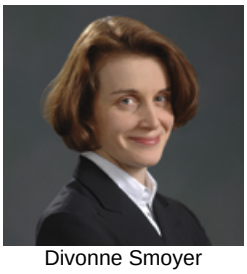
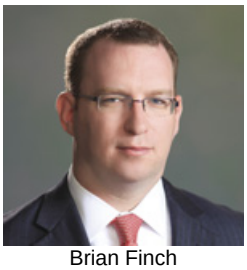
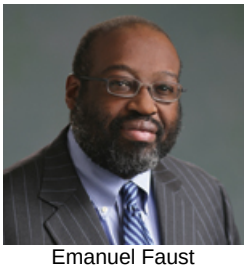
Ten Cyber Issues Boards and Chief Legal Officers Need to Know (and Worry) About

By Divonne Smoyer, Brian Finch, & Emanuel Faust


Divonne Smoyer


Brian Finch


Emanuel Faust

Boards of Directors have several fiduciary duties to uphold. Meeting such duties requires addressing cybersecurity and data loss. While this rapidly evolving area has its own unique challenges, boards, as well as the legal officers who advise them, face the same question about how to address cybersecurity, data loss, and data theft as they do any other critical issue—are they acting prudently, reasonably, and responsibly? More and more boards are now asking themselves**,** and the legal counsel who advise them**,** these questions and placing cybersecurity and data theft risks at a higher level of priority than even physical disasters. The factors below highlight 10 areas boards and their legal advisors should consider before their companies are faced with a real-world cyber threat.

1. **The stakes to share value and the bottom line are high.**
   Cybersecurity and data theft may sound like abstract concepts, but they have impacts—including financial ones—in the real world. It's been estimated that the global cost of cyberattacks in 2011 was $388 billion in direct financial loss and the cost of recovering from the attacks. Losses can take the form of stolen intellectual property or trade secrets, data destruction, disruption of critical systems, or even damage to physical assets. They also can include the exposure of customer and employee personal information. Any of these scenarios can result in material losses impacting a company's reputation, bottom line, and share price.

2. **The hackers are two steps ahead of you already.**
   While today's headlines are focused on standard types of data breaches and hacking activity—viruses, malware, physical break-ins, etc.—the next generation of threats, such as heretofore unforeseen attacks (so-called "zero day attacks")**,** has yet to make it into the public consciousness, but directors and their advisors have to be aware of them. The constantly mutating tactics cyber criminals employ will pose a serious challenge to any company that uses electronic systems. This means boards and their advisors, including GCs, will need to focus their attention on risk mitigation in this area for decades to come.

3. **Cyber and data loss threats pose merger risks.**
   Acquiring companies may be subject to significant losses and boards may be exposed to shareholder suits should adequate cybersecurity and other data protection measures not be taken in the context of corporate M&A activity. If a company acquires a target with a malware-infested IT system without appropriate due diligence to avoid that outcome, there is a potential for a wide range

of liabilities. Cybersecurity and other data protection methods should be added to the long roster of criteria a board and its legal and business advisors use when evaluating a potential acquisition and acquisition documents should contemplate and provide for appropriate representations, warranties, and indemnities related to cyber thefts and attacks.

4. **Lost or stolen intellectual property or customer or employee information can turn a deal from sweet to sour.**
   Imagine your company acquires a target for hundreds of millions of dollars. Then their systems are hacked and the blueprints for the widget that made the company attractive are stolen. Knockoffs flood the market and the company's value evaporates. Or imagine your company is about to launch a new software program, but it is swiped from your servers days before launch. Similar issues may arise if sensitive customer or employee data is exposed. Among the many questions that will be asked — by many, including investors, business partners and regulators — in the aftermath, is whether or not the board and its legal advisors acted with reasonable care to prevent such incidents.

5. **There is a maze of state and federal data protection and data loss notification requirements to navigate.**
   With State Attorneys General and an assortment of federal agencies, including the Federal Trade Commission, having a hand in data protection, breach notification, and disclosure requirements, companies should have plans in place for how to respond in a timely fashion should a breach occur (and, of course, be well-versed on its legal compliance obligations beforehand). The myriad disclosure and notification requirements and cybersecurity obligations will only grow and enforcement activity is likely only to increase, so it is incumbent on companies and their counsel to stay abreast of these developments.

