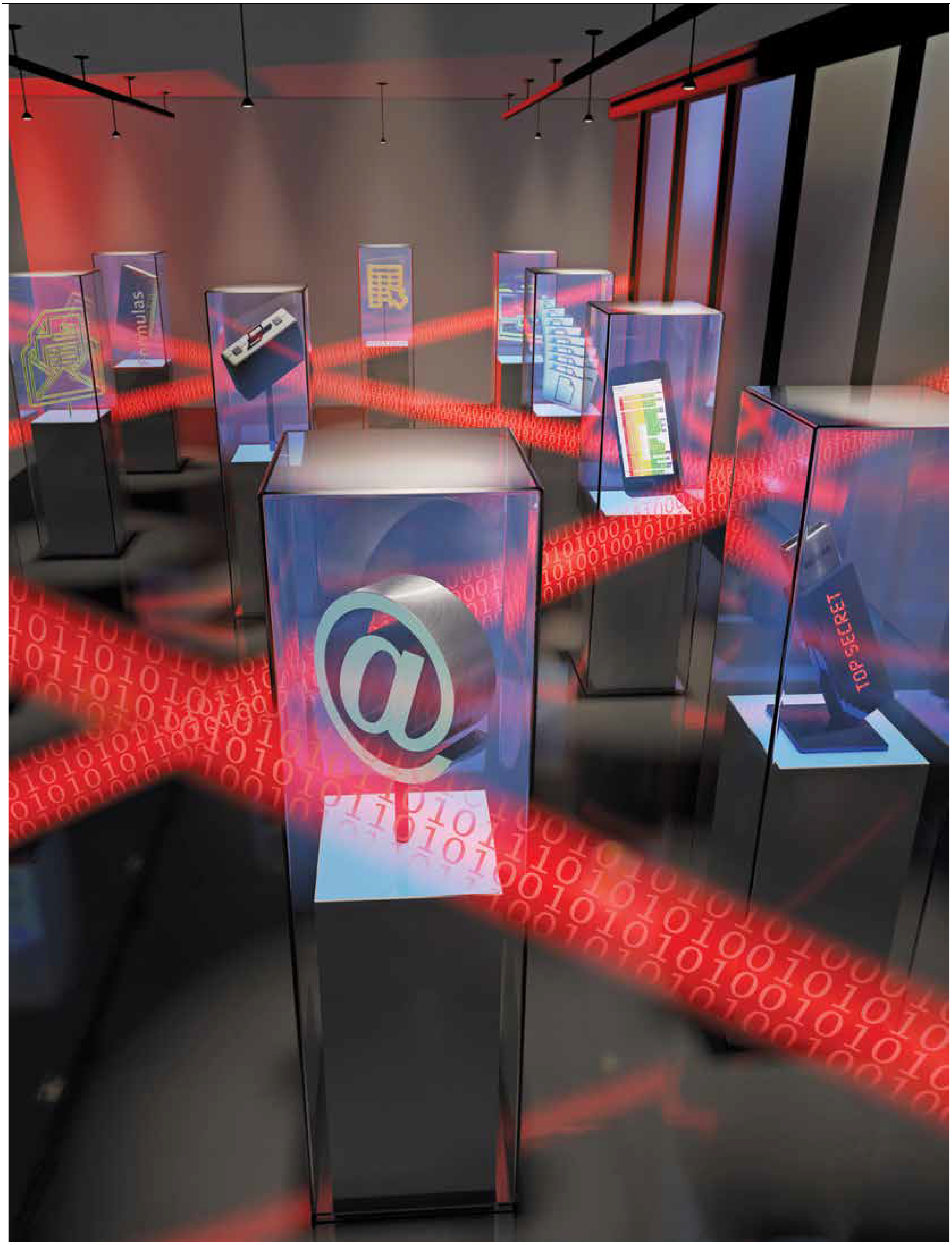
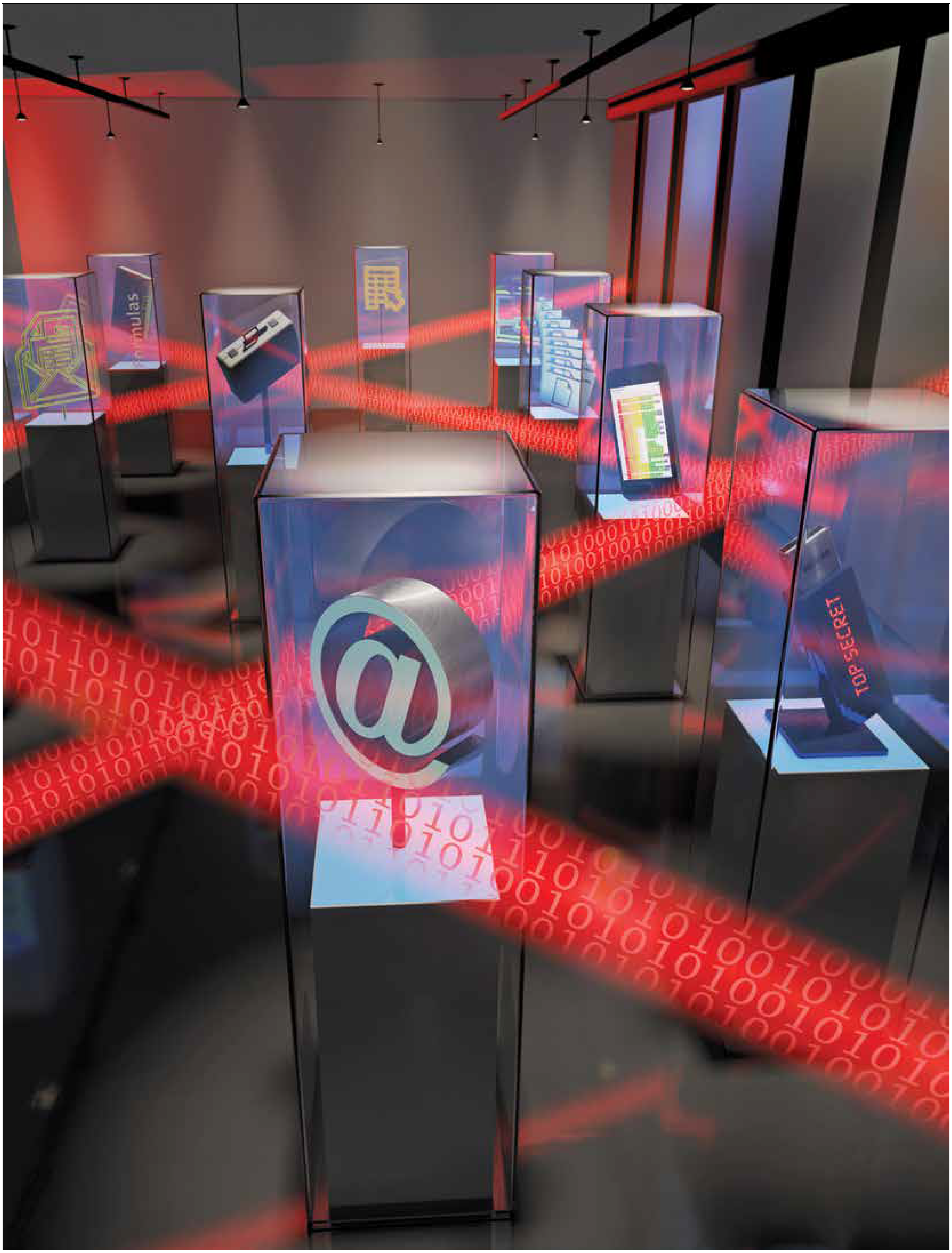
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

