Nasdaq

Top cybersecurity concerns for every board of directors, part one:

Cybersecurity Governance

by John Reed Stark

Cybersecurity Governance

Top cybersecurity concerns for every board of directors, part one

by John Reed Stark

Every board now knows it's company will fall victim to a cyber-attack, and even worse, that the board of directors will need to clean up the mess and superintend the fallout. The threat seems even more ominous as of late. Recently, two senior cybersecurity officials went so far as to say that the world should brace itself for more physically destructive hacks, warning that a more dangerous era of hacking was already upon us.

Paul Chi Chester, the director of operations at Britain's new National Cyber Security Center, told attendees at an event hosted by British defense think tank RUSI that electronic intrusions were on their way to becoming more "destructive, disruptive and coercive." "That will be our future," he told the crowd. Chichester was seconded by Air Force Lt. Gen. James K. McLaughlin, deputy commander at U.S. Cyber Command, who similarly stated that infrastructure-wrecking attacks were being seen "right now in the environment."

Yet cyber-attacks can be extraordinarily complicated and, once identified, demand a host of costly responses. These include digital forensic preservation and investigation, fulfillment of state and federal compliance obligations, potential litigation, engagement with law enforcement, the provision of credit monitoring, crisis management, a communications plan – and the list goes on. Additionally, constituencies that may require notice, briefings, and other information include customers, partners, employees, affiliates, insurance carriers and a range of other interested parties.

And besides the more predictable workflow, a company is exposed to other even more intangible costs as well, including temporary or even permanent reputational and brand damage; loss of productivity; extended management drag; and a negative impact on employee morale and overall business performance.

So what is the role of a board of directors amid all of this complex and bet-the-company workflow? Corporate directors clearly have a fiduciary duty to understand and oversee cybersecurity, but 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.

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

The second article will pertain 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 data mapping – and also provide some thoughts on this series overall together with some final thoughts.

By using these concerns as a guide, boards of directors can not only become more preemptive in evaluating cybersecurity risk exposure but they can also successfully elevate cybersecurity from an ancillary IT concern to a core enterprise-wide risk management item, at the top of a board's oversight agenda.

Cybersecurity Governance Generally

The cybersecurity policies, practices and procedures in place at any company provide a critical indicator of cybersecurity wellness and should be one of the primary focuses of any cybersecurity due diligence effort.

Threat landscapes, activists, random hackers and state-sponsored actors constantly evolve, refining their techniques, altering their motivations and shifting their resources, so the best approach for a cybersecurity due diligence team is to avoid checklists and conduct cybersecurity due diligence in a thoughtful and holistic manner. Effective cybersecurity due diligence carefully considers changing threat actors, advance network telemetrics and emerging attack vectors.

This article outlines the various policies, practices and procedures involved in the current board oversight paradigm, organizing data points into broad categories to facilitate the most effective and efficient approach.

Incident Response Plan

Having a cyber-attack incident response plan is a notion that has been preached over and over again to every company (public or private), and that is an important starting point for analysis during any cybersecurity due diligence exercise. Every company should have, available for review, a current documented incident response plan that is approved by senior management and is reviewed and re-approved at least annually.

When contemplating cybersecurity, most companies allocate significant resources to fortifying their networks and to denying access to cyber-attackers. However, it is now a cliché, well-founded in reality, that data breaches are inevitable. As cybersecurity experts have noted, "There's a saying in the cybersecurity industry that there are two types of businesses today: Those that have been breached and know it and those that have been breached and just don't know it."

Along those lines, just as a company has a fire evacuation plan for a building, it should have a plan in place to manage data breaches, an art form less about security science and more akin to "incident response." At the least, an incident response plan specifies the:

- Members/titles/contact details of the response team responsible for each of the functions of the plan (management, IT, information security, human resources, compliance, marketing, etc.);
- Communication lines in the event of a cyber-attack;
- Notification protocols and priorities (including law enforcement, regulators, customers, joint venture partners, vendors and anyone else who might require, or contractually be entitled to, notice);
- Documentation and logging plans in the event of a breach;
- Contact list of relevant outside parties such as outside counsel (who specializes in data breach response), outside digital forensics experts, local law enforcement agents, PR firms and relevant financial firms (including the company's bank and insurer);
- Company employees who have authority to speak and make certain decisions about the investigation;
- Cyber insurance information;
- Containment, remediation, recovery, training and testing plans; and
- Nature and location of any data that is covered by other legal obligations, like medical records under HIPAA, financial records under the Graham Leach Bliley Safeguards Rule or specific, contractually created data protection/breach notification requirements. Company executive management should understand its current incident response plans; when the plan was last updated (and how often); who prepared the plan; who approved the plan; and the plan's general approach and principles. There should also exist an accurate and current network topology diagram that is adequately documented and periodically re-assessed and revised as internal systems and external factors change.

