METROPOLITAN
CORPORATE
COUNSEL®

JULY / AUGUST 2015

WWW.METROCORPCOUNSEL.COM

MCC INTERVIEW: Michelle A. Reed / Akin Gump Strauss Hauer & Feld LLP

Buying Cyberinsurance Helps Uncover System Weaknesses

Michelle Reed talks about the cyber threat landscape and what companies need to know about insurance and risk management right now.

MCC: Let's start big. What are the most pressing cybersecurity risks facing corporations today?

Reed: The biggest risk in my view is the head-in-the-sand mentality of too many companies, wherein companies acknowledge the issue, hand it off to the IT department, and then check it off the list. In a dynamic threat landscape where threats, if realized, can affect not just your company but also your business partners and customers, relegating the management of such risks to IT rather than giving them the highest level of attention is our most pressing cyber peril. We can see the beginnings of change, for example, in the hiring of third parties to do gap analyses. But true risk assessment – the 10,000-foot view that allows you to see the ultimate risks created by data flows – isn't happening as often as it should.

MCC: In advising companies on these types of issues, who do you want to be talking to?

Reed: A lot of the risk management is falling on the doorstep of the general counsel, COO and CCO (chief compliance officer). That's where I've seen the most engagement as they are tasked with developing internal policies and procedures to comply with the latest government regulations and agency advisories. But I *want* to be talking to boards of directors as well. My recommendation for boards is to have a cybersecurity review committee, whether freestanding or within the audit committee, that includes members who have the technical expertise to issue-spot.

Michelle A. Reed
Partner at Akin Gump Strauss Hauer & Feld and co-leader of the firm's cybersecurity practice.
mreed@akingump.com

You don't have as much control over mobile devices, especially with a BYOD program.

MCC: How has the threat landscape changed in recent years?

Reed: There are different types of attacks and players. Lately, the high-profile data breaches are by nation-states, such as the government of North Korea's cyberattack on Sony Pictures. Then you have organized criminal groups, usually operating in Eastern Europe or East Asia, that typically target payment-card-type information. For purposes of sabotage, issue-oriented groups hack into the websites of companies that engage in animal testing or manufacture food with GMO (genetically modified organism) ingredients. Garden-variety hackers exist worldwide and are a significant threat. A staggering amount of personal information has been pilfered via phishing, which is an increasing threat given the sheer number of these thieves. They send what look like legitimate emails to induce unsuspecting recipients to give up more information. For companies facing this threat, employee training is critical because the best defense to phishing attacks is user knowledge and distrust.

While advances in vulnerability assessment and security governance have greatly mitigated risks, no company is immune to zero-day attacks, which exploit holes in software unknown to vendor and user. The company is literally blindsided. Examples include the sophisticated hacks on health insurer Anthem/Blue Cross Blue Shield, involving 80 million customers, and on the computer system of the U.S. Office of Personnel Management, which compromised the personal data of 4 million current and former federal employees.

Since there are no defenses to zero-day attacks, the critical factor is a company's ability to respond and quickly recover. Do you have your incident response plan in place? Do you know what data you hold and your notification obligations in the event of a breach? Do you have a relationship with law enforcement that ensures the right people will be brought in? Do you have the right people in place to identify the source of the breach and shut down the vulnerability?

In my experience, some companies (usually tech) are all over these situations,

but most are not. Their IT departments are good, but they need cutting-edge resources when the unexpected happens. Having the right plan in place and practicing it beforehand is key. While some of our clients are doing that, the majority are waiting for a major problem to happen before they invest that kind of money.

MCC: What's happening on the litigation front? Are there any cautionary tales from recent cases?

Reed: In terms of instructional value, topping my list are the Target lawsuits stemming from a massive data breach in 2013, which in round numbers involved stolen credit/debit card information from 42 million people and personal data stolen from 61 million people. Target settled the consumer class action for more than $10 million and is close to settling for about twice that amount with the bank card companies to cover costs of reissuing millions of credit and debit cards.

