Kroll

Cybersecurity:

The SEC'S Wake-up Call to Corporate Directors

by David R. Fontaine and John Reed Stark

The U.S. Securities and Exchange Commission's ("SEC") **recently issued guidance** for public companies on cybersecurity-related disclosures has garnered a great deal of attention for what it says about the threat and risk that cybersecurity presents for public companies – large and small (the "2018 Guidance"). With cyber-incidents capturing headlines around the world with increasing frequency, businesses and regulators have come to recognize that cyber-incidents are not a passing trend, but rather in our digitally connected economy, an embedded risk that is here to stay. Indeed, these cybersecurity risks represent a mounting threat to businesses — risks that can never be completely eliminated.

This article was originally published in the *Harvard Law School Forum on Corporate Governance and Financial Regulation* on March 31, 2018, and is republished here with the permission of Harvard Law School.

Much of the published commentary concerning the 2018 Guidance has focused on the technical aspects of the SEC's instructions regarding the need for additional disclosure in a company's periodic filings and the SEC's updated views on the timing of cyber-related disclosures and what that means for insider trading windows. Commentators, however, have yet to address squarely the implications of the 2018 Guidance as it relates to the duties and responsibilities of corporate boards. This article analyzes the SEC's expectations regarding, and vision for, corporate board behavior with respect to cybersecurity risks. As we discuss below, the SEC's views on the role of the board have evolved over the past few years, culminating with the release of the 2018 Guidance, which will undoubtedly prompt corporate boards to take tangible steps to translate their general awareness and high-level concerns around cybersecurity risks into specific behaviors and precise actions that are identifiable, capable of being readily implemented and heavily documented.

We believe the comments contained in the 2018 Guidance evidence the SEC's strong views regarding the board's essential role in this emerging area of enterprise risk and remove any doubt that for those who serve as corporate directors, "cybersecurity" can no longer be just a buzz word or a simple talking point. We have heard many board members characterize cybersecurity risks as "an existential threat," but few, if any, have taken the time to go beyond attaining a superficial understanding of what that really means for their companies. Corporate directors now must consider themselves on notice. When it comes to cybersecurity, they are expected to dig in and, therefore, must demand greater visibility into what is oft presented as a murky and highly complex area best left to technologists.

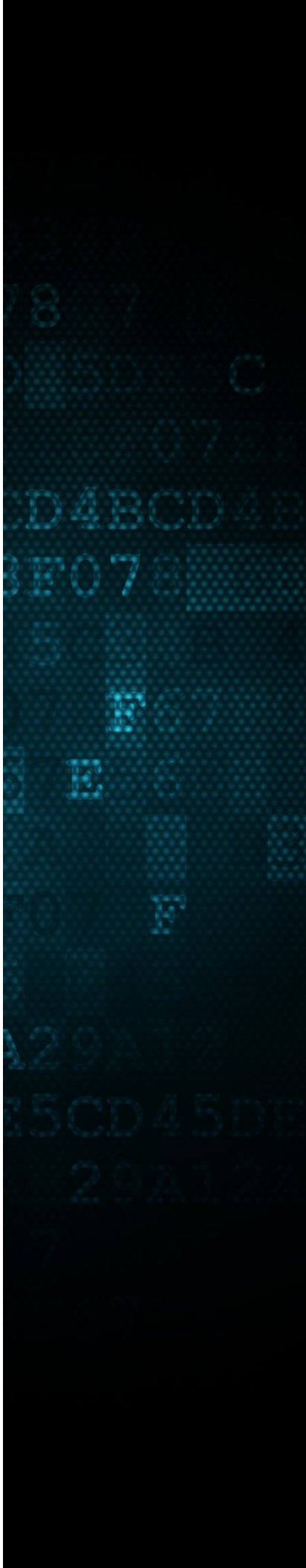
All of this being said, there has yet to emerge an accepted approach corporate directors can embrace, and rely on, in the performance of their governance duties. Moreover, regulatory pronouncements like the 2018 Guidance, presumably by design, fail to address what specific steps boards should undertake to carry out their required duty of care.

