Cyberrisk: A Peek Back at 2016 and a Look Ahead at 2017

Christopher M. Brubaker, The Legal Intelligencer

December 14, 2016

As 2016 comes to a close I want take a moment to look back at my cyberrisk predictions from a year ago and discuss what to expect in 2017 and beyond. In case you missed it, with the election and cyberfatigue, cyber-related incidents are still happening at an alarming rate. According to the Identity Theft Resource Center, as of Nov. 29, there have been 932 breaches and 34,305,616 compromised records so far in 2016. That is an average of nearly three breaches and over 100,000 compromised records a day. Looking back, my predictions were fairly close to the mark.

The 2016 predictions are in bullets and current analysis follows:

• **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.

Phishing and spear phishing attacks are reported to be a part of as much as 91 percent of all cyberattacks. Indeed, it has just been reported that the hacks of Cravath, Swaine & Moore and Weil, Gotshal & Manges were related to spear phishing attacks. The hack of the Democratic National Committee (DNC) has also been linked to spear phishing. Phishing and, more broadly, social engineering remain as high concerns for 2017. As noted in the 2016 Verizon Data Breach Investigations Report (DBIR) these range from opportunistic spam-style attacks to sophisticated nation-state attacks. The success rate for phishing attacks remains high and these attacks are frequently used as part of more sophisticated and multilayered attacks and are often just the tip of the iceberg. For example, phishing attacks are a common way that cybercriminals gain access to a system to download ransomware or steal credentials. As a possible effect of cyberfatigue discussed below the DBIR reported that the success rate for phishing actually increased over the previous year's report.

• **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.

This prediction was spot on, although to be fair it was not the boldest prediction and the same is likely to be true for the foreseeable future. The regulatory environment related to cybersecurity is evolving and changing at a pace similar to the threat vectors themselves. New agencies are dipping their toe into this regulatory pool and existing regulations are being revised and strengthened, and that is just in the United States. The European Union (EU) is undergoing major change in this area with the adoption of the Privacy Shield as a replacement to Safe Harbor, potential and continuing legal challenges to both the Privacy Shield itself as well as other compliance mechanisms for the transfer of data outside the EU (standard contractual clauses and binding corporate resolutions), and the adoption of a new directive on data privacy that is to be implemented by 2018. Canada and Australia are among the other countries adopting and implementing new regulations as well. The result is a complex web of overlapping and sometimes conflicting obligations. With high profile settlement of enforcement actions by the Consumer Financial Protection Bureau against Dwolla Inc. in March and the SEC against Morgan Stanley in June all signs point to regulatory enforcement remaining a big focus on the cybersecurity front. In addition, New York state is poised to join the fray with the Department of Financial Services in the middle of the rulemaking process on proposed regulations affecting the financial services industry including banks and insurers. The public comment period closed Nov. 14. As of the publication of this article DFS had not taken any further action on the proposed rule.

• 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.

Tension between the United States and Russia reached a level in the run-up to the election not seen for some time. Russia was behind the hack of the DNC during the election and was widely thought to at least be sowing the seeds of fear related to rigged election results if not actually attempting to alter the outcome of the election. While it remains to be seen exactly how relations with Russia will play out under the Trump administration it would be naïve to think that Russia will stop or slow down its cyberespionage efforts. And while relations with Russia, at least on the surface, may improve there are numerous indications that relations with China will deteriorate. Unfortunately this remains as one of the biggest potential threats given the potential for disruption of daily life if a true cyberwar were to break out between countries. It is also one of the more difficult to account for. Few companies have the resources to go toe to toe with a nation state when it comes to cyberissues. Think of the havoc wreaked by North Korea on Sony. While it is true that most companies will not have to worry about spite or ego-driven attacks such as the Sony breach, trade secrets remain one of the most valuable targets for cyberattacks and one of the more frequent targets by countries like China and Russia.

• **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.

Cyber or security fatigue is the latest hot topic. Google "cyberfatigue" and get some 715,000 results in 40 seconds. It has gotten to the point that the National Institute of Standards and Technology issued a warning in early October based on a study reporting findings of "security fatigue" in computer users' online behavior in both their work and personal lives. The warning focused on username and password issues that are often the first area affected by fatigue. This only underscores the importance of constant vigilance, monitoring, training and testing that are so vital to cybersecurity. Particularly for large organizations the number of users and passwords can be overwhelming and maintaining discipline across the organization can be a real challenge. This also ties in with the issues raised above. Phishing while a highly successful form of cyberattack has also been shown to be effectively managed through employee training. Compliance with regulations requires attention to detail and discipline to adhere to the procedures that are in place. Making yourself an unattractive target for cyberthieves and espionage requires constant attention to the changing threat environment as well as regular testing and probing of systems and defenses as well as monitoring both in-coming and out-going network traffic.

Sorry to disappoint those of you looking for a whole new slate of predictions but as discussed above, last year's look to hold true for 2017 and potentially beyond. Speaking of predictions, Experian just released its cyber forecast for 2017 "Data Breach Industry Forecast" and they too are piggybacking on last year's predictions with three of five being continuations of last year's predictions. The forecast includes five main predictions:

• "Aftershock" breaches will bring an end to passwords as we know them. This is where information from a breach resurfaces years later and continues to cause harm due to "bad" password habits. The 2014 Yahoo breach and its continued impact in 2016 is an example.

• Nation-state cyberattacks will escalate from espionage to war.

• Health care organizations will be the most targeted and new sophisticated types of attacks will be utilized. Personal medical information remains one of the most valued types of information by cybercriminals and health care is likely to see a continuation of ransomware-style attacks as well as new style or forms of attacks.

• Payment-based systems will continue to be a major focus even with EMV chip and pin technology becoming more commonplace. It is where the money is after all.

• Multinational companies will face nightmare from international data breach.

A final, familiar, word of advice—training. Innocent errors by employees continue to be a major cybersecurity concern and cause of data breaches. As already discussed, phishing campaigns are both a highly utilized and effective method of compromising computer networks. Training and awareness are proven to reduce if not eliminate phishing attacks. Some of the best methods involve 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 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.