The Metropolitan
# Corporate Counsel®
National Edition www.metrocorpcounsel.com
Volume 22, No. 9  September 2014

# Cybersecurity In Its Several Aspects

*The Editor interviews **Francine E. Friedman**, Senior Policy Counsel with Akin Gump Strauss Hauer & Feld LLP, who brings a decade of government affairs and lobbying experience to the firm; **Michelle A. Reed**, Partner, who focuses on complex civil litigation matters with an emphasis on representing public companies and their officers and directors in securities and privacy litigation; and **Bob Huffman**, Partner, who heads the firm's government contracts practice and who also is leader of the firm's National Security Industry Group.*


Francine E. Friedman


Michelle A. Reed


Bob Huffman

**Editor: Francine, please tell our readers about your background in government affairs and lobbying, including your data-protection practice.**

**Friedman:** During my high school and college years, I had various internships on Capitol Hill, mostly on the political fundraising side. My first job in that space was as an intern at the Democratic Senatorial Campaign Committee. I attended law school with the intent to practice law, which I did as a commercial litigator for three-and-a-half years. I found my clients often faced not bad facts, but bad law. In attempting to find a "fix" for this dilemma, I became interested in policy matters to which I subsequently switched. Essentially, we help to craft policy, help to impede bad policy and work with the administration and others to see that the right policies that serve our clients are moving forward. In my data-protection practice, I have represented a large data broker in the past as well as entities that collect, use and share large amounts of data in various ways.

**Editor: Why are privacy, advocacy and civil liberties groups concerned about sharing cyber threat information with the government?**

**Friedman:** There's a natural inclination to be concerned when private companies are required to share information with the government, and the public may feel that there is no opportunity for those about whom the information is being shared to rebut that information.

**Editor: As I recall, there have been several legislative attempts to get something like the Cybersecurity Information Sharing Act (CISA) passed, which were defeated by these groups.**

**Friedman:** They certainly voiced their concerns and played a role in seeing that some of these proposals did not become law.

**Editor: Congress has been examining and talking about various pieces of legislation related to privacy, data security and cybersecurity. What trends are you seeing? What should someone in the boardroom be concerned about (or encouraged by) with these developments at a federal level?**

**Friedman:** We're seeing a lot of interesting trends, one being that Congress is trying to figure out what can be done and where there is consensus, especially on the data security side rather than privacy or cybersecurity. Data security really deals with how you maintain and secure the privacy of information and what you do if there is a breach, as opposed to privacy, which generally is concerned with who gets to see your information. Data security protects information from unauthorized access. A determination of who should have access to the information is more of a privacy issue, and cybersecurity is a hybrid between the two – preventing people from getting information they should not have as well as letting the government know there has been a breach and doing what is needed to prevent one. Cybersecurity is often talking about more sensitive information that has a critical infrastructure component as opposed to data security, which is more often related to consumer information or personally identifiable information such as Social Security numbers and bank account information.

In terms of safeguarding information, there are various different data security regimes set up by the states because there is no federal standard by which companies have to secure data and no federal breach notification regime. Breach notification is something that creates a challenge for the vast majority of companies that span multiple states. Companies that suffer a data breach must determine the laws of each state in which the breach occurred or may have impacted somebody, figure out whether or not notification is required and also understand conflicts with laws of other states.

Industry groups may be coalescing around the concept of a uniform, federally preemptive data security breach notification standard. There has been some movement towards that, but, unfortunately, Congress has so many things that they're dealing with, they haven't been able to reach consensus despite breach after breach.

In the privacy area, there are many dif-

Akin Gump
Strauss Hauer & Feld LLP

***Please email the interviewees at ffriedman@akingump.com, rhuffman@akingump.com and mreed@akingump.com with questions about this interview.***

ferent positions and no coalescing around one concept. Some think that you need to "opt in" to have your information shared between parties, while others think you need to "opt out" if you don't want it shared. There are those who think the only thing we need is to make sure that the FTC enforces privacy policies – if you state a privacy policy that you actually practice.

The boardroom's first concern is this: What kind of information do we collect? How do we store, secure and share that information? What have we told people we will do with that information, and are we doing what we told people we would be doing with it? Many companies have tasked one individual with the responsibility to gain the best sense of the data flow because there is already action in many states on the privacy issue. On the data security side, almost all states have data security regimes.