Company executives should also avoid using templates for incident response plans. While templates can serve as a decent starting point, no two companies are identical and all have different business processes,

network infrastructures and types of data-sets. Along these lines, NIST, the National Institute of Standards and Technology, has published a Computer Security Incident Response Guide to help companies develop appropriate policies and procedures and provide a useful reference for companies when meeting with IT department heads. The abstract for the NIST Guide states:

"Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications."

Boards should carefully review incident response plans, including whether evidence of any data security incident is collected and retained so as to be presentable in court, to regulators, to customers, to partners and to any other interested constituency. Boards should also should carefully probe how the incident response plan is tested, what remediation occurs after testing and how often the plan is reviewed and revised.

THERE'S A SAYING IN THE CYBERSECURITY INDUSTRY THAT THERE ARE TWO TYPES OF BUSINESSES TODAY: THOSE THAT HAVE BEEN BREACHED AND KNOW IT AND THOSE THAT HAVE BEEN BREACHED AND JUST DON'T KNOW IT.

Business Continuity Plan

The critical importance of a business continuity plan in the event of a natural disaster is widely recognized and accepted. Yet, too often, such plans are not evaluated in the context of assessing cybersecurity risks.

Even when an organization's IT cybersecurity response fully aligns to IT best practices, there are benefits in utilizing or integrating IT's response into the existing business continuity structure, rather than having two separate response models. Business continuity is particularly important when dealing with the impact of, and recovery from, a cyber-attack. Speed and agility are key enablers in cyber-incident response, and business continuity enables nimble, rapid response limiting financial and reputational impact on the enterprise.

PAYING A RANSOM NOT ONLY EMBOLDENS CURRENT CYBER CRIMINALS TO TARGET MORE ORGANIZATIONS, IT ALSO OFFERS AN INCENTIVE FOR OTHER CRIMINALS TO GET INVOLVED IN THIS TYPE OF ILLEGAL ACTIVITY.

For instance, a rising threat to companies is so-called ransomware, a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. The FBI notes, "Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted recently by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them." Individuals and organizations are discouraged from paying the ransom, as this does not guarantee access will be restored. The FBI warns:

"The FBI doesn't support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee an organization that it will get its data back—we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."

A powerful data-recovery plan, which is properly integrated with an incident response plan, contemplates the threat of ransomware and plans for data recovery (perhaps with specialized back-up data systems). As ransomware techniques and malware continue to evolve, the FBI recommends that organizations in particular should focus on two main areas:

- Prevention efforts – both in terms of awareness training for employees and robust technical prevention controls; and
- The creation of a solid business continuity plan in the event of a ransomware attack.

Boards should determine if a company has properly evaluated the effectiveness of its business continuity plan in the context of a cyber-attack, and if the business continuity plan should be reconsidered and refreshed with these additional considerations in mind. Boards also should probe:

- Whether the policy is regularly reviewed to determine whether the controls are operating as intended;
- How often changes and enhancements to the policy are necessary;
- If (and how often) a company tests its business continuity plan from both a technical and operational perspective;
- If the company has established a dedicated location to retain backup copies of all critical data. Is off-site data encrypted and stored securely;
- Whether employees clearly understand business continuity procedures; and
- Whether a company initiates training and maintains established documentation for its business continuity plan.

Boards also should investigate whether a recovery plan is correlated with business needs, with designated recovery point and recovery time objectives, for situations (such as ransomware) when critical or other necessary systems become unavailable.

