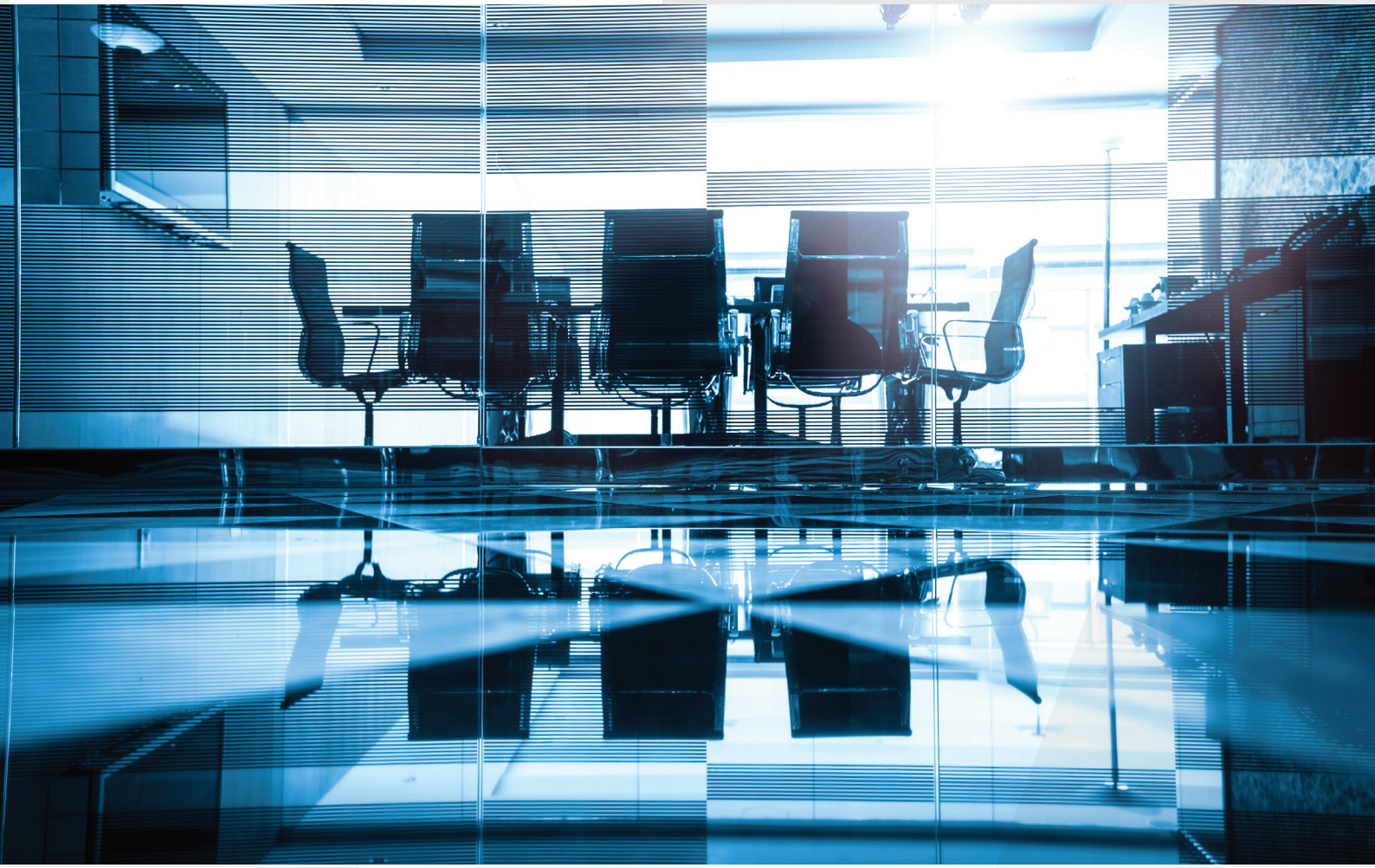
johnreedstark
CONSULTING, LLC



Top cybersecurity concerns for every board of directors, part three: **technology**

by John Reed Stark

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

Corporate directors have a fiduciary duty to understand and oversee cybersecurity. While managing cyber risk has become an increasingly complex and costly endeavor, there is no need for board members (many of whom have limited IT experience) to panic.

