Morgan Stanley

Cybersecurity and Corporate Governance

Critical Questions Public Companies Must Answer

"Cybersecurity" risks are the unique risks that interconnected network systems pose to a company or organization. The main street and business media universally portray cybersecurity as a technical or IT problem, and generally envision technological responses to the threats. However, for those who manage and advise public companies, there is a growing recognition that cybersecurity also poses challenges to the public company's existing corporate governance and compliance processes. This article will address some of those assumptions and attempt to answer critical questions facing public companies today.

Cybersecurity as a Business and Governance Challenge

Cybersecurity breaches such as the breaches at Marriott and Yahoo! Inc. have commanded headlines for years, and the damaging impact of the most recent high profile incidents have affected millions of Americans and disrupted the business operations and damaged the reputations of many of our best-known companies.

Incidents like these have caused government agencies, such as the Securities and Exchange Commission and the Federal Trade Commission, to heighten oversight and strengthen regulations, forcing permanent change to American business practices.

Looking at the broader economy, according to an October 2018 cybersecurity study released by First Data, 34%—essentially, one out of every three Americans—had experienced some compromise of their personal information over the past year.[1] Put another way, there were 2,216 data breaches and more than 53,000 cybersecurity incidents reported in 65 countries in the 12 months ended in March 2018.[2]

The costs of these data breaches can be devastating for a company. It is estimated that in the U.S., the average total cost of a data breach is $7.91 million, with a large breach of 1 million records costing $40 million and a mega breach of 50 million records costing over $350 million.[3]

SEC Engagement

The SEC has made it clear that cybersecurity is an area on which it intends to focus its enforcement resources. In just the last two years, the SEC has implemented a number of cyber-related programs. Specifically, a new "Cyber Unit" was created in late 2017 that brought 20 stand-alone cases related to cybersecurity in 2018, with 225 cyber-related investigations it deemed ongoing.[4]

The SEC Division of Enforcement's 2018 Annual Report highlights the Commission's focus on keeping pace with technological change. This included the action against Yahoo!, which represented its first case against a public company for failing to properly inform investors about a cyber breach. The SEC also took action against an investment adviser when a cyber-attack compromised the investment information of thousands of customers.[5] In February 2018, the SEC published Commission Guidance to public companies on cybersecurity disclosure. In its introduction, the Commission stated, "Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack."[6]

In introducing this Guidance, SEC Chairman Jay Clayton stated public companies should examine their controls and procedures with not only a focus on their securities law disclosure obligations, but on their insider trading monitoring obligations as well.[7]

With the SEC devoting significant resources to cybersecurity issues, we believe public companies need to assess the adequacy of their procedures and disclosure controls. This assessment is better done now than in the white heat of a cyber incident (or even the relative warmth of the annual audit process).

The balance of this article explores some of the critical questions companies must address in light of their cybersecurity risks. By reviewing your current controls, policies and procedures and implementing deliberate actions that may involve investments in training and infrastructure, you can better protect your company from potentially irreparable damage to its reputation and long-term valuation.

The SEC's Evolution on Cybersecurity and Public Disclosures

2009

SEC amends rules to require greater disclosure about the board's role in risk oversight generally.

2011

SEC's Division of Corporation Finance issues Staff Guidance on disclosure obligations relating to cybersecurity risks and incidents.

2014

SEC Commissioner Luis Aguilar states, "Directors should be asking themselves what they can, and should, be doing to effectively oversee cyber-risk management."

2017

SEC Cyber Unit is created.

