Cyber Roundup – December 2021

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

At the height of the cheesecake holiday season, there's a cream cheese shortage. Who would have thought it was due to a cyber incident? As you will see as you read on, the Grinch was a ransomware bad actor. What's next? Candy canes?

Our experts are here to help guard your firm against any imminent threat or possible attack by bad actors and provide real-time awareness of threats before they occur (as recommended by Elf on the Shelf).

Key Cyber Events

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

- **The FBI issued an alert that ransomware gangs are targeting companies during merger and acquisition activities.** The alert, found here, notes that "Impending events that could affect a victim's stock value, such as announcements, mergers, and acquisitions, encourage ransomware actors to target a network or adjust their timeline for extortion where access is established."

  Tom's Takeaway: M&A activity traditionally focuses on financial due diligence. To date, IT and cybersecurity are often not included in the analysis. Given business dependency on IT – and the potential financial, operational, and reputational ramifications of a breach – failure to perform adequate IT due diligence could prove to be costly. If you need assistance in performing IT due diligence as part of a transaction, we can help. For additional guidance, see the following article Digital Assets: Cybersecurity Considerations in an Acquisition.

- **The SEC issued an Investor Alert, found here, informing the public that threat actors are impersonating the SEC and contacting individuals by way of voicemails, e-mails, letters, and phone calls.** The threat actors alert their target victim of suspicious activity in their checking or cryptocurrency accounts. The goal of this scam is to entice the victim into providing additional more sensitive information. As a general reminder, the SEC will never make unsolicited communications confirming transactions, requesting funds, or obtaining sensitive information.

- **U.S. businesses on average paid the highest ransom when hit with a ransomware attack.** According to a study by Mimecast, the average U.S. ransom was $6.3 million. In comparison, the United Kingdom was $840,000 and Australia was $59,000.

- **Ohio-based DNA testing company, DNA Diagnostics Center, reported a breach that impacted over 2 million individuals.** The information consisted of such sensitive information as SSNs and payment information. The breach impacted an archived database that contained personal information obtained between 2004 and 2012.

- **The FBI's e-mail system was compromised.** The cyber threat actors crafted messages claiming to be from the Department of Homeland Security warning of a cyberattack. The compromise was the result of an insecure coding on an FBI online portal that allowed e-mails to be sent using the FBI's infrastructure.

Tom's Takeaway: Any website can be leveraged for malicious activities if not coded securely. The website could be leveraged to infect inspecting visitors, send malicious e-mails, or be defaced in a manner that negatively impacts the business' hard-earned reputation. When you do your cybersecurity assessments, don't forget about your websites. This is even more important if a business hosts a web application platform to service its customers. If you would like the security of your website assessed, we can help.

- **Banks will be required to report cybersecurity incidents within 36 hours to its primary federal regulator** if the incidents "materially affected — or are reasonably likely to materially affect — the viability of a banking organization's operations, its ability to deliver banking products and services, or the financial sector's stability." The final rule, found here, goes into effect May 1, 2022.

- **GoDaddy, a leading domain registrar, reported a breach that has impacted up to 1.2 million of its customers who used the Company's Managed WordPress hosting environment.** The breach included such data as e-mail addresses, customer number, and for a smaller subset of those impacted, sensitive information such as credentials.

- **Robinhood, the commission-free stock trading platform, suffered a breach impacting 7 million of its customers.** The breach was the result of a social engineering attack that manipulated an internal customer service employee to gain access to the internal systems. The threat actors demanded a ransom payment; however, it is not known if the ransom was paid. Highly sensitive data such as SSNs or payment information is not believed to have been impacted. In addition, it is not aware of any customer that has suffered a financial loss as a result of the incident.

  Tom's Takeaway: Incidents like this should always serve as a reminder how significant of an asset your employees are when it comes to managing your cyber risk. To manage that risk, you need to empower your employees with the awareness needed to defend against the ever-evolving cyber threat. Awareness comes from a cybersecurity training program that is consistent, meaningful, and tied to the culture of the company. If you need assistance in developing an awareness training program, we can help.

- **The cream cheese shortage in the U.S. was the result of a ransomware attack.** Schreiber Foods, a major cheese manufacturer, suffered a ransomware attack in October that suspended plant operations for seven days.

Contact Us

Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory
CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE

PKF O'Connor Davies, LLP
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, the Firm has 14 offices in New York, New Jersey, Connecticut, Maryland, Florida, and Rhode Island and more than 1,000 professionals providing a complete range of accounting, auditing, tax, and management advisory services. PKF O'Connor Davies is led by over 100 partners who are closely involved in the day-to-day management of engagements, ensuring a high degree of client service and cost effectiveness.

The Firm is a top-ranked firm, according to Accounting Today's 2021 "Top 100 Firms" list and was recently recognized as one of "America's Best Tax Firms" by Forbes. PKF O'Connor Davies was named one of Vault's 2021 Accounting 50, a ranking of the 50

best accounting employers to work for in North America and ranked among the top 50 most prestigious accounting firms in America in a complementary Vault survey.

PKF O'Connor Davies is the lead North American representative of the international association of PKF member firms. PKF International is a network of legally independent member firms providing accounting, tax, and business advisory services in over 400 locations in 150 countries around the world. With its tradition, experience, and focus on the future, PKF O'Connor Davies is ready to help clients meet today's ever-changing economic conditions and manage the growing complexities of the regulatory environment

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.