**Editor: Why has social networking allowed for a greater opportunity for cyber predators to enter data bases with malware and corrupt files or steal information?**

**Friedman:** My initial thought on this is that a lot of people don't really pay attention to what they're agreeing to when they are hopping around on the Internet, exposing themselves to cyber predators, allowing those predators to learn more about them. Those predators can actually go in and commit identity theft because you might have a password that is easy to figure out, or your privacy settings are not very secure.

**Reed:** The only thing I would add is that a lot of the social networking is done on mobile devices, and mobile devices are the single most dangerous touch point for companies in terms of securing their data. There are significant data breaches that can happen through mobile devices.

**Friedman:** There have been great developments in terms of being able to build firewalls within mobile devices in separating work-related information and personal information, similar to having two devices in one.

**Editor: Do you support the FTC's report that Congress act to support legislation that gives consumers more control over how their data is collected and used? The report recommends the creation of an online portal where consumers can view what data is being collected and "opt out" of data collection or correct errors in their profiles. What demands would this make on data brokers?**

**Friedman:** In full disclosure, I have represented data brokers in the past, and my opinion is going to be impacted by my experience. The correction of harmless errors (such as consumer preferences) in your profile would create a huge demand on data brokers with a cost that would outweigh the benefit.

I do not support the suggestion that Congress give consumers more control over how their data is collected and used but, instead, believe that the industries that are collecting and using that data should be open about what they're doing and how they're collecting and using information. This will allow the consumer to make that choice whether or not to engage with the business. I think industry can work out a solution once it becomes clear what consumers like or don't like and their preferences begin to be shown. Congress should not rush to put in place a regime that could ultimately be unworkable, doesn't keep up with changing technology, doesn't give consumers what they want or drives up costs.

**Editor: What are your views on the recent ruling of the European court regarding the "right to be forgotten"?**

**Friedman:** I think that it's one that we should watch closely in the U.S. and see how it plays out. We should see what kinds of requests are being made and whether or not there's cost-benefit data. There could obviously be some instances in which it would make sense to ask that search results not bring up things that should not be found. It may be good for the U.S. that this process is being tested in Europe to provide us with more data, allowing us to see how it works in practice.

**Editor: Should industry look to government for protection against cybercrimes or should it take full command of instituting its own protective measures, such as appointing a chief privacy official or introducing malware scanning processes?**

**Friedman:** Private companies should certainly take their own protective measures. I don't think government is really capable of keeping up with cyber criminals. The most you should look to the government would be for some sort of baseline that would potentially be a safe harbor – if you did certain things, then you wouldn't be held liable if there was a breach.

**Reed:** I agree; companies in different industries have different concerns and security risks. The security risk of a defense contractor is going to be different from the security risk of a retailer. That is why you have industry standards like PCI DSS and why the defense industry has its own standards. Industry self-regulation is key. Government definitely could have a central role on certain issues, such as data breach notifications. We have a mixed bag of up to 47 different state laws governing when, how and in what form you need to make a data breach notification. Some sort of federal centralization would decrease transaction costs for companies nationwide and would ultimately result in more predictability.

**Editor: Bob, please tell our readers about your practice area.**

**Huffman:** My practice area is government contracts. My specialty within this area consists of the allocation among contractors and the government of the risks and responsibilities for compliance with government regulations and contractual requirements. Our group has increasingly been focusing on compliance issues and investigations, including cybersecurity compliance issues.

**Editor: Why do cybersecurity concerns for the government contractors, especially in national security sensitive industries, such as aerospace, defense and technology, require superior vigilance against cyber attacks?**

**Huffman:** There are many reasons. The first is the sensitive nature of the information they have. For example, the Joint Strike Fighter Program has been targeted by foreign government cyber espionage groups. Second, many contractors are responsible for the government's own cybersecurity efforts and, therefore, need state-of-the-art practices for protecting against cyber intrusions. Third, many of these companies are also commercial cybersecurity-solution providers. Fourth, these contractors often have personal information about government employees. Finally, because these contractors have their own confidential data and labor force with personal information, they have to deal with cyber issues from a security standpoint, a trade secret standpoint and a privacy standpoint independent of their contractual requirements.