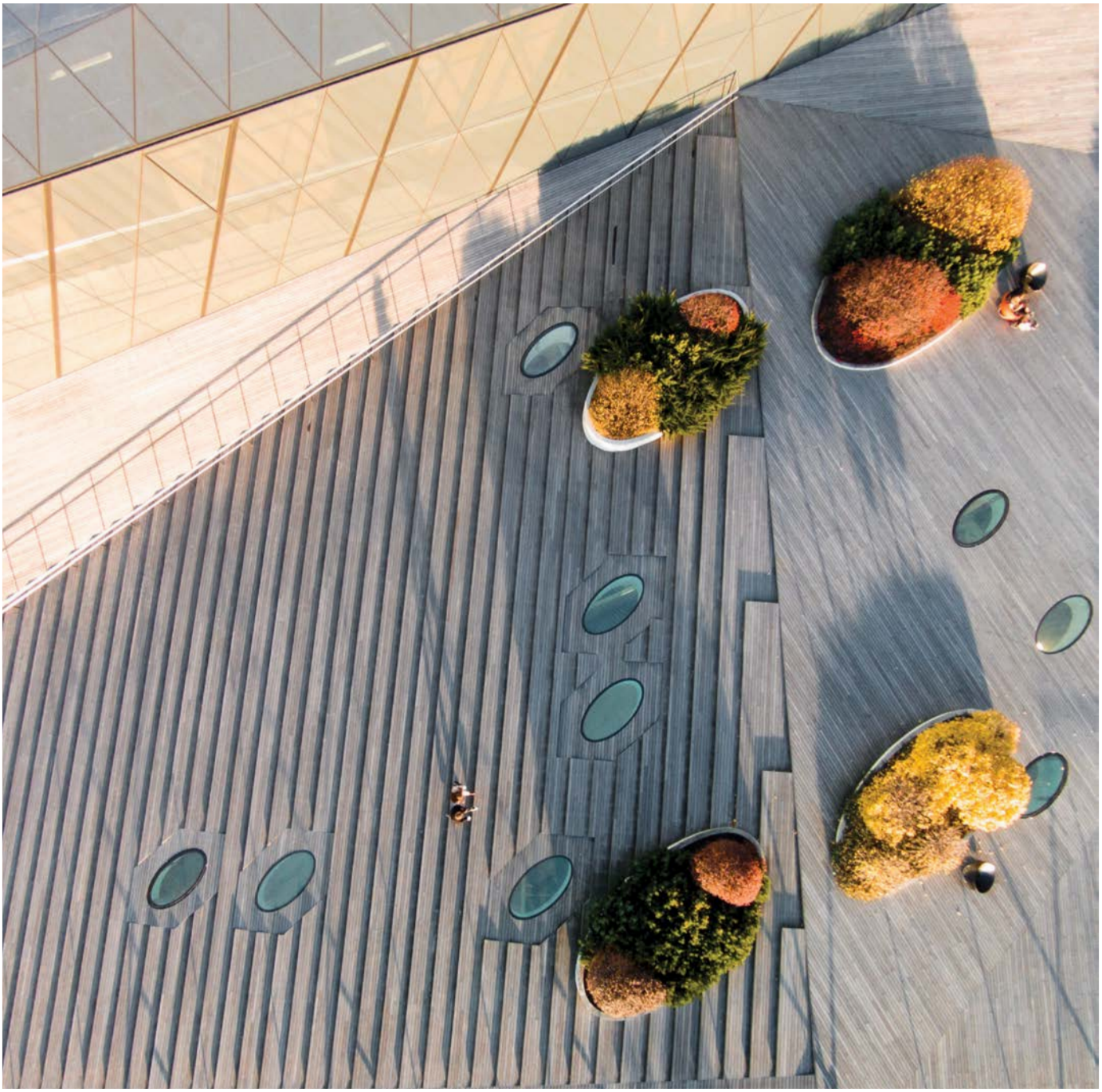
Chairman Jay Clayton advises, "Issuers should consider whether their publicly filed reports adequately disclose information about their risk management governance and cybersecurity risks, in light of developments in their operations and the nature of current and evolving cyber threats."

2018

SEC releases Commission Guidance making clear that corporate insiders may not trade while in possession of nonpublic information regarding a significant cyber incident and that companies should have policies in place to guard against such activity, in addition to clarifying the SEC's position that cybersecurity policies constitute disclosure controls, triggering CEO/CFO certification under the Sarbanes-Oxley Act.

Critical Questions About Cybersecurity and Corporate Governance

Public company cybersecurity compliance must begin well before any cyber incident. In the sections that follow, we raise a series of questions about oversight, policies and procedures, and disclosure controls, as well as the action steps we believe companies should consider to strengthen all of these areas.



QUESTIONS ABOUT OVERSIGHT

What does your board need to know about cybersecurity?

To help answer this question, we turned to the National Association of Corporate Directors (NACD), which prescribes five core principles for cybersecurity practices in its Directors Handbook on "Cyber-Risk Oversight"[8] :

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just a technology issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
5. Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Does your board need directors with specific cybersecurity expertise?

