Predictions on What Is Ahead for Cyberrisk in 2016

Christopher M. Brubaker

December 9, 2015

As 2015 winds down, it is a good time to take stock of where you are with cybersecurity. As you should be aware by now, cybersecurity is an ongoing process that requires constant evaluation, monitoring, testing, training and adaptation. The events of the last year only reinforce this notion. While large-scale payment card data and health care information breaches continue to dominate the headlines, the Ashley Madison breach shows that plenty of damage can occur when a financial windfall is not the hacker's objective. Following on the heels of the Sony breach, which was all about ideology, it is all too clear the harm that a breach can cause, regardless of the type of data that you have or the motivation for the attack. Here are a few predictions for what to expect in 2016:

- **Don't take the bait.** Phishing (socially engineered targeted email) will be behind the most newsworthy cyberevents in 2016 and will continue to be a leading cause of cybersecurity incidents. Employee training and awareness is the most effective defense against this threat.

- **Compliance is key.** Beware the regulator. All signs point to 2016 as the year of regulatory enforcement of cybersecurity. Make sure you have security protocols including incident response plans in place. Credit agencies are watching too.

- **Cyberwar/terrorism will lead to a major event.** This may not occur in—or impact—the United States directly, but odds are high there will be an event somewhere in the coming year. The United States and China are already at odds on the issue. Tensions with Russia remain high on numerous fronts, Anonymous has declared war on ISIS, and more and more nations are ramping up their capabilities in this area.

- **Beware cyberfatigue.** With all the attention and hype surrounding cybersecurity, it is only natural to expect that companies will begin to become tone deaf to the constant warnings, alerts, alarms and calls to be proactive.

While one of the hallmarks of cyberrisk is its changing and evolving nature, there are certain patterns that can be observed to help anticipate where the next trouble area will be. One of these patterns is the cyclical nature of threat methods. While overall cyberincidents continue to rise, the means and methods tend to change rather significantly year to year. This was illustrated in the 2014 Verizon Data Breach Investigations Report, which tracked 20 different threat factors between 2009 and 2013. Over the course of the five-year period, threat factors jumped up and down in terms of how frequently they were used. For example, brute-force hacking went from the most frequent method in 2009, to No. 4, back up to No. 1, down to No. 6, then down to No. 12. Over that same span, phishing ranked 14th, 17th, ninth, ninth, and third. What this data suggests is that cybercriminals stick with what works until it doesn't, then find something else. The 2015 Verizon Data Breach Investigations Report indicates that phishing attacks continue to be a prominent, and highly effective (90 percent success rate for a campaign of just 10 emails), threat method. While phishing attacks are usually just the first step in a larger, more sophisticated attack, there are demonstrated ways to lessen the risk. While filtering and screening emails is an important component, the best way to avoid falling victim is by training employees to recognize phishing emails.

While there is little chance of major federal legislation addressing cyberissues passing in 2016 given that it is a presidential election year, which only further exacerbates the current political climate in D.C., regulatory enforcement and rulemaking figure to be prominent players in the evolving cyberclimate. The Federal Trade Commission (FTC) had a major victory in August with the U.S. Court of Appeals for the Third Circuit upholding the agency's authority to regulate cybersecurity as an unfair and deceptive trade practice under the Federal Trade Commission Act. The recent ruling by an administrative law judge that the FTC had failed to prove actual or likely "substantial injury to consumers" in the LabMD Inc. matter, which the FTC is appealing, is unlikely to slow the FTC enforcement of cybersecurity. Other agencies have also signaled that they will be taking a closer look at cybersecurity. In early November, the Federal Communications Commission announced its first enforcement action ending in a consent decree with Cox Communications Inc. over allegations that Cox failed to properly protect its customers' confidential information. The U.S. Securities and Exchange Commission has also been active in this area, issuing an alert in September regarding a new round of examinations looking at cybersecurity at financial services firms. Among the areas included in the announcement that would be the focus of examiners were governance and risk assessment, access rights and controls, data loss prevention, vendor management, employee training, and incident response. The SEC also announced that it had reached a settlement with R.T. Jones over charges that the firm lacked an adequate cybersecurity plan. Both the Federal Financial Institutions Examination Council and the Federal Deposit Insurance Corp. recently released cybersecurity tools to help banks defend against cybercrime and assess their compliance with security regulations. Thus, all signs point to increased regulatory activity, particularly enforcement proceedings, in 2016.

One thing no one seems to dispute is that cyberrisk will continue to be one of the top concerns facing companies in the new year. According to some reports, the number of detected cyberincidents has risen more than eightfold from 2009 to 2014 to over 40 million. Ratings agencies have taken note. Just within the last two weeks Moody's announced that it would begin to include risk of cyberattacks as part of its overall credit rating analysis. While this will only be one more consideration in its analysis, it expects it to take a more prominent role in the analysis as it becomes more pervasive. Moody's stated that it viewed a cyberattack similarly to a natural disaster with unpredictability regarding the duration and severity of the event, which can also vary based on the nature of the target company. The three key factors that Moody's identified are:

- The nature of affected assets or business.

- The duration of the service disruption and expected time to restore impacted services.

- The scope of the affected assets or business (single entity versus geographic region or particular business sector).

Meanwhile, A.M. Best issued a report focused on the insurance industry and predicted that a global cyberevent could have a huge impact on the industry as a whole, up to $31 billion, multiple times the impact from a nuclear incident.

Speaking of predictions, Experian just released its cyberforecast for 2016, "Data Breach Industry Forecast." The Experian report echoes a familiar refrain about the need to stay focused on continually monitoring, testing and adapting your cybersecurity protocols including response plans to keep pace with an ever-changing threat environment. The forecast includes five main predictions:

- EMV chip and PIN technology will not stop payment breaches. In short, lags in implementation as well as yet to be discovered vulnerabilities with chip and PIN technology will mean that payment card data continues to be stolen.

- Health care-related companies will continue to be prime targets with smaller breaches causing most of the damage but large breaches garnering the headlines.

- Cyberwar between governments will cause collateral damage to businesses and consumers.

- At least one 2016 presidential candidate or campaign will be hacked. This well could tie in with the next prediction.

- Hacktivism makes a comeback. Ideologically-based cyberattacks will become more prominent and be a significant portion of cyberevents. The Sony and Ashley Madison breaches are good examples of the damage that ideologically-based attacks can cause.

A final word of advice: training. Innocent errors by employees continue to be a leading cause of data breaches. As already discussed, phishing campaigns remain a highly effective method of compromising computer networks. Effective awareness and training are proven to reduce if not eliminate phishing attacks. Indeed, it can even be a friendly competition as to who can spot the most phishing emails or spot them the fastest. A little training and a few gift cards as prizes can create a highly effective method of preventing phishing attacks and help guard against complacency. Regular training also boosts compliance with password security and other security protocols while helping to ensure compliance with regulatory requirements and best practices. Training is not a panacea and needs to be utilized in conjunction with technology (firewalls, spam filters, encryption, etc.), monitoring system activity, and other security methods. While there are no guarantees when it comes to cybersecurity, training is one area that you have the most control over, provides tangible dividends, and can help avoid regulatory fines and penalties.

Christopher M. Brubaker *of Clark Hill PLC concentrates his practice in complex commercial litigation and insurance matters. He regularly provides advice to companies on insurance and cyberrisk issues related to transactions and risk management and also advised companies on regulatory matters involving insurance and environmental laws, rules and regulations. He frequently speaks and writes on cybersecurity matters for legal and professional groups. He can be reached at cbrubaker@clarkhill.com.*

203841747.1 09999/09998-1816