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

Introduction

The technical systems in place at any company provide the foundation for cybersecurity infrastructure and should be one of the primary focuses of any board of directors. This article outlines the various technological system classifications involved in any cybersecurity undertaking, organizing data points into broad categories helpful for shaping analysis and scrutiny.

Logging Capabilities

A company's logging capabilities provide evidence on how a company is actively hunting for indications of compromise and whether the company is retaining sufficient system records to recreate attacker behavior and determine the scope of exposure in the event of a breach incident. After a data breach, in addition to analyzing user systems like laptop and desktop computers, servers, etc., the logs of other systems such as firewalls and intrusion detection systems will also require analysis.

Exactly what logs are available relating to a cyber-attack depends on a company's overall cybersecurity policies and practices. Logging information can include logs relating to events occurring with firewalls, operating systems, applications, antivirus software, LANDesk, web servers, web proxies, VPNs, change auditors, DHCPs and a broad range of other audit files.

Logging retention can differ dramatically among companies – and some companies may not have any log management system that aggregates logging information, which means that its logging information will be scattered and disorganized. Also, some companies may preserve logs only for a short period, such as thirty days, before "rolling over them" and thereby deleting the logs permanently.

Deficiencies in logging can become a major source of consternation for data breach first responders. According to the SANS Institute:

"Deficiencies in security logging and analysis can allow attackers to hide their location, malware, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records, victims can remain blind to the details of the attack and to subsequent actions taken by the attackers.

Properly aggregating logging information can be of critical use during the troubleshooting and investigation of a cyber-attack response.

Sometimes logging records are the only evidence of a successful attack and without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.

Sometimes logging records are the only evidence of a successful attack and without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Many organizations keep useful logs for compliance purposes, but attackers rely on the fact that such organizations might only rarely review their logs, and never discover that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the organization knowing, even though the evidence of the attack has been recorded in unexamined log files."

Most free and commercial operating systems, network services and firewall technologies offer logging capabilities and can contain a treasure trove of relevant evidence requiring investigative analysis and resources. Also, actual correlation and aggregation tools such as Security Incident Management (SIM) or Security Event Management (SEM) solutions can make audit logs far more useful for subsequent manual inspection and can be quite helpful in identifying subtle attacks.

For the best results, such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the logging information in the event a follow-up investigation is required. Operating systems, especially those of servers,

should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, IT personnel should periodically scan through their logs and compare them with the asset inventory assembled in order to ensure that each managed item actively connected to the network is periodically generating logs.

One important additional note: SIM/SEM analytical solutions for reviewing logs can provide value only when the right expert is conducting the analysis. These tools are neither a cure-all nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition (sometimes just old-fashioned gum-shoe detective work) often are required to identify and understand what is gleaned from log files.

Properly aggregating logging information can be of critical use during the troubleshooting and investigation of a cyber-attack response, and it is too often something management overlooks as a priority. Boards should confirm that a company has spent the requisite amount of time learning what logs to collect, what logs not to keep and how to search older records. Companies that do not conduct regular logging self-assessments to determine the sufficiency of current logging and to identify any reporting gaps, risk learning of deficiencies after a cyber-attack, when it is too late to remediate.

Companies that do not conduct regular logging self-assessments to determine the sufficiency of current logging and to identify any reporting gaps, risk learning of deficiencies after a cyber-attack, when it is too late to remediate.

Boards should also probe IT personnel about logging practices and procedures and make sure that an expert (internal or outsourced) is analyzing whatever logging information the company is amassing. Any logging deficiencies found could be an indicator of weak cybersecurity management, careless leadership and insufficient risk resilience.

Penetration Testing

Just as a CEO has an annual physical checkup by a physician, a company should undergo a risk and security assessment of its inner cybersecurity workings. Implementing cybersecurity solutions requires a comprehensive risk assessment to determine defense capabilities and weaknesses and ensure the wise application of resources. What works best is a disciplined yet flexible methodology that incorporates a company's organizational culture, operational requirements and tolerance for risk, and then balances those against current technological threats and risk. Since data breaches are inevitable, a proper risk and security assessment quantifies risk, develops meaningful risk metrics and conveys the effectiveness of risk mitigation options in clear and concise terms.