While we are not prepared to say every public company board of directors should have a "cybersecurity expert" with a technical background (corresponding to the board's audit committee financial expert), the business and regulatory expectations set forth above mean, as a practical matter, that one or more of the directors must be able to understand from the company's management and outside experts, and convey to others, the data privacy and other cybersecurity risks the company faces. (Commentators have observed that if regulators were to mandate a cyber expert on every board, a shortage of qualified directors would surely result.)

Who has responsibility for oversight of cybersecurity risks – the full board or a committee of the board?

According to a recent Ernst & Young LLP survey of proxy and Form 10-K disclosures, 84% of the Fortune 100 disclose that at least one board committee is charged with oversight of cybersecurity matters, with 70% using the audit committee for this purpose.[9]

How often should the board/committee discuss cybersecurity?

The same survey indicated that 34% of Fortune 100 companies provide management cybersecurity reports to the board frequently, with some companies using "regularly" or "periodically," while others citing "annually" or "quarterly."[10]

Is there sufficient focus and commitment at both the board and senior management levels with respect to cybersecurity?

We believe it is appropriate to focus on the "tone at the top." An organization reflects the priorities of its senior policymakers, especially when it comes to financial reporting and compliance measures. The business and regulatory imperatives discussed above mean that no public company can afford to ignore the corporate governance aspects of cybersecurity.

Do senior information technology executives have sufficient standing in your organization? Are they members of the senior leadership team, or at least reporting to them, so that the board can be well-informed?

According to the NACD principles above, boards should devote regular meeting time to reports from management about cyber-risk and should have adequate access to cybersecurity expertise. While many public companies have this cybersecurity expertise in-house, others cover it with a combination of in-house and third-party resources. Regardless of the source, the necessary information about the risks the company faces and the pros and cons of various responses must become part of the mix of information that makes its way to the board. This may require the regular participation of IT professionals who never imagined they would be dealing at the board level.

QUESTIONS ABOUT POLICIES AND PROCEDURES

Does your company's policy suite guide employees in protecting against cyber threats and responding appropriately should a cyber incident occur?

Securities exchange listing requirements, as well as corporate codes of ethics or business conduct, generally require companies to comply with all applicable federal and state laws. Data privacy and cybersecurity are part of this compliance.

Cybersecurity requires a coordinated approach that includes the board, senior management and all employees. It is not the sole responsibility of the IT department; all the stakeholders need to be aware of their roles before an incident occurs.

Within the suite of governance, compliance and conduct policies maintained by a public company, key information should be included on how to protect the company from a cybersecurity threat. The information should include specific details on handling customer and employee data, password protection, posting on social media, use of personal emails and unapproved devices, and the implementation of new software. The policies should also define clear lines of communication for questions and reporting issues if and when a cyber event is discovered. Further, policies and procedures should be implemented across the company — including training of personnel — to enhance compliance.

Does your company's insider trading policy state that potential cyber incidents could be material to your company?

If this article motivates you to do nothing else, we recommend you revisit your policies to clarify that discovery of a cyber breach may constitute "material non-public information." After the Equifax insider trading cases, it's clear your policy should include examples of various cyber events to educate employees and put them on notice. The SEC stated in the February 2018 release, "We encourage companies to consider how their codes of ethics and insider trading policies take into account and prevent trading on the basis of material nonpublic information relating to cybersecurity risks and incidents."[11]

Do your current controls address the SEC's cybersecurity concerns about corporate insiders and the trading window?

It's also important to determine when to close your insider trading window. The same SEC release warned companies to avoid the appearance of improper trading during the period between discovery and disclosure of a cyber incident.[12] Experts suggest companies consider the extent to which an insider has an informational advantage over the market with respect to the cyber incident when determining whether to close the trading window.[13]

The potential harm a cyber event can cause must also be a factor. This includes financial, reputational and competitive harm, damage to customer and vendor relationships, and the possibility of litigation or regulatory actions by state, federal and international authorities. As with all materiality judgments, the materiality of a cyber event will be viewed after the fact with 20/20 hindsight.

Is your company's pre-clearance list sufficient? Are the right information technology and information security officers on this list?

