PKF
O'CONNOR
DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – August 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

Doing nothing to protect your cyber infrastructure is not an option. This month's edition of *Cyber Roundup* underscores the need for action. Contact Tom DeMayo with your cyber concerns.

Key Cyber Events

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

- **Capital One reported a breach impacting approximately 106 million individuals**. 100 million are associated with U.S. accounts, while 6 million are associated with Canadian accounts. The bulk of the data disclosed consisted of information collected during the application of various credit card products from 2005-2019. The data consisted of such items as name, physical and e-mail address, date of birth and reported income. In addition, the breach also included more sensitive data such as 140,000 Social Security Numbers and 80,000 bank account numbers. The FBI has arrested an individual believed to be associated with the hack. The breach was the result of a misconfigured firewall. Capital One has set up the following FAQ page that can be used to answer many of your questions. We encourage you to visit this page if you believe you may be impacted. Capital One Breach FAQ

  Tom's Takeaway: Breaches will continue to happen and sensitive data like your SSN may at some point be exposed. I encourage you to be proactive with your identity protections and not reactive. If you have not already done so, consider implementing a credit freeze for yourself and your family. You must do so with each of the three major credit bureaus: Transunion, Equifax, Experian. In addition, monitor your accounts on a frequent basis and practice overall good cyber hygiene.

- Over the past year, the number of ransomware attacks affecting businesses has continued to grow exponentially. July proved to be no different with the trend. Below is a summary of the major ransomware incidents in July.

  - **Syracuse City School District in New York reported a ransomware attack that impacted all key systems such as human resources, payroll, student management and e-mail.** The district fortunately had backups and began the lengthy process of performing the necessary restores. The incident first started on July 9th and, as of July 17th, was still in the restoration process.

  - **Georgia's court agency reported a ransomware attack that resulted in the court websites being taken off line in an effort to contain the incident.** It is not believed that any sensitive information was impacted as the infected systems do not contain any sensitive personal information.

  - **The United Kingdom's largest police forensic lab contractor, Eurofins Scientific, suffered a ransomware attack.** The incident started in early June. Eurofins Scientific paid an undisclosed ransom amount to regain control of their systems. Based on their investigation to date, they indicated they do not believe any confidential data was transferred out of their systems.

  - **La Porte County Indiana suffered a ransomware attack that resulted in a payment of the 10.5 bitcoins ($132,300) ransom demanded.** The initial amount requested by the cyber criminals was $221,000; however, the amount was negotiated down. While the county contacted the FBI, they were unable to assist with the decryption.

- **Monroe College, New York, was hit with a ransomware attack with the cyber criminals demanding $2 million in bitcoin**. The ransomware attack impacted many of the College's key systems. The College actively engaged the FBI and law enforcement to assist with the investigation. Additional details regarding the incident have not yet been provided.

- **Louisiana Governor, John Bel Edwards, declared a state of emergency after three Louisiana school districts suffered a ransomware attack.** By issuing an emergency declaration, the Governor was able to allocate State resources to assist with the incident.

- **iNSYNQ, a QuickBooks cloud hosting provider, suffered a ransomware attack**. It resulted in customers unable to access their accounting systems and data.

Tom's Takeaway: While no security program can ever guarantee a breach won't happen, a well-designed cybersecurity program can help minimize the chance of it happening and further reduce the impact if and when it does. Don't blindly allow your business to be a victim. If you need assistance on assessing or developing your cybersecurity program, please contact us to learn how we may help.

- **In response to U.S. Senator Chris Coon's inquiry as to what happens with voice data after a customer speaks with Alexa, Amazon confirmed that the data is held until the customer chooses to delete it.** Even after deletion, it may still reside on Amazon subsystems. In a similar announcement, Google confirmed that contractors are able to listen to communications with the Google Assistant. Google responded that this is necessary to help improve the system to understand accents and patterns of speech.

  Tom's Takeaway: While I am not surprised by Amazon's and Google's responses, fundamentally it us up to the consumer to be aware and consider the tradeoff of privacy vs functionality when using any virtual assistant or smart device. I personally do not use any voice assistant and try to avoid any unnecessary smart device. While I am open to my view changing in the future, I believe too many unknowns currently exist with how these devices and data are protected and used.