In this case, Target's IT department allegedly ignored red flags, didn't follow up on warnings and never implemented the procedures it had already deemed necessary. Beyond the legal issues surrounding consumer standing and proving damages (there being no injury in fact), the optics of the situation – a company not responding to clear signals – complicated efforts to get rid of the case on motion or settle for nuisance value.

The takeaway? Be vigilant. Everyone understands that breaches are perpetrated by third parties, but the public also believes companies have a profound responsibility to protect private information – and woe to those who take that responsibility lightly. To the extent you have warning systems in place, adhere to them. And to the extent you've had a gap analysis done, make best efforts to fill those gaps.

MCC: Is there some kind of a cost-benefit analysis going on in terms of how much money a company is willing to invest in the problem of data protection?

Reed: It's largely unspoken that some companies perceive the need but are not prepared to make the necessary investment. There are also strategic reasons for holding off. For example, I advise companies not to do gap analysis right after a breach occurs because it creates a record that's not helpful. Instead, they should get through the breach, shore up their systems and then do the gap analysis.

And the perennial question is how to budget for a process that is legitimately daunting and difficult to control. Simplifying the process essentially requires assessing the available cybersecurity frameworks – NIST, CSC, COBIT or ISO standard compliant – to determine which one is most applicable to you. Get your IT department involved and then just march through the steps. Yes, there are different levels of risk protection, and small companies will not be able to afford the same protections as multi-billion-dollar enterprises. But a scalable framework like NIST at least enables you to look at all aspects and measure performance against your peers.

That said, everyone should look at certain controls, such as password protection, access limitations, proprietary encryption and effective policies on data retention and disposal. You also want to perform risk assessments on all software products and conduct top-notch employee training that includes exercises to ensure full awareness of necessary protocols.

MCC: Are any risks unique to mobile technology?

Reed: Absolutely. Fundamentally, you don't have as much control over mobile devices, especially if you have a BYOD (bring your own device) program. Part of protecting your own house is knowing how it's built, what materials went into it, the level of perimeter security, its unique wiring and what's been patched up. Introducing mobile technology forces companies to deal with many unfamiliar houses that are constantly changing with the addition of new apps, and with owners who bridle at any attempt to restrict their activities.

Knowing that, you need to be aware of what devices are in your system and ensure that systems are properly locked down. The rules need to be clear: use devices in a secure way, or access to the system will be blocked.

MCC: One of your areas of expertise is advising clients on insurance and particularly cybersecurity policies. Give us your view on the important issues here.

Reed: Before the advent of the cyber policy, companies brought claims under the property damage clause or the personal or advertising injury clauses of their commercial general liability (CGL) policies. Then certain cases came out – *Recall Total* was an early one in 2012 – holding that there was no coverage under such policies. To remove this risk of claim denial, the industry created separate cyber policies (while adding exclusions for cyber damages in CGL policies), leaving companies with little choice but to buy the new product.

When shopping for a cyber policy, determine whether you need first- or third-party insurance. Ask yourself, "What am I worried about? Someone suing me because of a data breach? Or the cost of notification and mitigation in the event of a security breach?" Probably, you're worried about both, and most policies offer both. First-person insurance covers direct loss and out-of-pocket expenses incurred by the insured. Third-person covers liability incurred from harm actually caused by the insured. So if you're the target of a consumer class action for failing to properly secure your systems, you would need third-party coverage.

You also want to look at the liability limits, a tricky area because the market is changing. Two years ago, it was a total buyers' market as insurance companies scrambled to place policies and get an edge in the cyberinsurance space. Clearly, today's market is not as soft. Retailers will need a greater amount of coverage and will pay higher premiums because of the types of data they hold. If payment card data is breached, the notification cost will be significant.

When handling a data breach for smaller clients who tell me that the breach was "very small and of limited duration," I invariably have to remind them that the notifications still involve fifty states and sixteen countries!

