Developments in Cybersecurity: Privacy Laws, Hacking Beyond Customer Data, and Communicating with Corporate Boards

03.01.2016 • John E. Clabby & Joseph W. Swanson

I. Legal Exposure to Federal and State Privacy Laws

A. Federal Statutes and Enforcement

1. Federal Trade Commission Act, 15 U.S.C. §§ 41-58

The Federal Trade Commission (FTC) has emerged as the leading federal regulator for privacy and data security. The FTC enforces a number of statutes that relate to, or provide the basis for, enforcement proceedings related to privacy and data security. Those statutes include the Federal Trade Commission Act, 15 U.S.C. §§ 41-58.

Section 5 of the Federal Trade Commission Act grants the FTC authority to prevent unfair or deceptive acts or practices in commerce. 15 U.S.C. § 45. The FTC is empowered to bring enforcement actions under Section 5 and obtain various forms of relief, including equitable remedies. Id. The FTC has commenced nearly 100 such actions against entities for failing to protect their consumers' privacy and personal information, breaching the entities' privacy policies or other representations about data privacy, and similar violations. The FTC's website (www.ftc.gov) includes a number of resources addressing the agency's efforts in this area.

2. Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.

The Fair Credit Reporting Act (FCRA) requires fair and accurate credit collection and reporting, and it aims to protect consumer privacy. 15 U.S.C. § 1681. The FCRA, which applies to "consumer reporting agencies" and furnishers of information to such agencies (e.g., credit card issuers, car dealers, etc.), requires "consumer reports" to be accurate and limits the dissemination of those reports to certain circumstances (such as where directed by the consumer) where a third party intends to use the report in connection with a credit transaction with the consumer, and so forth. *Id.* §§ 1681b, 1681e, 1681s-2.

The FCRA includes a private right of action and provides various remedies for violations, including damages, costs, and attorneys' fees for a successful action. *Id.* §§ 1681n-1681p. The Act also empowers the FTC and other federal agencies, including the Consumer Financial Protection Bureau (CFPB), to bring enforcement actions against violators. *Id.* § 1681s. States are empowered to maintain enforcement actions under the Act as well. *Id.*

3. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809

The Financial Services Modernization Act, more commonly referred to as the Gramm-Leach-Bliley Act (GLBA), was enacted in 1999 and generally imposes obligations on financial institutions to safeguard the nonpublic personal information of their customers and consumers. 15 U.S.C. §§ 6801-6809. "Financial institutions" are subject to GLBA; this is a broad term that encompasses companies that provide loans, financial or investment advice, insurance, and other financial products or services. *Id.* § 6809(3); 12 U.S.C. § 1843(k). The distinction between "customers" and "consumers" turns on the extent of the relationship with the financial institution, and there are different requirements under GLBA depending on which constituency is at issue. *Id.* § 6809(9), (11).

GLBA and its implementing regulations generally require the protection of "nonpublic personal information" and govern the uses of that information by financial institutions (particularly their ability to share the information with third parties). The former set of regulations are referred to as the Safeguards Rules, while the latter are referred to as the Privacy Rules. The Safeguards Rules establish standards for financial institutions to ensure the security and confidentiality of customer records and information. *Id.* § 6801(b). The Privacy Rules address, among other things, the frequency and manner in which a financial institution must provide its customers and consumers with that institution's privacy policy and how the institution's customers and consumers may prohibit the sharing of their information with third parties. *Id.* § 6803.

The CFPB bears primary responsibility for promulgating rules and enforcing GLBA, although other federal agencies, such as the FTC and the Securities and Exchange Commission (SEC), possess authority under the GLBA for entities subject to those agencies' oversight. *Id.* § 6805.

For example, the SEC has issued regulations pursuant to GLBA for registered investment advisers, brokers, dealers, and investment companies. Those regulations include obligations to establish written policies and procedures reasonably designed to protect customer data. 17 C.F.R. § 248.30(a). In 2015, the SEC used that regulation to bring an enforcement action against an investment adviser for failure to implement any such policies and procedures and suffering a data breach, which resulted in the exposure of personally identifiable information for the firm's clients and others. As part of the enforcement action, the investment adviser agreed to a $75,000 penalty.

Meanwhile, GLBA permits states to implement similar statutes that are more protective than the Act. *Id.* § 6807. In that way, the GLBA sets a floor, with some states, such as California, availing themselves of the opportunity to pass more stringent protections. See Cal. Fin. Code §§ 4050-4060.

4. Communications Act of 1934, 47 U.S.C. §§ 151 et seq.

The Federal Communications Commission (FCC) enforces privacy and data security provisions contained within the Communications Act of 1934. 47 U.S.C. §§ 151 et seq. Those provisions require telecommunications carriers to protect their customers' personal information, also referred to under the Act as "customer proprietary network information" (CPNI). *Id.* § 222(a), (c). CPNI includes information related to a customer's use of a telecommunications service and information contained in the bills for that service. *Id.* § 222(h)(1). In general, telecommunications carriers may only use or disclose CPNI as necessary to render their services or in response to a written request by the customer. *Id.* § 222(c); see also 47 C.F.R. § 64.2005. The FCC's regulations require carriers to protect against attempts to gain unauthorized access to CPNI, and those regulations impose mandatory law enforcement notification and response requirements on carriers. 47 C.F.R. §§ 64.2010-.2011.

The FCC has instituted enforcement actions against carriers that fail to abide by these provisions. In one case, the FCC obtained a $25 million civil penalty from a carrier that failed to protect the confidentiality of several hundred thousand customers' personal information, which was compromised in data breaches at call centers outside the United States.

5. HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996), and HITECH Act, incorporated into 45 C.F.R. Parts 160 & 164

The Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), and the Privacy Rule promulgated pursuant to it, 45 C.F.R. Part 160 and Part 164, Subparts A and E, apply to "covered entities," which include health care providers, pharmacies, health insurers, HMOs, and health care clearinghouses. 45 C.F.R. § 164.500 et seq. The Privacy Rule prohibits covered entities from disclosing without authorization protected health information (PHI) that has not had identifying features removed from that

information. The Rule also requires covered entities, in contracting with "business associates," such as plan administrators, transcription companies, and other service providers, to safeguard PHI provided to them (those business associates are also subject to regulation in their own right). And, covered entities must develop written policies and procedures and designate a "privacy official" responsible for them, as well as establish reasonable and appropriate safeguards to prevent improper uses and disclosures of PHI. *Id.* 164.530.