For starters, consulting firms and cybersecurity shops market a myriad of services: penetration testing, risk and security assessments, data security audits, application security evaluations, code reviews and other similarly described services. Given that even the consultant jargon is unclear, for purposes of this article, all categories will fall under the label of penetration (or "pen") testing, which is standard parlance and is considered the lowest common denominator for evaluating cybersecurity.

A company's pen tester should have substantial technological abilities, including expertise in testing web applications, mobile applications and devices, software products, third-party service providers, cloud solutions and IT infrastructure.

One mark of a good pen tester is to be a thought leader in the information security community – authoring theoretical publications, giving peer conference presentations, contributing to open source projects, writing blogs or publishing vulnerabilities. It also helps if a pen tester has so-called blue team experience, (that is, he or she has managed networks or systems or developed applications).

Good pen testers mimic the methods used by sophisticated attackers to identify vulnerabilities before they can be exploited.

Good pen testers mimic the methods used by sophisticated attackers to identify vulnerabilities before they can be exploited. That is best achieved by using specialized manual testing, not by running automated tools. Automated tools do have a place (it's a good practice to run them internally looking for low-hanging fruit), but custom tools will typically prove far more effective. No two pen testing engagements are ever the same; even the same vulnerability can vary wildly in different environments, and having a proprietary set of tools evidences a pen tester's ability to venture off-script and improvise when necessary. Proprietary tools also typically allow for a more detailed explanation of the so-called "kill chain" or path of an attack.

Pen testing has no standardization (not like some sort of emissions or DNA test), so company executives should give careful consideration to who should conduct a company's pen testing and how to best interpret the results. Before conducting any test or assessment, company leaders should make sure IT departments document all cybersecurity policies and procedures, not just to get credit for good behavior and practices, but also because documentation is a beneficial compliance exercise.

Common types of pen testing for companies include: an external penetration test or vulnerability scan to assess Internet-facing computers, including firewalls, VPNs and other online gateways; an internal penetration test or vulnerability of a company's internal network, such as desktops, laptops, servers, printers, VoIP phones and other online devices; a web application assessment to analyze a company's website security; and social engineering testing to assess the "human firewall" of a company and gauge company staff cybersecurity awareness.

In addition, companies should conduct unannounced spear-phishing tests. Spear-phishing tests help determine employee resistance to one of the most common methods of remote compromise. The tests also help gauge the risks associated with permissive egress filters, targeted malware, the establishment of remote command and control channels and the susceptibility to undetected bulk data exfiltration.

Companies will want to avoid engaging pen testers who present deliverables that, though intended for a company's benefit, provide a written laundry list of problems in need of solutions or a so-called heat map, which identifies the most serious potential weaknesses. Given the reality that most companies will not be able to cure all weaknesses (because of cost concerns, logistical impossibilities, practical barriers, etc.), heat maps and laundry lists unfortunately also can provide regulators, law enforcement, class action lawyers and other disgruntled parties with a handy and helpful road map for liability. Thus, the primary deliverable for any pen test should begin with a briefing, where company executives can discuss the format of any ultimate deliverable of the pen testing results.

Board oversight regarding pen testers should not only include a thorough review of pen testing reports, communications and findings, but also any resultant remedial efforts or corrective measures implemented afterward. Boards should also explore whether a company's pen tester is the trusted adviser of the executives of the company engaging its services, which can be a solid indicator that a company is looking at cybersecurity through the appropriate lens. If the pen tester engaged by a company is a fly-by-night, check-the-box, short-term vendor and not a long-term, faithful partner, then the paradigm is unwise – and should raise a significant red flag. If possible, Boards should interview a company's pen tester and discuss the company's overall approach to cybersecurity, including strengths and weaknesses.

The primary deliverable for any pen test should begin with a briefing, where company executives can discuss the format of any ultimate deliverable of the pen testing results.

Data Loss Protection

Companies should work toward adopting security mechanisms such as data loss protection (DLP) systems (also known as "data leak prevention systems"), to help detect and prevent the potential unauthorized transmittal of confidential information by employees. DLP systems aim to prevent end users from sending sensitive or critical information outside a company's network.

Such systems classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could place the organization at risk. For instance, by installing data loss prevention technologies that "tag" certain files, phrases and code names, a company can block or flag transmissions of those tagged files, with the aim of preventing sensitive information from leaving the company's network. DLP software can also identify strings of digits resembling Social Security numbers in an outbound email, quarantine the email before it leaves the organization's network and alert the employer's IT department of a potential data theft.

