johnreedstark
CONSULTING, LLC

Top cybersecurity concerns for every board of directors, part two: **people**

by John Reed Stark

This white paper was first published on the Nasdaq Governance Clearinghouse.

We are all experiencing the dawning of a new era of data breach and incident response, where trying to avert a cyber-attack is like trying to prevent a kindergartener from catching a cold during the school year. Members of corporate boards therefore have no choice but to become actively involved in ensuring the organizations they oversee are adequately addressing cyber-security, approaching the subject much the same way an audit committee probes a company's financial statements and reports: with vigorous, skeptical, intelligent, and methodical inquiry.

This four-part series discusses cybersecurity considerations that provide a solid bedrock of inquiry for corporate directors who want to take their cybersecurity oversight and supervision responsibilities seriously.

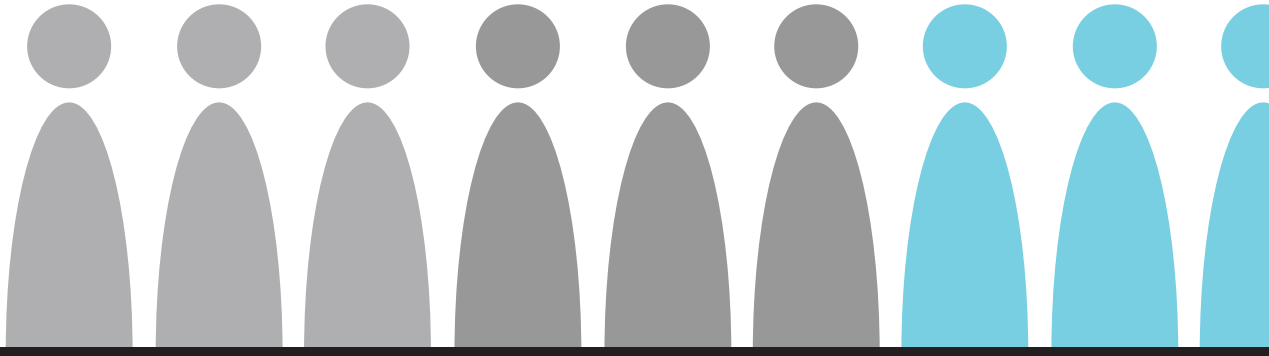
These recommendations provide the requisite strategical framework for boards of directors to engage in an intelligent, thoughtful and appropriate supervision of a company's cybersecurity risks.

The first article of this series discussed cybersecurity considerations relating to the governance, practices, policies and procedures of a strong cybersecurity program.

This second article pertains to cybersecurity areas that involve people, while the third article of the series will discuss the more technical areas mandating meaningful board oversight. The final part of the series will discuss the board's oversight responsibilities with encryption and provide some final thoughts.

Introduction

Companies can invest heavily in top-of-the-line security software and state-of the-art systems, but without the proper approach toward their IT employees, those efforts will all be for naught. This article focuses on a board's cybersecurity oversight pertaining to a company's most important cybersecurity resource (and threat): its employees.



Cybersecurity Recruitment and Retention

The greatest virtual threat today is not state sponsored terrorism, newfangled clandestine malware, or a hacker culture run amok. The most dangerous looming crisis in information security is instead a severe cybersecurity labor shortage– expected to reach 1.5 million job openings by 2019.

SG recently teamed up with the Information Systems Security Association and conducted a survey of 437 global cybersecurity professionals, resulting in a recently published research report, presenting an alarming picture of the languishing state of the cybersecurity profession. In one particularly salient note, 55% of the 437 cyber-security professionals surveyed strongly believe that, "The cybersecurity skills shortage is a far bigger problem than is being communicated."