**Editor: When there is a breach, is the penalty more severe for these contractors?**

**Huffman:** Yes, because it includes the contractual and the compliance penalties that accompany government contracts.

For example, there is the False Claims Act (FCA), which has treble damages and penalties. There will be a growing number of FCA cases, including cases bought by *qui tam* relators, alleging that a contractor obtained a contract or billed for work while not in compliance with cybersecurity requirements. One of the big issues for government contractors under the FCA is whether they are in reckless disregard of standards for compliance with the new National Institute of Standards and Technology (NIST) framework standards for cybersecurity (more than 50). Prime contractors and upper-tier subcontractors will have to impose these standards on their subcontractors. This may come as an unwelcome surprise to many small businesses and commercial contractors**.**

**Editor: You have experience as head of Akin Gump's National Security Industry Group. Who are the members of this group? What is its overall purpose?**

**Huffman:** The group includes Paul Butler, head of our litigation group in DC, who has a national security background in DOD as well as prosecuting terrorist cases as an assistant U.S. attorney; Scott Heimberg, my partner in government contracts, who is very knowledgeable about national security clearances and the apparatus for controlling classified information; and Tom McLish, another government contracts partner. The group also includes several associates who have worked on the national security side.

The purpose of the National Security Group is to advise clients on contractual and other requirements and liabilities that are being imposed both by the government and by other contractors.

**Editor: Is it possible to obtain insurance against unauthorized use of information?**

**Huffman:** The government is largely self-insured, which means when it contracts with its contractors, it agrees to immunize them from certain kinds of liabilities or damages. For example, the FAR Government Property Clause says that if a contractor damages or loses government property, it is not liable for damages except under certain circumstances. If there is a loss of technical secrets in a government program, is that a loss of government property? There'll be plenty of disputes over these kinds of questions because the clauses weren't written with cybersecurity in mind.

**Editor: In protecting your privileged information, has the firm also adopted the framework proposed by the NIST?**

**Huffman:** Yes. We implement these standards to protect our client information, using encryption in many cases. The firm does a lot of international trade work, especially for aerospace companies, that requires protection from sharing this information with foreign offices because that information cannot be distributed to a non-U.S. person.

**Editor: How can your corporate clients best protect themselves against a cyber attack, either by outsiders or by employees and other "insiders"?**

**Huffman:** That's really where the technical issues come in. We are not experts on the technical side, so I'm not qualified to say this vendor's software is the best tool there is, and that's what you should use. We counsel clients to ask their IT folks to study the NIST requirements and compare them to the software they are using.

**Editor: Is there anything more that I should have asked you?**

**Huffman:** One question often asked is: What is a cybersecurity lawyer? With few exceptions, cybersecurity is not a separate branch of law. It affects many existing disciplines. What you do in cybersecurity depends on whether you're a government contracts lawyer, an SEC lawyer, a corporate lawyer or a labor lawyer. So far, I haven't seen a law firm that has a cybersecurity practice that is anything more than a collection of people who are looking at cybersecurity aspects of various industries. What it amounts to is a collection of best practices for each of the industries involved. It is a combination of tort and contracts law that involves indemnity and liability issues in a variety of industry settings.

**Editor: Michelle, please describe your practice and the way it encompasses cybersecurity risk assessment and privacy litigation.**

**Reed:** I'm a litigator with a focus on defending companies and officers and directors in class actions, merger and acquisition litigation, derivative suits and SEC and other investigations, including those relating to data breach, cybersecurity assessments and data privacy compliance. I advise companies on data breach risk mitigation to decrease their exposure in the event of a breach. Often, having an attorney involved with the forensic investigation may provide some degree of privilege protection to the internal investigation surrounding a data breach.

**Editor: Do cyber attacks target particular industries?**

**Reed:** Based upon the press coverage, you would think that retail would top the list. However, the amounts spent on compliance are the greatest in defense companies, followed by utilities and energy companies, financial services and education. Retail is at the bottom.

**Editor: Should every company have a company-wide cybersecurity risk-management and data-protection program? Should the board be kept apprised of such a program?**

**Reed:** Absolutely, to both questions. Every company should have a company-wide cybersecurity risk-management and data-protection program. It just needs to be tailored depending on the size of the company and its industry. Companies will all want to do the basics, which include: identifying what legal requirements apply to them, mapping their internal processes, identifying data that needs to be protected and listing foreseeable security risks in their particular industry, implementing measures to prevent employees from accessing information not needed for their jobs, training employees on basic security measures and detecting unauthorized access to protected data. Loss of data through employees is one of the most significant risks that companies face.