The Security Rule, *id.* § 164.302 et seq., also promulgated pursuant to HIPAA, imposes additional obligations on covered entities to include drafting written policies and procedures for the protection of electronic PHI, training employees, and conducting risk analyses (with implementation of appropriate measures to address risks identified therein).

The Health Information Technology for Economic and Clinical Health (HITECH) Act, incorporated into 45 C.F.R. Parts 160 & 164, became law in 2009 and expanded the scope of HIPAA's privacy and security provisions, while also increasing liability for non-compliance and strengthening enforcement. For example, the HITECH Act contains a breach notification requirement, whereby covered entities must report breaches affecting 500 or more individuals to those individuals, the Department of Health and Human Services (HHS), and media outlets. *Id.* § 164.400 et seq. Breaches involving fewer than 500 individuals must be reported on a yearly basis to HHS. *Id.* § 164.404 et seq.

Although there is no private right of action under HIPAA or the HITECH Act, HHS' Office for Civil Rights (OCR) routinely brings enforcement actions for violations of these statutes and their implementing regulations by covered entities and business associates (state attorneys general may also bring actions). There are tiered penalties assessed per violation, with a maximum of $1.5 million. *Id.* § 164.400 et seq.; 42 U.S.C. § 17931 et seq.; 42 U.S.C. § 1320d-5. Recent investigations into data breaches and other data loss events have resulted in payments into the millions of dollars, including one that involved the theft of a single unencrypted laptop containing electronic PHI.

6. Cybersecurity Information Sharing Act of 2015

Although it is not a federal privacy law per se, the Cybersecurity Information Sharing Act of 2015 (CISA), currently available as part of the Consolidated Appropriations Act, Pub. L. No. 114-113, 129 Stat 2242 (2016), bears mention. CISA established a mechanism for sharing between the private sector and the federal government information related to cyber threats. Specifically, CISA called for the creation by the Department of Homeland Security (DHS) of a means by which the private sector could share information about cyber threats and defensive measures implemented in response to those threats. On February 16, 2016, DHS issued guidance as to how companies can report that information electronically to the federal government through a dedicated portal and receive the full protections afforded by the Act.

Those protections include a provision that no cause of action can be brought against private entities that conduct activities authorized by and in accordance with the Act. One requirement under CISA is that companies remove any known personally identifiable information before they share the cyber threat information with the government. CISA ensures that applicable legal privileges and protections, such as trade secret protection, will not be waived by sharing information with the federal government. Further, the Act contains provisions exempting (i) shared information from disclosure under the Freedom of Information Act, and (ii) participating private entities from antitrust laws. CISA states that cyber threat information shared with the federal government will not be used to regulate lawful activities. CISA also makes clear that participation by private entities is voluntary.

7. EU-U.S. Safe Harbor and Privacy Shield

The transfer of personal data from foreign jurisdictions, particularly the European Union (EU), to the United States poses significant challenges

for companies. Those challenges include potential liability for noncompliance with foreign privacy laws, which may be more stringent than similar domestic statutes. In the EU, data can only be transferred to countries with adequate protections for personal data. Historically, the EU did not consider the United States sufficiently protective of personal data, thereby complicating efforts to transfer such data from the EU to the United States. From 2000 to 2015, the Safe Harbor Agreement between the EU and United States addressed that problem by permitting companies to transfer personal data from the EU to the United States so long as companies agreed to satisfy a set of privacy principles. Those principles were enforced by the FTC.

In October 2015, the European Court of Justice invalidated the Safe Harbor Agreement over concerns about the extent of government surveillance in the United States and what that surveillance meant for the privacy of personal data. Case C-362/14, Schrems v. Data Protection Comm'r, 2015 E.C.R. I-650. Without the Safe Harbor Agreement, the EU and United States returned to the status quo, which meant that although data transfers were not automatically enjoined, there was great uncertainty in how to comply with myriad European privacy laws. In February 2016, however, the EU and United States agreed on a framework to replace the Safe Harbor Agreement. That framework will be known as the Privacy Shield. It imposes various requirements on American companies to protect the personal data of Europeans. The Privacy Shield, which remains subject to final approval, also calls for stronger monitoring and enforcement by the Commerce Department and FTC, with a mechanism for EU citizens to lodge complaints and to pursue alternative dispute resolution. Complaints must be resolved within forty-five days.

B. State Statutes, Enforcement, and Litigation

1. State Privacy and Data Security Statutes

Many states have enacted privacy and data security statutes that supplement the statutes outlined above and are in addition to states' more general consumer protection statutes. Some of those statutes pertain to the privacy of financial information. These state analogs are generally more protective of consumers than GLBA.

Meanwhile, there are state privacy statutes governing medical records and other health information, which supplement HIPAA and the HITECH Act. For instance, the California Confidentiality of Medical Information Act (CMIA), Cal. Civil Code § 56 et seq., imposes a number of requirements regarding the disclosure of medical information by health care providers in that state. Notably, CMIA includes both a criminal enforcement provision, a civil enforcement provision, and a private right of action.

Like California, Texas has a medical records privacy statute. Tex. Health & Safety Code § 181.001 et seq. Although the Texas statute provides for civil enforcement – with the possibility for significant fines – it does not include a private right of action.

2. State Breach Notification Statutes

In addition to privacy statutes and other laws imposing an affirmative obligation to protect personal data, there are a patchwork of notification statutes that could apply in the event of a breach. Presently, there are breach notification statutes in forty-seven states, as well as in the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands (the three states without such a law are Alabama, New Mexico, and South Dakota). The residency of the affected individuals is frequently the trigger for whether one or more of these statutes applies, making it important to know generally where one's consumers and employees are located. While many of these statutes are similar, there are certain important differences in terms of (i) what is protected information, (ii) the form of protected information, (iii) notification requirements (deadlines, whom to notify, and so forth), and (iv) whether there is a private right of action. These differences are noted briefly below, but, as a practical matter, in the wake of a breach, a company will comply with the most stringent notification statute triggered by the event.