Boards should probe carefully how a company protects its data from unauthorized or inadvertent transmittal.

As an aside, companies using DLP technologies should work with counsel on their implementation, so as not to inadvertently violate federal or state surveillance statutes. For instance, employers who capture email content in real time without robust, prior notice to employees may be exposed to civil lawsuits and even criminal prosecution. Multinational employers face broader, potential exposure for violating local data protection laws, particularly in the European Union.

Boards should probe carefully how a company protects its data from unauthorized or inadvertent transmittal, including: what DLP technologies a company uses; what DLP training a company conducts; and what types of monitoring and logging a company maintains to detect data transmittal.

Patching and Updating

Similar to the way fabric patches are used to repair holes in clothing, software patches repair holes in software programs. Patches are updates that fix a particular problem or vulnerability within a program. Sometimes, instead of just releasing a patch, vendors will release an upgraded version of their software, although they may refer to the upgrade as a patch.

The need to update software when a patch is issued to address exposed software security flaws is as basic as the need to take out the trash at the end of the day – and may not at first glance seem worthy of due diligence scrutiny.

Yet, many security breaches still occur because software was not updated in a timely manner, and attackers may target vulnerabilities for months or even years after patches are available. For instance, the recent Panama Papers hack was most likely accomplished via an outdated and unpatched version of Drupal and/or WordPress. The Mossack Fonseca site apparently contained outdated, unpatched and vulnerable versions of both types of software that could have been leveraged to compromise the Internet reachable servers.

Patch management, simple and easy to execute, remains a vast security hole for many organizations. A 2015 Verizon

data breach investigations report found that "99.9% of exploited vulnerabilities had been compromised more than a year after the associated common vulnerabilities and exposures (CVE) was published." CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cyber security issues. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories and services) with this common enumeration – and enable rapid and timely patching.

The Verizon study confirms that completely preventable exploits were successful simply because basic patch management had been neglected for over a year. Unfortunately, companies continue to use software versions with known security vulnerabilities in spite of their risk. Basic procedures to update software with patches offering the latest protection are a necessity and a basic expectation of all company stakeholders – so due diligence teams should probe both IT and management about a company's software patching practices.

Boards should ensure that patching and updating procedures are tightly controlled, methodically documented and universally followed. Boards should take note when a company's patch management is a routine IT operation that is too disconnected from security. Without a security approach, operations teams are left with the difficult task of guessing which patches to apply, and where.

Endpoint Detection and Response

Endpoint detection and response (EDR) tools are quickly becoming an important aspect of the cybersecurity landscape. Typically installed within a swath of IT equipment including domain controllers, database servers and workstations, EDR tools conduct real-time "intelligence feeding" and are moving toward becoming a corporate cybersecurity standard.

By providing continuous monitoring and recording of activity on endpoints and servers, EDR tools aggregate relevant data before a cyber-attack, which in turn:

- Reduces the need for after-the-fact data breach manual data acquisitions, user system forensics and log file analysis;
- Decreases the cost, complexity and time of internal investigations and regulatory response; and
- Accelerates the identification of root causes and attack vectors of data breaches.

EDR technologies also provide a richer depth of behavior-based anomaly recognition and better visibility into threats of all varieties, not just malware. For example, by providing instant aggregate threat information and decreasing the "dwell time" of targeted attacks, EDR solutions enhance enterprise visibility and also help counter internal threats and malfeasance.

By identifying adversary activity expeditiously, the company can isolate and mitigate the attackers' impact on its systems.

When reviewing the overall cybersecurity efforts of a company, Boards should inquire about a company's use (if any) of EDR technologies. Implementation of an EDR platform into a cybersecurity infrastructure, which monitors endpoints continuously, evidences a forward-thinking C-suite and is a sign of a company's transition from reactive security to proactive hunting and detection.

Moreover, aggregating large swaths of data and looking for anomalous behavior across the enterprise will help to identify indicators of attack. By identifying adversary activity expeditiously, the company can isolate and mitigate the attackers' impact on its systems.

