JUNE 2015

Legaltech® news

An ALM Publication

The Art Of CYBERWARFARE

As data breach liabilities escalate, general counsel must address a minefield of cybertroops, weak partnership loops and regulatory groups.

BY CHRIS DIMARCO

Cybersecurity is at a crossroad. No longer resigned to the confines of server rooms overseen by information technology, decisions regarding the protection of data have been forced into the boardroom by events that include breaches at main street businesses and revelations of clandestine government hacking activities.

In an interview with Legaltech News, Google Inc. General Counsel Kent Walker explains: "You only need to read the news—from credit card theft to photo hacks to widespread email breaches—to see the increase in cybercrimes by vandals, criminal hackers and even state-sponsored entities. And those attacks are becoming more sophisticated, even as people grow more wary. Our growing use of multiple connected devices improves productivity, but also expands the attack surface."

Legal teams may be prepared to navigate compliance and risk issues, but the complexity of cyberthreats—not to mention the unpredictable ways damage wrought by them can ripple—demands new partnerships and resources. And while corporations will never get ahead of the strategies employed by cybercriminals, the partnerships engendered by the challenge can make available defenses stronger.

KNOW YOUR ENEMY

In the "The Art of War," Sun Tzu wrote, "If you know the enemy and know yourself, you need not fear the result of a hundred battles." That wisdom holds true today in the cybersecurity space, yet while legal teams may have an inkling of where they need to shore up their defenses, the threats are that much harder to know.

The lineup of malfeasants hoping to crash corporate gates is an evolving mélange of insiders, hackers, government-backed organizations, activists and criminals. Each year, Verizon's Data Breach Incident Report (DBIR) offers an in-depth look at the changing roster of usual suspects in the cybercrime field, along with an examination of the vectors used and the industries targeted.

According to the most recent DBIR, for the largest organizations in the world, cybersecurity events accounted for $400 million in damages and 700 million compromised records in 2014. The most common method used to gain access to records was through program errors, which accounted for 29.4 percent of the recorded incidents. Malware and insider misuses claimed 25.1 and 20.6 percent respectively. Surprisingly point-of-sale intrusions accounted for only 0.7 percent of recorded attacks, despite having made headlines in some of the most public data breaches of 2014.

While this information shows which types of methods have been used to gain access, it belies the diversity of bad actors responsible for such attacks.

FireEye, Inc., which offers advanced cybersecurity monitoring, defense services and security software to companies around the world, has played a significant role in the investigation and remediation of some of the most widely publicized attacks of the last three years. The company's intelligence indicates that, to date, over 95 percent of the world's top companies have already been breached but may not know it yet, and according to FireEye SVP, General Counsel and Corporate Secretary Alexa King, cybercriminals on the whole are growing in strength.

"The landscape is rapidly evolving with extremely sophisticated attacks through well-funded campaigns. From our perspective, it's a new level of organized crime and

Alexa King, SVP, general counsel and corporate secretary of FireEye, Inc.

PHOTOGRAPH BY WINNI WINTERMEYER

espionage. Today's attacks are advanced, stealthy, targeted and persistent, and those responsible are often unknown," King says.

Given that stealth is an underlying goal of cybercrime rings, a full view of usual suspects is difficult to come by. Anecdotally, however, there appears to be a trend: in May 2014, the Department of Justice indicted hackers with ties to the Chinese government for allegedly stealing trade secrets from nuclear and infrastructural focused organizations, and the North Korean government is widely held to be the source of December 2014's Sony Pictures data breach. In addition, groups like Anonymous, Lizard Squad and LulzSec, have been tied to hacking events motivated by vigilante justice, relying on a hidden network of skilled members to damage their victims.

"PERFECT SECURITY DOESN'T EXIST, BUT EVERY ORGANIZATION CAN LEARN TO BE STRONGER."

Brenda Sharton, partner at Goodwin Procter

Elaborating further on the mushrooming threat of organized cybercrime networks, King explains, "The reason we think about it as organized crime is that it's really escalated in sophistication from the solo hackers of years ago. These are nation states, they are organized criminals, and they are entities that are spending a lot of time and resources learning how to attack organizations. Their goal is sometimes financial, either directly or through non-public information they can use for financial benefit. It can be intellectual property, a nation state or organization may want to see the latest designs or innovations that your company is developing, for example. It's a heightened threat level with much higher risk for organizations and higher reward for cyberattackers."

KNOW YOURSELF

If knowing your enemy is step one in building a better cybersecurity defense, then knowing yourself is the critical phase two of that process. The legal team may not have historically had the technological chops to address cybersecurity liability itself, but it can find a number of allies both inside and outside of the organization to make the calls necessary to reduce business and legal liability resulting from data breaches.

"We rely on thousands of people across Google to provide security measures. That's just not realistic for most companies, but security is undeniably a cross-team discipline. You need technical engineering experts who can detect and protect against incidents. But it doesn't end there," Walker explains. "Legal, business and customer support teams all need to build cybersecurity into their work, including how they build services and work with vendors. Your CEO and board need to understand and buy into the company's approach, and GCs can help get this issue on the agenda."

As Walker correctly points out, many companies, including those outside the Fortune 500, are not sufficiently staffed to devote resources to the fight against cyberassailants. However, those companies still have options for accessing expertise.