IT Security Budgeting

C-suite executives need to view cybersecurity as their company's immune system, which needs flexible funding and talent to avoid the severe losses commonly associated with cyber-attacks. Most budgeting at companies is conducted annually and planned carefully and thoughtfully before the beginning of a company's fiscal year, which makes good sense and is also a sign of a well-run financial team. Yet cybersecurity budgetary priorities can shift quickly and are not well-suited to the standard budgetary planning regimen. A one-year budgetary cycle might not be swift or agile enough to manage rapidly emerging cyber-threats, and an overly rigid, lengthy, cumbersome or otherwise bureaucratic approach toward cybersecurity can create cybersecurity challenges at even the well-run companies.

Boards should understand how cybersecurity budgeting works; how emergency items are identified and funded; and if the budget appropriately provide for contingencies in the event of a cyber-attack or cybersecurity need.

A ONE-YEAR BUDGETARY CYCLE MIGHT NOT BE SWIFT OR AGILE ENOUGH TO MANAGE RAPIDLY EMERGING CYBER-THREATS, AND AN OVERLY RIGID, LENGTHY, CUMBERSOME OR OTHERWISE BUREAUCRATIC APPROACH TOWARD CYBERSECURITY CAN CREATE CYBERSECURITY CHALLENGES AT EVEN THE WELL-RUN COMPANIES.

Drills and Table-Top Exercises

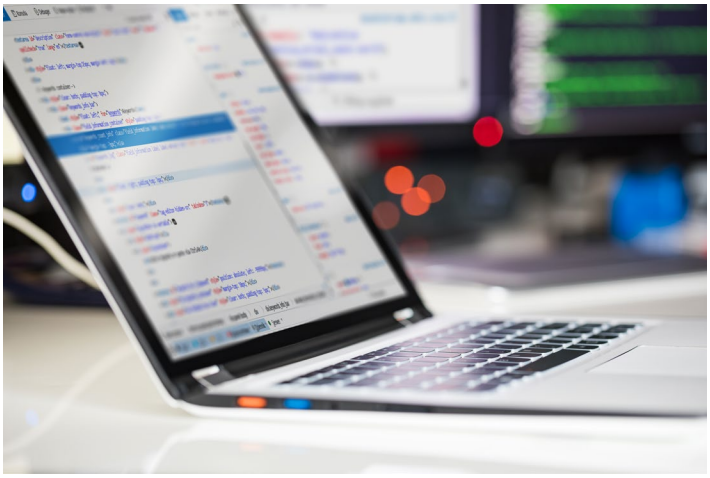
Table-top exercises enable organizations to analyze potential emergency situations in an informal environment and are designed to foster constructive discussions among participants as they examine existing operational plans and determine where they can make improvements. Such exercises are a natural fit for information and physical security because they provide a forum for planning, preparation and coordination of resources during any kind of attack.

Most cybersecurity firms and pen-testing firms offer some form of table-top exercise program, which should, in order to be successful: involve detailed preparation; include multiple parties throughout the company; leverage resources from within the company industry and government; and be timely and realistic. Companies (after consulting with counsel) should also reach out to law enforcement agencies such as the Federal Bureau of Investigation (FBI) and request that a federal agent participate in the table-top drill or exercise. The FBI supports participation and collaboration with U.S. companies, and can provide valuable insight throughout the drill.

Boards should review carefully the efficacy, timeliness, frequency and overall results of a company's table-top drill and even more importantly, analyze what remediation and other corrective measures were taken after those exercises.

Cyber Insurance

A near certainty for public and private corporations is that, at some point, they will be subject to a cyber-attack. And what is indisputable is that cyber-attacks are almost always extraordinarily complicated and will require a host of costly responses. So it seems that for today's risk-averse companies, the best way to gain insight into the question of cyber insurance is not only by understanding the growing and complicated hazard



of cyber-attacks, but also by obtaining a stand-alone cyber insurance policy that contemplates carefully the workflow that typically occurs during their aftermath.

Traditionally, purchasing insurance coverage begins with a policy review, a risk breakdown and a range of other risk-related analytics. However, when contemplating a cyber insurance policy, companies should initiate more of a "reverse-gap" approach toward that calculus, analyzing and scrutinizing the typical cyber-incident response workflow that follows most cyber-attacks.

By analyzing and revisiting the realities and economics of this workflow, a company can then collaborate with its insurance sales representatives and originators to allocate risk responsibly and determine, before any cyber-attack occurs, which workflow costs will trigger coverage; which workflow costs will be outside of coverage; and which workflow costs might be uninsurable.

