastly, the Cyber Breach Coach can be used so serve as an advocate of the other business departments. For example, for initial planning and testing with the IT team, the Cyber Breach Coach can provide IT insight into the common requirements and timeline dependencies of Finance, Legal, Public Relations, Management, Directors, Insurers, Law Enforcement, and Regulators.

Once IT is prepared, the Cyber Breach Coach can provide non-technical participants the opportunity to see what a cyber-breach experience might be like and better understanding of the demands this event can have on the broader organization. As with IT, the Cyber Breach Coach can be used to help set expectations of what would be required immediately after a breach and to help various departments rehearse for an actual cyber breach. For these departments, the Cyber Breach Coach can provide insight into what will be demanded by regulators, customers, vendors, and stockholders. As with a mock incident for IT, Cyber Breach Coach services can be used to help identify gaps in business function preparedness and formulate action plans for improving business response.

Coordinating a mock cyber-breach incident that includes all parts of the organization at once is not always practical for a business. This can be a huge expense and tactically challenging. Break-out sessions can be created that target specific

functions of the business and their role in cyber-breach response. This is similar to approaches some BCP leaders take for testing and IT departments take to internally focus on database, system admin, helpdesk, or security expert response improvement. This effort to ramp up key business departments might be out of the traditional domain of responsibility of IT. If an organization is not large enough to have a dedicated Corporate Security department, then the Cyber Breach Coach can be a helpful orchestrator of this planning, training and testing of business departments.

6. Tips for selecting a Cyber Breach Coach

Unfortunately there is no professional certification that easily identifies a Cyber Breach Coach. Neither accreditation nor college major is in place to help organizations to distinguish a qualified individual or service provider. As noted earlier, a cyber -liability insurance provider might be the best first step to find a Cyber Breach Coach. Also, current Legal and PR business partners can be a big help identifying candidate providers of Cyber Breach Coaching services. Once a group of candidates have been found, how do organizations select a Cyber Breach Coach?

The following are a few considerations to help identify the ideal candidate:

- Vendor partnership with insurance companies
- Vendor partnership with Public Relations firms
- Industry of expertise (e.g., Healthcare, Retail, Government, etc.)
- Demonstrable experience preparing organizations for cyber attack
- Demonstrable experience leading cyber breach response
- Service Level Agreements (SLA) for cyber-breach response and engagement lead time
- Incident Response certifications (e.g., SANS GCIH, EC-Council CIH, etc.)
- IT Audit Certifications (e.g., SANS GSNA, ISACA CISA, etc.)
- Project Management certification (e.g., PMI PMP)
- Proximity of service provider to corporate headquarters

Author: Michael Hoehl, mmhoehl@gmail.com

Before advancing too far into the selection process, be sure to have executed Non-Disclosure Agreements (NDA) in place with prospect vendors. This is necessary because confidential information including data classification, compliance status, and prior breach events might be shared. Having the service provider on-site to meet with business leaders is also recommended. During the crisis of a cyber-attack, tension will be high. Identifying personality conflicts early can be beneficial.

As mentioned earlier, having external agencies contracted and secured prior to an actual breach is vital. Same is true for the Cyber Breach Coach. A retainer is typically requested. This is proposed for two reasons. The first is to ensure a prioritized response in the event a breach is suspected. The second is to eliminate any delays associated with spend approval (e.g., Finance Delegation of Authority, Purchase Order, etc.). Different rates for pre (planned) and post (unplanned) breach services should be considered.

7. Conclusion

Although a Cyber Breach Coach was considered in the past for engagement when a cyber-breach was suspected, their services are valuable prior to a cyber-breach to help an organization identify risks, improve controls, and educate executives. Keys to success for the CIO and Security Manager to get commitment to this service are:

- Evaluate the data classification and flows internally and with vendor partners
- Quantify direct loss to organization and probability of a cyber-breach
- Socialize the role of a Cyber Breach Coach including how the investment will save money, save time, and reduce risk
- Make the risk of Cyber Breach Coaching relevant by educating business leaders with recent cyber breach events targeting peers and elaborate how the risk could have been reduced/avoided with this service
- Ask business leaders of the organization “what if?”

