CYBER SECURITY LESSONS FROM 2016 AND TRENDS FOR 2017

By Marissa M. Maldonado, Senior Manager, Information Systems Security Officer| Coker Group

Before we begin to forecast what new trends in cyber security will evolve in 2017, we must first look at the major pivots we witnessed in 2016. There are two critical events from 2016 that will continue to shake things up across all major industries—including healthcare--that must adhere to some measure of compliance. The general theme for 2017 is how do we simplify and consolidate technology and automate resolutions of cyber security breaches.

In 2016, industries across the board experienced one of the most aggressive and destructive cybercrime campaigns to date--Ransomware. Ransomware was first sent to nearly half a million victims on February 16th, 2016. It came in the form of a word document with a malicious macro. Victims were sent the infected document via an email masked as an invoice requiring payment. It changed the wallpaper on their computer to instructions on what to do next. All of their files were converted into Locky Files, which are inaccessible encrypted files. To access the files required paying a "ransom" to the hackers. Once the ransom was paid, the encryption key was released for victims to retrieve their files.

With such a new form of a cyberattack that spread at an epidemic rate, there was confusion with how to respond to a ransomware security breach. We witnessed an interesting back-and-forth debate within the healthcare arena on whether the data is considered compromised during ransomware attacks. Midway through the year, it was determined that a practice is legally required to report ransomware attacks as a HIPAA breach and to offer credit report monitoring to the patients whose data was compromised.[1] This event was the tipping point for cyber security insurance within the healthcare community. The case studies for the practices without cyber security insurance were devastating. We witnessed major ransomware breaches in 2016 at an alarming rate, with some cases reaching headline news, such as the SRS ransomware attacks.[2]

Another major event that stirred the cyber security community was the DDoS attacks on Dyn on October 21, 2016.[3] DDoS attacks are not new by any means within the cyber community. However, the Dyn DDoS attack was twice as powerful as any similar attack on record. DDoS attacks are primarily orchestrated data traffic jams which cause instability for their target victim. The victim of this DDoS attack, Dyn, is a Domain Name System (DNS) service company. DNS service companies are an address book for the Internet, which means when someone types in "www.google.com" into their web browser, a company like Dyn will take the request and point the user to the correct host server to browse that website. When Dyn was

[1] https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf. Accessed January 11, 2016.
[2] http://www.grhealthcarepulse.com/category/ransomware/. Accessed January 12, 2017.
[3] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet. Accessed January 12, 2017.

attacked, it created Internet instability for the Northeast region of the United States. The code that was used is called Mirai, and it specifically used Internet-of-Things (IoT), such as digital video recorders and surveillance cameras to create the data traffic jam. Mirai is a DDoS-for-hire service, which means it is resold on the dark web for whoever wants to utilize it.

The DDoS attack was the first major exposure of the vulnerabilities of IoT. It is a widely-known fact within the cyber security community that IoT devices are not secure. However, the exposure of their insecurity illustrates how the collective stability of the Internet can be compromised if we do not secure our individual networks. This situation leads into the conversation of how we are monitoring and responding to our networks. The consensus within the cyber security community is that networks need to be simplified, and our responses to security incidents need to be automated. This trend is taking place throughout the healthcare industry with more and more practices moving to true cloud-based systems or virtualization of their in-house system.

Today, most networks are using Security Information and Event Management (SIEM) to monitor their systems. SIEM does log management, security event correlation, and security analytics. Essentially, these tools are put in place to alert the IT department of any anomalies within the network. The next step is for the person to respond to the irregularity. However, given the precarious nature of our cyber security breaches nowadays, the thought is that once the irregularity has been noticed and alerts are sent for personnel to respond, it is already too late. The new trend is to start utilizing Security Operations and Analytics Platform Architecture (SOAPA). These monitoring tools also have artificial intelligence scripted in so it can begin to consume, process, and analyze security data.

After a tumultuous year with medical practices and hospitals becoming victims of cyber security breaches, the demand for this shift in cyber security is to address how we automate resolution. How do we prevent the ransomware attack once the user opens the attachment in the email? How do we prevent code such as Mirai from using our system to orchestrate a DDoS attack? As we see stricter HIPAA guidelines and enforcement, this question becomes more relevant and more expensive to ignore. You hear experts across the board say, “It’s not a matter of if, but when,” in regards to having a cyber security breach. It is up to your trusted IT professionals to keep you and your network systems ahead of the curve. One thing we know for certain, cyber criminals’ creativity will not diminish. Unfortunately, their business model is lucrative as long as we continue to remain vulnerable.

Please share your thoughts about Cyber Security Lessons from 2016 and Trends for 2017 by contacting Marissa M. Maldonado, Senior Manager, Information Systems Security Officer at mmaldonado@cokergroup.com, or by calling 678-832-2021.