It also is crucial that companies conduct the necessary due diligence to be sure that their cyber insurance carrier has a good claims-paying and claims-handling history and has a proven record of rapid and supportive response. When a cyber-attack occurs, too often there are doubts as to coverage, which can affect incident response.

Cyber insurance policies also can differ dramatically in their goals and objectives. For example, some policies are designed to cover HIPAA and PCI violations, as well as other regulatory noncompliance, while other policies are geared more for direct financial losses due to wire transfer fraud. For instance, if a company manages trust accounts on behalf of customers, the company likely will require insurance coverage for direct cash losses in the event of a network intrusion that results in the unlawful transfer of funds.

WHEN CONTEMPLATING A CYBER INSURANCE POLICY, COMPANIES SHOULD INITIATE MORE OF A "REVERSE-GAP" APPROACH TOWARD THAT CALCULUS, ANALYZING AND SCRUTINIZING THE TYPICAL CYBER-INCIDENT RESPONSE WORKFLOW THAT FOLLOWS MOST CYBER-ATTACKS.

Cyber insurance policy premiums are "not one size fits all", as premiums are factored on a company's industry, services, data risks and exposures, computer and network security, privacy policies and procedures and annual gross revenue. At present, there are 70 or so insurance carriers writing cyber insurance policies, and nearly all of those policies are issued on a surplus lines basis with potentially significant differences in policy wording from one cyber policy to the next.

Boards should ask if their senior executives have considered reviewing actual cyber-attacks, analyzing and scrutinizing the typical cyber-incident response workflow and so-called "workstreams" that follow most cyber-attacks. By analyzing and revisiting the realities and economics of these workstreams, a company can then collaborate with their insurance sales representatives and originators to allocate risk responsibly and determine, before any cyber-attack occurs, which workstream costs will trigger coverage; which workstream costs will be outside of coverage; and which workstream costs might be uninsurable.

It is also crucial that boards confirm that the cyber insurance carrier their company uses has a good claims paying and claims handling history and has a proven history of rapid and supportive response. When a cyber-attack occurs, too often there are doubts as to coverage, which can impact incident response.

Whatever the type of insurance held by a company, an insurance claim will undoubtedly follow, and insurance adjusters will scrutinize all invoices pertaining to the response to the cyber-attack and the overall cybersecurity of the company, and will require briefings and documentation regarding all investigative efforts. For maximum objectivity, credibility and defensibility, rather than the company itself, boards should make sure that the independent digital forensic firm investigating the breach, at the direction of counsel, should lead any briefings with insurance carriers.

As an aside, boards should make sure that during any sort of data breach response, a professional on the incident response team, preferably counsel, will

maintain carefully written documentation of all efforts of the response. This will help later on when gathering the "documentation package" to present to an inquisitive insurance adjuster when seeking an insurance reimbursement for the costs of the breach.

WHEN A CYBER-ATTACK OCCURS, TOO OFTEN THERE ARE DOUBTS AS TO COVERAGE, WHICH CAN IMPACT INCIDENT RESPONSE.

Third Party Cybersecurity Due Diligence

Outsourcing of services (such as IT, payroll, accounting, pension and other financial services), which typically involve the transfer of, or allowing access to, PII from a company to its vendor, has become increasingly common for today's corporations.

Given that cyber-attackers will often traverse across a company's network and into the networks of its vendors or vice versa, cyber-attacks can often result in disputes as to the culpability for an attack. As a result, in most data breach scenarios, vendors and companies can end up pointing the finger at one another for their respective cybersecurity failures.

Thus, boards should be concerned if any third party vendor has access to a company's networks, customer data or other sensitive information – or if there exists any sort of other cybersecurity risk of the outsourced function.

In addition, boards should understand if and how the company incorporates requirements relating to cybersecurity risk into its contracts with vendors, these requirements may trigger notification responsibilities. In the event of a data breach, corporate vendors will want to know all relevant facts relating to the cyber-attack, especially: if their data has potentially been compromised; if services will experience any disruption; the nature of remediation efforts; if there are any official or unofficial findings any investigation; or if there is any other information which can impact their operations, reputation, etc.