Background

Close to two years ago, we co-authored an article that touched on many of these topics and proposed a new framework for tackling the challenges faced by corporate boards working to exercise their cybersecurity oversight responsibility. Back then we phrased it this way:

> **Boards of Directors formulating their cybersecurity oversight should put in place the same governance procedures to oversee a corporation's cybersecurity wellness that has proven effective and sufficiently flexible to assess and validate financial statement accuracy and reliability.**

We went on to note, "most corporate boards fail to allocate to cybersecurity the same level of oversight routinely afforded to the area of financial reporting." We believe the 2018 Guidance further reinforces and underscores the logic and prudence of our suggested approach. Make no mistake, the SEC is now viewing cybersecurity risks as it does all other economic and business risks – particularly as it relates to internal controls, financial reporting and requisite related public disclosures. The SEC certainly is calling for a meaningful change in the approach corporate boards have been taking with respect to cybersecurity oversight and the discharge of their governance responsibility over this core area of enterprise risk. Corporate boards should take heed and adjust their practices.



Recommended Board Actions

1 It Starts with the CEO

2 Reject the "Check the Box" Approach

3 Assign Clear Board-level Oversight Responsibilities

4 Require Periodic External Assessments, Testing & Reporting

5 Do Not Fall Prey to a False Sense of Confidence

6 It Is More than Just Prevention

7 Take the Time to Understand What Has Gone Before

8 Looking Forward

1

It Starts with the CEO

If the CEO does not embrace and understand the importance of cybersecurity, the board has little chance of effectively carrying out its responsibility to ensure proper risk-based measures are in place and functioning. It is the CEO who is charged with day-to-day management responsibility and, as history tells us, those in the organization will, in fact, "follow the leader." This may seem like an obvious point, but its criticality cannot be overstated.

Why would a CEO not take the issue of cybersecurity seriously? CEOs have a lot on their plate. And, like it or not, it is a reality of human behavior that there is a tendency to downplay the potential for certain risks – "this is not going to happen to us" – until those risks manifest themselves and then it is just too late. By then, the damage is already done, and the consequences can be immediate and, at times, catastrophic.

Accordingly, boards must take proactive steps to ensure the CEO, as the linchpin of management, is doing more than just paying "lip service" to the importance of cybersecurity and is truly making cybersecurity readiness an organizational priority. Without the CEO's day-to-day leadership and focus, the board has no place to start and any cybersecurity program will likely fail.

Recognizing this reality, the 2018 Guidance actually offers corporate boards an assist in the effort to focus the attention of the CEO. The SEC explicitly recognizes the importance of "tone at the top," as demonstrated by one of its more specific and impactful directives, requiring that so-called executive certifications regarding the design and effectiveness of disclosure controls now encompass cybersecurity matters (such as certifications made pursuant to the Exchange Act Rules 13a-14 and 15d-14 as well as Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F).

Effective disclosure controls and procedures should ensure that relevant cybersecurity risk and incident information is escalated to senior executives so that they can make the required certifications and related disclosure decisions. The expanded certification rule seeks to drive executive-level ownership and accountability with respect to the reporting of cybersecurity incidents and the broader area of data security. Indeed, the 2018 Guidance states, "These certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact." The SEC certainly understands the centrality of the CEO's role and now the CEO must affirmatively certify to the adequacy of the organization's cybersecurity controls.

Given this unambiguous direction, corporate boards should meet with the CEO and other key senior leaders and dedicate the time necessary to reinforcing the view that cybersecurity can no longer be treated as a problem for the IT department or as a task that can be outsourced and put to the side. The CEO's career is at risk for a misleading — whether by act or omission — certification, which can translate quickly from certification failure into certification fraud. And, if the CEO falls short, the board's actions or lack thereof will also be scrutinized and called into question.