# Cybersecurity: Emerging Trends and Regulatory Guidance

## Technology, Privacy, and eCommerce


formulas
TOP SECRET


Formulas
TOP SECRET

## CHEAT SHEET

- ***Step one.*** Assess your company's exposure to a cybersecurity threat by figuring out what your company needs to protect.
- ***Step two.*** Identify where the vulnerabilities exist. This is a complex and multilayered issue.
- ***Step three.*** Prepare and coordinate among the key stakeholders in your company. The legal department should be able to identify legal requirements and ways to limit liability.
- ***Step four.*** Develop a plan. Your plan should include - among many other things - guidance on a potential media response by your company.

Cyberthreats are ever-present. The US Office of the Director of National Intelligence identified cyberthreats as the top threat in 2014, surpassing terrorism. There has been a 10,000-fold increase in the number of new digital threats over the past 12 years. Hacking attacks increased 62 percent in 2014 alone. As the assistant director of the FBI's Cyber Division stated in April 2011, Cyberthreats have "reached the point that given enough time, motivation and funding, a determined adversary will likely be able to penetrate any system that is accessible directly from the Internet." But if you think data security is only an issue for Fortune 500 companies, you are wrong. Any company that has confidential information or employee, customer or client data needs to think about cybersecurity.

A company cannot eradicate cyberthreats. But it can manage the threats and develop a plan to respond to an incident. This process requires cooperation and teamwork across company departments, including the active participation of in-house counsel, who play a critical role in this process. Recent guidance from industry groups and regulators provides a framework for in-house counsel to answer two key questions: What should my company do to prepare for a data breach, and how can I help?

## The challenges: an ever-present threat and the absence of national regulation

There is no simple fix and no single solution to cyberthreats. Each company must examine its own structure, its own systems and its own data to determine what needs to be protected and how best to protect it. Data security threats exist not just at the enterprise level but at other points of entry as well, such as point-of-sale (POS) registers, employee smartphones, social media, personal email accounts, Wi-Fi printers and the “Internet of Things.” In addition, a company cannot focus only on its own information systems to identify vulnerabilities but must consider the systems of critical third parties, including vendors. Threats exist not only from hackers but employees, independent contractors and third-party vendors.

The Internet of things is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure that could be clearer. The Internet of things refers to everyday devices like refrigerators, chips in pets, thermostats and gas meters that can now connect to the Internet, and these devices are also susceptible to cyberhacks.

Managing these risks involves multiple levels of a company. It requires knowledge at the board level of what the issues are and what your company is doing to address them. Some public companies have cyber-risk committees. On a daily operation level, managing the risk requires the input of multiple management groups in a company, including, for example, legal, IT, human resources, accounting, payroll and sales. It also requires a culture where every employee understands the importance of what is at stake and her role in maintaining security.

To add to this internal complexity, a patchwork of local, state and federal regulations governs data security issues. For example, 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands require that companies notify individuals of security breaches of information involving personal information. Moreover, a number of states impose obligations on companies to safeguard personal information relating to consumers. In many instances, these obligations may be high level (i.e., maintain reasonable security procedures to protect data), but some states impose detailed security standards, including, for example, the Massachusetts data security regulations.

For a discussion of relevant state laws as well as key court cases, see the Morrison & Foerster Privacy Library.

In addition, depending on your company's industry, the company may also be subject to federal regulation, such as the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, Sarbanes-Oxley, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act, the Privacy Act, the Electronic Signatures in Global and National Commerce Act, the Federal Information Security Management Act or the Homeland Security Act of 2002. Along with these acts, various federal agencies may also have oversight or input regarding how a company handles data, such as the Federal Trade Commission, the Department of Health and Human Services and the Office of the Comptroller of the Currency.

Trying to comply with all the applicable laws can be confusing and daunting. But ignoring data security can have far-reaching ramifications beyond the loss of critical data, including federal and state penalties, civil suits and reputational harm. A company's legal group plays a critical role in the company's security preparedness. For example, your legal department distills the regulatory framework to which your company is subject. And if your company does not have a separate risk or compliance department, then the legal department likely is responsible for assessing your company's preparedness.

## A framework for thinking about company information and cybersecurity threats

The first step in assessing your company's exposure to a cybersecurity threat is to figure out what your company needs to protect. It is not possible to protect all data or every access point on your network. Prioritization is key. What data and systems are critical? What servers or other critical network systems does your company use? How are your systems segmented? How is access to your systems from the Internet controlled? What data are your company legally required to protect? What data are your company contractually or legally required to protect? What other data do your company want to protect? Does your company have personal information relating to employees or customers? What health information does your company possess? Does it have strategic or competitive information? Does it have market-sensitive information? What proprietary or trade-secret information does your company possess?