Author: Michael Hoehl, mmhoehl@gmail.com

- Involve the cyber-liability insurance provider to determine what if any Cyber Breach Coaching services are already available and what service providers will be covered
- Use the Cyber Breach Coaching opportunity to integrate business functions into the Computer Security Incident Response Plan

For today's cyberspace connected business, Cyber Breach Coaching is a welcome and much needed addition to risk management and threat response for the increasing frequency of cyber attacks.

8. References

Akhgar, Babak. Etal. (2014). "Cyber Crime and Cyber Terrorism Investigator's Handbook". Amsterdam: Syngress.

American Bar Association. (2014). "Experts warn law firms to protect themselves against cyberattacks". Retrieved from http://www.americanbar.org/newsletter/publications/youraba/201403article06.html

Anderson, Ross et al. (2012). "Measuring the Cost of Cybercrime". Retrieved from http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Angelo, Scott. (2014). "How to survive a data breach". Retrieved at http://www.computerworld.co.nz/article/554302/how-survive-data-breach/

Bruemmer, Michael. (2013). "Experian Data Breach Resolution Reveals Five Common Mistakes Made When Handling a Breach". Retreived from http://www.prnewswire.com/news-releases/experian-data-breach-resolution-reveals-five-common-mistakes-made-when-handling-a-breach-225774251.html

Day, Paul. (2014). "Cyber Attack". London, England: Carlton Books.

Author: Michael Hoehl, mmhoehl@gmail.com

Deloitte. (2010). “CyberCrime: A Clear and Present Danger”. Retrieved from http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf

DeMarco, Joseph. (2012). “What Every CEO Should Know to Survive a Data Breach”. Retrieved from http://www.amazon.com/What-Every-Should-Survive-Breach-ebook/dp/B00BCA1TJI

Ferrillo, Paul. (2014). “Cybersecurity, Cyber Governance, And Cyber Insurance: What Every Public Company Director Needs To Know”. Retrieved from http://ftp.metrocorpcounsel.com/articles/29012/cybersecurity-cyber-governance-and-cyber-insurance-what-every-public-company-director

FTI Consulting. (2014). “14th Annual Law and the Boardroom Study by Corporate Board Member and FTI Consulting”. Retrieved from http://www.fticonsulting.com/global2/critical-thinking/fti-journal/managing-cyber-risk-job.aspx

Germano, Judith. Goldman, Zachary. (2014). “After the Breach: Cybersecurity Liability Risk”. Retrieved from http://www.lawandsecurity.org/Portals/0/Documents/CLS%20After%20the%20Breach%20Final.pdf

Giblin, Annmarie. Magner, Matthew. (2014). “Cyber Insurance: The Basics Of The Coverage”. Retrieved from http://ftp.metrocorpcounsel.com/articles/29249/cyber-insurance-basics-coverage.

Giszczak, James J. Etal. (2014). “Board Members Beware: The SEC is Watching”. Retrieved from http://www.martindale.com/securities-law/article_McDonald-Hopkins-LLC_2176798.htm

Author: Michael Hoehl, mmhoehl@gmail.com

Greisiger, Mark. (2013). “Cyber Liability & Data Breach Insurance Claims - A Study of Actual Claim Payouts”. Retrieved from http://netdiligence.com/files/CyberClaimsStudy-2013.pdf

Infosecurity. (2014). “Cost of Data Breaches Spikes 15% in Last Year,”. Retrieved from: http://www.infosecurity-magazine.com/view/38270/cost-of-data-breaches-spikes-15-in-last-year/

Kastiel, Kobi. (2014). “Cyber Governance: What Every Director Needs to Know”. Retrieved from http://blogs.law.harvard.edu/corpgov/2014/06/05/cyber-governance-what-every-director-needs-to-know/