a. Protected Information

In general, state breach notification statutes apply to a person's name plus one other identifying feature, such as that person's Social Security number, driver's license number, or financial account number with access information. For example, Florida's notification statute applies to medical and health information, financial information, military information, insurance information, and online account information. Notably, Florida's notification requirements could be triggered where data is compromised that does not include an individual's name. So long as the compromised information would enable identity theft, the notification statute applies. Florida is not alone in including medical and health information within this definition, as a number of other state breach notification statutes contain similar definitions of protected information. Also, Florida and at least two other states include, or will include, email addresses with password information among their definition of protected information. Other states' notification statutes include additional items within their definitions of protected information, such as biometric data. North Dakota, for example, goes so far as to include a person's digital or electronic signature, employment ID number, birthdate, and parent's surname before marriage.

b. Form of Protected Information

In general, state breach notification statutes apply to compromised personally-identifying information in electronic format (if not encrypted), although some laws also apply where that data resides in any form, including hard copy paper records.

c. Notification Requirements

If triggered, the various state statutes impose a range of requirements in terms of whom must be notified and the deadlines for doing so. For notifying the affected individuals, the statutes often direct action without specifying a number of days. States in this category include Alaska and Oregon, which both require notification "in the most expeditious time possible and without unreasonable delay." Others specify a number of days. Florida allows up to thirty days after discovery of the breach, but an additional fifteen days are available for "good cause." Ohio and Wisconsin permit forty-five days.

In addition to notifying the affected individuals, other constituencies must be informed under certain state statutes. For example, many states require notifying credit agencies under various conditions (e.g., a breach involving more than 1,000 affected persons). Other state entities, such as the state attorney general and/or the state police, must be notified under various state laws.

Often, a state's statute will permit a delay in notification if law enforcement is consulted and deems such a delay to be warranted because of an ongoing investigation.

d. Private Right of Action

Some state notification statutes expressly create a private right of action, while others explicitly bar such an action. In the middle of that spectrum are the remaining notification statutes, which are silent on the issue. In those states, the attorneys general typically will enforce the notification statutes, which generally provide for fines or other penalties.

3. Enforcement Actions and Other Litigation

State attorneys general have become important figures in enforcing the statutes described above. In the wake of a data breach or similar event, it is not uncommon for the attorneys general in the affected states to launch investigations, possibly culminating in an enforcement action or actions against the company.

Supplementing those investigations and proceedings are private actions filed by affected individuals. Those private actions often involve an array of claims, both provided for by statute and under common law. Typical claims in the former

category include claims premised on violations of state privacy and data security statutes, as well as consumer protection and unfair competition statutes. The claims also may include violations of any applicable notification statutes. The common law claims frequently include negligence, breach of contract, breach of implied contract, breach of fiduciary duty, and unjust enrichment. The theories underpinning these various claims are generally that the company (i) failed to adequately protect the personal data that was compromised, and (ii) failed to respond to the breach or other event in an appropriate and timely manner.

Thus far, litigation following a data breach has frequently focused on the issue of standing, especially on whether the plaintiffs can show an injury-in-fact. This requirement can be challenging for plaintiffs who cannot show any harm caused by a breach (such as identity theft or fraudulent charges on their credit card) but who instead allege a generalized fear of future harm. Where a risk of future harm is alleged, the Supreme Court has said (in a different context but nonetheless relevant to data breach litigation) that there is no standing unless the plaintiffs can show that the feared future injury was "certainly impending." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143, 1147-50 (2013). The Supreme Court also said in *Clapper* that plaintiffs cannot manufacture standing by incurring costs in anticipation of that feared future injury. *Id.* at 1151. In the data breach context, such costs might be purchasing credit monitoring or taking other prophylactic measures.

Following *Clapper*, many federal courts have dismissed, on standing grounds, data breach litigation alleging a fear of future injury. *See, e.g., Whalen v. Michael Stores Inc.*, 14-CV-7006 (JS) (ARL), 2015 WL 9462108 (E.D.N.Y. Dec. 28, 2015); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949 (D. Nev. 2015); *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847 (S.D. Tex. 2015). Other courts, however, have permitted such litigation to proceed where the claimed fear of future injury is reasonable. *See, e.g., Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

Aside from consumer or employee litigation in the wake of a data breach, companies may also face suits from financial institutions that issued credit or debit cards that needed to be replaced as a result of the breach.

II. Risks of Hacking Beyond Privacy: Vulnerability of Products and Business Models

Under the legal and regulatory framework discussed above, legislatures and regulators have focused on the loss of customer or employee data. This framework has developed in response to voter and citizen concern about identity theft, and addresses, in large part, massive breaches of personally identifiable information. These threats have been well-known since at least the TJX Companies Inc. suffered a breach of its point-of-sale payments systems in 2007, exposing 45 million credit card numbers.

Less well known are the cyber risks that do not target customer data. These risks are typically malicious and criminal in origin, and aim to steal the company's proprietary data, shut down its communications systems or website, or otherwise damage the company's reputation. Related concerns are the use of a company's systems to commit crimes, and the potential effect on a company's reputation from cooperating with the government in a criminal case. A brief overview of these risks follows, and this section will conclude with potential risks when a company's products incorporate connected technology but things go wrong, causing customers damage.

A. Compromised Trade Secrets and Other Intellectual Property

One of the principal risks to a corporation's bottom line, apart from theft or loss of customer or employee data, is the threat to corporate trade secrets and other proprietary information. While consumer data losses tend to garner headlines, this risk may be even greater. It is difficult to measure because, in general terms, no law requires a

company to disclose the theft of intellectual property. But there is no doubt that it is staggering in the aggregate. General Keith B. Alexander, then-director of the National Security Agency, famously stated – all the way back in 2012 – that thefts of proprietary data from public and private networks represent "the greatest transfer of wealth in history." In that same speech, he estimated the annual loss to the U.S. economy at $250 billion.

Trade secrets can take many forms, from proprietary manufacturing processes, to in-pipeline code, to customer lists. A strong pre-breach defense is important, because there are few tools available to a company once such a breach occurs. There is no federal trade secret statute that would allow a private company to sue for the theft of its data. Instead, private parties who have had their data stolen rely on a patchwork of state civil law, usually based on the Uniform Trade Secrets Act. The federal criminal justice system has available the Economic Espionage Act (18 U.S.C. §§ 1831-39) and the Computer Fraud and Abuse Act (18 U.S.C. § 1030), but that system is often reserved for the most egregious cases, and the government can otherwise be slow to motivate to help a large corporation in what often appears to be a purely civil dispute between companies.