"What we're seeing now is that companies may not have the robust and complex internal cybersecurity teams that are needed to address advanced persistent threats, but more and more are considering outsourcing that role to a third-party cyberdefense partner that can help them," King says. "Unless you have the time and resources to train experts internally, you may miss something."

In addition to the partnerships required to protect a company from cybersecurity risk, consideration must be given to the prevailing regulatory atmosphere in the U.S. Regulatory risk should also be considered in internal explorations of cyberdefense and strategy.

Brenda Sharton, a partner in Goodwin Procter's privacy and data security practice, has been a practicing privacy and cybersecurity litigator since the late 1990s. She's seen regulation surrounding data security evolve and how it's become a challenge for corporate legal departments that are victims of attacks.

As it relates to navigating the complicated regulatory environments, Sharton advises, "At the board level some of the things you may consider are having a component chief information and security officer, or alternatively engaging outside technical expertise when necessary."

Consulting experts that can offer benchmarking and auditing of regulatory and technical risks can provide experience when an actual event occurs.

"Perfect security doesn't exist, but every organization can learn to be stronger, and If you're learning from the experience of others, that's even better. Additionally, by facilitating open lines of communication to the board, you can ensure that things are caught early," Sharton adds.

As of yet, cybersecurity legislation creating a minimum bar of compliance across all sectors and industries has eluded passage in the U.S. Congress.. The patchwork of state

JESSICA RINALDI/GETTY; ASA MATHAT (WALKER)

laws and regulation is likely to prevail for some time, and with no safe harbor provided by compliance, cyberattacks carry an increasing legal and business risk for organizations

Take the findings of a recent Mayer Brown survey, for example. Researchers there sought to unearth the prevailing attitudes of corporate lawyers and executives surrounding cybersecurity. When respondents were asked to assess how cyberissues have increased the risk of lawsuits, 57 percent indicated that cyberrisk had a modest impact on litigation risk, and 63 percent agreed that the potential legal fallout from such events has now become a "cost of doing business."

King says, "If you think about some of those high-visibility breaches we've all read about in the past few months, we've seen among other things; stock price drops, shareholder suits, government investigations and even executive resignations. There's even a risk that private communications can leak. On the consumer end, customers can lose faith in your systems or your integrity as a company and if that happens, they will go elsewhere. The costs associated with those risks can be in millions or billions of dollars and loss of reputation and relationships with customers can be irreparable. In my mind, the legal and business ramifications are intertwined because as you experience business losses, you'll also experience potential legal exposure."


Kent Walker, general counsel of Google Inc.

And as if managing the challenges of reputation and regulation weren't enough, Walker reminds us that the legal team's involvement with vendors, law firms and other external organizations can also pose a risk. Insider misconduct was the third most common vector of attack for data breach, according to Verizon's DBIR, and as such, weak cybersecurity precautions within that network can manifest downstream for organizations.

"Your data is only as safe as the weakest link in the chain," Walker adds. "Given the sensitive materials handled by law firms, any firm should be using strong, cloud-based security, two-factor verification of access and other protective measures."

KNOW WHERE TO START

As has been stated many times about cybersecurity, it's not a matter of if a company will be attacked, but rather when. Breaches reported in the news are a small tip of a much larger iceberg, and traditional modes of defense have become antiquated in the face of new and increasingly organized dangers.

"THE FIRST PRIORITY IS THE TECHNICAL RESPONSE—BEING CLEAR ON WHAT HAPPENED."

With that in mind, legal department and organizations as whole must fill their cyberdefense quivers with a combination of technology, training and process management.

King says, "The critical issue is to fill the security holes that are left open , those left by firewalls, intrusion protection systems, gateways and antivirus software. For example, at FireEye we've invented a purpose built virtual machine and threat prevention platform that differs from traditional signature based security. If you think back to the era of Bonnie and Clyde, there were wanted posters on the wall for the bad guys, so the security officer or anyone else could recognize them when they walked into a bank. Today's cyberthreats are shape shifters, so you can't recognize them based on what they looked like yesterday. Through concepts like signature-less environments you can detect threats in real time, and use the time saved to contain threats. We think a winning solution requires more than just that technology, but it's a combination of technology training and expertise."

But even with those novelties included in a cyberdefense plan, when data security precautions are inevitably breached, planning and proactivity can help mitigate the liabilities associated with data loss; this means thinking about the breach in advance, and having representatives from potentially affected departments ready to assess the situation and react accordingly, even if the internal resources needed for cybersecurity defense teams are unavailable.

"Incident response is not a simple matter. It can be hard to assess the extent and scope of the damage to your systems and to your customers' information," Walker adds. "You need established procedures and committed resources so that you can move quickly and in the right direction; it's critical to avoid the kind of panic that leads to errors (and can even make matters worse). The first priority is the technical response—being clear on what happened, how it happened, and how best to restore security. But you also want to notify affected parties promptly, so the legal team needs to move rapidly as well, and to manage the communications carefully, since the details matter. You want all the right people in the rapid-response team. Manage internal discussions to avoid wild (and often incorrect) speculation. And make sure you do an after-action report to ensure that the company learns the right lessons for the inevitable next time." ■