Vendors may also request images of malware and IOCs or to visit/inspect the company with its own investigation team. Venders may ask for weekly or even daily briefings and may demand attestations in writing with respect to any findings pertaining to their data. Some customers may also have contractual language establishing their rights when a cyber-attack occurs, which can range from notification, to on-site inspections, to the option of an independent risk and security assessment of the victim company (at the victim company's, and not the customer's, expense).

Moreover, if third party vendors conduct remote maintenance of a company's networks and devices, in the event of a cyber-attack, the company may want to confirm it can obtain copies of any relevant logs, as well as access the third party system to scan for IOCs.

Boards should probe the practices and procedures with respect to the cybersecurity of third party vendors. Boards should also ask about the company's information security procedures (including training) concerning third party vendors authorized to access a company's network.

BOARDS SHOULD BE CONCERNED IF ANY THIRD PARTY VENDOR HAS ACCESS TO A COMPANY'S NETWORKS, CUSTOMER DATA OR OTHER SENSITIVE INFORMATION– OR IF THERE EXISTS ANY SORT OF OTHER CYBERSECURITY RISK OF THE OUTSOURCED FUNCTION.

Bring Your Own Devices

Many companies allow their employees to "bring your own devices" (BYOD), especially given customer expectations of 24-7 communication lines; work-at-home situations; and the travel demands on corporate employees. Despite all of the security risks BYOD poses to an IT environment, the trend of companies embracing BYOD in the workplace continues to grow at a rapid pace. In fact, in 2013, more than six out of ten small and medium-sized businesses had a BYOD policy. By 2020, it is estimated that 85 percent of businesses will have some kind of BYOD program in place.

The security risks surrounding BYOD are obvious: loss of control and visibility of the enterprise data that is being transmitted, stored and processed on a personal device; malware infiltration of the device; potential data leakage or disclosure of enterprise data on a device; physical loss or theft of the device; and devices with compromised integrity, such as smartphones that have been rooted or jail-broken by their owners.

Boards should make sure that a company has total control over all BYOD devices, including all applications contained therein, as well as the ability to remotely

wipe all data from devices. Boards also should focus on whether a company has put into operation robust mobile device management platforms that support containerization of business and personal data, enhanced security controls, encryption key escrow and tracking and management of laptops, tablets, mobile phones and other mobile devices.

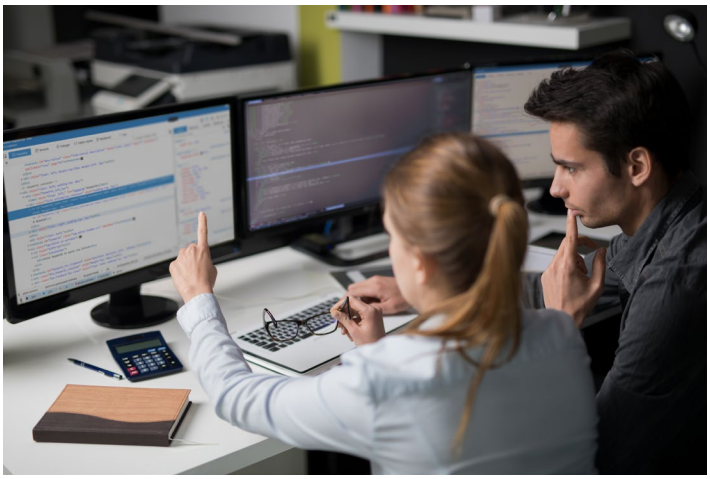
The Cloud

Cloud storage has many potential advantages for companies, including cost savings, scalability, increased mobility and easier collaboration. However, when a company stores critical and/or confidential information in the cloud, that information is essentially stored off-site, possibly in another country, and companies should make sure their respective companies are using cloud providers that can reasonably protect and provide assurances on overall data security.

Along the same lines, cloud-based file sharing services, such as Dropbox, Google Drive, Box and others, are another way confidential information leaks out of a company. Such cloud services often are used through personal accounts, despite many large companies prohibiting, as a matter of policy, the use of such services for these purposes. Some companies also block access to such services from the company's desktop computers with effective security controls, while other companies are less sophisticated or simply resist the notion of becoming the automated "data nanny" for their employees.

Given the increased adoption of cloud-based services by enterprises of every kind, cyber-attacks on cloud environments have reached almost the same level as attacks on traditional IT. Boards should probe a company's cloud-related practices. Questioning should include especially: an assessment of any enterprise-grade security systems and analytics; a determination of the attack vectors; and a review of data security measures.