Even if there were a private right of action, often the theft occurs remotely, and the criminals are located abroad and sponsored by foreign nations. The United States government for the past year has taken serious efforts to combat the growing and serious threat of nation-state hackers seeking to access, steal, and exploit U.S. trade secrets. On April 1, 2015, the President announced an Executive Order, "Blocking The Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," to help address this threat by arming the government with the authority to impose personal sanctions against individuals working with enemy governments to hack U.S. businesses. The Order declared a national emergency with respect to the "unusual and extraordinary threat to the national security, foreign policy, and economy of the United States" posed by "the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States." A few weeks later, on April 27, 2015, DHS announced that it would open an office in Silicon Valley, in recognition of the significant challenges to technology companies from foreign actors.

Apart from foreign actors, the risk of hacking from domestic or foreign competitors is also significant. This has always occurred at multinational companies with the resources to undertake competitive intelligence programs, but the prevalence of technology and the ease of use of some hacking tools has made even small businesses vulnerable. In December 2015, a New Hampshire linen company – General Linen Services, LLC – pleaded guilty to hacking their local rival's computer systems to steal "1,100 of their competitor's invoices for use in sales efforts directed at the competitor's customers."

Many of these foreign actors or competitors gain access through rogue employees. In conjunction with nation states or competitors, or acting on their own, rogue employees present an acute threat, and a particularly difficult one to uproot because these individuals have legitimate access to the systems. One of the authors of this article, when he was an Assistant U.S. Attorney, prosecuted a rogue employee of a U.S. defense contractor who had access to the contractor's library of export-controlled military technical drawings because she was a computer systems analyst.

There are two main methods of protection of trade secrets and proprietary information: (i) hardening the physical and electronic systems that protect the information, and (ii) actively managing and limiting the amount of confidential information that a company holds.

As to the first, protection can take many forms. Beyond passwords, encryption, monitoring, and testing, companies should deploy segmented networks or off-network computers to restrict access to the company's crown jewels to only those who

truly "need to know." This segmentation should include restriction from the IT staff themselves. In so doing, companies should take care to deploy IT and physical security resources wisely so that the state-of-the-art portion of the defense is protecting the proprietary data, and lesser protections are given to general operating data and public information. Non-tech protections are important as well, particularly including (i) rigorous badging programs that control physical access to portions of the facility, and (i) a renewed focus on the hiring/on-boarding and firing/off-boarding of technical, sales, and IT staff.

Second, recognizing that there will be breaches if the information is important enough, companies must manage their proprietary processes and data in such a way as to limit their existence. Companies must regularly audit the location of their crown jewels to purge excess copies. Systemic deletion is a big part of reducing a secret's footprint and lowering risk. As Benjamin Franklin wrote: "Three can keep a secret, if two of them are dead."

Restricting third-party vendor access to trade secrets is also key, as non-disclosure agreements are often not worth the paper they are written on, particularly if a vendor has already disseminated, negligently or maliciously, the secret, and if that vendor is undercapitalized such that it cannot make the victim company whole. Dissemination to a vendor also means trusting that the vendor's systems are protected at least as well as the owner's systems are protected, which is often overlooked in the hiring process or addressed with indemnities and insurance rather than inspection or auditing.

Finally, proprietary processes or products that are patentable should be patented as soon as possible, to avoid loss in the runway phase to stout legal protection.

B. Business Interruption and Destructive Malware

Some of the earliest threats to corporate computer systems were brute force attacks that were no different from vandalism. These attacks would shut down the corporate website or change its front page to something embarrassing. Recent versions of this, however, are far more aggressive, more planned, and more sinister in nature than vandalism.

The overall threat can be described as a Denial of Service ("DOS") attack when it originates from a single Internet connection, and a Distributed DOS ("DDOS") attack when that attack is launched form multiple Internet connections. These can include attacks that shut down websites, prevent employees from logging into their work networks, or disrupt cell phone or point-to-point communications. Such attacks are common. In January 2015, for example, a hacking group took down both the BBC's website and Donald Trump's campaign website using a form of a DDOS attack.

The costs to a company from losing its ability to do business in this way can be significant, as can attempting to reconstruct destroyed or locked records if the attack is permanent in nature. Besides a good initial defense to prevent such attacks, a company's resilience to such an attack depends on a company's contingency planning, the robustness of its disaster recovery and data back-up, and finally, the existence of redundant systems for real-time communication or customer interface.

A common attack, with a profit motive, is "ransomware." In a ransomware attack, the criminal will penetrate a company's systems and then encrypt the data unless and until the company or individual makes a payment. The amount sought is usually relatively low, and embarrassed or desperate companies often make the payment. For example, a hospital in Los Angeles in February 2016 paid $17,000 in Bitcoin digital currency to unlock its systems after a ransomware attack.

Some attacks have been linked to nation-state actors, and no ransom is offered before systems are destroyed. The November 2014 attack by North Korea on the computer systems of Sony Pictures included hard drive-erasing malware.

The federal government has made efforts to fight these attacks, but they have relied in large part on private industry. As an analogy, there are far fewer policemen then there are residential homes to defend from burglary. In March 2015, the Federal Financial Institutions Examination Council, the federal interagency body comprised of five banking regulators, including the CFPB, released a Joint Statement on Destructive Malware. The statement urged banks to prepare for destructive malware attacks as they would for a natural disaster, and then some, warning that such a cyberattack could reach both primary systems and "backup data centers (e.g., mirrored sites)" located elsewhere.

C. Use of Company Systems to Commit Crimes

Companies that provide electronic communications services, such as e-mail, phone, or website hosting, are usually agnostic as to how their systems are used. Many have controls that seek affirmatively to identify violations of the law, as good customer and civil service, but most are passive, responding only to third-party claims of trademark or copyright violation or more nefarious criminal activity and, at that time, making efforts to stop it. Few companies want their systems to be used for crimes and, when they have determined their systems were used for crime or fraud, cooperation with law enforcement is usually routine. For example, when law enforcement subpoenas a bank for account records reflecting an alleged fraud scheme, the bank responds to the subpoena, produces records, and little to nothing is ever said about it publicly. To this end, privacy policies for websites usually include clear exceptions for cooperation with legal process.