2

Reject the "Check the Box" Approach

Cybersecurity risks represent an evolving threat to businesses across all industries and sectors. No business is immune. These risks, of course, can and do vary by industry and nature of business. But in order to fulfill their proper governance role, board members must demand more than just general management assurances concerning the overall status of a company's cybersecurity program. Generic management responses that might range from "we have it covered" to "we have all the right policies in place" to "we have a CISO who is responsible for that" – just simply are not adequate. Board members have a much higher duty to understand and probe exactly what is behind such general assertions of cybersecurity program sufficiency.

A "check the box" mentality can also contribute to a false sense of confidence. The key questions for boards are: Does the company have in place a cybersecurity program that is tailored to the unique needs of the company? And, if so, is that program effective? In order to gauge the latter, board members must look beyond the surface and seek to understand whether the policies and procedures in place are truly suited to address the unique needs of the organization or are they just words on a page with no real substance behind them. Boards should also be asking and demanding answers to questions such as: "Have we tested how these policies and procedures would operate if we suffered a cyber-attack?" "Where do we store our data?" "What kind of data are we keeping and why?" "What steps have we taken to validate the adequacy and sufficiency of the procedures we do have?" "How can we best gauge program effectiveness?" "Do we have adequate cyber insurance coverage in place?" "Are we investing in a manner that aligns with our true risk?"

When meeting with a CEO and other senior executives, 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 the IT department. While, as we have mentioned, the CEO ultimately must drive home the importance of the program to the company, the CEO cannot carry this burden alone.

Boards also should look to traditional control functions to oversee and guide the company's cybersecurity program formulation as well as its response to any incidents that might arise. For most companies, this will mean placing more authority and resources in the legal department. The general counsel or chief legal officer is typically well suited to understanding, investigating, reporting, and managing risks — and the risks associated with cybersecurity are no exception. For instance, just like any other independent and thorough investigation, the work relating to a cyber-attack will necessarily require the involvement of lawyers with a broad array of skills and expertise (e.g. regulatory; e-discovery; data breach response; privacy; white-collar investigations; and litigation).

The board's task is not to take on the day-to-day implementation of the company's cybersecurity program. But the board must be engaged, utilize available management resources, understand and assess the adequacy of the measures being taken, and demand active and ongoing visibility.

3

Assign Clear Board-level Oversight Responsibilities

It is essential that public companies formalize and document the governance processes over cybersecurity matters. According to the 2018 Guidance, ***"[a] company must include [in its disclosures] a description of how the board administers its risk oversight function."***

As with other audit and risk issues, such oversight could logically be assigned by the board to its existing audit or risk committee. However, for those companies that have the necessary resources and board capacity, we recommend a stronger and more forward-thinking approach — designating a new board committee to deal exclusively with cybersecurity issues, just as an audit committee deals primarily with financial oversight and financial reporting issues. In addition, just as is the case with financial expertise, every board should have at least one member who possesses some level of cybersecurity expertise, and that individual (much like a board's "financial expert") should chair the cybersecurity committee. A board's cybersecurity committee can oversee the broad range of cyber-related issues public companies face, including: cyber insurance; incident response plans; business continuity plans; insider threats and so-called bad leavers (those who leave a company and present a threat, for instance wreaking havoc on technology systems); third-party cybersecurity due diligence; ransomware prevention and response; IT recruitment of personnel; cybersecurity training; data security budgeting; and the list goes on.

If a board does not have a cybersecurity expert, then the board should consider engaging an external expert to serve in this role. Without a qualified and experienced cybersecurity professional on a board (or engaged by the board), a board is leaving a significant enterprise risk unchecked, as well as exposing itself to finger-pointing for the failure to adhere to the 2018 Guidance and the failure to meet its fiduciary obligations.