Academia has unfortunately failed to keep up with industry trends and is not producing enough data cybersecurity specialists to handle surging demand. According to one recent study, only a handful of the 50 top university computer science programs in the U.S. require that students take even one cyber-security course. There exist world-renowned schools and academic programs of law (despite an extraordinary glut of attorneys and 200+ accredited law schools); business (despite the decreasing value of an M.B.A. and almost 400 U.S. business schools); and journalism and politics (as if we need more pundits). Yet there remains a dearth of campuses dedicated to computer science, cybersecurity and data breach response.

The challenges are complex. Cybersecurity is an ambiguous and wide-ranging field – involving network engineering, encryption, firewalls, logging tools, analytic tools, forensic tools and more. Moreover, cybersecurity threats are constantly evolving, so that by the time students graduate, some lessons are already obsolete. Meanwhile, the nature of the legion of cyber-attackers has similarly progressed, from "black hat" hackers and profiteers

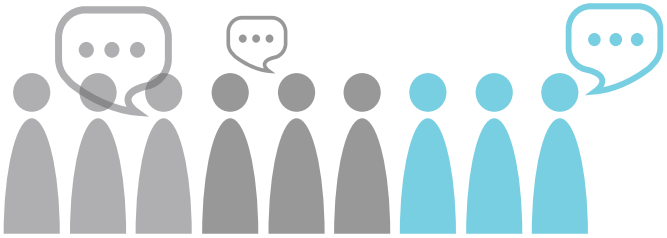
55% of the total **437** cybersecurity professionals surveyed believe that, "The cybersecurity skills shortage is a far bigger problem than is being communicated."

to organized cyber gangs and rogue nation states. The cybersecurity response field is a lot like the medical field: building a skillset takes experience as an intern, resident and attending.

Thus, competition for talent in the information security space is intense, while the pressure on IT security senior executives is infinite and exhausting. Moreover, despite their rapidly rising salaries, turnover remains constant and there is a serious shortage of experienced and capable IT senior executives, especially chief information security officers (CISOs).

Boards should understand what the company is doing to recruit and retain IT security talent. Relatedly, when a company loses key senior IT security personnel, it is not only a red flag but also an opportunity for a board to examine succession plans and to obtain an unbiased, albeit possibly disgruntled, view of any cybersecurity flaws. The art and the benefit of the exit interview is lost on so many companies today – too often because departing employees are dismissed as resentful and unreliable. In the case of a resigning IT executive, boards should confirm that a proper exit interview takes place – and use the departure as an opportunity which could reveal critical cybersecurity weaknesses.

Top Down Commitment



Strong cybersecurity is a business imperative, yet too often cybersecurity is far down on a board or C-suite's priority list or, because it is so complex, simply delegated to lower-level technical personnel. Top-down commitment to cybersecurity also can be lacking in companies where departments and business lines are isolated and "siloed" or where management is diffuse and not hierarchical (such as management systems found in professional services companies like law and accounting firms).

Given the tumultuous risk associated with cyber-attacks, boards of directors and the C-suite must address cybersecurity, not as an IT issue, but as a governance issue and a risk resilience issue. Boards and the C-suite should enforce the notion

Boards and the C–suite should establish a cross-organizational team that regularly convenes to discuss, coordinate and communicate cybersecurity issues

that the company has an institutional commitment to protect client data reflected by involvement and engagement by senior firm leaders – not just IT. At the least, boards and the C-suite should establish a cross-organizational team (including practice chairs, procurement, finance, human relations, communications, office management, IT and security personnel) that regularly convenes to discuss, coordinate and communicate cybersecurity issues.