This picture changes when the company has advertised the security or integrity of its systems against third-party or government access, by touting its encryption method or aligning a company's sales tactics with a more modern sense of internet privacy. One example of aligning with customer expectations is the promises of companies such as Yahoo!, Apple, and Dropbox, in their respective privacy policies or on their websites, that they will inform account users of any government request for information to allow those customers a chance to file an objection. The Electronic Frontier Foundation tracks such polices on their "Who Has Your Back" list. In these companies' views, taking this approach helps them recruit and retain modern customers. But it impacts the government's view of those companies as good actors in the law enforcement community, and – intentionally or not – there are often regulatory repercussions for a company that is not seen as a corporate actor who is friendly to law enforcement. This tension has existed for some time, and where a company ends up is ultimately a business decision.

An example of this tension is in the advertisement of encrypted systems as part of a company's greater assurances of privacy against government or third party inquiry. Apple and federal prosecutors are presently battling in at least two jurisdictions over whether Apple must unlock an iPhone in separate, ongoing investigations. In its marketing for this version of the iPhone, Apple had promised its customers that the operating system for the phone did not have a backdoor that would allow a nonuser access to the data. To make good on this promise, Apple never developed a backdoor that would allow entry beyond the password gate. That is, without the password or specialized software – which has not been written – an iPhone is only good as a paperweight. Now the government is seeking to compel Apple to write such software. Apple has argued that, once such software is written, it would work for any and all iPhones running that operating system, which would undermine its ability to ensure systems security to all of its other users.

An evaluation of the respective legal positions in these cases is beyond the scope of this paper. As companies see promises of privacy as a competitive advantage, tension between legitimate law enforcement and private sector entities that hold evidence will increase, at least until the law is settled.

The idea of advertising data privacy policies or encryption as a competitive advantage is relatively

new. A few consequences flow from it. First, when challenged by a criminal subpoena or for evidence even in a civil case (such as a divorce case that seeks encrypted text messages with a paramour), the company may find itself either paying for a costly and public fight, or losing the confidence of its customers. Second, making these promises to a customer base – that a company's cyber protections are better than its competitors' – ratchets up the reputational loss when a copy does suffer a major data breach. The company loses the "this happens to everyone" defense in the court of public opinion, particularly among customers who chose that business in reliance on its promises of better security. Third, if these promises of comparatively better security or specialized consumer protection are made in public disclosures such as SEC filings, then a breach by a third party may lead to a securities fraud suit if the "corrective" disclosure leads to a drop in stock price. The relative infrequency of competitive-advantage disclosures touting data privacy may be one explanation for why there have been few stock-drop suits to date.

D. The Internet of Things: Opportunity and Risk

The "Internet of Things" is a term that covers the expansion of wireless technology and digital sensors into consumer products and other devices that were not traditionally connected. Common examples are home thermostats and alarm systems that can be operated from a smart phone; fitness trackers and watches that automatically upload location, step, and speed data to the web; and televisions that track what shows are watched and commercials skipped. As the price of such technology drops, its expansion is inevitable, from smart pillows that analyze sleep patterns, to refrigerators that know when their owners are running out of milk, to driverless cars.

These devices are amassing incredible amounts of data on consumers, and much of that data contains extraordinarily sensitive information. The collection of this "big data" poses security concerns, because the greater the amount of data, the greater the risk of a breach. Increasingly, too, questions are being raised about how companies use the data they collect and the extent to which consumers should be able to have a say on that topic.

In addition to the concerns about the explosion of data heralded by the Internet of Things, there are the security risks posed by the devices themselves and their connectivity. Medical devices are at the forefront of this discussion. On the one hand, allowing devices such as pacemakers to connect wirelessly can help patients and doctors enormously, both in monitoring where it was not possible before and for allowing check-ups without invasive surgery and lengthy hospital stays.

But the risks are obvious. At a tech show in Melbourne in 2012, a well-known hacker named Barnaby Jack demonstrated how a pacemaker transmitter could be reverse-engineered to deliver deadly electric shocks. This occurred the year after the same hacker developed a method that could locate and seize control of any insulin pump located within 300 feet of the user. In light of these risks, it is not surprising that the Food and Drug Administration published a draft of detailed guidance earlier this year on cybersecurity for medical devices.

Driverless cars have tremendous benefits as well, whether in reducing traffic or accidents. Although driverless cars are still in the prototyping phase, problems with wireless connectivity in existing vehicles have already led to recalls and safety concerns. In 2015, Chrysler had to recall 1.4 million vehicles because a software vulnerability allowed hackers to wirelessly take over vehicle dashboard functions, steering, transmission, and brakes.

Although the risks posed by connected medical devices and driverless cars are relatively obvious, there are security risks even for common household items. One example involved VTech Electronics, which makes "electronic learning products" for children, including handheld educational gaming systems with Internet connectivity through online accounts. Hackers struck VTech in November 2015, exposing the data of approximately 6.4 million children and 4.8 million parents, including account information, mailing addresses, and even pictures

of children. This case shows that any company with an internet-connected product must think through security and privacy issues – and address those issues – in every phase of the product lifecycle, from design to release to post-production.

That is among the themes stressed by the FTC, which is at the forefront of education and enforcement related to the Internet of Things. In January 2015, the FTC released its Staff Report on the Internet of Things, which provides the FTC's recommended best practices for privacy and security in this area. The report is the culmination of a workshop that the FTC held in 2013, and it draws not only on that event but also on privacy and data security enforcement actions commenced by the FTC. The themes discussed in the FTC's report were reiterated by FTC Commissioner Julie Brill during a January 2016 speech: "Consumers want reasonable assurances that companies are keeping the data collected about them, as well as their connected devices themselves, secure."

The discussion above outlines the extent to which the Internet of Things brings with it not only vast opportunities but also great risks, including the risk of a products liability lawsuit, customer alienation, or regulatory action. When consumers are demanding more and more privacy and data security (to say nothing of regulators and plaintiffs' attorneys), companies must be mindful of how the Internet of Things will affect their business and their risk profile.

III. How to Talk to a Corporate Board about Data Security

A. The Expanding Risk of Board Liability for IT Security Controls

The federal government and regulators promote or are moving toward a model where a board must actively oversee a company's cybersecurity controls and systems. Sophisticated private companies are likely already there. But at the same time, enterprising plaintiffs' attorneys are experimenting with shareholder derivative lawsuits, after breach events, that accuse boards of failing to oversee these same controls. This table-setting can and should capture the attention of boards and those in management who are responsible for helping their directors. The section of the paper offers some practical advice and best practices for how to structure board reporting and how management should communicate with its board on issues related to cybersecurity.

