Preparing for a Cyberattack by Extending BCM Into the C-suite

Gary Lieberman, Ph.D., CISSP, is director of enterprise computing and information security for a global investment bank where he has designed a highly available and secure global infrastructure supporting all critical business functions. He is responsible for and oversees all information security functions within the global infrastructure. He has published numerous research papers and journal articles covering topics such as application-to-application credential management, vulnerability scan and audit finding quantification, and security considerations relating to segregation of duties. Lieberman is also an adjunct professor in cybersecurity, network security, database design and disaster recovery at St. Leo University (Florida, USA) and Caldwell University (New Jersey, USA). He can be reached at *gary@lieberman.us.*

In 2001, a survey of 250 US companies found that three in 10 companies had formal business continuity/disaster recovery (BC/DR) programs in place.[1] That has changed. Since then, nearly all regulatory requirements and risk frameworks have been enhanced and expanded to require formal BC/DR programs that address the ever-growing threat environment.[2] Events such as the 11 September 2001 terrorist attack in the US, the 2011 earthquake and tsunami in Japan, Super Storm Sandy in 2012 in the US, and Ingrid and Manuel in 2013 in Mexico have shown that having a well-developed and thoroughly rehearsed BC/DR plan is key to corporate survival. With 2014 being known as The Year of the Mega Breach,[3] cyberattacks have quickly become a key focus in almost every BC/DR program. The primary goal of a BC/DR program is to reduce the risk and impact of a business interruption.

Megabreaches of companies such as eBay, JPMorgan Chase, Home Depot, Nieman Marcus, Staples and Target have shown that the financial consequences of plummeting sales and crashing stock prices and damage to an organization's reputation from negative press can be catastrophic.[4] Cyberbreach-related lawsuits filed by business partners, customers, investors and the US Federal Trade Commission (FTC) have demonstrated that C-suite executives and the board of directors (BoD) are not immune to being held individually responsible for failure to take reasonable steps to maintain their organization's customers' personal and financial information in a secure manner. Many complaints go on to allege that the individual defendants aggravated the damage to the company by failing to properly handle the cyberbreach once it was discovered. This accountability phenomenon has caused many C-suite and boardroom occupants to find themselves looking for new employment.[5] Home Depot alone is facing at least 44 civil lawsuits as a result of its cyberbreach.[6] Just as the US Sarbanes-Oxley Act of 2002 holds C-suite executives criminally accountable for their firm's accounting and audit practices, it is not unthinkable for those same C-suite executives responsible for the firm's information security to be held criminally negligent for a successful cyberbreach.

In any well-designed BC/DR program, there are three roles that provide leadership: sponsorship, ownership and custodianship. The ownership and custodianship roles generally include the BC/DR plan development, implementation and task execution. Most programs assign middle management to own and oversee the BC/DR plan with the overall responsibility falling squarely on the IT organization. Traditionally, a successful program starts with sponsorship that flows from the C-suite and BoD to the rest of the firm. The impetus to develop and implement a business continuity management (BCM) program may originate from regulatory compliance, risk assessments or business impact analysis. Whatever the reason, socialized support and financial backing from the BoD and the C-suite are key factors in a successful BC/DR program.

Another key factor in a successful program is the maintenance function, which includes constant updating, testing and practice drills. Traditionally, BC/DR preparedness and testing have fallen to middle management and are considered predominantly an IT function. With the exception of some chief information officers (CIO), participation by the C-suite in BC/DR testing is virtually nonexistent. More often than not, the testing and rehearsals are considered a nuisance by C-suite occupants who may be inconvenienced or prevented from working during rehearsals. Perhaps this C-suite distancing is because BC/DR activity is generally viewed as a technical function better left for IT personnel or perhaps it is simply because C-suite executives do not understand the depth and scope of the BC/DR program, even though they are committed to supporting the plan itself.[7] Whatever their reason for staying on the sidelines, the changing BC/DR

risk landscape and the new C-suite cyberbreach accountability is changing the game plan forever.

In 1988, Robert Morris, a student at Cornell University (Ithaca, New York, USA), became the first person convicted under the US 1986 Computer Fraud and Abuse Act for releasing a worm into the wild that caused widespread computer crashes.[8] A little more than 10 years later, three out of 10 US companies had BC/DR plans in place, and even then, only a few considered cyberattacks a valid risk.[9] Today, it would be hard to find a company whose BC/DR plan does not place cyberattacks high on the list of major corporate risk. This is all well and good, but the focus still sits with middle management and on the shoulders of IT and not in the C-suite or the boardroom. The last three Carnegie Mellon CyLabs biennial surveys (2008, 2010 and 2012) reporting on how boards and C-suite executives are governing the security of their organizations have shown only a slight improvement. The overall conclusion of the survey report is that boards and C-suite executives are not actively addressing cyberrisk.[10, 11, 12] One of the most cited reasons for this is that C-suite executives and the BoD consider cybersecurity too technical for them to adequately understand and participate.[13] Perhaps, from a purely technical perspective, the execution of cybersecurity defense programs should remain with middle management, IT and the tactical security operation center (SOC), but with the current atmosphere of executive accountability, one can delegate the authority, but cannot escape the accountability for a cyberbreach.