Boards should assess whether a company's executive management team possesses cross-functional awareness about cyber risk, and does not view cybersecurity as a problem handled primarily by an IT department. Boards should query executive management of a company with respect to their commitment to cybersecurity, by asking such questions as:

- Describe the commitment from the top down, both culturally and financially, to rigorous cybersecurity;
- Who in leadership is driving the cybersecurity agenda;
- Is it a C-level accountability and part of the day-to-day cybersecurity business focus;
- Do current reporting lines and assigned areas of responsibility make sense;
- Have executives and senior managers participated in data security training/been involved in the development of data security protocols;
- Is there a carefully monitored and structured manner in which employees or members of the public (such as independent security researchers) report potential vulnerabilities/breaches, including irregular activity or transactions;
- Given the responsibilities and accountability needed to execute the incident response plan, are the right employees, possessing the appropriate skillsets, adequately empowered; and
- Is the team charged with overseeing cyber-defense the same team that reports up the chain about cyber-attacks and would oversee any response (that dual-role can indicate an inherent conflict of interest)?

Training programs

The most significant cybersecurity vulnerability at any company will always be its employees. If employees do not adhere to cybersecurity rules and requirements, an attacker's exploit becomes all the more effective and capable of doing damage.

For financial firms, the SEC's Cybersecurity Module emphasizes the importance of cybersecurity training of employees at SEC registered entities, and cybersecurity due diligence teams may want to mirror the SEC's approach. The SEC's Cybersecurity Module states:

"Without proper training, employees and vendors may put a firm's data at risk. Some data breaches may result from unintentional employee actions such as a misplaced laptop, accessing a client account through an unsecured Internet connection, or opening

messages or downloading attachments from an unknown source. With proper training, however, employees and vendors can be the firm's first line of defense, such as by alerting firm IT professionals to suspicious activity and understanding and following firm protocols with respect to technology. Examiners may focus on how training is tailored to specific job functions and how training is designed to encourage responsible employee and vendor behavior. Examiners also may review how procedures for responding to cyber incidents under an incident response plan are integrated into regular personnel and vendor training."

Like the SEC, FINRA endorses a similar approach to the importance of cybersecurity training of a company's employees, recommending that FINRA-regulated firms provide cybersecurity training that is tailored to a firm's needs. Per FINRA, effective practices for cybersecurity training include:

- Defining cybersecurity training needs requirements;
- Identifying appropriate cybersecurity training update cycles;
- Delivering interactive training with audience participation to increase retention; and
- Developing training around information from the firm's loss incidents, risk assessment process and threat intelligence gathering.

Boards should query corporate executives regarding: 1) the frequency and efficacy of the firm's cyber-safety training programs; 2) who participates in the training and how the company handles policy violations, especially violations by senior executives (who studies have shown are typically the least compliant with cybersecurity policies).

A Digital Forensics/Data Breach Response Firm on Call

When a company experiences a cyber-attack, the company will likely need to hire an expert and experienced digital forensics/data breach response firm to investigate for several reasons.
First, very few companies employ the kind of personnel who have the technological expertise to understand and remediate today's cyber-attacks.

Second, like any company in a crisis, engaging an independent and objective investigator not only insures integrity in the response but also creates a defensible record if challenged later on (e.g. by regulators, class action lawyers, partners, customers, etc.). Finally, if the digital forensics/data breach response firm is engaged by outside counsel,

a company can (arguably) maintain and secure the attorney-client privilege for the reports and other investigative documents pertaining to the attack.

Given the scarce number of firms who can truly investigate a cyber-attack, especially those with malware reverse engineering expertise, it makes sense to search for a firm before experiencing a cyber-attack and establish a master service agreement if possible (many forensic firms will agree to a master service agreement which has no financial obligation).

Law Firm That Specializes in Data Breach Response On Speed Dial

Data breach response workflow requires careful navigation because, among other things, the legal ramifications of any failure can be calamitous or even fatal for any public or private company. Outside counsel or inside counsel is best suited to lead data breach investigations, quarterbacking the workflow for the C-suite and sharing with senior management the ultimate responsibility for key decisions.

The list of potential civil liabilities in the aftermath of a cyber-attack is almost endless, including lawsuits.

