PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – July 2023

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

If your organization's cybersecurity is breached, according to a recent Verizon report it will be by one or more of these means: stolen credentials, phishing, and/or vulnerability exploitation. Having the mindset that it's going to happen, will best position you to do what you can to mitigate these malicious techniques and to ensure your cybersecurity program is functioning effectively.

- **Stolen Credentials –** evade with Employee Training**,** Multi-Factor Authentication and Dark Web Monitoring
- **Phishing –** avoid by Employee Training, Testing and Reporting
- **Vulnerability Exploitation –** guard against through Monitoring, Patching and Penetration Testing

Cybersecurity is not an issue, until it is an issue. With PKF O'Connor Davies, you will know better service.

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.

- **Verizon's 2023 Data Breach Investigation Report, an industry staple in trending the cyber landscape, notes the following interesting stats:**
    - Business email compromise has doubled from the prior year, now accounting for 50% of incidents in the social engineering category.
    - 83% of incidents involve external threat actors.
    - 74% of breaches are attributed to the human element, e.g., error, use of stolen credentials, privilege abuse, social engineering.
    - 49% of breaches involve credentials.
    - The three primary ways organizations are breached are stolen credentials, phishing and vulnerability exploitation.

- **A major vulnerability is a file transfer tool called MOVEit.** It has resulted in the breach of data across hundreds of different companies around the globe impacting countless individuals. A vulnerability in the software allowed external parties access to data used by the software. The vulnerability was actively exploited before an official patch could be provided by the software creator, Progress Software. A class action lawsuit as a result of the breach is pending. An active listing of impacted companies can be found here.

- **Over 100,000 stolen credentials belonging to ChatGPT accounts have been found readily available in Dark Web marketplaces.** Depending on how the account is used, this may result in the exposure of sensitive company information. ChatGPT by default retains all conversations or information entered.

  Tom's Takeaway: The use of AI and tools, such as ChatGPT, need to become, if not already, an area of risk discussion within your organization. As a business, you need to think about if and how you may allow the technology and under what circumstances. The development of AI-related policies and controls has become an area in which we are actively assisting. While these tools may provide great value, if not managed and understood effectively, they can also present great risk.

- **In response to Texas' transgender legislation, the City of Fort Worth suffered a targeted attack that resulted in a breach of data.** The cybercriminal group SiegedSec declared that they accessed approximately 500,000 internal documents.

  Tom's Takeaway: While the majority of attacks may be financially motivated, as you can see from this incident, that isn't always the case. Being targeted as a result of political positions or issue support could very well place your organization in the cross hairs. As part of your risk assessment process, you should be aware of your exposure to these types of attacks.

- **Access to a military satellite was spotted for sale on a Russian-speaking hacker forum.** The quoted price is $15,000. The seller is offering to place the sale in escrow to ease any buyer concerns of just handing over the cash. If true, the security implications could be significant.

- **Toyota suffered a data breach as a result of a cloud misconfiguration that has existed for over eight years.** Over 260,000 customer accounts were impacted. Toyota has taken measures not only to correct the misconfiguration but also to implement software to monitor all cloud configurations going forward.

  Tom's Takeaway: Security in the cloud is what you design it to be. Many still have the notion that because it is "in the cloud" it is inherently secure. For example, simply subscribing to Microsoft's Office 365 to manage and access your email is not going to cover **all** your risks. Various administrative and technical controls still need to be implemented and monitored. As we continue with the theme of risk management in ***Roundup***, your cloud exposure is another area that needs to considered.

The following are **ransomware-related events** in the month of June.

- **In a report released by Kaspersky's Digital Footprint Intelligence Team, ransomware accounted for 57% of the Malware-As-A-Service (MAAS) offerings on the Dark Web.** MAAS is a business model in which individuals or cyber groups lease access to the software and platforms needed to commit the attacks.

- **Reddit, which suffered a breach in February 2023, is now being subjected to a $4.5 million ransom to prevent the leakage of the 80GB of confidential information claimed to have been stolen.** The attackers are also requesting that the Company abandon its new Application Programming Interface (API) pricing. An API is what allows developers to create code to interface (i.e., talk) with other applications.

- **Point32Health, a non-profit health insurer, reported a breach as a result of a ransomware attack that impacted 2.5 million customers.** The attack was launched on April 17 disrupting operations; however, the attackers were actively exfiltrating data between March 28 and April 17, 2023 when the attack was fully executed.

- **The Des Monies Public School District, the largest District in Iowa, reported that 6,400 individuals had their data compromised stemming from a ransomware event that occurred In January 2023.** The District has stated they will not pay any ransom. Based on statistics tracked by Emisoft, 37 school districts across the U.S. have suffered a ransomware attack year-to-date.

- **St. Margaret's Health, an Illinois-based hospital, is closing down its business due in part to a ransomware attack that occurred two years ago.** The impact of the attack resulted in the Hospital being unable to submit claims for payment to the insurers, ultimately resulting in a financial domino effect from which they could not recover.

  Tom's Takeaway: The cost of not having an effective cybersecurity program, designed to not only protect, but respond and recover, can be the difference between remaining in business or closing down. A core value proposition of our services is to do everything we can to help you ensure the sustainability of your business.

- **Enzo Biochem, a New York-based life sciences and molecular diagnostics company, reported a breach stemming from a ransomware attack impacting 2.5 million individuals.**

Highly sensitive information such as Social Security numbers and health information were compromised as part of the attack.

Contact Us

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
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.