We recommend reviewing the list of company employees who are covered under your insider trading policy. Commentators have observed that the SEC and Department of Justice are willing to push the envelope when it comes to what "knowledge" is required to support insider trading charges. For example, in the Equifax case, an IT employee accurately guessed the data breach involved Equifax, despite being told by management that it involved another company.[14]

Is your company's process to close the trading window sufficient? That is, are the information technology and information security functions sufficiently connected to the administrator of the insider trading policy?

One of the difficult aspects of securities compliance in the cybersecurity arena is the delay between a data breach or hacking event and its discovery, and then a further delay while the incident is evaluated, appropriate safeguards are implemented, the damage is assessed, and response and recovery actions begin. The company's insider trading pre-clearance officer must be brought into the loop of these discussions when there is any chance the event might be deemed to be material and must be kept advised as the situation develops. This includes awareness of disclosures about the incident that the company may be making to state, federal or international data privacy regulators or consumers.

When can you open your company's trading window?

In general, the window could open one or two business days after full disclosure of a cyber incident. The more thinly-traded the stock, the longer the recommended wait.

Does your company's Regulation Fair Disclosure (Reg FD) program account for cyber events?

The SEC expects companies to have policies and procedures in place to prevent selective disclosure of material non-public information, which could include cybersecurity matters. Specifically, your policy should address who is authorized to speak for the company and make everyone at your organization aware that cyber events are potentially material non-public information. Those responsible for securities compliance should be aware of contemporaneous disclosures the company may be making to enumerated persons, including securities market professionals and holders of your company's securities that would be reasonably expected to trade on the information.

Does your Reg FD training extend to the appropriate information technology and information security personnel?

Given the nature of technology, a large number of employees outside the financial reporting areas of the company may be aware of a cyber event. As a result, we recommend reviewing the full scope of your Reg FD training efforts. It's important to include all those who could potentially be involved in a cyber event. This group must be educated that disclosure of technical information is potentially market-moving.

QUESTIONS ABOUT DISCLOSURE CONTROLS AND PROCEDURES

What makes cybersecurity a unique challenge for securities disclosure compliance? How does the SEC connect cybersecurity risks to disclosure controls and procedures?

The NACD has noted certain characteristics that distinguish cybersecurity risks from other business risks a company faces: Complexity, speed of evolution, potential for significant financial, competitive and reputational damage, and the fact that complete protection is an unrealistic objective.[15]

The SEC recognizes that cybersecurity risk management is just one key element of enterprise-wide risk management, as it relates to securities law compliance. Companies should regularly assess whether they have sufficient disclosure controls and procedures in place to ensure relevant information about cybersecurity risks is reported up the corporate ladder.[16]

Should your company's disclosure committee membership include an information technology or data security representative?

The SEC expects disclosure controls and procedures to provide a mechanism by which the material risks of potential cyber incidents are appropriately identified and disclosed. While this would suggest the answer to the above question is yes, it also suggests turning the question around and, if possible, including one or more representatives of the disclosure committee in the risk management group that assess the company's cybersecurity risks.

Does your company's upward certification process adequately cover information technology and data security personnel?

The SEC envisions a process that crosses functional lines within the company. The February 2018 cybersecurity release stated, "Controls and procedures should enable companies to identify cybersecurity risks and incidents, access and analyze their impact on a company's business, evaluate the significance. . . provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents."[17]

What is the best way to implement disclosure controls regarding cybersecurity issues?

In analyzing this issue, The Corporate Counsel recommends "piggybacking" on your company's existing risk management and compliance infrastructure.

Your company likely already has a formal cyber incident response plan that involves participation from representatives of all key business units, senior management and board oversight. Since such a plan is integrated across the business units, it can be leveraged for the purpose of cybersecurity disclosure.

Cyber incident response plans generally classify the potential magnitude of an incident and provide for escalation of the company's response based on the assessment of the magnitude of the threat. Elements of such plans that facilitate timely and complete disclosure include:

Incidents are classified on a scale that begins with those involving low or negligible risk to the company and escalating to those involving high or extreme risk.

A response team — including representatives from the key business units and outside experts — will be assembled and staffed based upon the perceived magnitude of the incident.