> "The more prepared the c-suite and BoD are for and the more precision and speed with which they react to cyberbreach will favorably influence the seriousness of the impact on the business."

Despite the ever-increasing attention being paid to cyberattack prevention, the general consensus among cybersecurity experts remains that "there are only two types of companies: those that have been hacked and those that will be."[14] With there being an almost 100 percent certainty of a successful cyberbreach, it is surprising that more attention is not being paid to the handling of the inevitable cyberbreach, especially considering that in 2014 the average cyberbreach had a price tag of almost US $6 million.[15] Most practitioners have seen the benefit of a well-developed and rehearsed game plan. Many sports championships have been won on game plan preparation and practice. That same level of game plan development, preparedness and razor-sharp execution needs to find its way into the C-suite and the boardroom when the inevitable cyberbreach happens. The more prepared the C-suite and BoD are and the more precision and speed with which they react to a cyberbreach, the more they can mitigate the seriousness of the impact on the business. Lisa J. Sotto, Esq., a partner at Hunton & Williams and one of the top cyberbreach attorneys in the US, says, "When facing a cyberthreat, preparation will mitigate harm. It is essential to have identified in advance the trusted advisors who will guide the company in the event of a cyberattack."

So what is the best way to achieve the right level of preparation for handling the inevitable cyberbreach? Considering the foundation for this is most likely already in place, companies today would be well served to extend their BC/DR plan into the C-suite and boardroom. The plan would simply need to be expanded and enhanced to include the postcyberbreach activities of the C-suite executives and the board and, most important, these activities should be updated, tested and rehearsed with the same reverence, attention and level of energy that is given the rest of the BC/DR plan by middle management and IT.

On 10 June 2014, US Securities and Exchange Commissioner (SEC) Luis Aguilar spoke at a Cyber Risk and the Boardroom conference at the US New York Stock Exchange (NYSE). He emphasized that the duty of the BoD is to ensure that the company's cybersecurity stance is on solid ground. He said companies should accomplish this by educating themselves about cybersecurity and making it a part of the board's regular duties. Besides the regular duties of the BoD, it can also arrange for formal training and/or consulting with an outside expert on

cybersecurity to ensure that relevant directors have the required technical understanding to subjunctive evaluate current and future risk.[16] It is key that the BoD understand the full gravity, importance and benefit its participation will play in ensuring that the proper cyberbreach response plan is incorporated into the firm's BC/DR program along with the full participation of the C-suite executives in the program.

The tasks required for handling a cyberbreach by the C-suite will vary from company to company and no two cyberbreaches will ever be identical. Therefore, each cyberbreach must be analyzed and evaluated on its own merits and an action plan formulated that is appropriate for that particular cyberbreach. There are, however, many cyberbreach response tasks that can be enumerated in general and specifically applied in keeping with the individual situation. In the following steps, the general counsel (GC), the CIO, the chief financial officer (CFO) and the chief executive officer (CEO) all play significant roles. The GC plays the most significant behind-the-scenes role, while the CEO and the head of public relations (PR) present the public face of the cyberbreach.[17] The CFO is responsible for the financial, insurance and investor cyberbreach-related considerations:

- **Initial briefing**—Generally, the CIO or IT director will initiate the cyberbreach response and gather the cyberbreach response team together for a full debriefing. This step varies widely between companies. Usually there is a single individual or team that assesses the incident and makes the determination whether or not it warrants the initiation of the formal cyberbreach incident response. Once that decision is made, the cyberbreach team is gathered for a situational debriefing. If the BC/DR cyberbreach program is fully implemented, tested and rehearsed, this will not be the first time the team has met. The debriefing should be a short *who, what, where, when, why* and *how bad* presentation. It is important to gain an initial understanding of the breadth and scope of the cyberbreach. Is it a data-gathering or a destructive cyberattack? This is important as it will dictate the initial technical response by the IT group and the forensic experts. The breadth and scope assessment of the cyberbreach can, and most likely will, be modified and updated numerous times as the investigation continues, new information and insight are gained, and the breach response is underway.
- **Outside counsel and forensic experts**—As part of the development and implementation of the BC/DR cyberbreach program, and prior to any cyberbreach actually happening, the GC should locate an experienced outside cyberbreach expert legal counsel—one who understands the technical, legal and regulatory implications of particular types of cyberbreaches. The outside counsel and forensic experts will advise on and/or perform the following duties:
  - Help further define the breadth and scope of the cyberbreach.
  - Develop a containment strategy.
  - Preserve logs and evidence.
  - Document the cyberbreach.
  - Advise and assist with postbreach remediation activities.