As for boards of directors, I can't emphasize enough how important it is for them to be involved. SEC Commissioner Luis Aguilar outlined some expectations for directors of public companies to manage cybersecurity risk. He suggested that they evaluate the NIST standard and that they consider structural changes to the board to focus on cyber risk management, making sure that a director or a committee is engaged in this effort. He suggested that everyone prepare for a cyber attack since this is a risk that every company will face. Ultimately, the standard for the business judgment rule and fiduciary duty is different where the board acts and exercises its business judgment versus cases where the board fails to act and doesn't exercise its business judgment.

**Editor: Which governmental authority in the U.S. has taken the lead as principal federal regulator? On what basis has it assumed the role of a protector? What other agencies have drafted rules to alert companies to risk of identity theft?**

**Reed:** The Federal Trade Commission has taken the lead role in the cybersecurity and the data-protection spaces. As opposed to specifically regulating one industry, the FTC regulates deceptive and unfair trade practices generally. It has characterized a company's failure to adopt appropriate cybersecurity measures as an unfair practice and failure to properly communicate its practices as a deceptive trade practice to the extent it is not following its pronounced policies. The FTC has most definitely taken the lead in this, but there are regulators all across the board that are concerned.

The SEC also may get involved. Reportedly, it is now investigating Target for failure to provide investors with a proper notification of its cyber breach. Once you trigger scrutiny by the SEC, then every time you have another problem you face greater likelihood of future penalties.

**Editor: What role do the states play in protecting consumers against deceptive trade practices?**

**Reed:** The states also play a significant role in protecting consumers. The dollar amounts recovered by the states are significant, but perhaps not as significant as might be typical in a securities litigation suit. For example, the TJ Maxx Company had a data breach of 90 million records exposed, resulting in a $12.25 million settlement. You also face ongoing regulation and multifaceted negotiations with different state attorneys general when you have a data breach.

**Editor: What failures on the part of companies might draw the attention of the FTC?**

**Reed:** One example is the failure to adopt and implement a comprehensive cyber breach response plan. Wyndham Hotels is still in litigation with the FTC over its data breaches. They didn't just have one data breach; they had three data breaches, with hackers breaching their system three times. The FTC alleged that Wyndham misrepresented its privacy protections, failed to adopt cybersecurity risk management procedures and failed to properly implement a comprehensive cyber breach response plan. Although the Wyndham case has not concluded, the FTC settlements typically will not only provide for a fine, but also will include a consent order requiring a company not only to implement a comprehensive, information security program, but also implement independent, third-party security audits every year for 20 years.

**Editor: To what extent is a company exposed to liability if it fails to timely discover an intrusion or notify those affected?**

**Reed:** Companies are exposed to significant liabilities from failure to give timely notification of a data breach. Target recently announced that its cost estimate for its 2013 data breach is more than $148 million. This includes the cost of an internal investigation and defending class action litigation and defending the many separate actions that were filed against Target. It also faces derivative lawsuits against the board for breach of fiduciary duty, a DOJ investigation, an FTC investigation and now a formal SEC investigation. Although I don't know the details of Target's cybersecurity and breach response systems, I do know that it's a good example of the risks that one faces and why one should be prepared with countermeasures. I recommend that clients document every step that they took before and after a breach occurs so that they will be able to say that they did everything they could to protect against it and to mitigate its effects.

**Editor: Is there a body of case law developing with respect to cybersecurity and cyber crimes? What are the key issues in both criminal and civil violations? What remedies are being sought in civil cases and what criminal penalties are being imposed?**

**Reed:** With cyber crimes issues, the perpetrators face criminal actions for introducing malware, committing computer fraud, money laundering or conspiracy. Identity theft is a crime within itself. When you look at the issues, those are pretty much meat-and-potatoes sorts of criminal cases. Some have gone to prison for years for cyber crimes.

On the civil side, the jurisprudence is in its infant stages. My advice to companies is they need to look very closely at their industry standards and the NIST standards, documenting their due diligence so they can say we followed up on this, and we did that. The SEC has issued significant guidance on what needs to be disclosed with respect to cyber risk. I usually tell companies, "It's a lot easier to disclose on the front end the risk of a cyber attack than to face a securities class action later."

**Editor: The question often raised is, why is not the perpetrator of cyber crime brought to justice rather than the victim?**

**Reed:** That's a great question. I don't think it's an either-or situation. Cyber criminals are being pursued and prosecuted, but companies that are targets of a breach are also being pursued by federal regulators, shareholders and identity theft victims. That system recognizes that the credit card company is in a position to develop internal fraud detection controls. The risk is allocated to the company in an attempt to force the company to mitigate risk by improving its internal controls to identify fraud early and to prevent loss.