McDonald-Hopkins. (2012). “Data security is top concern for directors and general counsel”. Retrieved from http://www.mcdonaldhopkins.com/alerts/data-privacy-network-security-data-security-is-top-concern-for-directors-and-general-counsel

United States Securities and Exchange Commission - Division of Corporation Finance. (2011). “CF Disclosure Guidance: Topic No. 2”. Retrieved from http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

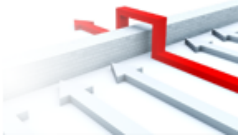
Author: Michael Hoehl, mmhoehl@gmail.com

Last Updated: December 13th, 2019

Upcoming SANS Penetration Testing

SANS PENETRATION TESTING

Click Here to {Get Registered!}



Community SANS Portland SEC542	Portland, OR	Dec 16, 2019 - Dec 21, 2019	Community SANS
SANS Austin Winter 2020	Austin, TX	Jan 06, 2020 - Jan 11, 2020	Live Event
Mentor Session - SEC504	Minneapolis, MN	Jan 08, 2020 - Feb 19, 2020	Mentor
Mentor Session - SEC504	Colorado Springs, CO	Jan 10, 2020 - Jan 31, 2020	Mentor
Miami 2020 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Miami, FL	Jan 13, 2020 - Jan 18, 2020	vLive
SANS Threat Hunting & IR Europe Summit & Training 2020	London, United Kingdom	Jan 13, 2020 - Jan 19, 2020	Live Event
SANS Miami 2020	Miami, FL	Jan 13, 2020 - Jan 18, 2020	Live Event
Community SANS Columbia SEC542 @UKI	Columbia, MD	Jan 20, 2020 - Jan 25, 2020	Community SANS
SANS Amsterdam January 2020	Amsterdam, Netherlands	Jan 20, 2020 - Jan 25, 2020	Live Event
SANS Anaheim 2020	Anaheim, CA	Jan 20, 2020 - Jan 25, 2020	Live Event
Cyber Threat Intelligence Summit & Training 2020	Arlington, VA	Jan 20, 2020 - Jan 27, 2020	Live Event
SANS Vienna January 2020	Vienna, Austria	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Las Vegas 2020	Las Vegas, NV	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS San Francisco East Bay 2020	Emeryville, CA	Jan 27, 2020 - Feb 01, 2020	Live Event
Community SANS Quantico SEC504	Quantico, VA	Jan 27, 2020 - Feb 01, 2020	Community SANS
Mentor Session - SEC504	Online, TX	Jan 29, 2020 - Apr 01, 2020	Mentor
SANS Security East 2020	New Orleans, LA	Feb 01, 2020 - Feb 08, 2020	Live Event
Security East 2020 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	New Orleans, LA	Feb 03, 2020 - Feb 08, 2020	vLive
Security East 2020 - SEC560: Network Penetration Testing and Ethical Hacking	New Orleans, LA	Feb 03, 2020 - Feb 08, 2020	vLive
Community SANS Seattle SEC504	Seattle, WA	Feb 03, 2020 - Feb 08, 2020	Community SANS
Mentor Session - SEC504	Seattle, WA	Feb 04, 2020 - Mar 24, 2020	Mentor
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	SEC504 - 202002,	Feb 04, 2020 - Mar 12, 2020	vLive
SANS Northern VA - Fairfax 2020	Fairfax, VA	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS New York City Winter 2020	New York City, NY	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS London February 2020	London, United Kingdom	Feb 10, 2020 - Feb 15, 2020	Live Event
Mentor Session - SEC504	Ann Arbor, MI	Feb 12, 2020 - Apr 22, 2020	Mentor
SANS Dubai February 2020	Dubai, United Arab Emirates	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS San Diego 2020	San Diego, CA	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Brussels February 2020	Brussels, Belgium	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Scottsdale 2020	Scottsdale, AZ	Feb 17, 2020 - Feb 22, 2020	Live Event
Community SANS Omaha SEC504	Omaha, NE	Feb 17, 2020 - Feb 22, 2020	Community SANS