This notion of requiring boards to have a cybersecurity expert within its ranks has already picked up traction, not just from a regulatory perspective, but also as a matter of federal law. Legislation introduced in the U.S. Senate would require publicly traded companies to disclose to regulators whether any members of their boards of directors have cybersecurity expertise – and actually goes a bit further. Specifically, the proposed Cybersecurity Disclosure Act of 2017 while not mandating companies to have a cybersecurity expert on their boards, instead, requires companies to explain in their SEC filings whether such expertise exists on their boards and, if not, why this expertise is unnecessary because of other steps taken by the company.

The takeaway here is that a successful board traditionally engages all kinds of experts to fill gaps where director expertise may be absent or where external points of view can clearly add significant value, e.g. compensation experts, legal advisors, financial auditors. The same goes for the use of external cybersecurity resources that can bring needed expertise into the boardroom.

4

Require Periodic External Assessments, Testing & Reporting

As with financial controls and audits, a board should put in place quarterly or bi-annual reporting requirements regarding the status and health of the company's cybersecurity program, training, staffing, etc., and hear directly from responsible management team members regarding any incidents that may have been encountered. In addition, it makes sense for the board or its designated committee, working in cooperation with the legal function, to receive and review any third-party assessments, test results, or other feedback on the overall status of the company's cybersecurity posture. Implementing cybersecurity solutions requires a comprehensive risk assessment to determine defense capabilities and weaknesses and ensure the wise application of resources. Even more importantly, cybersecurity readiness is an active and ongoing process. A static or inflexible approach will never prove sufficient, since those intent on hacking are evolving their methods constantly.

Establishing a routine around this type of reporting is fundamental, because it will reinforce and evidence the board's level of engagement and commitment to ensuring that the company's cybersecurity measures are appropriate, ever-evolving, and that the effectiveness is being tested and measured on an ongoing basis. As it relates to the 2018 Guidance, all of these steps will enable the company to address in its disclosures how the "board of directors is discharging its risk oversight responsibility in this increasingly important area."

A complete reliance on management to provide the board with this objective and detached view would be misplaced, for the same reasons that companies engage outside auditors to assess, review, and report on the company's financial controls, its accounting practices, and the accuracy of its financial results. As we observed in our **earlier article on this topic**, "Historically, when it comes to their CFOs and the financial reporting function, the successful board paradigm has been one of vigorous and independent supervision, requiring the participation of independent third parties. The same should hold true for CTOs, CIOs, and CISOs, and the maxim of trust but verify should be equally operative…"

And, to ensure the unfiltered and independent flow of information, this same external resource should periodically meet with the board or appropriate committee thereof in executive session, just like a board's audit committee routinely confers with independent auditors outside of the presence of management. It is a time-tested process that enables unchilled and candid dialogue on what are critical risk management topics. Its utility is certainly operative in the cybersecurity context.

Board oversight regarding cybersecurity audits should not only include a thorough review of risk and security assessments, penetration testing reports and other similar cyber-related auditing, but also any resultant remedial efforts or corrective measures implemented afterward. Boards should also explore whether a company's outside cybersecurity firm is the trusted advisor 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 cybersecurity firm 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.

Along these same lines, boards should also mandate that executives engage in table-top exercises, which 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. 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.

The need for an independent third-party perspective strikes us as indisputable and consistent with general principles of sound governance. We would never expect CFOs to audit the very books and records that they are responsible for producing. Logic and experience dictates that the same reasoning should apply to the area of cybersecurity.

5

Do Not Fall Prey to a False Sense of Confidence

Many companies now have in place technology designed to identify anomalies and threats. They also likely have written policies and procedures intended to provide a roadmap in the event that a cybersecurity incident occurs. All these tools and written procedures may well be “state of the art” in that they may reflect and embody what is understood to be general best practices. But as with any system or written policies, they alone may be insufficient to address the risks. Policies without oversight, testing, and ongoing modifications can either be ill-suited to reality or rapidly become stale and, therefore, not fit for purpose.