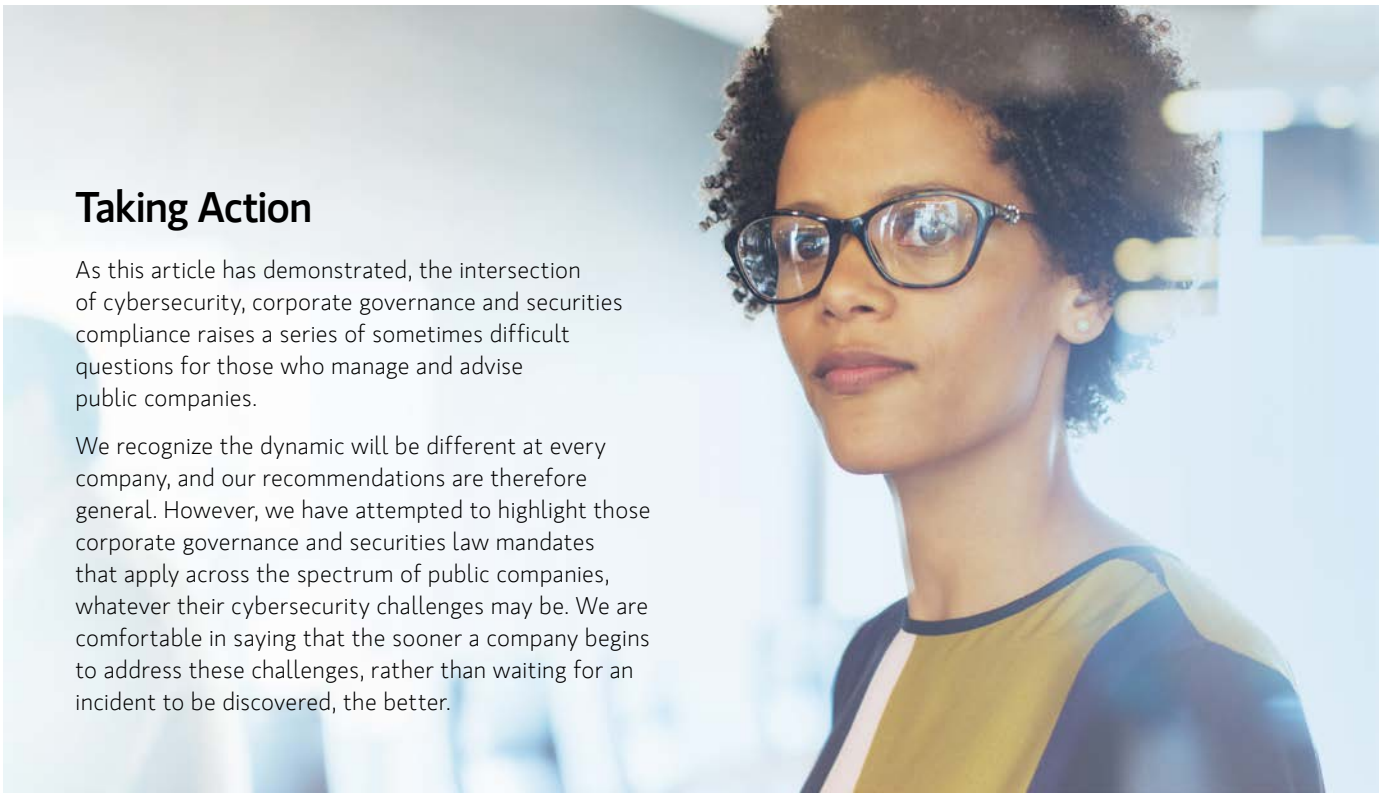
Incidents exceeding a certain magnitude can automatically trigger other responses, such as the closing of a trading window or the implementation of additional measures to prevent selective disclosure.[18]

To what extent should cybersecurity expenses, risks and trends be discussed in your company's Form 10-K or proxy statement?

The 2018 Ernst & Young survey analyzed cybersecurity-related disclosures in the proxy statements and Form 10-K filings of the Fortune 100 companies. The report stated that all companies (100%) included cybersecurity as a risk factor in their SEC filings.[19] Beyond the risk factors, the SEC advises that cybersecurity disclosure may belong in the MD&A, business description, legal proceedings and financials.

Does your company's proxy statement describe the board's oversight regarding cybersecurity, as well as its expertise in this area?