What client information does it have? Making this assessment requires input from all the stakeholders who have data or systems at issue. Who these actors are depends on what your company does. In fact, every business line or department may have meaningful input. At a minimum, it will likely involve your IT, facilities, audit, human resources and accounting departments. It could also involve your sales department or other client or customer-facing groups within your company.

Then your company needs to identify where vulnerabilities exist. This is a complex and multilayered issue. Examples of questions to ask: Who handles or has access to the data or systems that need to be protected? How do the data enter your company? Where are the data stored? How are the data handled within your company? Where are the critical systems kept? What security is already being deployed to protect those systems? Related questions include thinking about how your company handles access to these data and these systems, including not only internal access but external access by third parties such as vendors. Another way to approach this facet of the issue is to consider what threats exist regarding these data or these systems. Potential threats include access to your systems by hackers, destruction or loss of the data by internal or external parties, external disruptions such as a denial of service or distributed denial-of-service attack or intentional or unintentional disclosure of the data by internal or external parties.

Your company also needs to consider who will watch the watchers. What systems, controls and processes are in place to make sure that the parties who have day-to-day oversight of these issues are doing what they are supposed to be doing? Technology and company processes play a vital role here. Another aspect of this issue is the board’s knowledge of and input into these systems, controls and processes. As cyberthreat issues become more prominent, it becomes increasingly important for a board to, at a minimum, have knowledge of who has responsibility for cyberissues, what the issues are and what your company is doing to address them. Beyond this, the specific role the board plays in cybersecurity depends on the size of your company and its needs. Some public companies have cybersecurity committees. In other companies, this function may reside with the audit committee. In smaller companies, the entire board may be involved. At the Cyber Risks and the Boardroom Conference held on June 10, 2014, Commissioner Luis Aguilar of the US Securities and Exchange Commission touched on potential measures for boards of directors to consider taking, which is useful guidance for private and public companies. Those measures include reviewing annual IT budgets relating to cyber-risks and cyber-risk education for directors.

As you can see, none of this can be just one person’s job. Evaluating and managing these issues requires preparation and coordination among the key stakeholders in your company. The legal department plays a critical role in this process, between bridging the legal requirements and limiting the liability and identifying the measures that are needed to address these issues.

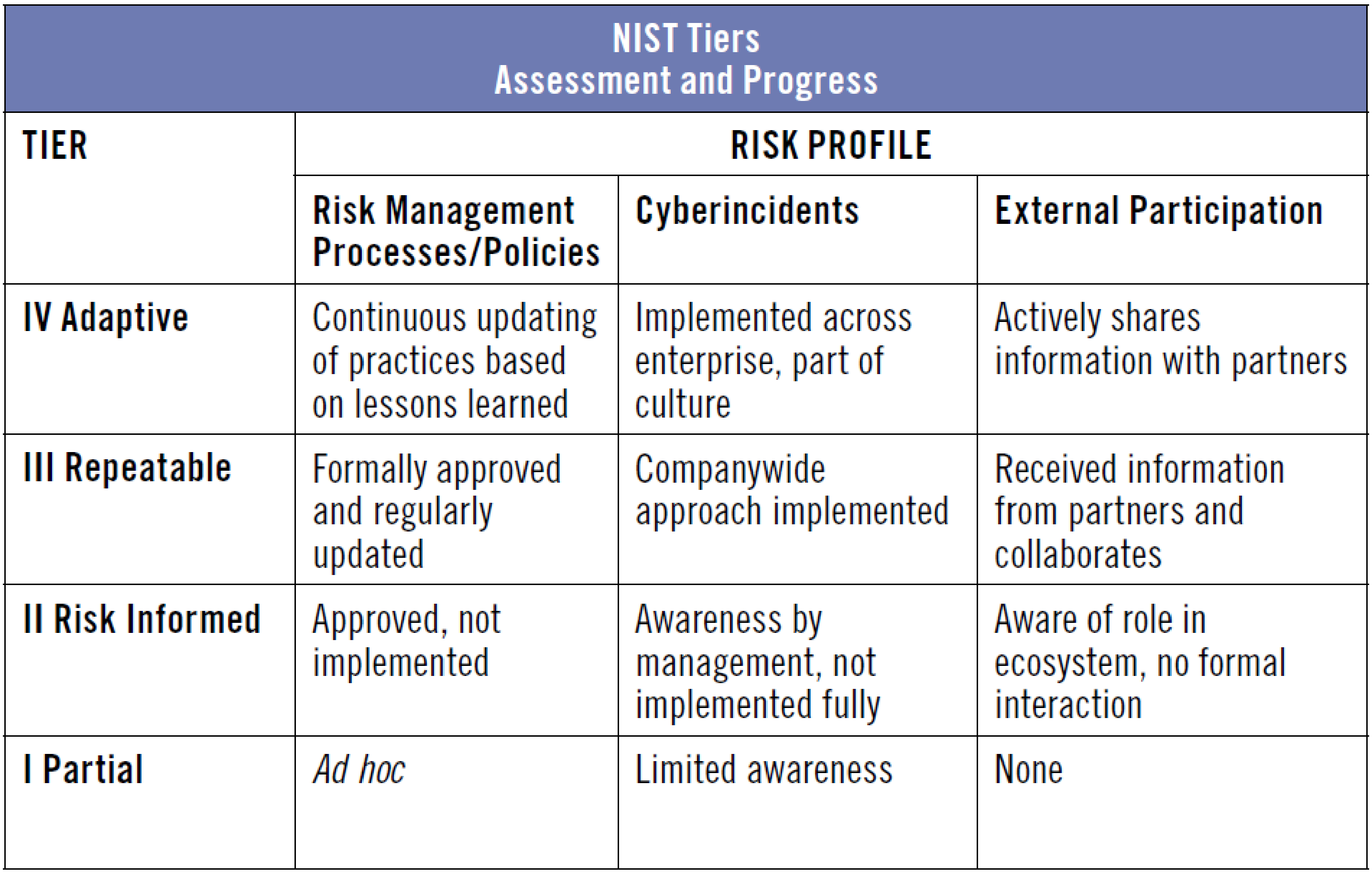
## The NIST framework: one alternative to a national approach

In the dynamic environment where cyberthreats are becoming more frequent, sophisticated and severe, having effective cyber-risk management policies and programs in place has become increasingly important. Like other risk-management policies and programs, those that address cybersecurity risk must be specifically tailored to the company’s business, risk tolerance and resources. But companies should assess their cyber-risk management policies and programs against conceptual frameworks, industry standards and best practices that have been developed to manage cybersecurity risk.