1. The Cybersecurity Disclosure Act of 2015

A recent Senate Bill is an example of the growing focus on a top-down approach to cyber governance favored by lawmakers and regulators. Introduced on December 17, 2015, the Cybersecurity Disclosure Act of 2015 would require public companies to disclose in their SEC filings whether a board member has "cybersecurity expertise or experience." If the company did not have such an expert director, it would have to disclose why one is not necessary and what additional measures it is taking to improve cybersecurity. The bill would leave to the SEC and the National Institute of Standards and Technology (NIST) just what would qualify as "cybersecurity expertise." This proposal might seem familiar to veterans of advising boards because it borrows from the Sarbanes-Oxley Act's similar requirement that a company disclose whether it has an "audit committee financial expert" on its Audit Committee and, if not, why not.

But unlike Sarbanes-Oxley, it does not appear that this bill has significant momentum. Its introduction, however, does occasion a broader conversation about the role of a board in ensuring controls around information security. The SEC already requires companies to disclose material cybersecurity risks, and Audit and Risk Committees at large companies and financial companies, at least, are familiar with their companies' major cyber exposure through approving such disclosures and governing those risks, respectively. Naming at least one director as a point person for cyber risk, which is what

the Act aims for, is a good practice, as will be discussed below. Whether a board needs an expert in cybersecurity, rather than someone who is just broadly skilled in enterprise risk, depends on the company.

2. Derivative Lawsuits

It is critical for a board to understand the legal implications of cybersecurity both to the company (as noted above in point heading I of this paper) and for their personal liability as directors. Apart from Congress, the SEC, and plaintiffs' attorneys in the well-publicized data-breach class actions, plaintiffs' attorneys have been experimenting with derivative lawsuits against directors whose companies have suffered a data breach. These lawsuits, which are presently few, allege that the directors breached their fiduciary duties by failing to exercise sufficient oversight of the company's data integrity.

One of the derivative complaints that followed the Target data breach in late 2013, filed on July 18, 2014, sounded in traditional notions of Caremark oversight (named after the seminal Delaware case that outlined its contours). The shareholders alleged that the directors and officers "failed to ensure" that "the Company had formal data security risk management guidelines, policies, and procedures," that "individuals with the requisite expertise and understanding of data security issues were appointed to appropriate positions," and that "a Chief Information Security Officer with the ability to explain the risks and vulnerabilities to the defendants was in place."

The shareholder derivative complaint that followed Home Depot's 2014 breach (unsealed version filed on September 2, 2015), was much more granular as to its expectations of the board. According to that complaint, the directors and officers "failed to ensure" that "Home Depot installed and maintained an adequate firewall," that "Home Depot encrypted cardholder data that was transmitted and stored on its systems," and that "Home Depot installed and maintained up-to-date antivirus and antispyware software."

While the Target complaint was concerned with traditional board responsibilities – establishing policies and procedures and appointing skilled C-suite executives – the Home Depot complaint charged the board with installing technical defenses, such as a firewall and particular anti-virus software. These matters are not yet resolved, and it is unclear where the line will be drawn for the expectation for board behavior. Below, this paper offers some commonsense ideas for working with a board in the shadow of such uncertainty.

B. Knowing the Risks But Not How to Mitigate Them

Most members of public company boards are now aware that cybersecurity is a major risk for their companies. They know this through director education, industry newsletters, and general networking. Being aware of a risk and knowing how to structure oversight to mitigate that risk, though, are two very different things.

A recent survey of *Forbes* 2000 company directors revealed that 63 percent are actively addressing computer and information security, up from only one third in 2012. *Jody R. Westby, How Boards & Senior Executives Are Managing Cyber Risks, Governance of Cybersecurity 2015 Report, Georgia Tech Security Center (Oct. 2, 2015).* According to the survey, boards are focusing on a review of top-level policies and receiving reports of breaches and general IT risks, but they are still weak on reviewing cybersecurity budgets and assigning responsibilities to key privacy personnel. Attention to cyber risk also varies across industry, the survey reported, with the financial sector boards having the strongest engagement.

Smaller companies are not faring as well. The National Association of Corporate Directors' 2015-16 Public Company Governance Survey reported that a quarter of the directors of the smallest

public companies had “little knowledge” regarding cybersecurity risks, compared to only 10 percent at the largest companies.

This is confirmed by the anecdotal experience of the authors of this paper. Directors of sophisticated companies are now aware of the importance of cybersecurity, they see it accurately as part of enterprise risk management, and they are still searching for guidance on how to track these risks over time and how to devote the right level of attention to the oversight of data security and management. They are at phase two – they know they have a problem and want to know what to do.

Board members who have been alerted to cybersecurity but not have not yet been briefed on a company’s defenses will have many questions, and the organization and briefing protocols should seek to address these questions. Those questions might include the following:

1. What are the major cyber risks to the business?
2. What would happen if those risks came to pass?
3. What controls are in place to mitigate and compensate for these risks?
4. How does management stay informed of the risks and mitigation?
5. What are the company’s policies and procedures for information security and management and how does management test for compliance?
6. What industry standards or national standards does the company follow and how does management test for compliance?
7. Who determines the IT security budget and is the company spending money efficiently?
8. What is the company’s breach response plan?
9. What third-party consultants are testing the company’s data security and what is their assessment?

C. Corporate Governance for Board Oversight of Cybersecurity

1. Structure and Organization

Perhaps the best way to approach the issue is to start with the oversight architecture, to determine which board committee should have primary oversight. The growing best practice is to lodge the oversight of cybersecurity with the Risk Committee. This is in line with the evolved corporate governance practice to separate Risk from Audit; for example, in the Georgia Tech survey cited above, 86% of financial sector boards had a separate Risk Committee. And cybersecurity is a strong example of the advantages of this. Because IT security is a permanent risk that will always be with a company, it should be identified, compensating controls should be installed, and the risk-control relationship should be tracked. The reporting format of a Risk Committee is best suited to this task.

Many companies either do not have a Risk Committee or entrust the technicians of the their Audit Committee with the task of IT security. Caution should be taken to add yet another responsibility to what is often the most engaged, and most burdened, of the board’s committees. There is an additional potential conflict with the Audit Committee overseeing cybersecurity, as that committee also audits the security program. For smaller companies or companies with minimal cyber risk, though, tasking the Audit Committee with cyber risk is reasonable.