GIVEN THE INCREASED ADOPTION OF CLOUD-BASED SERVICES BY ENTERPRISES OF EVERY KIND, CYBER-ATTACKS ON CLOUD ENVIRONMENTS HAVE REACHED ALMOST THE SAME LEVEL AS ATTACKS ON TRADITIONAL IT. BOARDS SHOULD PROBE A COMPANY'S CLOUD-RELATED PRACTICES.



Important questions include:

- Whether the cloud data is encrypted (in transition and in motion);
- Who holds the encryption keys for cloud data;
- Whether the cloud data is subject to search and seizure (both domestically and internationally);
- The nature of data protections used by the cloud firm;
- How transparent are the cloud providers' own security systems;
- What access can the company get to the cloud provider's data center and personnel to ensure the security system is in place and functioning and make sure it can make a risk assessment and design a response plan;
- Have company customers given approval for cloud storage of their data;
- What are the cloud servicers' responsibilities to update their security systems as technology and cyber-attack sophistication evolves;
- How do the cloud providers continuously monitor, detect and respond to security incidents;
- What cloud logging exists and how long are logs maintained;
- How and when is cloud data destroyed;
- Can (and how) cloud data be subject to a litigation hold and what technologies allow for the cloud data's perusal;
- What auditing is permitted of the security capabilities of the cloud company;
- What regulatory and privacy requirements for PII, personal financial information, personal healthcare

information or other customer data are triggered by the cloud data;

- Do the cloud firm and the company have any indemnification agreements or evidence of cyber insurance;
- Do the company's insurance policies cover losses from activities undertaken by the cloud service providers in the event of a cyber-attack;
- What types of pen testing are undertaken by the cloud firm; and
- What are the specific details and efficacy of security policies and procedures of the cloud firm?

Boards also should confirm that a company has a comprehensive means to prevent sensitive data from being uploaded for inappropriate sharing, and the requisite visibility and access to detect anomalies, conduct further investigation and take quick and decisive remedial action. Along these lines, questions should cover: technologies used to prevent the unauthorized use of cloud applications by employees; internal controls regarding an cloud applications used by employees; an incident response plan for handling an attack on any cloud application; and employee training concerning use of cloud applications.

Staying Current

Not all companies face the same cybersecurity risks. There is no one-size-fits-all approach. Companies that house and maintain large amounts of critical information and data need to tailor any defense, mitigation and response plans accordingly. By taking steps to ensure that information flow about data breaches within the industry and the latest intelligence about rising threats are considered by IT management on an ongoing basis, companies can stay current on the latest threats and prepare accordingly. Preparedness is the key.

Boards should determine what steps a company has undertaken in the realm of security science to stay current about the latest cybersecurity intrusion modus operandi, data breach trends, etc. Staying current should be an active aspect of cybersecurity defenses and a required (and encouraged) goal for all IT and other cybersecurity employees. The C-suite also should be briefed routinely about current threats, together with practices, policies and procedures for addressing suddenly emerging cybersecurity threats.

Lessons Learned from Prior Attacks

When a company experiences a cyber-attack, aside from the cyber-attack's investigation, remediation, etc., a company should also engage in a bona fide review after the fact – and organize and document the lessons learned.

For example, DOS (Denial of Service) or DDOS (Distributed Denial of Service) attacks continue to pose a serious threat to most companies, especially those with an active online commerce component to their operations – and should always be an important Board concern. Boards should have an understanding of how many DOS/DDOS attacks the company has experienced; the specific actions a company is taking to deter DOS/DDOS attacks; and how the company has learned from prior DOS/DDOS attempts.

BY TAKING STEPS TO ENSURE THAT INFORMATION FLOW ABOUT DATA BREACHES WITHIN THE INDUSTRY AND THE LATEST INTELLIGENCE ABOUT RISING THREATS ARE CONSIDERED BY IT MANAGEMENT ON AN ONGOING BASIS, COMPANIES CAN STAY CURRENT ON THE LATEST THREATS AND PREPARE ACCORDINGLY. PREPAREDNESS IS THE KEY.

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

Stay Tuned for the remainder of this series:

Part 2 (People); Part 3 (Technology); and Part 4 (Encryption, Data Mapping and Final Thoughts).