Insights

Cyber Summary – February 2020

By Richard Freiberg, Cyber Risk Management

Healthy **skepticism** can help to avoid falling for phishing schemes and other scams; **testing** can help ensure the data system actually works and supports your company's stated policies and procedures; and, **knowledge** allows for expanding data enhancements and securing the necessary and appropriate hardware, software and the data. It is hoped that incidents reported in *Cyber Summary* provide you with helpful material so you can avoid similar events, and that our "takeaways" give you actionable information.

Significant areas discussed below are systems, data exposure, ransomware, phishing, malware and malicious insiders.

Key Cyber Events

The following is a rundown of what happened during January. We welcome your comments, insights and questions.

- **Amazon-owned home security camera provider Ring has made the headlines again as it reported having to terminate employees who improperly accessed the video data of Ring users.** In addition to terminating the employees, Ring has increased the limitations on the number of employees who can access the stored videos.
- **iPhones -** The mobile phone belonging to Jeff Bezos, the founder and chief executive of Amazon, was allegedly hacked when he clicked a video sent through WhatsApp, essentially turning over control of his phone and all of its contents to the hackers

Richards Takeaway: As the world becomes more connected, it is imperative that you step back as a consumer and make informed decisions regarding the technology you utilize and your expectations of privacy. While technology has its advantages, at times the security and privacy implications will often exceed the benefits. As a consumer, you need to be aware and prepared to make that determination. One of our hopes with our monthly *Cyber Summary* is that we continue to increase your awareness and empower you to make informed decisions.

- **Microsoft was identified as having mistakenly exposed 250 million customer records.** The records date as far back as 14 years ago. Security researchers had identified a set of servers improperly secured that granted anyone access to the customer service and support logs. The logs detailed conversations between the support agents and the Microsoft customers and included such information as e-mail address, support ticket number and the nature of the call. The issue was immediately fixed upon notification to Microsoft.

- **On January 2** restaurant conglomerate Landry's announced a point-of-sale malware attack that targeted customers' payment card data. This is their second data breach

since 2015. The collected Personally Identifiable Information (PII) included credit and debit card numbers, expiration dates, verification codes, and cardholder names.

Richard's Takeaway: With all the technology solutions that companies persistently market, it is often easy to forget that while technology does have a role, a large part of solving the cyber challenge is the education and awareness of the users. For cybersecurity to be effective, it needs to account for **People**, **Process** and **Technology**, in that order. In this circumstance, in many of the incidents above had the entity implemented the correct controls around the awareness of the people and the process this could have been prevented. If you need assistance in developing and ensuring a security posture across your people, process, and technology, please feel free to contact me.

- **Ransomware continues to be one of the prominent cyber threats.** As the months go by and we continue to publish our *Cyber Summary*, one thing is certain: the risk of ransomware is not only increasing, but the tactics used are evolving. The silver lining is that you do not have to become a victim. If you need assistance and want to reduce the likelihood of becoming another statistic, please feel free to contact us. Below are the ransomware events for January:

- On January 8th, the **City of Las Vegas** alerted of a ransomware event that impacted systems and caused service outages. The City responded quickly to the incident and was able to resume full operations within 12 hours.

- **Nassau County NY,** Comptroller Jack Schnirman said controls in place at the comptroller's office immediately identified the fraudulent activity, leading the funds to be frozen and recovered $710,000 paid out of the comptroller's office to scammers pretending to be a county vendor thus taxpayers were protected due to the efforts of this coordinated investigation.

- Other cyberattacks have targeted school districts in Lynbrook, Mineola and Rockville Centre, where Rockville Centre school officials paid nearly $100,000 after their server was hacked and locked behind a ransomware virus.

- The **Lincoln County School District** was attacked last year, with hackers demanding money in exchange for the keys to decode the school district's stolen data. The attack shut down technology in the district including phone lines and internet Wi-Fi, and files on infected computers were scrambled. The district hired a company to help negotiate with the hackers. Ultimately no ransom was paid

Richard's Takeaway: Many breaches though are all too reminiscent of the Target breach back in 2013 that arose through a third - party vendor. It is very common when we perform our assessment that we find client networks unknowingly over-exposed to third parties. Understanding and managing your third - party risk is key. If you need assistance, please contact us.

- **The stolen payment details for 30 million Wawa customers has surfaced for sale in the dark web.** In December 2019, Wawa reported that it suffered a breach of its point of sale systems that resulted in the theft of payment card data. The cards have been made available for sale in the dark web marketplace called Joker Stash. The average price of the number for sale is $17.

- **On January 20** an undisclosed number of shoppers of the children's clothing retailer, **Hanna Andersson**, had sensitive payment information exposed. This breach is the latest in a string of Magecart attacks, where hackers install malicious malware in Point of Sale (POS) systems to skim credit card information. Customers who made online purchases from September 16, 2019, to November 11, 2019, had their names, shipping addresses, billing addresses, payment card numbers, CVV codes, and expiration dates skimmed and put for sale on the Dark Web.

Richard's Takeaway: Dark web exposure is a serious issue today and one which contributes to identity theft and loss of production at work and home while the victim works with numerous sources attempting to mitigate the problem. Understanding and managing your risk is key. If you need assistance, please contact us.

Just as the world settles down post the Iranian cyber-hype in the aftermath of Suleimani, now multiple U.S. government agencies have warned of a newly intensifying threat from North Korea. Some of the malware is new and some of it is updated. And this particular threat group has pretty terrifying form—remember WannaCry?

As almost always these days, the hackers have mounted a phishing campaign to exploit weaknesses in non-governmental sectors. The objective is not political, it's financial.

Richard's Takeaway: Defensive holes, lack of patching, network and IoT vulnerabilities and poor user training contribute to vulnerability. Understanding and managing your risk is key. If you need assistance, please contact us.

February 11: Fifth Third Bank, a financial institution with 1,150 branches in 10 states, claims a former employee is responsible for a data breach, which exposed customers' name, Social Security number, driver's license information, mother's maiden name, address, phone number, date of birth and account numbers. The total number of affected employees and banking clients remains undisclosed yet is an eerie reminder of the recent Capital One breach.

February 13, 2020 The theft of an employee laptop from **GridWorks IC, a third-party vendor of Health Share of Oregon**, has exposed the personal and medical information of 654,000 members. The Health Share of Oregon data breach disclosed sensitive data, including names, addresses, phone numbers, dates of birth, Social Security numbers, and Medicaid ID numbers. This represents yet another reminder of a business' responsibility of their third-party vendors.

Richard's Takeaway: Malicious insiders and third - party vendor risks remain two critical areas of exposure for firms of all sizes. If they can get into Capital One, Target and Home Depot to name a few how confident are you in your approach? If you need assistance in developing and ensuring a security posture across your people, process, and technology, please feel free to contact me.

Additional Considerations: Although this summary addresses direct financial exposure in many cases attackers want to access intellectual property, or cause system disruption without direct financial consequences the latter remains a serious reminder to ramp up your approach to **People**, **Process** and **Technology.** Although cyber insurance is a MUST HAVE it is not a panacea for poor cyber hygiene.

Contact Us:

Richard Freiberg, CPA
Director Business Development
Cyberlitica
Office: 980-339-3352
Mobile 914-393-0033
Email: rich@cyberlitica.com
Web:www.cyberlitica.com