MCC: What's your advice for companies in assessing their insurance needs and risk factors?

Reed: In practical terms, liability limits should be determined based on what's realistic; they will be different for an investment fund versus an online retailer. Be aware of exclusions, and make a conscious decision as to whether you can live with them. Evaluate coverage for acts by

third parties. Are you covered if a benefits administrator has a data breach that compromises the personal information of your employees (and their dependents)? Read the policy carefully, and don't rely on an indemnification provision in your third-party contract.

Third-party threats are tremendous. In fact, at least 50 percent of the breaches I work on each year are caused by third parties that either held or had access to my client's data. Whether it's a breach of my client's system (through a third party) or a breach of a third party's system that held my client's information, the notification obligations are on the client. Assessing third-party risk is a big job and only adds to the already hard work in doing an adequate assessment of your own systems. My advice to clients is to look closely at what data is going to the third party and impose significant restrictions on access.

The more personal data you hold and make accessible to a third party, the more you should evaluate its system controls and whether it conducts sufficiently rigorous audits. And if you're a retailer, don't make the mistake of ignoring third parties that may not hold your data but can somehow hit your points of sale, rendering you vulnerable to the security of their system.

Make sure a third party has its own cyberinsurance policy because this can offer protections you can't get from your own carrier. For example, a third party's policy will often cover the loss of your intellectual property. If you lose your own IP through a hack, your policy won't cover that loss.

Finally, the process of obtaining cybersecurity insurance can help a company improve its systems by identifying vulnerabilities. I've seen it happen every time in working with my clients. And the carrier usually plays an ongoing role in ensuring that such systems are kept up-to-date – a real added value for clients.

MCC: Talk about any recent guidance from regulatory agencies.

Reed: In April, the SEC put out high-level guidance for investment management firms, emphasizing the need to know the nature, sensitivity and location of information that you collect. It encourages you to know what internal and external threats you face, what security controls and processes are currently in place and what would be the impact if they were compromised. And it asks you to evaluate the effectiveness of corporate governance structure in helping you manage cybersecurity risk.

All companies should look at April 2014 guidance that came out of the SEC's Office of Compliance, Inspections and Examinations. The risk alert contained 28 sample exam questions – essentially geared for investment advisors but really applicable to any company – that provide an overview of important concerns and questions companies should be asking internally.

This guidance is accessible to a general counsel or chief compliance officer, meaning you don't have to be tech savvy to *ask* the questions. When a breach involving personally identifiable information occurs, the obligation to notify the world is a given. But when the regulators come knocking at your door, showing that you followed the agency's advice will make it more difficult for them to find your data protection subpar.

MCC: To wrap up, would you tell us about Akin Gump's cybersecurity initiative?

Reed: Absolutely. Cybersecurity issues vary widely by industry and type of business, so we created a powerhouse cross-practice team that includes cyber specialists working with attorneys from various practice groups to develop analysis that helps our clients get ahead of the game.

Our team regularly helps clients develop incident response plans, which many companies outside of retail and healthcare don't have, but should strongly consider. Disaster recovery plans won't fill the bill, and incident response plans are not cookie-cutter: what's going to be effective at company A is not going to be effective at company B. Once a plan is created, we test it with different scenarios.

When the worst happens, we help clients work with forensic investigators to conduct internal investigations, identify the source of the breach and develop a remediation plan. We make sure that notifications are made to law enforcement, affected consumers, consumer reporting agencies and, as needed, state attorneys general and other agencies. When consumer or insurance-related litigation arises, we help clients navigate that process.

In broadest terms, vulnerabilities baked into our nation's cybersecurity systems for years have left us dangerously at risk. As a nation, we are woefully behind, and the hackers are light-years ahead. We're going to have to run full sprint for a very long time to catch up, and Akin Gump has made a strong commitment to joining this race. I'm hopeful that companies will recognize the need for investment to improve systems and meet compliance obligations. For my own part, it's been a busy ride in the cyber space, and I'm happy to be on it.