In any event, including if the company has decided to leave cyber at the full board level, the directors should designate a lead cyber director. Such a director is important for a few reasons. First, it develops a director who over the long term will have substantive knowledge on cyber concerns across the company, across the industry, and across that director’s range of experience. Second, it allows a director to become fully invested in the determination, the improvement, and the success of controls around the company’s cybersecurity. Third, the lead cyber director can be the single

point of contact for management during a crisis, and someone who can assist with determining what should be reported to the cyber-designated committee or the full board, and how.

Who from management should report to the board on these issues is evolving. Most major companies have a Chief Information Security Officer (CISO) or equivalent position in a framework that allows and encourages direct, unfiltered contact between the board and the CISO. The segregation of privacy and security will become a larger corporate governance issue in the coming years as the CISO continues to gain prominence. Most CISOs report into the Chief Information Officer (CIO), but a better practice is a direct report into the CEO or even to a board committee, with a dotted line to the CEO. There is something of a conflict in a CISO reporting to a CIO, because a CIO must cut costs and improve efficiency in the IT department, while a CISO must often promote technology expenditures that reduce loss in the long term. That is a manageable conflict, though, and the primary reason for a direct report to the CEO is so that the CEO can learn, unfiltered, the state of the company's security.

As for board reporting, the CISO should provide the board or committee with an overall view of the threats to the company from intrusions and a complete picture of the company's cyber defenses, with a focus on what is new or has changed since the last briefing. More on the nature of that briefing will be discussed in the next section.

The General Counsel's (GC) office has an important role in reporting on cyber risk to the board. There is a strong argument that reports from the business units on actual breaches, compliance lapses, and investigations into those incidents, should run through the legal department if they are for the purpose of providing legal advice to management and the board. In that way, even though the underlying facts are not protected, at least the reports themselves will be insulated by the attorney-client privilege. The hiring of consultants, in particular, to audit and to find holes in the systems or to investigate an incident, should only be at the direction of counsel; their hiring is to harden the defenses in many instances but also, quite clearly, to allow the company's legal team the facts they will use to provide legal advice on exposure to lawsuits or regulatory action. Unless a company has a Chief Privacy Officer, it also makes good sense for privacy policies to originate from the GC's office rather than with the CISO's team. In sum, legal can provide the board with an unvarnished view of performance, be the link to outside expertise, and spot icebergs from changed legal risk profiles.

The role of the Chief Risk Officer (CRO) is integral to a company's cyber organization because, as discussed above, cybersecurity is part of enterprise risk management. Cybersecurity will be part of the CRO's periodic reporting to the board, in the context of the other major risks and compensating controls. Regardless of the CISO's responsibility in an organization, which is highly focused on systems integrity, the CRO should track cybersecurity in the context of the company's mix of other risks. In this view, cyber is just another risk, and the existence of a CISO herself is just another mitigating or compensating control. The CRO can provide this important context to the board.

Best practice is a combination of all three players, and likely others, with the CISO at point for board communications on threats and the defense posture, the GC's office reserved for privilege-protected communications, and the CRO tracking cyber risk as one of many relative risks, for context.

2. Form and Content of Briefings

Briefings to the board should be periodic and part of the annual plan for budgeting board time. Quarterly briefings to the Risk Committee are a good starting point, with more or less depending on the company's profile. One of these four should be an annual deep dive, perhaps where there is reporting on one of the firm's third-party systems testing or a "tabletop exercise," as will be discussed below. There is no reason not to invite the whole board to each of the Risk Committee meetings at which cyber is discussed, unless that would stymie

honest conversations based on that particular board dynamic. Regardless, at least one such meeting each year should include the full board.

As to the substance of these meetings, the quarterly briefing should focus on changes and new events. It should include major changes to the company's risk assessment as to cybersecurity, to the policies and procedures for data security, and to the company's incident response plan. More ambitious boards can include updates on employee training, assessment of the cyber risk from third-party vendors, a discussion of penetration testing and other auditing, and a discussion and approval of the IT security budget. The IT security budget conversation is particularly important, even if only to make sure that a $100 fence is not being built around a $10 horse. The CISO should lead most of these conversations, with assistance from the GC's office and the CRO as needed.

What actual intrusions and breaches to report depends on the company. For a large company in retail or banking that sustains contained intrusions on a daily basis, a full accounting is neither possible nor warranted. Working with the risk management team, the CISO should consider developing thresholds for particular breaches, either by estimated cost to contain and mitigate, amount of data accessed, types of data accessed, or a qualitative measure.

A major complaint of corporate boards that have integrated cyber risk reporting is that the CISO's presentations are too detailed, and too much time and paper are spent by a CISO discussing each of the dozens of technical tools that he or she uses to monitor and safeguard the company's systems. If data will be relied on, it must be presented in an actionable way, either by comparing activity quarter by quarter or by proposing a change to allocation of funds and time and showing why that allocation is justified. The board's role is not to understand what the various tools are and what they are reporting, but to understand what the CISO is asking them to do with what the tools are reporting. In sum, the CISO needs to say what has changed in terms of risk and what has changed in terms of budget.

If management uses consultants on an annual basis, an ongoing basis, or for special projects such as stress or penetration testing, management should consider having them attend a committee meeting and allowing the directors to ask frank questions of them. Many such consultants are practiced speakers, with a range of experience across a company's industry and across various industries.

And, whether it is the CRO, CISO, or a consultant, management should be mindful of bridging the gap between its frame of reference and vocabulary and those of the directors, as not all presenters to a board are created equally in cooking technical information into digestible chunks. Some companies have had success when the GC or other in-house lawyer conducts a direct examination or a deposition-style interview of the CISO or consultant, in front of the board. What results from this guided interview is that those individuals end up communicating the issues such that the board can understand. It is also then the in-house lawyer who asks the "simple" follow-up questions that many directors might have, but would be reluctant or embarrassed to ask otherwise. Done with tact, this technique can also calm the CISO or consultant so that they can focus on giving the best information possible.