Just like any other independent and thorough investigation, the work relating to a cyber-attack will involve a team of lawyers with different skillsets and expertise (e.g., regulatory, ediscovery, data breach response, privacy, white collar defense, litigation and law enforcement liaison). Counsel makes the most sense to supervise all incident response workflow for obvious reasons, including:

- Consider the many competing constituencies during an incident response. On one hand, the FBI, Secret Service, U.S. Air Force and other law enforcement agencies may be trying to identify and prosecute the intruders. On the other hand, myriad attorneys general and other regulatory agencies are issuing requests and demanding answers about the safety of the personal information of their respective citizenries. Only a qualified attorney can manage this delicate balance;
- Law enforcement agencies also may request forensic images of affected systems, or may ask to attach a recording appliance to a victim company's network in hope of capturing traces of possible future attacker activity. These requests raise a host of legal issues, including whether providing information to law enforcement could violate customer privacy or inadvertently waive the attorney-client privilege;
- In addition to the governmental investigations and litigation mentioned earlier, the list of potential civil liabilities in the aftermath of a cyber-attack is almost endless, including shareholder lawsuits for cybersecurity failures or declines in a company's stock price as well as consumer/customer-driven class action lawsuits alleging a failure to adhere to cybersecurity best practices;
- In the case of a cyber-attack investigation, attorney client privilege will arguably apply to the work product from the digital forensic investigators retained by outside counsel. Malware reverse engineering results, exfiltration analysis, logging review, digital forensics exploration and the rest should all be cloaked with the protections of attorney-client privilege and work product. This is not done to hide information; rather it helps protect against inaccurate information being released in an uncontrolled fashion and allows for more careful deliberation and preparation for litigation or government investigation/prosecution, two scenarios more and more likely nowadays; and

- This same model already applies when investigating corruption, bribery and other criminal behavior, where the General Counsel (GC), not the Chief Operations Officer (COO), Chief Information Security Officer (CISO), or Chief Information Officer (CIO), quarterbacks investigative workflow; superintends remedial efforts; and governs intelligence sharing. An independent data breach SWAT team, under the direction of the GC, also reduces the scrapes that can arise among compliance, operations and legal, especially relating to the GC's disclosure obligations, including disclosures to shareholders (via the SEC), the states and law enforcement.

Prior to a cyber-attack, integrating the GC into the creation and ongoing review of cybersecurity provides strategic benefits as well, such as:

- Serving as an objective sounding board to IT staff tasked with designing, implementing and reviewing data practices;
- Reviewing privacy policies;
- Testing representations made to consumers, and evaluating how outsiders might exploit those representations in court; and
- Serving a critical role in litigation-testing the "reasonableness" of cybersecurity practices.

Boards should first confirm that a company already has retained (with master service agreements firmly in place) a law firm that specializes in data breach response. Without a competent data breach response team, staffed with professionals who are skilled at handling the intricacies and complex demands created by a cyber-attack, a company may end up feeling like a homeowner with a rapidly flooding basement – yet no plumber to help find the leak and plug it up, no engineers or technicians to rebuild affected systems, and no electrician to make sure the power safely returns.

Boards, if possible, should meet with the law firm to seek their respective impressions of the company's overall approach to cybersecurity and confirm their expertise,
as well as their commitment to the company and to the appropriate principles and edicts of successful incident response.

Pre-Breach Law Enforcement Liaison

Keeping up with the latest developments in cybersecurity and the latest tools and techniques being utilized by cyber-attackers is a career within itself – and requires building relationships with law enforcement, including the FBI, U.S. Air Force, DHS and the U.S. Secret Service.

The U.S. Department of Justice (DOJ) has specifically made cybersecurity a primary focus of its attention. Two common scenarios in which companies can interact with the DOJ on cyber issues are: (1) ongoing investigations into data breaches or other security incidents, some of which involve an investigative agency affirmatively notifying a company that it is a cybercrime victim; and (2) general public-private party outreach efforts including sharing of potential threats and vulnerabilities.

