Cyber Roundup – June 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

Sometimes “sound bites” help us to remember actions we need to take. With this edition of *Cyber Roundup*, some readers might consider the following statements made in this issue as good advice which, if heeded, can help to secure your cyber peace of mind:

- Patching is one of the top items to focus on.
- Cybersecurity is no longer an expense to your business, it is your business.
- What many businesses find out when it is too late [after a ransomware attack] is that they either don’t have a backup or they don’t know how to restore the data in a timely manner.

Security and privacy by design and by default is a philosophy every company should embrace and every consumer should expect.

Key Cyber Events

The following is a rundown of what happened during the month of May 2019. We welcome your comments, insights and questions.

- **Microsoft issued an alert and fix for a critical vulnerability identified in its Remote Desktop Protocol.** Similar to WannaCry, the major vulnerability that circled the globe back in 2017, this vulnerability could spread from computer to computer with no user-driven interaction. Because of the severity, Microsoft has issued fixes for Windows XP and Server 2003, both of which have long since been end of life. Windows 8 and 10 remain unaffected; however, Windows 7, Server 2008 and 2008 R2 are impacted. If you have not done so, it is critical that you patch this flaw. Details and the patch can be found here.

- **The Department of Homeland Security issued Binding Operation Directive (BOD 19-02).** The directive mandated that federal agencies and departments must patch vulnerabilities rated as critical within 15 days and those rated as severe within 30 days. This reduces the prior order by 30 days.

  Tom’s Takeaway: Patching is by far one of the most important things every company – big and small – should strive to do quickly and consistently. I am often asked what are the key areas we should focus on. Patching is one of the top items on that list.

- **2019 is shaping up to be one of the worst years on record with regard to data breaches.** Based on a report by Risk Based Security, in the first three months of 2019 there were 1,903 disclosed data breach events resulting in the exposure of 1.9 billion records. This is the most activity on record reported in a first quarter.

- **The City of Baltimore is one of the latest on the list to suffer a major ransomware attack.** The ransomware attack began on May 7. As of this writing, it is still in the initial recovery phases and is projected to continue for coming months. The cyber criminals demanded a ransom of $76,000; however, the decision was to not pay. It is estimated that this will cost the City $18.2 million. The attack is believed to have used one of the compromised NSA hacking tools, EternalBlue. Patches designed to defend against this tool have been released over two years ago. If this is ultimately the case, the attack will indicate a break down in Baltimore’s patching methodology and the overall effectiveness of their security program.

Tom's Takeaway: For many businesses, cybersecurity isn't an issue until it is. It's when the breach occurs that management will reflect on what they should have done. Don't fall victim to this approach; rather, be proactive. Cybersecurity is no longer an expense to your business, it is your business***.*** Until all businesses adopt this mentality, issues like the City of Baltimore will continue to occur, having an impact not only to the business and the bottom line, but more often than not, the personal lives of those they employ or serve.

- **CCH, a subsidiary of Wolters Kluwer and a major provider of software and information services for accounting, tax and audit firms, was the victim of a ransomware event.** The incident resulted in the company shutting down many of their key systems as they attempted to isolate and resolve the incident. The company claims no customer personal data was breached as part of the incident. Because of the timing of the incident in relation to the May 15th IRS filing deadline and the extensive reliance on CCH by numerous accounting firms to process tax returns, the IRS granted a seven-day extension to anyone that was impacted.

- **Malware can also be a piece of art – at least based on a malware-infected laptop that sold for $1.35 million in auction.** A laptop that was purposely infected with six of the most dangerous viruses of recent times was placed up for auction and sold. The cumulative damage caused by these viruses is estimated at close to $100 billion. The laptop, running Windows XP, was infected with the following viruses: "ILOVEYOU," "MyDoom," "SoBig," "WannaCry," "DarkTequila," and "BlackEnergy."