One conceptual framework, developed by the National Institute of Standards and Technology (NIST framework) in early 2014 in response to an executive order issued by President Barack Obama has garnered much attention as a standard of care for company readiness against cyberattacks. The

NIST framework consists of three interrelated parts that can be used to identify, assess and manage risk: the framework core, the framework implementation tiers and the framework profile.

President Obama issued an executive order in February 2013 that directed NIST to develop a voluntary framework for reducing cybersecurity risks to critical infrastructure. NIST released the first version of its framework, “Framework for Improving Critical Infrastructure Cybersecurity,” on February 12, 2014. NIST also issued a companion roadmap that discusses next steps with the NIST framework and key areas of cybersecurity development, alignment and collaboration.



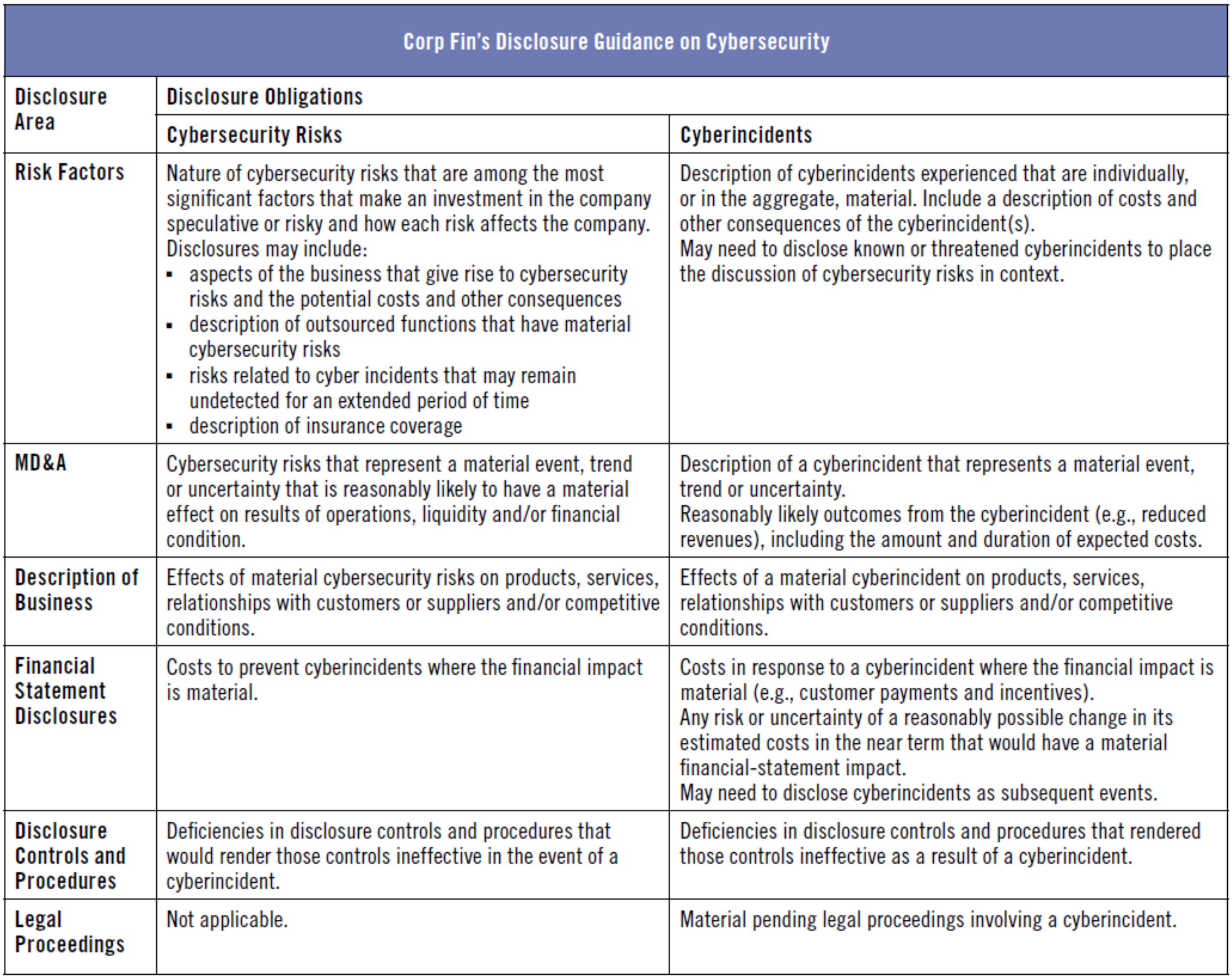
NIST Tiers
Assessment and Progress

| TIER | RISK PROFILE | | |
|---|---|---|---|
| | Risk Management Processes/Policies | Cyberincidents | External Participation |
| IV Adaptive | Continuous updating of practices based on lessons learned | Implemented across enterprise, part of culture | Actively shares information with partners |
| III Repeatable | Formally approved and regularly updated | Companywide approach implemented | Received information from partners and collaborates |
| II Risk Informed | Approved, not implemented | Awareness by management, not implemented fully | Aware of role in ecosystem, no formal interaction |
| I Partial | *Ad hoc* | Limited awareness | None |

The framework core includes five functions that are performed concurrently and continually to create a culture that addresses the dynamic nature of cybersecurity risks:

- **Identify**– understand the business context, resources that support critical functions and the related cybersecurity risks to focus and prioritize efforts.
- **Protect**– develop and implement safeguards to limit or contain the impact of a potential cyberincident.
- **Detect**- develop and implement activities to detect a cyberincident in a timely manner.
- **Respond**– develop and implement activities to contain the impact of a potential cyberincident.
- **Recover**– develop and implement activities that support timely recovery to normal operations to reduce the impact of the cyberincident.

The framework-implementation tiers represent a lens through which the company can view the characteristics of its risk management approach. Implementation tiers range from partial (tier 1) to adaptive (tier 4), with increasing levels of rigor and sophistication of cybersecurity risk management at successive tiers. Companies select a tier based on current cybersecurity risk management practices; however, those companies in the partial implementation tier (tier 1) are encouraged to move toward risk informed (tier 2) or higher tiers. Figure X below summarizes the risk management processes, programs and external participation at each tier.