6. **The failure to be fully informed of and proactive against cybersecurity and data loss risks could lead to litigation.**
   Companies, directors, and corporate managers could be exposed to litigation risks and potential liability for compromised data, systems, and infrastructure resulting from a cyberattack or data loss. Such claims could include third-party claims for breach of contract, breach of warranty, and/or statutory or common law legal requirements under both state or federal law; claims by state and federal regulators for failure to comply with specific data protection and cybersecurity laws (as well as more general unfair and deceptive trade practice-type laws), shareholder claims for breaches of fiduciary duty in failing to take appropriate steps to protect the company's assets, and business from cyber theft or other cyberattacks; and for publicly traded companies, investor securities law claims and SEC actions for failing to adequately disclose cyber risks.

7. **If the breach doesn't get you, the litigation will.**
   Even in those instances where a company or its directors are successful in defending a claim following a cyberattack or data loss, such litigation is likely to be expensive and a time-consuming distraction for management and the board. Beyond this, the cyberattack and the resultant attention from related legal proceedings could result in serious reputational harm.

8. **There are federal programs available to help mitigate corporate liability through the SAFETY Act**.
   Companies can gain valuable protections offered through an advanced approach to the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (known as the SAFETY Act). This

law provides tort liability protections for products and services that can be used to detect, defend against, or respond to cyberattacks. It is essential that boards and their legal advisors be aware of these programs and assess their applicability to cybersecurity products and services they either procure or deploy on their own.

9. **Insurance coverage is available through traditional or tailored policies.**
The demand for cybersecurity/data loss-specific coverage is incredibly high, placing pressure on availability, though some forms of traditional—and widely available—coverage such as Commercial General Liability may provide coverage for some types of claims. However, insurers are quickly working exclusions into these kinds of policies. Working with experienced coverage counsel can ensure the right kinds and amounts of coverage are in place.

10. **Outside counsel comes with the benefit of attorney-client privilege.**
While there are armies of consultants at the ready to advise companies should a cyber or data loss incident occur, only legal counsel can offer the shield of attorney-client privilege, thereby ensuring that sensitive information about investigations cannot be used in litigation. Having your cybersecurity/data privacy attorney on speed dial is a good idea.

Is liability inevitable or can steps be taken to mitigate or eliminate it?
Cybersecurity and data loss liability and litigation is in a similar stage as environmental law in the 1970s: there has been a broad awakening that liabilities exist—and that they may be vast. Companies have no choice but to assess their exposure and plan accordingly. That means in today's technology, dependent of business environment, it has become imperative that boards (or their equivalents) and their business and legal advisors devote appropriate attention to cybersecurity issues as a matter of good corporate practice and appropriate risk management.

This could mean causing management to (i) undertake a thorough cyber/data loss risk assessment that includes both company-specific risks and risks to critical third parties that would adversely impact the company, and (ii) identify and implement best practices relevant to the company's cyber and data loss risks.

Most importantly, boards and their senior management, including GCs, have to be aware of the threats and have management take measures to mitigate them. Failure to do so could easily lead to losses and liability.

Certified Information Privacy Professional Divonne Smoyer (@CyberDataPriv)is a partner in Dickstein Shapiro LLP's State Attorneys General Practice, where she represents clients in connection with state government investigations, data breaches, data privacy, and information security compliance (smoyerd@dicksteinshapiro.com). Partner Brian Finch (@BrianEFinch) is the leader of Dickstein Shapiro's Global Security Practice, where he counsels clients on regulatory and government affairs issues involving the Department of Homeland Security, Congress, the Department of Defense, and other federal agencies on a range of issues including cybersecurity (finchb@dicksteinshapiro.com). Emanuel Faust, Jr. serves as a deputy practice leader in the firm's Corporate & Finance Group. His areas of practice include corporate finance, mergers and acquisitions, joint ventures, project finance, and general corporate advice (fauste@dicksteinshapiro.com).