- **The City of San Francisco has become the first city in the U.S. to ban the use of facial recognition technology by local government departments, including law enforcement.** This prohibition is part of larger legislation requiring city departments to have specific-use policies and obtain board approval for the use or procurement of any surveillance technologies. The ban does not affect the use of the technology at the Federal level.

- **Proven Data Recovery and MonsterCloud, two companies "specializing" in ransomware recovery and avoiding ransom payment, were identified as more often than not actually paying the ransoms and charging the victims/clients the cost of the ransom and additional fees.** While paying the ransom is not illegal, the issue of misleading the client and not disclosing the payment to the client could be classified as a misleading and deceptive business practice by the Federal Trade Commission (FTC) Act. The companies claimed to have proprietary technology that could unlock the files, avoiding the payment.

  Tom's Takeaway: When it comes to ransomware, the reason it is so dangerous is because of the limited options the victim has. In most situations, unlocking the files without paying is not likely – it doesn't matter who you call for assistance. The ransomware is designed to use industry standard encryption – the very encryption used by businesses to protect their data from the criminals. Once infected and you want your data back, you either have to restore from backup or pay. What many businesses find out when it is too late is that they either don't have a backup or they don't know how to restore the data in a timely manner. Data backup and restoration strategies are core components of every assessment we perform and are key questions that senior management and the board should be asking.

- **WhatsApp, a popular messaging app, was identified as having a vulnerability that could result in the device automatically installing spyware.** To execute the vulnerability, all the attacker would have to do is place a WhatsApp call to the device with no interaction required by the recipient. Facebook, the parent company of WhatsApp, could not provide an indication of how many people were targeted by the vulnerability. Facebook has indicated that the NSO Group, an Israeli security company known to sell various types of spyware to governments, has leveraged the vulnerability. A patch has been released to address the issue. If you are a user of the App, it is important that you ensure you are using the latest version.

- **First American Financial Corp., a title insurance and settlement services company, leaked approximately 885 million records containing highly sensitive personal data provided in the course of a real estate transaction, such as social security number, banking, and driver's license information.** The leak was the result of a vulnerability in the website that allowed anyone with a link to a document to view other unrelated documents by simply replacing

a single digit in the link. For example, if a link provided to me to access a file was www.docs.com/file/1234, by changing one of the digits in the sequence, 1234 to 1235, I could access a different document. No username and password would have been required to view these documents. Digital documents as far back as 2003 could have been viewed. The company has hired a forensic team to identify if any of the data was accessed by unauthorized parties.

Tom's Takeaway: Security and privacy by design and by default is a philosophy every company should embrace and every consumer should expect. This vulnerability is as basic as it comes in the realm of web security. Issues like this are the result of not factoring in security to the development lifecycle and not sufficient and prudent testing relative to the sensitivity of the data the website provided access to.

- **Russian President Vladimir Putin signed into law the isolation of the Russian internet (Runet).** The law will give Russia the ability to safely disconnect its internet from the global internet. The purpose of the law has been stated to ensure the continued operations and stability of the Runet in the event of a future attack that attempts to target and sever its connection to the global internet. Critics have warned that with this level of control the new law will allow for censorship, surveillance, and the control of information presented to its citizens.

- **New Jersey expands its breach notification law.** It now includes the following that would trigger a "duty to notify" if breached: a user name and/or email address in combination with a password or security questions and answers that would allow access to an online account. Expanding "duty to notify" to these identifiers is currently limited to the following 11 states: Alabama, Arizona, California, Colorado, Delaware, Florida, Nebraska, Nevada, Puerto Rico, South Dakota and Wyoming. The New Jersey law goes into effect September 1, 2019.

Contact Us

Thomas J. DeMayo, Principal, Cyber Risk Management
CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE

PKF O'Connor Davies, LLP
665 Fifth Avenue, New York, NY, 10022
212.867.8000 or 646.449.6353 (direct)
tdemayo@pkfod.com

www.pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, eleven offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 29th on *Accounting Today*'s 2019 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today.* In 2019, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.