Corp Fin's Disclosure Guidance on Cybersecurity

| Disclosure Area | Disclosure Obligations | |
|---|---|---|
| | Cybersecurity Risks | Cyberincidents |
| Risk Factors | Nature of cybersecurity risks that are among the most significant factors that make an investment in the company speculative or risky and how each risk affects the company.<br>Disclosures may include:<br>▪ aspects of the business that give rise to cybersecurity risks and the potential costs and other consequences<br>▪ description of outsourced functions that have material cybersecurity risks<br>▪ risks related to cyber incidents that may remain undetected for an extended period of time<br>▪ description of insurance coverage | Description of cyberincidents experienced that are individually, or in the aggregate, material. Include a description of costs and other consequences of the cyberincident(s).<br>May need to disclose known or threatened cyberincidents to place the discussion of cybersecurity risks in context. |
| MD&A | Cybersecurity risks that represent a material event, trend or uncertainty that is reasonably likely to have a material effect on results of operations, liquidity and/or financial condition. | Description of a cyberincident that represents a material event, trend or uncertainty.<br>Reasonably likely outcomes from the cyberincident (e.g., reduced revenues), including the amount and duration of expected costs. |
| Description of Business | Effects of material cybersecurity risks on products, services, relationships with customers or suppliers and/or competitive conditions. | Effects of a material cyberincident on products, services, relationships with customers or suppliers and/or competitive conditions. |
| Financial Statement Disclosures | Costs to prevent cyberincidents where the financial impact is material. | Costs in response to a cyberincident where the financial impact is material (e.g., customer payments and incentives).<br>Any risk or uncertainty of a reasonably possible change in its estimated costs in the near term that would have a material financial-statement impact.<br>May need to disclose cyberincidents as subsequent events. |
| Disclosure Controls and Procedures | Deficiencies in disclosure controls and procedures that would render those controls ineffective in the event of a cyberincident. | Deficiencies in disclosure controls and procedures that rendered those controls ineffective as a result of a cyberincident. |
| Legal Proceedings | Not applicable. | Material pending legal proceedings involving a cyberincident. |

The final part of the NIST framework is the framework profile (profile). The profile is designed to meet the company's unique needs. It should be aligned with the company's goals, reflect risk-management priorities and should be developed in consideration of legal and/or regulatory requirements and industry best practices. A current profile identifies the outcomes that the company is achieving in the five core functions (identify, protect, detect, respond and recover). A target profile can also be developed to identify the outcomes needed to achieve the company's goals. Gaps between the current and target profile can be used to create a prioritized action plan for continuous improvement of cyber-risk management policies and programs.

Recognizing the need for flexibility in establishing a profile as a roadmap for reducing a company's specific cybersecurity risk, the NIST framework does not prescribe a template for the profile.

Companies should take seriously the self-assessment and continuous improvement concepts included in the NIST framework. Companies should also consider the importance of maintaining attorney-client privilege in conducting assessment and making recommendations for improvement.

## SEC guidance regarding cybersecurity risk disclosures for public

## companies

Determining the information to disclose to investors about cybersecurity risks and incidents is complex and challenging for public companies. Of critical importance is balancing the need to provide timely, comprehensive and accurate information to investors while not disclosing information that could serve as a roadmap to those who seek to exploit a company's vulnerabilities. Adding to the complexity is the potential for litigation, regulatory action or both. There may be a disincentive to disclose cyberincidents that may not otherwise become public because the disclosure may trigger litigation and/or regulatory action (e.g., consumer class actions). At the same time, companies have an incentive to disclose cybersecurity-related information to help avoid attention from the SEC's Division of Corporation Finance (Corp Fin), Division of Enforcement, and/or a shareholder derivative action.

Over the past few years, the SEC has focused increasingly on a company's obligation to disclose material cybersecurity-related information to investors. The disclosure obligation arises from SEC requirements and accounting standards that, although not specifically tailored to cybersecurity-related issues, set forth requirements for disclosures of business risks and the consequences of those risks. Corp Fin provided its views regarding disclosure obligations in its "CF Disclosure Guidance: Topic No. 2 Cybersecurity" (disclosure guidance) that was issued on October 13, 2011. Corp Fin's disclosure guidance addresses two important issues: when a cybersecurity risk or cyberincident rises to the level of a disclosure obligation, and what cybersecurity-related information needs to be disclosed.

Corp Fin's disclosure guidance provided specific requirements regarding when and what cybersecurity risks and cyberincidents require disclosure in six specific areas: risk factors, management discussion and analysis, description of business, financial statement disclosures, disclosure controls and procedures and legal proceedings (see sidebar below). While recognizing that disclosures that could increase cybersecurity risk are not required under federal securities laws, Corp Fin indicates that a company should provide information tailored to its specific circumstances rather than describe generic risks that apply to all companies or provide boilerplate disclosures. Companies should also review the adequacy of cybersecurity-related disclosures on an ongoing basis.

### Cybersecurity around the world

With the growing number of data security breaches around the world, security remains a great concern. Seventeen countries have enacted mandatory breach-notification laws that require organizations to notify individuals and/or government regulators in the event of a data breach. Ten other countries have issued voluntary data-breach notification guidelines. With respect to data safeguards, there is a broad range of data security obligations. Some countries, such as those in the United Kingdom, simply require that companies use reasonable organization and technical measures to protect personal information. Other countries have detailed security obligations such as South Korea (which requires encryption of certain types of data at rest) and Argentina (which requires encryption of sensitive data over the Internet).

With respect to privacy, more than 90 countries now have comprehensive privacy statutes. Most privacy laws outside the United States are broader than US law, covering any personally identifiable information, not only customer or consumer information. Generally, these laws require that the existence of databases be publicly disclosed and that the databases be registered with the government or with an independent data protection authority. They also require that individuals whose personal information is maintained in these databases be given notice of, and in certain circumstances consent to, the collection, use and transfer of their personal information as well as the right to access and correct the information held about them.

