PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

DGC
ACCOUNTING • TAX • ADVISORY
A DIVISION OF PKF O'CONNOR DAVIES, LLP

Cyber Roundup – December 2022

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

Long gone are the days when to be a “hacker,” you needed significant drive and technical knowledge to be a real threat. With an estimated annual cybercrime cost of $10.5 trillion globally by 2025, a portion of that growth will be directly attributable to the ease of access and low barrier of entry for the cybercriminal community. The cyber threat will not only persist, it will thrive in the coming years. Creating a true cyber strategy now – more than ever – is critical.

Talk to us here at PKF O’Connor Davies for assistance with designing and/or updating your cybersecurity plan.

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.

- **Across 1,489 ransomware-related incidents, $1.2 billion in ransom payments were made through U.S. banks in 2021, according to a report by the Department of Financial Crimes Enforcement Network.** The dollar amount processed is almost three times the amount in 2020. The report further notes that almost 75% was tied to Russian cyber criminals.

- **U.K. intelligence official, Sir Jeremy Fleming, warned about the increased threat of hackers-for-hire to governments and businesses.** He notes that the “grey market” which allows an individual to procure either hacking services or hacking software is fueling the unpredictability and severity of attacks from countries and individuals with no true cyber capabilities or knowledge.

- **According to a report issued by CyberSheath, nearly 87% of U.S. defense contractors are lacking basic cybersecurity measures in the protection of information classified as Controlled Unclassified Information.** According to the report, non-compliance is primarily driven by a lack of understanding of the regulations.

Tom’s takeaway: Defense contractors play a key role in ensuring national security. As part of their contracts, they are entrusted with information that needs to be controlled and protected. As a firm that specializes in working with defense contractors to protect their information, we are sympathetic to the complexity, and sometimes confusing nature, of the regulations they are required to follow. If you are a defense contractor, don’t risk losing your contracts or procuring new ones as a result of weaknesses in your cyber program. Should you need assistance, we have a dedicated team ready and willing to help you navigate the requirements and build an effective cybersecurity program

- **Dropbox reported a breach as a result of a cybercriminal successfully phishing an employee and gaining access to Dropbox source code stored in GitHub**. The code and date related to it exposed the information of current and past employees, customers, leads and vendors. Dropbox has claimed that customer accounts, passwords and payment information have not been compromised. While Dropbox did have Multi-Factor Authentication enabled for GitHub, the phishing attack was designed, as such, to bypass it.

- **An international law enforcement effort resulted in the take down of a phone number spoofing service called iSpoof.** The service, which was actively used by criminals to commit fraud, allowed them to impersonate the phone numbers of trusted companies and organizations to trick individuals into providing sensitive information or granting access to their devices. The service, which started operations in December 2020, had amassed 59,000 users.

Tom's takeaway: While law enforcement took down one of these services, many still remain and are easily accessible to any individual who can utilize Google. As penetration testers, we utilize such services to mimic the tactics of the cybercriminals and trick the employees we target. I personally have noticed an increase in spoofed calls of financial institutions over the past year. What is important is that your awareness training program educates your users on this threat. One of the key tactics we teach in our awareness training is transferring the control of the call from the attacker to the user. While an attacker can manipulate and spoof the call coming in, they cannot intercept the outbound call if the user follows their training and calls a known trusted number, should they believe it to be legitimate, even if it matches the caller.

- **Zurich, a leading insurance provider, settled a $100 million lawsuit from Mondelez International, a victim of the NotPetYa computer virus that circled the globe in 2017 causing massive damages to companies at an estimated $10 billion globally.** The insurance provider initially denied the claim, stating it was an act of war. A New Jersey court of law ruled in favor of Mondelez under the premise it was not an act of war; however, what Mondelez suffered was collateral damage from a conflict to which they were not a direct party. The implications of this ruling could have a drastic impact on the cyber insurers and their categorization of an act of war.

- **The SEC has set their sights on SolarWinds for the massive breach it suffered in 2020, announcing an enforcement action.** The SolarWinds hack resulted in a piece of software that is installed on countless company networks across the world being manipulated so the attackers can gain access to the SolarWinds customers that use the software. The enforcement action is the result of violations of U.S. securities laws related to "cybersecurity disclosures and public statements, as well as its internal controls and disclosure controls and procedures." This action continues to set the tone that companies must have a strong cybersecurity program or they will be held accountable when failures occur.

- **Cybercriminals were identified taking advantage of a popular TikTok trend where a user creates a video using a filter called "Invisible Body," that leaves just a silhouette of the person in the video.** The criminals would post videos and links claiming to have software that would remove the filter. If a user installed the software, it was designed to steal passwords, cryptocurrency accounts and other types of sensitive information. The accounts have since been suspended; however, it reached over a million users before being taken down.

Tom's takeaway: The cyber threat is more than just a business issue or matter of national security, it is a problem that can impact you, your family and those you care about on a personal level. The impact to a person could be significant and, at times, life-altering. Cybercriminals have no boundaries, so the young and impressionable are very much a target. Take the time to ensure your children and family members understand the cyber threat. Education is half the battle and the future of cyber awareness could very well start in the home.

- **The Cybersecurity and Infrastructure Security Agency (CISA) has published a decision tree to help companies prioritize vulnerabilities and their response thereto.** Vulnerability management is something many organizations struggle with given the sheer volume of vulnerabilities that exist and continue to be identified. In an ideal world, security teams could tackle and remediate all vulnerabilities; however, that is not realistic. As a vCISO that helps manage the vulnerability programs of multiple companies, a risk-based approach is the only feasible option to control the risk with often limited resources. I encourage you to review the decision tree here or share with your IT teams. It may just help make what feels like an impossible task, that much more manageable.

Contact Us

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Principal
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Nick DeLena, CISSP, CISA, CRISC, CDPSE
Partner
Cybersecurity and Privacy Advisory
ndelena@pkfod.com | 781.937.5191

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.