Technology may be leading-edge, but if no one is making sure its outputs are being reviewed, understood, and remediated in a timely manner, it is not advancing the goals of an effective cybersecurity program. For example, we have encountered situations where companies have invested heavily in the "best" new technologies, but those technologies either were incorrectly deployed (e.g. improper settings) or the company was never adequately reviewing the alerts/reports generated by these technologies due to lack of staffing or just simple oversight. Only when trouble hits, do these weaknesses come to light. But that is too late. Boards need to press for the details and require more than broad assurances that amount to "don't worry, we just bought the latest and the greatest solutions."

Further, keep in mind the human element is always operative, and what can go wrong, will go wrong. Employees make mistakes and can be tricked into handing over extremely sensitive data and, in the extreme, the insider threat of intentional misconduct looms heavily at every company. For these reasons, the board has to demand that cybersecurity is a companywide imperative. And, a program that incorporates employee awareness and education must be incorporated into the mix. All employees must be vigilant and encouraged to escalate perceived issues as they are encountered. Keeping in mind, speed to response is essential and the key to recovery.

Consider, for example, corporate training programs for cybersecurity. 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.

Boards should query corporate executives regarding: a) the frequency and efficacy of the firm's cyber-safety training programs; and b) 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). It goes without saying, board members should themselves participate in these training exercises not only to educate themselves, but to demonstrate the overall importance of cybersecurity readiness to the organization.

6

It Is More than Just Prevention

No matter how "good" a cybersecurity program is or may appear to be, boards must recognize that no program is perfect or fool-proof. The miscreants who attack public companies evolve their methods every day and it is virtually impossible to create an environment that is impervious to attack. In addition to having an understanding of the steps taken to reduce the risk of a cybersecurity incident, it is equally critical, perhaps more so given the assumed inevitability of such an incident, to consider and understand how the company would respond if faced with such an event. As recent large-scale breaches have demonstrated, the ability to detect and respond to a cyber-incident is essential and can be outcome determinative. An effective program can position the company for rapid recovery and insulate it from reputational harm. In contrast, a program that fails can further exacerbate the underlying incident, exposing the company to great legal risk as well as reputational damage.

Here is where the board's role can and should be most pronounced. Boards should be informed immediately by the company's leadership when a cyber-incident of a serious magnitude has been identified. This is not a call for daily updates, but if there is a true concern about a cyber-incident, the board should demand that it be placed on notice. This will not only enable effective oversight and management of the incident at hand but will also demonstrate to all external constituencies that the board is fully engaged and takes its governance responsibility for such issues seriously. Yes, there may be some false alarms along the way, but that is a minimal cost for avoiding the real fires that might otherwise emerge. The ability to snuff out the fire early is invaluable, reducing the chance of the fire taking hold and raging uncontained. It also will force issues to the surface early and provide opportunities for a true lessons-learned risk culture to take hold.

It is not surprising that the 2018 Guidance reinforces this notion of board notice. The importance of notice being given "up the chain" hits close to home for SEC Chairman Jay Clayton, who when testifying before Congress about the data breach suffered at the SEC, was clearly miffed that the SEC staff had not shared certain critical data breach information with the various SEC Commissioners, including the Chairman.

At that time, then-SEC Commissioner Michael S. Piwowar even went so far as to issue a formal statement about the lack of communication to him about the SEC data breach, stating:

> ***I commend Chairman Clayton for initiating an assessment of the SEC's internal cybersecurity risk profile and approach to cybersecurity from a regulatory perspective. In connection with that review, I was recently informed for the first time that an intrusion occurred in 2016 in the SEC's Electronic Data Gathering, Analysis, and Retrieval ("EDGAR") system. I fully support Chairman Clayton and Commission staff in their efforts to conduct a comprehensive investigation to understand the full scope of the intrusion and how to better manage cybersecurity risks related to the SEC's operations. (Emphasis added).***

This approach also dovetails nicely with the 2018 Guidance's regarding insider trading policy in the event of a cyber-incident. If everyone in leadership and the board is on notice, the trading policy can more readily be administered in a consistent and clear manner.