## The importance of timeliness and an on-the-shelf response plan

“[T]he primary distinction between a cyberattack and other crises that a company may face is the speed with which the company must respond to contain the rapid spread of damage. Companies need to be prepared to respond within hours, if not minutes, of a cyberevent to detect the cyberevent, analyze the event, prevent further damage from being done and prepare a response to the event.” Whether to disclose the event, what and how your company discloses of the breach and what it does to address it depends in part on your industry, how the cyberincident occurred and what data were compromised. Depending on the nature of the cyberattack, a timely response and the time available to respond can be dictated by regulations or even contractual obligations. Failure to disclose a loss of data can expose your company to a regulatory investigation by state and even federal authorities.

There are many publications that discuss what steps to take in the event of a breach, including what steps are mandated by the various laws that regulate the differing types of information that may be compromised, and so this topic will not be addressed in-depth in this article.

The key to being able to respond in a timely manner is having an incident response, crisis management, disaster recovery or business continuity plan that addresses these issues. At a minimum, the plan should include identifying and grading risks. What internal response and escalation is required for which sort of incident? A company may experience many different types of incidents, many of which do not require action beyond the company’s IT response. Some incidents will require internal escalation within the IT department and beyond, including to the legal department and senior management. A good plan sets out when this needs to occur and what type of incident necessitates this type of escalation. Your plan should also include guidance on a potential media response by your company. For example, when a media response is required, who should be involved in drafting the response, and who should give the response? Finally, you should also consider including in your plan key internal contact information as well as external contact information such as who your company needs to call to conduct a forensic analysis, who your cyberinsurance carrier is, who your outside counsel is for these incidents, and who your public relations firm is. In a time of crisis, you do not want to be researching these issues.

What each of these plans should include and what type of each of these plans is right for a company are subjects in their own right. Again, there are many publications regarding this topic and consultants who specialize in providing this guidance.

## Further Reading

National Intelligence Strategy of the United States of America, 2014 (NIS Publication) available at [www.dni.gov/files/documents/2014_NIS_Publication.pdf](www.dni.gov/files/documents/2014_NIS_Publication.pdf).

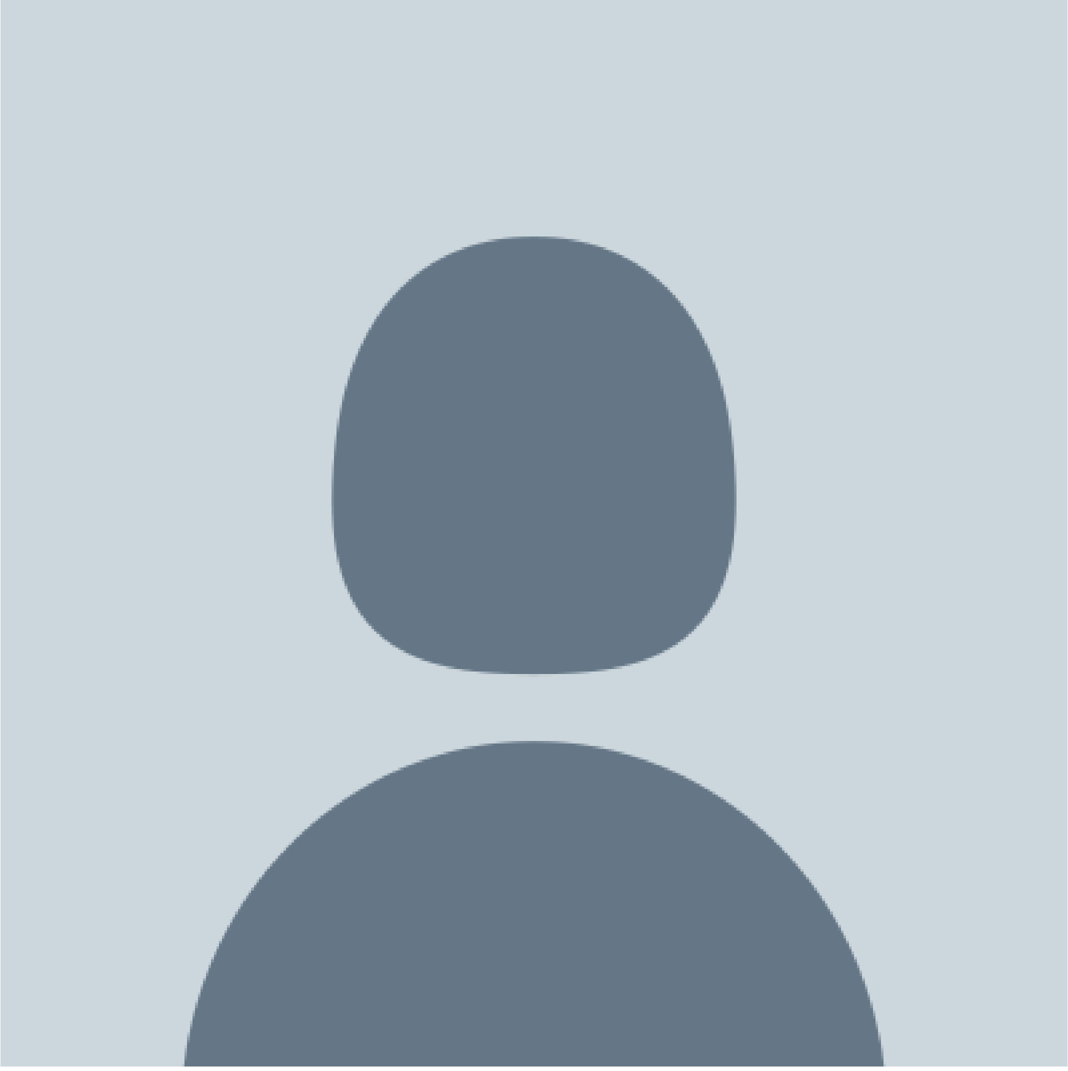
Statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, April 12, 2011, Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation, available at www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism.

In a June 2014 speech at the New York Stock Exchange, SEC Commissioner Luis Aguilar stated: “While the [NIST] framework is voluntary guidance for any company, some commentators have already suggested that it will likely become a baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes.… At a minimum, boards should work with management to assess their corporate policies to ensure how they match up to the framework’s guidelines-and whether more may be needed.” (“Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus,” Commissioner Luis A. Aguilar, June 10, 2014, emphasis added.

