Cyber Roundup – October 2021

By Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory

Looking through the cyber incidents reported in this edition of *Cyber Roundup*, you will see that the SEC is weighing in on cybersecurity of their regulated entities. When considering the specifics of the SEC actions, the following common themes were present and can be applied to all businesses, public and private:

- Must have written cyber and information security policies and procedures.
- Just having formal cyber and information security policies and procedures is not enough – they must actually be followed as written.
- Upon identification of known cyber weaknesses, must take corrective actions in a timely manner.
- Must be forthright in providing information in breach notifications.

Having worked with many entities, it is very common to find that policies and procedures are not formally defined or policies and procedures have been defined by way of a template **and never customized.** We work with many clients in developing policies and procedures that are well-defined and consistent with the operations of the company. If you need assistance, please contact us.

Key Cyber Events

The following is a rundown of trends and what's been happening recently. We welcome your comments, insights and questions.

- **According to Rob Joyce, Director of Cybersecurity at the National Security Agency (NSA), every country has developed a cyber-exploitation program used to obtain intelligence or espionage.** Leading the charge in capabilities and resources are China, Iran, North Korea, and Russia. Joyce dubbed them the "Big Four."

- **The U.S. Cybersecurity and Infrastructure Security Agency (CISA) released a tool to help private and public sector companies to assess their risk to the insider threat and devise a plan to address that risk.** The tool is labeled the Insider Risk Mitigation Self-Assessment Tool Kit. The tool and further information about it can be found here.

- **An IT technician from Suffolk County, NY is facing up to 15 years in prison for using the County's IT systems to mine cryptocurrency.** The technician installed and concealed 46 mining rigs costing the County thousands of dollars in additional electricity usage charges.

- **A terminated employee of a New York credit union plead guilty to destroying approximately 21GB of information out of revenge after being let go.** Although a request was issued by the credit union's human resources department to disable access, the request was not processed in a timely manner. The individual accessed the systems two days after termination and deleted the files.

  Tom's Takeaway: The insider threat is equal, if not greater, a risk as the external threat. An insider – unlike an external party – has the benefit of trusted access as a start. As you perform your risk assessments, be sure to incorporate the insider threat to your operations. How to handle a contentious termination is a good area to start.

- **The SEC published an announcement sanctioning eight firms in three actions for insufficient cybersecurity policies and procedures.** The firms included investment advisors and broker-dealers that experienced e-mail account take overs that resulted in the exposure of the personal information of thousands of clients and customers.

- **A vulnerability was discovered in Microsoft's managed database service, Cosmo DB, allowing the researchers to break out of Microsoft's secure multi-tenancy.** The secure multi-tenancy model is what keeps data secure from any other Microsoft customers using the same platform. The vulnerability ultimately allowed access to thousands of Microsoft client accounts and data. It was identified that the vulnerability was introduced as a result of a misconfigured new feature that was introduced.

  Tom's Takeaway: Although I have never directly opined for or against Cloud computing services, I do believe it has its place depending on the client's environment, size, resources, and ultimate objectives. Like anything else, the Cloud comes with risk. It is not a panacea that will solve all cybersecurity and data problems. What is important is that users understand and don't lose sight of the risk in continuing down the Cloud path.

- **According to a report released by Positive Securities, 69% of all attacks involving malware were ransomware attacks in Q2 2021.** The following is a summary of the ransomware events in September.

  - Howard University in Washington, DC suffered a ransomware attack on September 3 disrupting key operations and resulting in the suspension of classes.

  - Crystal Valley, a Minnesota-based farming cooperative, suffered a ransomware attack severely disrupting operations. A second farming cooperative, New Cooperative, was also targeted in a separate incident with the cyber actors demanding a $5.9 million ransom.

  - Forward Air, a major trucking company, announced that it recently concluded that the ransomware that impacted its operations in December 2020 also may have resulted in the exposure of highly sensitive personal information such as SSN, driver, passport, and bank account numbers.

  - A group of ransomware gangs has introduced a new tactic and has begun threatening to destroy all the company data of their victims should they contact a negotiator.

Contact Us

Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory
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, fourteen offices in New York, New Jersey, Florida, Connecticut, Maryland and Rhode Island and more than 1,000 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.

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.