- **Facebook, in a record settlement with the U.S. Federal Trade Commission (FTC), has agreed to pay $5 billion as a result of the allegations of mishandling consumer personal data.** In addition to the $5 billion to be paid, Facebook must create a board committee on privacy and provide executive certifications that personal data is being properly handled and safeguarded.

- **The FTC also reached a $700 million settlement agreement with Equifax as a result of the 2017 data breach impacting the sensitive personal information of approximately 147 million Americans**. As part of the settlement, impacted individuals may file a claim to be compensated for the costs incurred in recovering from the breach and the cost of protecting yourself from future identity theft. To obtain full details on what you may be entitled to and how to file a claim, please visit the following site: FTC Equifax Breach Settlement Info.

  Tom's Takeaway: Please be extra careful on what sites you interact with regarding this; it is inevitable fake sites will be created by cyber criminals to take advantage of individuals seeking assistance.

- **A cybercriminal infiltrated Bulgaria's National Revenue Agency's tax system, stealing the sensitive personal and financial data of every working citizen.** Approximately half of the stolen records of the estimated 5 million Bulgarian citizens impacted was subsequently posted online in hacker forums. A 20-year old Bulgarian cybersecurity professional has been arrested in connection with the crime.

  Tom's Takeaway: While I often focus on U.S.-based cyber issues, the Bulgarian incident is a reminder that cybersecurity is a global issue. In an interconnected world across a globally-shared internet, a solution to the cybersecurity problem will require a collective global effort to combat and defeat. No one country can do it alone.

- **Iran launched a new military cyber command unit to defend against U.S. cyberattacks**. In last month's *Roundup*, we discussed the U.S. cyber offensive launched against Iran's rocket and missile control systems. Iran's Islamic Revolutionary Guard Corps (IRGC) revealed its new tactical communications unit, Sepeher 110, designed to withstand any future offensive cyber operations by the U.S. against Iran's military command and control infrastructure.

- **The U.S. Department of Education issued an alert after 62 U.S. colleges were targeted by cybercriminals.** They attempted to exploit a vulnerability in a commonly used higher education enterprise resource planning (ERP) system known as Banner. Details on the alert can be found here.

- **Security researchers identified a flaw in a smart home hub that could allow attackers to unlock the doors.** The impacted hub is by Zipato called Zipamicro. The flaw has since been fixed. The security researchers did not publish their findings until after a confirmed fix had been released.

- **The U.S. Coast Guard issued a recommendation that ships enhance their cybersecurity protections in the wake of a cyberattack on a ship.** The attack degraded the ship's computer systems; however, it is reported that the ship's control systems were not impacted. While this ship's control systems were not impacted, it is possible for other ships to be impacted depending on their network design.

- **IBM Security released their annual study Cost of a Data Breach Report.** In this year's report, the Company estimates that the cost of data breach has risen 12 percent over the course of five years with an average breach cost of $3.92 million. While the cost of the breach will vary with size, of significance is that it reports that businesses with less than 500 employees on average suffered losses over $2.5 million per incident. The average cost per personal record stolen is $150. Further, the report claims that it takes an organization on average 263 days to identify a data breach, followed by 73 days to contain it.

- **New York Governor Cuomo signed into law the SHIELD Act (Stop Hacks and Improve Electronic Data Security Act).** In our last month's *Cyber Roundup*, the Act was awaiting the Governor's approval. The Act will expand upon New York's existing breach notification requirements and require reasonable administrative, technical and physical security practices on any person or business collecting personal information on New York residents. Safeguards will include such things as employee cyber training and regular testing and monitoring of the company's information security controls and systems. The law will take effect March 21, 2020.

- **In addition, Governor Cuomo signed into law the Identity Theft Prevention and Mitigation Services Act.** The law will require a reporting agency that has a breach to provide five years of identity theft prevention and mitigation services. In addition, consumers have a right to implement credit freezes at no additional cost. This law will go into effect on September 23, 2019, 60 days after becoming law.

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.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.