Although disclosure practices vary, as noted above, Ernst & Young's Fortune 100 survey found that 84% of companies disclosed that at least one board committee was responsible for oversight of cybersecurity matters. Approximately 25% of the Fortune 100 identified one or more "point persons" among the management team on cyber issues. Finally, 41% of companies identified cybersecurity experience as a key director qualification highlighted or considered by the board.[20]

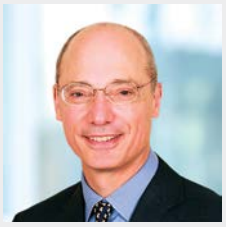


Taking Action

As this article has demonstrated, the intersection of cybersecurity, corporate governance and securities compliance raises a series of sometimes difficult questions for those who manage and advise public companies.

We recognize the dynamic will be different at every company, and our recommendations are therefore general. However, we have attempted to highlight those corporate governance and securities law mandates that apply across the spectrum of public companies, whatever their cybersecurity challenges may be. We are comfortable in saying that the sooner a company begins to address these challenges, rather than waiting for an incident to be discovered, the better.

About the Authors



Stephen T. Giove
Partner
Shearman & Sterling
sgiove@shearman.com

Stephen is a partner in Shearman & Sterling's Capital Markets practice. He is one of the founders of the firm's Corporate Governance Advisory Group. His practice is principally focused on counseling corporate clients with respect to strategic, governance, financing and public company matters.

Michael L. Andresino
Partner
Arent Fox LLP
michael.andresino@arentfox.com

Mike is a partner in Arent Fox's Corporate & Securities practice group, where he represents primarily early-stage through middle-market clients in technology and other industries. He guides management and boards through difficult securities compliance and corporate governance challenges.

Thomas S. Brennan
Partner
Arent Fox LLP
thomas.brennan@arentfox.com

Tom is a partner in Arent Fox's Corporate & Securities practice group, where he represents technology companies, angel investors and venture capital firms. He advises executives, boards and investors on capital raises, corporate governance, securities disclosure and strategic transactions.

A Cybersecurity Checklist for Your Business

As cybersecurity threats intensify, it's important to ensure you have the proper safeguards in place to bolster the protection of your data and assets. The checklist below serves as an important reminder for business leaders and their employees to stay vigilant and focused on arming your organization against the perils of cybersecurity breaches and concerns.

Develop and Maintain a Detailed Cybersecurity Policy

Do you have a documented cybersecurity policy? If not, it's time to put one together. Your employees are both your first line of defense and greatest point of vulnerability. Ensure they know your expectations and responsibilities and be sure to regularly educate, train and test them to ensure compliance. How should sensitive information be stored or transmitted? If an employee clicks on something suspicious, what should he or she do? Is access to sensitive information restricted to only those employees who require access to perform their job functions? It only takes a single person to make one very costly mistake. There's no substitute for clear, enforceable policies and procedures.

Develop and Practice an Incident Response Plan

Virtually every business will need to navigate a data breach at some point. The question is not just how to prevent an incident, but what to do if one occurs. Incident response plans are critical to being prepared for and mitigating the consequences of a breach. An effective response plan will delineate roles and responsibilities for key stakeholders both within the organization (IT, senior management, inside counsel, communications) and externally (outside counsel, computer forensics experts and public relations). Plans should be tested through various scenarios and reviewed and improved as appropriate.

Be an Email Skeptic

Email is often a cyber criminal's favorite tool. If an employee clicks on a link or opens an attached spreadsheet without thinking, that employee could be unwittingly downloading malware onto your network.

Business Email Compromise (BEC) is another popular, if nefarious, tactic. A BEC attack is a scheme whereby a fraudster impersonates an executive or client with the aim of getting a target to send money or sensitive information. Sometimes the fraudster is simply spoofing a publicly available email address. In other cases, the criminal has compromised a server or has hijacked account credentials.

Whatever the method, the lesson is the same — never reflexively trust an email you receive. Always rely on multiple methods beyond email to confirm the sender's identity and intent before engaging, and never transmit sensitive information via unsecured email or text.

Protect Your Systems

Training employees to spot and thwart social engineering schemes is part of the puzzle, but on its own is insufficient. Just as you would use antibiotics and vitamins to bolster your body's immune system, you need to do the cyber equivalent at your company.

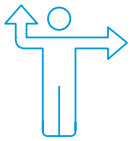
Start by running a reputable, American-made anti-virus product on all personal computers and laptops being used for business activities. Doing so will protect these devices from future malware invasions and clean up any existing infection.