Physical Security

Contrary to many popular notions of hacking, cyber-attacks can sometimes begin with a physical breach. For instance, a cyber-attack can start when an outsider surreptitiously gathers fodder for a social engineering scheme (such as a spear-phishing campaign) or when an insider (such as a bad leaver) gains access to a company's network and wreaks havoc, without initially using malware or other clandestine technological means.

Concerns about physical security should already be incorporated into a company's cybersecurity approach. Many of the IT security management standards or frameworks such as ISO/IEC 27001:2013, the Information Security Forum Standard of Good Practice for Information Security and NIST's Cybersecurity Framework all cover the need to manage physical access and apply relevant controls to protect IT assets.

The connection between physical security and cybersecurity became particularly apparent in a 2014 cyber-attack using a piece of malware called Tyupkin, for illegally withdrawing funds from eighteen ATMs in Malaysia. According to published reports and Interpol, the attackers worked in two stages. First, they gained physical access to the ATMs and inserted a bootable CD, which installed the Tyupkin malware. Next, after rebooting the system, the attackers gain control of the infected ATM while the malware runs in an infinite loop waiting for a command.

The malware-in-the-ATM attack is a good reminder that a company should consider the importance of physical security. To insert the disc and infect the machine with the virus, the attackers literally opened the ATM's top panel. Once the disc was ejected, they closed the panel, and their accomplices withdrew money by typing automatically generated codes, usually sent to vendors through their mobile phone.

Boards should engage in a review of physical security of facilities, including management's plans for reception and entry checkpoints; ID scanner and other access records; video or still footage; physical logs; and even elevator and garage records. Questions about physical security should probe whether:

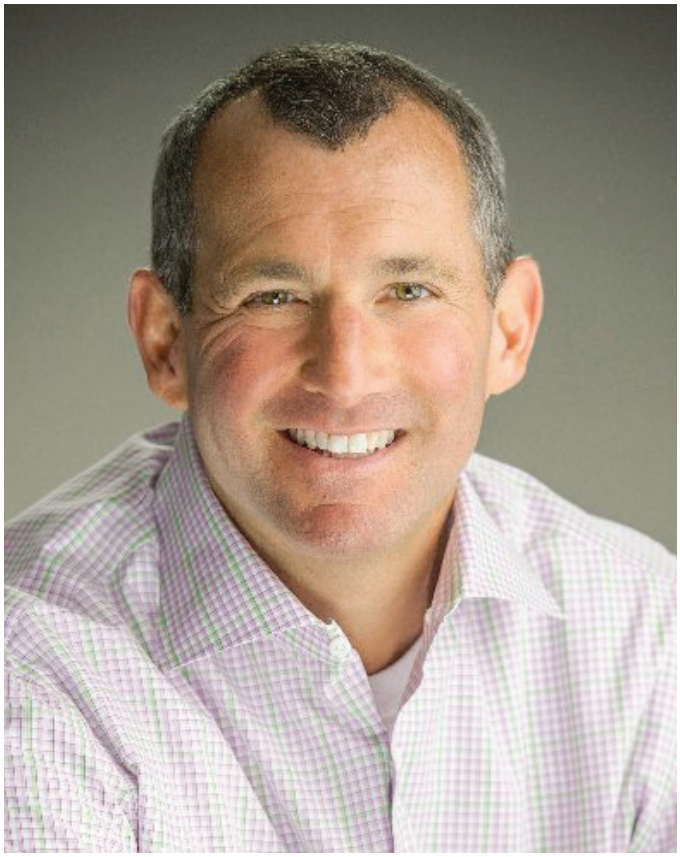
- A company has developed a formal and well-documented physical security policy;
- A company's physical security policies and procedures are regularly reviewed to determine if the controls are operating as intended;
- Changes and enhancements to a company's physical security policies and procedures are implemented when necessary;
- Access controls are in place for the company's key IT locations;
- Physical access to the company's critical systems has any additional controls for authorization, as well as logging records and alerts;
- Procedures managing company visitors are consistently reviewed and updated; and
- A company has adequate protections in place to ensure that authorized visitors do not have the ability to observe or access sensitive employee systems and documents.

Contrary to many popular notions of hacking, cyber-attacks can sometimes begin with a physical breach.

Stay Tuned for the remainder of this series: Part 4 (Encryption, Data Mapping and Final Thoughts).

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
