Cyber Roundup – September 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

In a world dramatically reshaped by the Pandemic, one constant remains: **cybercrime motivation.** While the number of breaches dropped during the first half of 2020, my prediction is that it will return to an upward shift. During the Pandemic, based on various studies, the general consensus is that the cyber criminals focused on using the massive data sets of personal information they already had to monetize the opportunities afforded by the Pandemic. At some point, they will need to continue to replenish and refresh their stock pile. So beware. Please contact us for support services.

Key Cyber Events

The following is a rundown of what happened during the month of August 2020. We welcome your comments, insights and questions.

- **The FBI and CISA released an alert in regard to increased vishing attacks against corporations.** Vishing is voice phishing where cyber criminals call employees in an effort to obtain information. The vishing attacks were specifically designed to gain access to the victim company's network by way of remote access VPNs. To best illustrate the attack, the following is noted in the alert:

  "Actors first began using unattributed Voice over Internet Protocol (VoIP) numbers to call targeted employees on their personal cellphones, and later began incorporating spoofed numbers of other offices and employees in the victim company. The actors used social engineering techniques and, in some cases, posed as members of the victim company's IT help desk, using their knowledge of the employee's personally identifiable information — including name, position, duration at company, and home address — to gain the trust of the targeted employee."

  "The actors then convinced the targeted employee that a new VPN link would be sent and required their login, including any 2FA [2-factor authentication] or OTP [one-time passwords]. The actor logged the information provided by the employee and used it in real-time to gain access to corporate tools using the employee's account."

Tom's Takeaway: Given the dramatic shift to work from home, it is clear that the cyber criminals are leveraging the transition to their advantage. The solution to this problem and combating this specific threat is not technical; it is through training and awareness. If you need assistance in developing or enhancing your training program, we can help.

- **As the year 2020 is more than half way over (pshew!), the following statistics from various studies has been released:**

  - In a study by Malwarebytes, it identified that 20% of the respondents suffered a data breach as a result of a remote worker. Further, 24% experienced unexpected expenses to address a breach or cyberattack.

  - 27 billion records have been exposed in the first half of 2020 according to a study by Risk Based Security. In comparison to the same time period in 2019, the overall number of breaches has dropped 50%; however, the number of records exposed has increased by 80%.

  - The average cost of a data breach has dropped slightly in 2020 from $3.92 million in 2019 to $3.86 million according to a study by Ponemon Institute. In 8 out of the 10 breached organizations, Personally Identifiable Information (PII), was the target of

interest with the average cost per breached record at $146. The most costly implication to a business following a breach, was lost customers. 40% or $1.52 million of the breach cost can be attributed to customers not returning.

- The global cost of cybercrime is predicted to reach $11.4 million per minute by 2021 according to RiskIQ. That represents a 100% increase since 2015.

Tom's Takeaway: Of all the statistics I present each year, the one that resonates most with me is the percentage of breach cost associated with the loss of a customer. This shows that customers expect any business that has their information to protect it. I have said this in many past editions of Cyber Roundup, and it now – more than ever – holds true. Cybersecurity can no longer be viewed as a cost of doing business, but a necessary and strategic component to ensure the success of your business.

- **Ransomware attacks continue to persist and mature. The following entities reported a ransomware attack in August:**

  - Lafayette City, Colorado, ultimately paid $45,000 to recover from a ransomware attack. The City was unable to restore from backup to avoid payment. The attack impacted smartphones, e-mails, payment services as well as other key services of the City.

  - Canon suffered a ransomware attack that resulted in the exfiltration of 10GB of data. The ransomware also resulted in service disruptions across its U.S. website, e-mail, and other external and internal systems. Of the 10GB of data that has been stolen, the cyber actors have posted 2GB of that data online for public viewing.

  - The Metropolitan Community College of Kansas City suffered a ransomware attack. The attack impacted sensitive information such as Social Security numbers, medical information, financial information and drivers' license numbers. While the College does not believe any of the information has been ex-filtrated, it is notifying the affected individuals proactively.

  - R1 RCM, a medical debt collection firm, suffered a ransomware attack. The company has over 19,000 employees and works with a large number of 750 healthcare organizations. Given the nature of the business, it handles large volumes of highly sensitive information. The company has not yet released any additional details.

  - Haywood County School District in North Carolina suffered a ransomware attack that resulted in the closure of the schools. The District had to resort to rebuilding their systems to restore access and resume operations.

  - Carnival reported a ransomware attack that impacted one of their entities. As a publicly registered company, Carnival reported the attack in an 8-K form filed with the Securities and Exchange Commission. The filing notes that the data impacted may result in claims as the data included personal data related to customers and employees. Additional details have not yet been disclosed as Carnival continues to investigate the incident.

  - The University of Utah suffered a ransomware attack that resulted in the payment of $457,000. Although the University was able to restore their systems without the decryption key, the University paid the ransom to prevent the cyber criminals from leaking the stolen student data.

  - CWT, a travel management company, paid $4.5 million to recover from a ransomware attack and to prevent the leakage of stolen data. The cyber criminals originally demanded $10 million; however, settled for $4.5. CWT is one of the largest travel companies in the U.S. The Company noted that because of the severity of the attack, it opted to pay the ransomware.

Tom's Takeaway: From Fortune 500 companies to small community colleges, everyone is a target. It truly is not a matter of if, but when, a cyber incident will occur in your business. As a business you are faced with a multitude of choices on a daily basis, choosing to defend and prepare for a cyber incident, is something that can't be disregarded. Your board, stakeholders, customers, and employees are dependent on your success. As a company, we are deeply committed to facilitating the success of every

one of our clients and readers. If you need assistance in how to make meaningful, impactful, and cost-effective decisions in managing the cyber threat, we are here to help.

- **The National Security Agency released a document offering guidance on how to limit location data exposure.** Given the multitude of devices that are now programmed to leverage our location, it is important that people understand the implications of that exposure. If you have the time, I strongly encourage you to read the document here.

- **Salesforce and Oracle** are subject to a $10 billion class action lawsuit in a claim that they breached their obligations under GDPR, specifically in the way they process and share personal data that is sold online for advertising.

- **Egor Igorevich Kriuchko, a Russian cybercriminal, has been charged for trying to bribe a Tesla employee to install a malicious application on the network**. The bribe consisted of offering a $1 million payout. The malware was designed to launch a denial of service attack that would distract the internal security team while sensitive data could be siphoned off and a ransom demanded. Fortunately, the employee alerted the FBI.

Tom's Takeaway: We often correlate the cyber threat with external actors, but the internal threat is equally, if not more, dangerous and important to consider. In comparison, the internal threat could be far more devastating as it has already been provided what external actors have to work to obtain, trust and access. When creating your information security program, you need to be holistic in your approach and during your risk assessment, consider both the internal and external threat.

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, twelve offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 800 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 27th on *Accounting Today*'s 2020 "Top 100 Firms" list. It is also ranked among the top 20 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.