Of particular importance to engaging the board are interactive exercises, which can take the form of a "tabletop." Sometimes called "wargames," these exercises can simulate a breach either at the company or at a fictional, similar company, and walk through what would happen, who would make the decisions, and what the consequences would be. Considering the demands on board time, particularly at meetings, interactive components are an effective exercise to show the lifecycle of a breach, tailored to the particular company, in such a way as to draw the directors out so that they ask specific questions about the company's own preparedness. The authors of this paper have participated in such sessions with a cross-section of industries and government and military personnel, and have learned through those experiences that there is no better way, apart from living through an

actual breach, to move a director from disinterest to engagement on this topic.

For the lead cyber director, it may make sense for there to be additional meetings throughout the year to cycle through others in the company who are critical to pre-breach planning and post-breach response but who do not attend the periodic committee meetings. These extra meetings might include media relations, compliance, government relations, and others whom the lead cyber director should not be meeting for the first time during a crisis. These cross-department round tables, with only one director present, provide an easier give-and-take outside the formality of a board meeting. This is similar to how the Chair of an Audit Committee will have more interaction with the accounting firm's engagement partner, the CFO, the Chief Accounting Officer, and the GC, and their teams, than do the other members of that committee. This also takes into account that board meetings are short on time and long on content, and that the lead cyber director presumably would be willing to put in extra hours for a stimulating meeting with high-level management on a key issue.

Finally, while the Risk Committee is the best place to lodge cyber responsibility, there is one significant responsibility that will remain with the Audit Committee, namely, risk disclosures related to cyber in the Forms 10-K and 10-Q. Guidance from the SEC has placed emphasis on risk factor disclosures that take into account information from past attacks and the probability and magnitude of future attacks. Through comment letters, the SEC is showing an increasing emphasis of disclosure of cyber incidents, even if not material. Whether and how to disclose a major cyber incident in a Form 8-K is an issue that is highly fact-dependent, and it will be the Audit Committee, in consultation with counsel, that also makes that decision.

3. Record Keeping

The importance of documentation is twofold. First, it creates routine and discipline to ensure that these meetings occur and that the topics are hit. Second, it allows quick compliance with regulatory requests or responding to shareholders who might be contemplating a suit or a demand letter.

For later regulatory actions and updates, it is important to "show your work." In other words, management charged with keeping board records should document the fact of the meetings. This includes keeping complete minutes and comprehensive pre-meeting packets, as well as retaining consultant PowerPoints and agendas, and the results of stress testing. If there are tabletops or other trainings, consider documenting those or providing certificates of attendance. This is not unlike documenting acknowledgements of employee training. These materials should be kept by the corporate secretary along with the other board records. Duplicates or a log should be kept of all cyber-related briefings, independent of the main record, so that in the event of an investigation into a cyber incident, a complete picture for the board's cyber readiness can be passed across the table to a regulator on short notice.

The GC's office should consider, if using the privilege because of the sensitivity of any particular investigation or engagement, going paper-light on the substance of the briefing to the board or the committee. The records in such a case could instead capture the time spent and who attended.

D. The Search for Standards

There is no set national or international standard for how a board should oversee its information security controls. There are a number of general cybersecurity frameworks that are worth examining, but one is worth particular mention for its suggestions on dividing responsibilities between the board and management. The International Organization for Standardization (ISO) has published guidance on information security that includes delineation of the role of executive management and the board. ISO/IEC 27014 provides concepts and principles for the governance of information security, "by which organizations can evaluate, direct, monitor and communicate the information security related activities within the organization." This standard covers information security, which includes physical-

environment security and paper-document security in addition to IT controls. This aggregation makes sense because physical access to a server is often much easier than hacking that same server remotely, particularly for an insider; and there is no need to hack a password when it can be retrieved from the note card in the administrator's top desk drawer.

The role of the board in this framework is to establish the corporate risk thresholds, allocate adequate resources, ensure that compliance and legal obligations are met, report out to the shareholders, and order independent reviews and audits. Management's role is to align information security to support the business objectives, develop a security strategy and overarching policy, determine metrics to measure the security program, and then inform the board of key security issues. This is a classic risk-based approach, and one that could be deployed for any number of risk matters facing a modern company.

E. Mid-Breach and Post-Breach Reporting

Finally, a word is necessary about what to do after a breach. For insulation from regulatory scrutiny, for inoculation from a lawsuit alleging breaches of other duties of oversight, and, generally, to get the best advice and guidance from the board, management should be sure to attend to post-breach communication with the board. Some of the early-filed derivative cases have alleged not only inadequate preparation but also missteps in the post-breach investigation period, including that the board did not act quickly enough either to stop the ongoing damage or to make disclosures.

Not every breach needs to be reported to the board. As noted above, management should set thresholds for board reporting, in consultation with the board. This is particularly important for frequently or continually breached companies. Management should report first to the lead cyber director, in any event, for guidance on the format of the briefing of the larger board or committee and in cases near the margins of the predetermined thresholds.

When management is reporting to the board or the committee charged with cyber issues, it should actually have something to report; the first full briefing needs some content to it. Once the initial investigation is underway, management should report often to the board, if only through phone updates. If at any point the nature of the breach is such that litigation or a regulatory investigation is likely, as will be the case with most breaches large enough to convene special meetings, the GC or outside counsel should be involved to protect this reporting under the privilege. The company can always waive that privilege later if necessary. Management should at this time allow direct, unfiltered access to the company's consultants and their work product.

When the breach is resolved, and the plan is in place to deal with the legal, public, regulatory, and business fallout, the board, through the cyber committee, should be involved in the post-mortem. This will include a determination of why the event happened, what could have prevented it, whether and how the company's existing controls worked to mitigate or limit the damage, and whether the right employees and third parties were involved during the immediate aftermath. This review should lead to an evaluation and revision, if necessary, of the company's risk assessment, data management policies and procedures, and breach response plan.

* * *

John E. Clabby and Joseph W. Swanson are attorneys in Carlton Fields's Tampa office, where they represent companies, executives, and directors in investigating data loss events and in securities and corporate governance litigation, as well as in white collar criminal matters. Both are former criminal Assistant U.S. Attorneys and Computer Hacking and Intellectual Property ("CHIP") prosecutors. Clabby leads the firm's securities and derivative litigation practice group. Swanson co-leads the firm's data privacy and cybersecurity task force. Clabby can be reached at jclabby@carltonfields.com. Swanson can be reached at jswanson@carltonfields.com. *Clabby and Swanson would like to thank Tampa appellate associate Nicholas A. Brown for his assistance with this white paper.*