It's also critical to keep all software, operating systems and browsers up to date across your devices — and to turn on automatic updates where available. Software companies often include security upgrades (called "patches") in every update they release. Installing those updates immediately will help protect your devices. Of course, doing this properly requires having an accurate inventory of all devices and software the business is using.

Avoid Password Pitfalls

Password reuse is risky business. When individuals reuse passwords across multiple accounts, a breach of one account threatens the others. To avoid this risk, the best strategy is to use complex, lengthy and unique passwords for each account—but such passwords are very difficult for anyone, let alone an office or group of individuals, to remember. This is where a password manager can assist. A reputable password manager will create strong passwords and then store them in a cryptographically-sound way.

In addition to using strong passwords, enable Multi-Factor Authentication (MFA) whenever available. This is especially important to protect access to your company's high-consequence systems. MFA allows you to add additional verification — beyond a username and password — to confirm users' identities and protect access to accounts. Registered trusted devices, fingerprint scans and security keys are all examples of MFA.



Enlist an Expert

To bring your cybersecurity to the next level, you may wish to engage the services of a cybersecurity expert. An expert can conduct a vulnerability assessment, educate your staff and clients, evaluate your vendors and advise on encryption tools, cyber insurance, document storage, network monitoring and much more.

Whatever your cybersecurity needs, a Morgan Stanley Advisor can help you evaluate the particular challenges of your situation to best address the vital issues of staying safe in an increasingly complex digital world.

Travel Wisely

Traveling or accessing information from a remote location poses a unique set of cyber risks and challenges. A good "best practice" is to avoid using public Wi-Fi hotspots, which puts you at risk for having your communications and internet traffic intercepted. Instead, create a personal hotspot with your phone and connect through an LTE, end-to-end encrypted channel.

You can and should apply additional protection in the form of a Virtual Private Network (VPN). In general, when traveling, be picky about the devices you bring and never leave them unattended. Refrain from using public computers or publicly available charging cords or USB ports.

About the Author

Rachel Wilson
Managing Director, Technology
Morgan Stanley
Rachel.Wilson@morganstanley.com

A former senior executive at the National Security Agency (NSA), Rachel is now the head of Cybersecurity for Wealth Management at Morgan Stanley.

[1] SOURCE: https://www.businesswire.com/news/home/20181017005273/en/Data-Releases-Cybersecurity-Study-Personally-Identifiable-Information/?feedref=JjAwJuNHiystnCoBq_hl-Q-tiwWZwkcswR1UZtV7eGe24xL9TZOyQUMS3J72mJlQ7fxFuNFTHSunhvli30RlBNXya2izy9YOgHlBiZQk2LOzmn6JePCpHPCiYGaEx4DL1Rq8pNwkf3AarimpDzQGuQ==

[2] SOURCE: https://enterprise.verizon.com/resources/reports/dbir/.

[3] SOURCE: https://www.ibm.com/downloads/cas/861MNWN2.

[4] Securities and Exchange Commission, Division of Enforcement, 2018 Annual Report ("SEC Enforcement Annual Report").

[5] SEC Enforcement Annual Report.

[6] Securities and Exchange Commission, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," Release Nos. 33-10459; 34-82746, February 21, 2018 ("Cybersecurity Release").

[7] Statement on Cybersecurity Interpretive Guidance, by Securities and Exchange Commission Chairman Jay Clayton, February 21, 2018.

[8] National Association of Corporate Directors, "Cyber-Risk Oversight," Directors Handbook Series, page 4.

[9] EY Center for Board Matters, "Cybersecurity Disclosure Benchmarking," September 2018 ("EY Survey").

[10] EY Survey.

[11] Cybersecurity Release, page 21-22.

[12] Cybersecurity Release, page 22.

[13] The Corporate Counsel, Vol. XLIII, No. 5, September-October 2018 (the "Corporate Counsel"), page 2.

[14] The Corporate Counsel, page 2.

[15] SOURCE:https://nacdonlinel.org/insights/publications.cfm?ItemNumber=10687.

[16] Cybersecurity Release, page 18.

[17] Cybersecurity Release, page 20.

[18] The Corporate Counsel, page 2-3.

[19] EY Survey.

[20] EY Survey.