The 2018 Guidance should also prompt boards to evaluate their insider trading policies and procedures overall. Board's should review, with data security incidents in mind, their trade restriction policies, permissible trading windows, insider trading training curricula, codes of ethics, trade authorization procedures, trading training manuals and the like.

The SEC plainly is expecting thoughtful and well-documented consideration of data security incidents in the context of possible trading on material, nonpublic information – and carefully drafted, robust and precise policies, practices and procedures evidence a rigorous culture of compliance.

7

Take the Time to Understand What Has Gone Before

As the writer James Baldwin expressed, *"Know from whence you came. If you know whence you came, there are absolutely no limitations to where you can go."* There certainly are lessons in history and the board should understand any historical cybersecurity events that may have impacted the company, its competitors or other relevant parties, perhaps events that the board may not have even known about at the time they occurred. This effort to understand history is purposeful and necessary for the board to gain an appreciation both for the potential for a cyber-incident as well as for providing a baseline against which future progress can be measured. And, as we noted earlier, it is also the reason for the board requiring some type of independent third-party assessment that can help to establish a baseline against which progress can be measured.

The 2018 Guidance touches on the critical need for cybersecurity risks to be understood and presented in context. It provides:

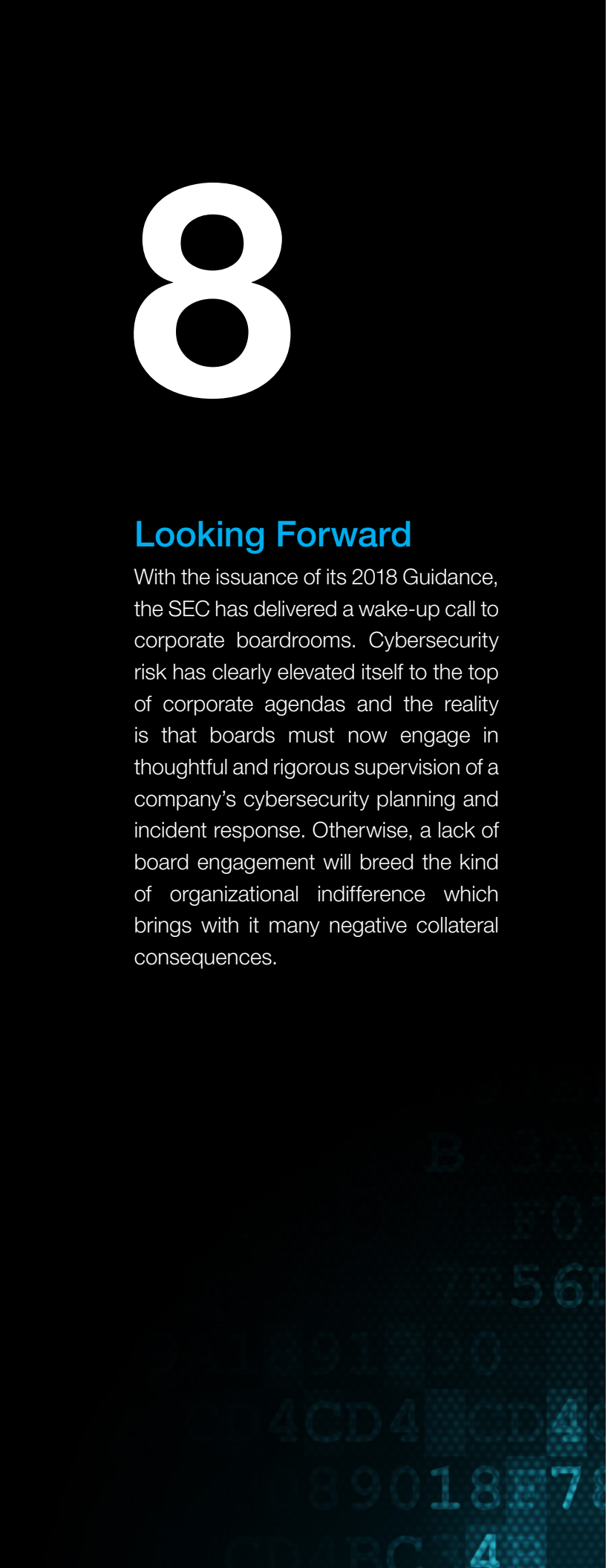
> ***In meeting their disclosure obligations, companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context. … Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure.***