For additional discussion of potential shareholder derivative actions, see “SEC Continues to Target Cybersecurity Disclosures” Law360, November 1, 2013.

CF Disclosure Guidance: Topic No. 2 Cybersecurity. Commissioner Aguilar, in his March 26, 2014, public statement at the SEC’s Cybersecurity Roundtable, noted that “Some have suggested that such disclosures fail to fully inform investors about the true costs and benefits of companies’ cybersecurity practices and argue that the commission (and not the staff) should issue further guidance regarding issuers’ disclosure obligations.” See letter from U.S. Senator John D. Rockefeller IV to chair White (Apr. 9, 2013).

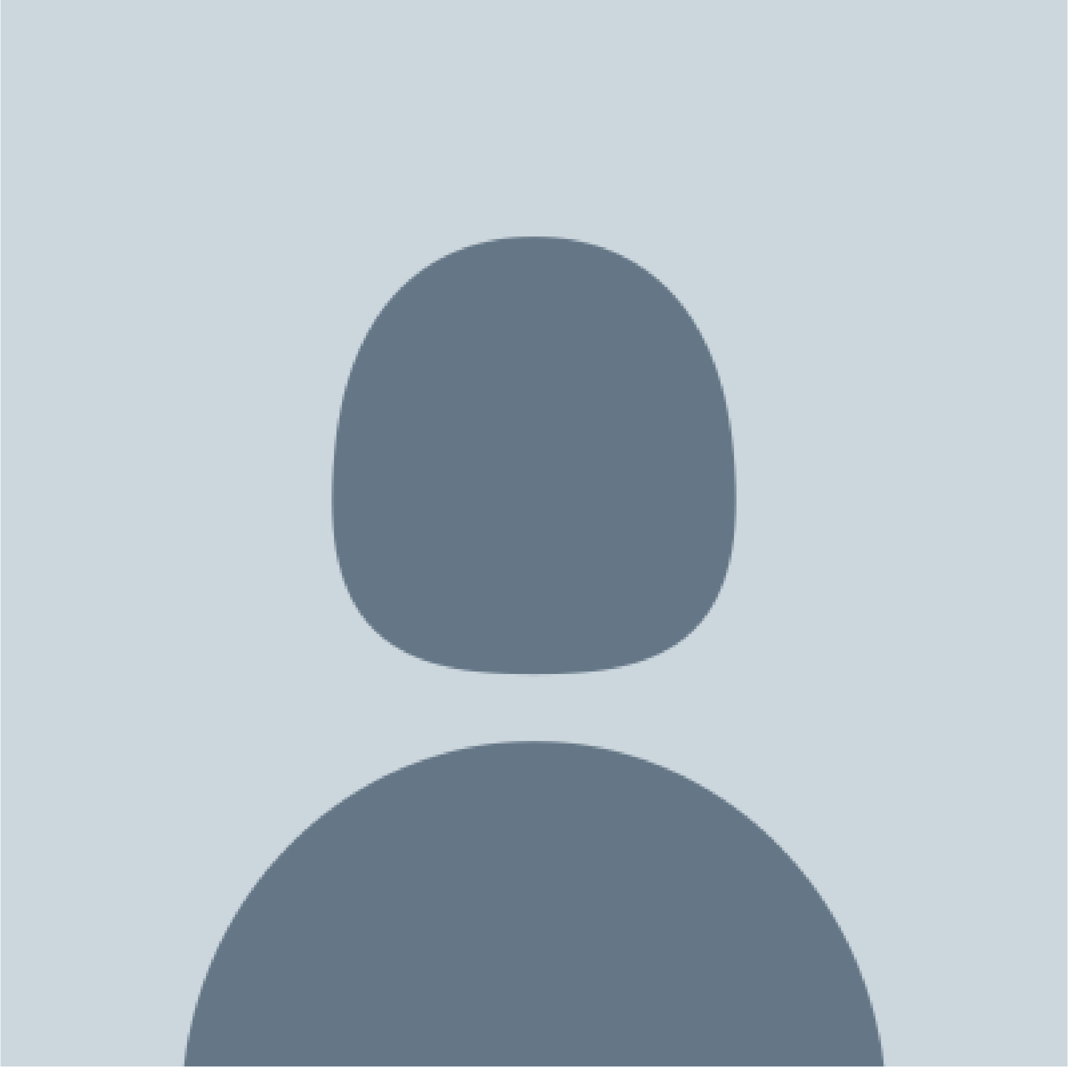
Fernanda Schmid



General Counsel

Cornerstone Research

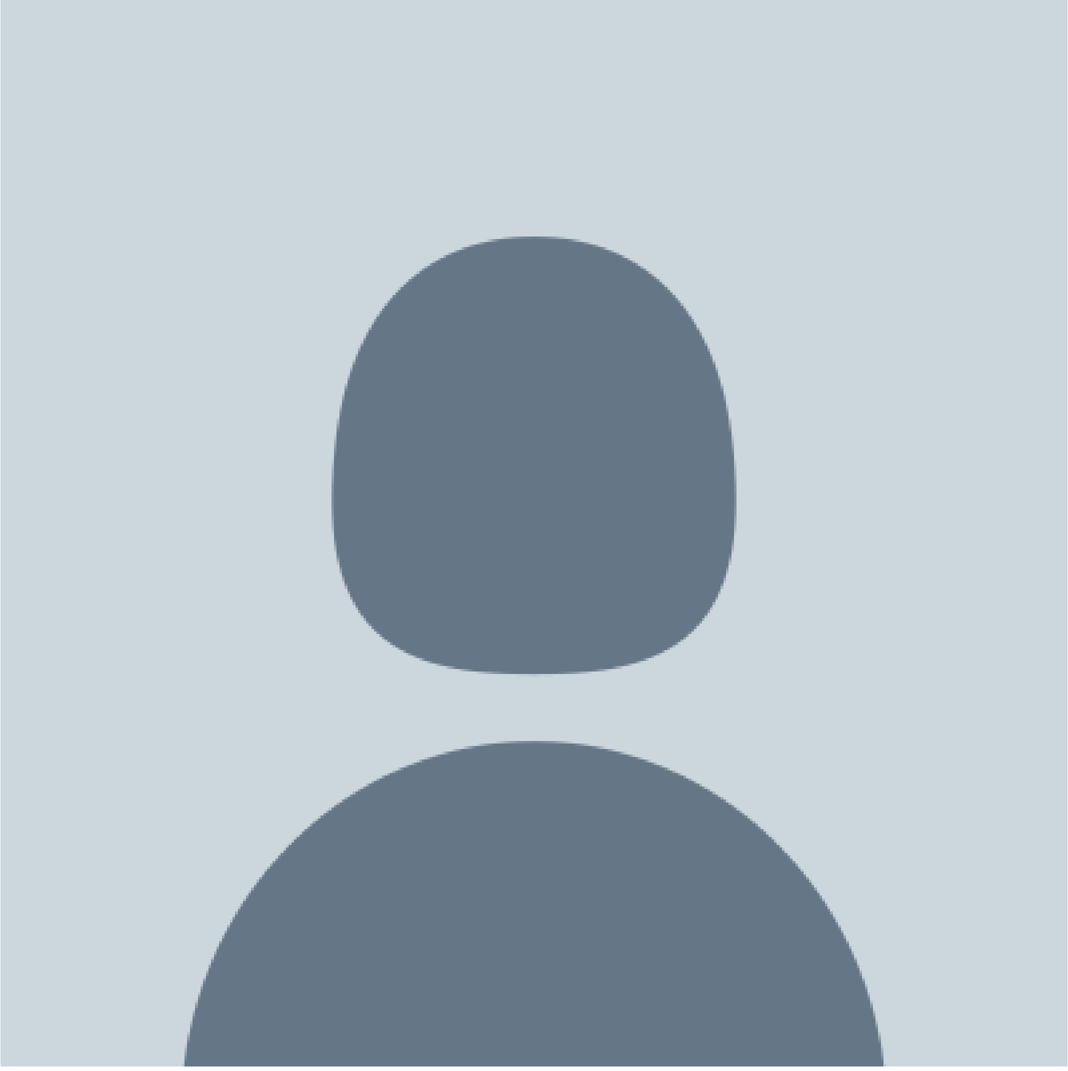
Robert B. Hubbell



Partner

Morrison & Foerster’s securities litigation, enforcement and white-collar defense group

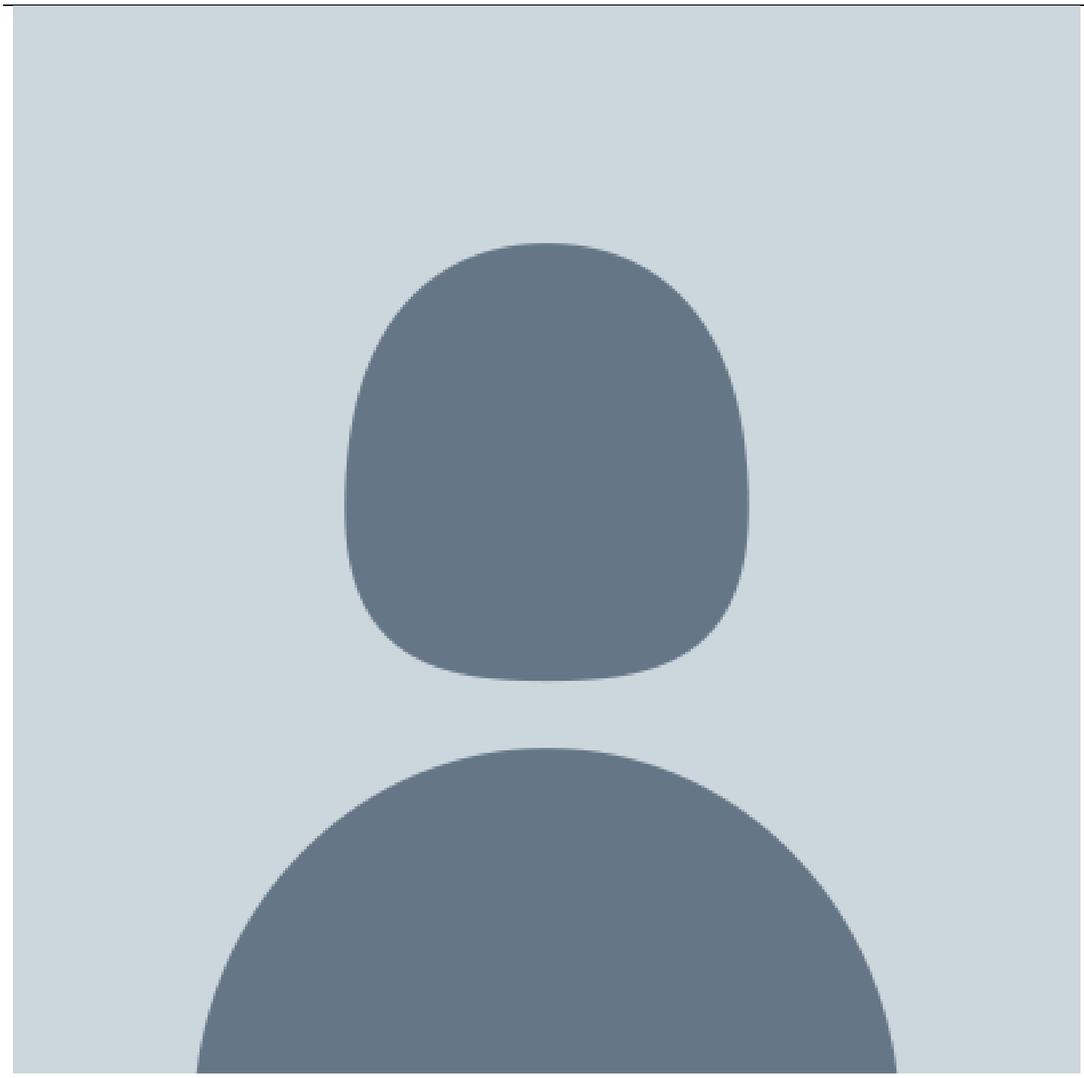
[Nathan D. Taylor ]



Partner

Morrison & Foerster’s financial services group

Daniel A. Nathan



Partner

Morrison & Foerster’s securities litigation, enforcement and white-collar defense group