Cyber Roundup – December 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

The 21st century holiday Grinch is now a "smart" TV (or any other "smart" household product) nosing into your family's privacy. The new Scrooge is represented by ransomware cybercriminals trying to waste your resources and/or steal your money. Enter, the Elf on a Shelf. He's watching everything – while reading *Cyber Roundup* – and suggesting that you remain tech vigilant and get us involved. We can keep you alert to cybercrimes and, if asked, can provide your organization with our expertise in risk assessment and mitigation.

Joy and peace to all our readers.

Key Cyber Events

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

- **As we move into the holiday season, the FBI has offered some advice regarding smart TVs.** They specifically remind users that a smart TV is connected to the internet; as such, it can potentially be compromised by an external party. They note the following risk considerations:

    - Smart TVs may come with cameras that are capable of facial recognition so the TV recognizes who is watching and can suggest programming. While not only a privacy issue, this may be activated to allow unauthorized third parties to see into the room.
    - Microphones may be installed to allow for voice control and interaction. This may allow these third parties to hear conversations and interact with you.
    - Unauthorized third parties can manipulate the TV by changing channels, volume, etc.

    The FBI offers a number of considerations to protect yourself and your family at this link here.

- **The M2 smartwatch, made for kids by SMA (a Chinese company), was identified by security researchers as exposing the personal information and location data of approximately 5,000 children and parents.** The watch, one paired and registered with a mobile app, would allow the parents to track the child's location, call them, and be notified should they leave a specific location. The researchers identified that the internet-based system that would collect this data had no basic security measures in place and any one on the internet could extract that data.

Tom's Takeaway: While the FBI article specifically focuses on smart TVs, we should take this time to remind ourselves that any device that is "smart" poses a risk. If connected to the internet in any way, there are specific considerations you should have not only from a security perspective but a privacy perspective. The smartwatch is a prime example of that consideration. While I think smart technology is certainly interesting, I personally am still OK with having to use a remote to change the TV channel. You – as a consumer, now armed with the awareness of the risk – will also have to make the determination of how smart and exactly what smart devices you are comfortable with in your home used by you and your family.

- **In a report published by Risk Based Security, they highlight that 2019 is turning out to be a new record-breaking year as it relates to breaches.** Specifically, they note the following:

    - **5,183 breaches** were reported through September 30, exposing over **7.9 billion records**.
    - Compared to the Q3 of 2018, the number of reported breaches was **up 33%** and the number of exposed records was **up 112%.**
    - **Three** breaches have made the list of the **ten largest breaches of all time.**

- **A ransomware attack on an IT vendor resulted in 110 nursing homes being impacted, disrupting care.** Virtual Care Provider, a Wisconsin-based IT consulting, cloud data hosting, security and access management provider, suffered a ransomware attack that significantly impacted their operations and the nursing homes that were dependent on them. In terms of significance, reports indicate that the nursing homes were unable to place orders for prescriptions, access medical records, and perform billing.

Tom's Takeaway: As we have noted throughout our *Roundups* this year, the cyber criminals have made cloud providers and IT managed service providers (MSPs) focal points. As with anything, cloud providers and IT MSPs can offer a lot of value and help better manage certain risk; however, they also introduce new types of risk. What is critical is that the users of these services identify and account for that risk. When we work with any health care provider and facilitate risk assessments, part of our approach is to evaluate any critical dependencies on third parties and determine the reasonableness of the plans, should they exist, in continuing without those third parties. While operations may certainly slow down, what is important is that they continue. In the context of healthcare providers, that can be a life or death situation.

- **The University of Rochester Medical Center was issued a $3 million HIPAA penalty.** The Department of Health and Human Services' Office for Civil Rights (OCR), upon receipt of breach reports by the Center, launched an investigation and found multiple HIPAA violations. Specifically, they focused on the lack of encryption and failure of the Center to have performed a comprehensive risk assessment to effectively understand and manage their risk.

Tom's Takeaway: If you are a covered entity under HIPAA (i.e., you are required to be in compliance with HIPAA), we can't overemphasize the importance of completing a true risk assessment. One of the key conversations we often have with our health care clients is whether or not they have done a true risk assessment that will meet the requirements set forth by the OCR. Should you be subject to a breach or an audit, OCR will push heavily on the existence and completeness of the risk assessment. Should you need assistance in evaluating the sufficiency of your risk assessment or in conducting a vigorous risk assessment, we would be happy to help.

- **Livingston School District in New Jersey is one of the latest municipalities to fall victim to a ransomware attack.** The event took place on November 21, 2019 and resulted in delayed school openings. The District did not pay the ransom and opted to recover the data. The ransomware impacted all key systems including payroll, learning management, and student records. In unrelated attacks, the Town of Dover and Union County, both also in New Jersey, reported cyberattacks. The extent of the attacks have not been fully disclosed.

- **Macy's reported that their online store had been compromised and malware had been installed that stole customers' personal and payment information.** The malware is believed to have operated for only a week before being detected. Affected customers have been notified. Macy's has not specified the number of impacted customers.

- **A federal privacy bill, entitled the Consumer Online Privacy Act (COPRA), has been introduced by U.S. Senator Maria Cantwell.** The bill is designed to expand the rights of individuals insofar as how personal information is collected, shared, used, and maintained.

- **The U.S. Federal Trade Commission (FTC) has brought a lawsuit against a Utah-based IT company, InfoTrax Systems, for a breach that resulted in the compromise of 1 million personal records.** The data included sensitive personal information such as Social Security Numbers, payment card numbers, government identification numbers and account User IDs and passwords. The complaint alleges that the cyber attackers first compromised the system in May 2014 and 17 more times over a 21-month period. The attack remained undetected until the cyber criminals maxed out the storage of one of the servers. Should the storage not have maxed out, it would have likely remained undetected. The FTC claims that InfoTrax systems and its CEO failed to protect the data and had insufficient security practices. The settlement would ban the company from handling personal data until a security program is implemented that would correct the deficiencies identified.

Tom's Takeaway: If you operate a business that requires the handling of sensitive data, you have not only a legal responsibility, but a moral and social responsibility to protect that data. This lawsuit by the FTC makes the legal aspect clear. While I understand that cybersecurity is not traditionally considered core to a business, in many cases, it needs to be. Whether operating a business that is for profit or not-for-profit, there needs to be an understanding and management of the risk of the data processed and the dependency on the systems you utilize. Security doesn't necessarily need to be expensive, it needs to be effective. But before you can manage the risk, you need to understand it. If, as a board member, a senior executive, or an IT provider, you need assistance in understanding and managing that risk, we are here to help.

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 800 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.