If this type of context should be taken into account when crafting investor disclosures, it seems unquestionably true that the company's board should have this same context so that it can draw on history to anticipate and frame its future approach to governance of the issues. Without a lessons-learned culture, it is hard to avoid repeating the errors of the past.

8

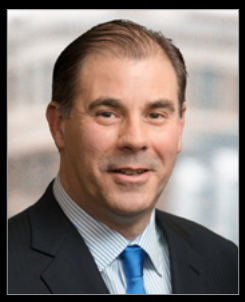
Looking Forward

With the issuance of its 2018 Guidance, the SEC has delivered a wake-up call to corporate boardrooms. Cybersecurity risk has clearly elevated itself to the top of corporate agendas and the reality is that boards must now engage in thoughtful and rigorous supervision of a company's cybersecurity planning and incident response. Otherwise, a lack of board engagement will breed the kind of organizational indifference which brings with it many negative collateral consequences.



Though the steps we recommend may seem daunting, keep in mind nothing proposed deviates from widely accepted practice with respect to financial reporting requirements and oversight. Moreover, boards soon will have little choice but to implement some type of clear and articulable program, not merely to protect their companies but also to protect themselves. Given the current class action litigation landscape relating to cybersecurity issues, data security incidents not only create regulatory and other legal liability for corporations, but they can also create potential personal liability for board members. Whether a board makes an affirmative decision regarding cybersecurity measures that permitted a breach (such as overseeing the implementation of a woefully inadequate security program) or just fails to take action with respect to cybersecurity risks, boards face a heap of potential liability.

For board members worried about taking on the technical challenges of data security, there is no need to panic. Cybersecurity engagement for boards does not mean that they must obtain computer science degrees or personally supervise firewall implementation and intrusion detection system rollouts. By approaching cyber in much the same way they approach other areas of risk under their purview – with vigorous, skeptical, intelligent, independent and methodical administration and inquiry – boards will not just execute on their newfound cyber-jurisdiction, they might actually grow to embrace it (just like they do with financial audit).



David R. Fontaine is Chief Executive Officer of Kroll and its parent company, Corporate Risk Holdings, LLC. Previously, Mr. Fontaine held senior leadership roles and served as the Chief Legal Officer, Chief Risk Officer, General Counsel, Chief Administrative Officer and Corporate Secretary for several public and private companies, including Travelex Global Business Payments, Inc., American Management Systems, Inc., and Proxicom, Inc. Before moving into a corporate executive role, Mr. Fontaine was a partner at the highly respected Washington, D.C. litigation firm of Miller, Cassidy, Larroca & Lewin, LLP, practicing primarily in the areas of white-collar defense and commercial litigation. Immediately after graduating from Yale Law School, he served as a law clerk to the Honorable Stanley Sporkin, U.S. District Court for the District of Columbia, and later as a law clerk to the Honorable Thomas J. Meskill, U.S. Court of Appeals for the Second Circuit.

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 has taught most recently as Senior Lecturing Fellow at Duke University Law School Winter Sessions and will be teaching a cyber-law course at Duke Law in the Spring of 2019. Mr. Stark 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 global data breach response firm, Stroz Friedberg, including three years heading its Washington, D.C. office. Mr. Stark is the author of, "The Cybersecurity Due Diligence Handbook."

kroll.com

Kroll