In each of these scenarios, companies might interact with one or more of the following three principal DOJ components involved in cybercrime prosecutions: the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS), the National Security Division
(NSD) and any one of the 93 individual U.S. Attorney's Offices (USAOs). CCIPS is the DOJ's cybercrime subject-matter expert. NSD is the DOJ's national security subject-matter expert; it combats cyber-based threats to national security. USAOs are the DOJ's front lines in prosecuting cybercrime, and frequently interface with cybercrime victims. These three groups combined form a network of over 300 DOJ cyber prosecutors.

This law enforcement network has become increasingly willing to work with private sector companies in an effort to protect U.S. companies from cyber-attacks. For example, the FBI has created

the FBI Liaison Alert System, or FLASH. Through the system, the FBI releases high-confidence data to the private sector with indicators and alerts related to computer intrusions and DOS (denial-of-service) attacks. From April 2013 to July 2014, the FBI disseminated 34 FLASH messages, about 20 of which dealt with threats against the financial sector. The FBI disseminated, among other information, indicators for approximately 115,000 compromised systems in these FLASH messages. These declassified, technical indicators, associated with intrusions, are meant to enable industry partners to be on the lookout for and defend their infrastructure from nefarious traffic on their networks.

Boards should make sure a company is taking advantage of the networks created by law enforcement for public outreach and is receiving FLASH alerts. If a company has not considered forging relationships within the law enforcement cyber community, it might indicate a lack of sophistication in its cybersecurity efforts; a lack of consideration of the severity of a potential cyber-attack; and a lack of commitment from corporate higher-ups.

John Reed Stark wishes to thank and acknowledge the authors and experts of the following list of articles, presentations, cases, etc., which he used as resources for the many authoritative conclusions and opinions used herein. Without these excellent resources, this white paper and all of the articles in this series would not have been possible -- what an amazing group of experts and wordsmiths (!)

Cybersecurity workforce shortage to reach 1.5 million by 2019

Top U.S universities failing at cybersecurity education

There Are Too Many Lawyers, Say Law Firms

List of law schools in the United States

Challenging Times Ahead For Business Schools And MBA Jobs

List of business schools in the United States

Journalism schools need to adapt or risk becoming irrelevant

Cybersecurity Personnel: Recruiting the New Fighter Pilots

NATIONAL EXAM PROGRAM RISK ALERT

Report on Cybersecurity Practices

GCs Now 'Quarterbacks' of Cyber Incident Responses: John Reed Stark

Sony Hit With Fourth and Fifth Class-Action Lawsuits Over Stolen Data (Exclusive)

Community Health Systems Faces Lawsuit

Law firms offer cybersecurity advice and attorney-client privilege to hacked companies

United States: Reasonable Doubt: Data Privacy, Cybersecurity, And The FTC

Unprecedented Hacking and Trading Scheme Highlights Key Cybersecurity Lessons

Understanding Denial-of-Service Attacks

Cyber Security: Enhancing Coordination to Protect the Financial Sector

About John Reed Stark

John Reed Stark is President of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Mr. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, the last 11 of which as Chief of its Office of Internet Enforcement. He also worked for 15 years as an Adjunct Professor of Law at the Georgetown University Law Center, where he taught several courses on the juxtaposition of law, technology and crime, and for five years as managing director of a global data breach response firm, including three years heading its Washington, D.C. office. Mr. Stark is the author of, "The Cybersecurity Due Diligence Handbook," available as an eBook on Amazon, iBooks and other booksellers.

SERVICES:

Cybersecurity and Incident Response
Penetration Testing
Board of Directors Advisory Services
Cyber Insurance
Law Firm Cybersecurity Assessments
SEC and FINRA Compliance
Expert Witness
CybersecurityDocket.com

CONTACT US AT:

www.johnreedstark.com
John Reed Stark Consulting LLC
Phone: (301) 335-8387
Email: info@johnreedstark.com