  These steps are important to perform with the advice of outside cyberbreach counsel as the findings gathered may be protected under attorney-client privilege. An additional benefit of bringing in outside expert counsel is that they already have established relationships and connections with law enforcement and other government agencies that can significantly speed up the investigation and smooth out the entire cyberbreach response process. If the cyberbreach was not brought to the attention of the company by law enforcement, these relationships will be even more important when the time comes to report the incident to law enforcement and ask for their assistance.
- **Financial oversight**—The CFO must closely watch all financial channels for inappropriate transactions that may be breach-related. If the company handles credit cards, the CFO will need to alert the appropriate financial institutions. Additionally, the CFO should, with the advice of legal counsel, initiate claims against the firm's insurance policies that cover first-party and third-party loss due to cyberbreaches. Last, if news of the cyberbreach has reached the press, the CFO will need to deal with possible dropping stock prices and a jittery investor community.
- **Employee considerations**—Depending on the nature of the cyberbreach, employee personally identifiable information (PII) may have been compromised. Human resources (HR) will need to advise employees and guide them through the steps necessary to personally protect themselves. If the company has a bring your own device (BYOD) policy, it may be necessary to acquire and inspect personal property

as part of the investigation. In cases where BYOD is in effect, devices may need to be confiscated and held as evidence or for discovery. HR should research these possibilities well in advance of a cyberbreach; understand the firm's rights under federal, state and local law; and be prepared to act as necessary. Even if there are employee-signed personal device usage waivers in place, there may still be privacy issues that need to be addressed related to a cyberbreach. Again, this is where outside counsel's advice can be invaluable.

- **CEO and PR staff**—Once the cyberbreach becomes public knowledge, the CEO and the PR staff will become the public face of the cyberbreach response team. All press releases and public contact should be reviewed by the GC and outside counsel prior to being released. Companies want to avoid public comments that may be inaccurate or cause further damage. It is also important to have a single public face for the cyberbreach and avoid having multiple people talking to the press. How the company's response to the cyberbreach is viewed by the public is a key factor in such things as sales, stock prices and future litigation.

CONCLUSION

There are many steps that can be taken to avoid a cyberbreach, but statistically speaking, the odds are that every company has been or will be breached at some point. It is wise and prudent to make every effort possible to avoid a cyberbreach. However, when a cyberbreach happens, a well-developed, well-tested and well-rehearsed cyberbreach response plan is paramount. The plan must include a detailed playbook; advice and guidance from legal and forensic cyberbreach experts; rehearsals that include in-depth, table-top exercises and constant updating and modification of the plan; and a list of knowledgeable designees who can step in and cover for traveling C-suite executives at a moment's notice. A well-designed BC/DR cyberbreach program that is executed with speed and precision will ultimately make the response process smoother and more efficient and will help to ease any resulting regulatory burden. It will also position the company to better deal with the expected litigation that seems to follow all significant cyberbreaches these days.

ENDNOTES

1 Erbschloe, M.; *Guide to Disaster Recovery*, Thomson/Course Technology, USA, 2003
2 Protiviti, *Guide to Business Continuity Management*, 2013
3 Ponemon Institute, *2014: A Year of Mega Breaches*, 2015, *www.ponemon.org/library/2014-a-year-of-mega-breaches*
4 *Ibid*.
5 Ali, Syed V. P.; J. Dixon; *Why Cyber Security Is a Strategic Issue*, Bain & Company, 2014
6 Calia, M.; "Home Depot Facing at Least 44 Civil Suits in Data Breach," *The Wall Street Journal*, 25 November 2014, *www.wsj.com/articles/home-depot-facing-at-least-44-civil-suits-in-data-breach-1416917359*
7 Deloitte, *"Aware" vs. "Committed" Where Do You Stand?*, Deloitte Touche Tohmatsu Ltd., 2013, *www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-aers-ers-bcm-aware-vs-committed_Dec2013.pdf*
8 O'Dell, P. L.; C. Scott; *Cyber 24-7: Risks, Leadership, and Sharing: Sound Advice for the Board, C-Suite, and Non-technical Executives*, CreateSpace Independent Publishing Platform, 2014
9 *Op cit* Erbschloe
10 Westby, J. R.; *Governance of Enterprise Security: CyLab 2008 Report*, Carnegie Mellon, USA, 2008
11 Westby, J. R.; *Governance of Enterprise Security: CyLab 2010 Report*, Carnegie Mellon, USA, 2010
12 Westby, J. R.; *Governance of Enterprise Security: CyLab 2012 Report*, Carnegie Mellon, USA, 2012
13 *Op cit* O'Dell
14 Cowley, S.; "FBI Director: Cybercrime Will Eclipse Terrorism," *CNN Money*, 2012, *http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity*
15 Ponemon Institute, *2014 Cost of Data Breach: Global Analysis*, 2014
16 Tewell, C. M.; *SEC Clarifies Duties of Board of Directors Regarding Cybersecurity and Data Breaches*, Davis, Wright, Tremain, July 2014, *www.dwt.com/SEC-Clarifies-Duties-of-Board-of-Directors-Regarding-Cybersecurity-and-Data-Breaches-07-18-2014/*
17 Smith, R.; W. Cook; "The GC's 30-Minute Breach Drill," Primary Opinion, 10 May 2015, *https://www.primaryopinion.com/articles/gc%E2%80%99s-30-minute-breach-drill*