PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – February 2023

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

As the saying goes, *fool me once, shame on you; fool me twice, shame on me.* One of the bulleted items this month concerns the breach of confidential customer data by a cellular service provider. In this particular case, the company failed to protect consumer information **eight times in a five-year period**. While you are probably thinking this will never happen to my business, let us help you not to fail – even once. No guarantees, but *better safe than sorry*.

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 dark web job market is booming, according to a report by Kaspersky that analyzed 200,000 job ads across 155 dark web sites.** The highest paying jobs consisted of developers at $20,000 per month and attack specialists at $15,000 per month. Developers accounted for 61% of the job ads posted by the Hacking and APT groups. In direct competition with commercial employment, the jobs also offer such things as remote work, paid time off and sick leave, close-knit teams and career prospects. The article includes a number of interesting statistics and is worth the read.

- **Cyber-Crime-as-a-Service continues to fuel the cyber threat landscape, according to Sophos' 2023 Threat Report**. The "as-a-service" model consists of what they dub the "naughty nine" as follows:

    1. **Access-as-a-Service** – Access to already compromised accounts and systems are sold.
    2. **Malware distribution-as-a-Service** – Facilitates the distribution of malware within specific regions or sectors.
    3. **Phishing-as-a-Service** – Phishing campaign design, execution and monitoring.
    4. **OPSec-as-a-Service** – Designed to hide Cobolt Strike infections and reduce the likelihood of detection and attribution.
    5. **Crypting-as-a-Service** – Facilitates the encryption of malware to avoid detection by malware solutions.
    6. **Scamming-as-a-Service** – Facilitates the design and execution of a scam.
    7. **Vishing-as-a-Service** – Facilitates the renting of a voice system to receive calls with an AI option so a bot can be used to handle the call.
    8. **Spamming-as-a-Service** – Facilitates spamming activities.
    9. **Scanning-as-a-Service** – Provides access to commercial security tools to find and exploit vulnerabilities.

- **For the eighth time in five years, T-Mobile has again reported a data breach, this time exposing the data of approximately 37 million customers.** Information breached consisted of customer data, such as customer name, billing address, email, phone number, date of birth and T-Mobile account number were exposed. The Company has stated no sensitive customer financial information was compromised.

- **PayPal reported a breach that impacted 35,000 customer accounts**. Impacted information consisted of highly sensitive information, such as social security and tax identification numbers. The attack was the result of a credential stuffing attack against their users. PayPal has offered two years of identity monitoring services.

Tom's Takeaway: In the case of PayPal, the breach wasn't the result of any security flaw or breakdown in security at PayPal; it was, instead, the result of poor password practices by its user base. Credential Stuffing is the result of an individual using the same password across multiple different sites. Should one of their accounts be breached, all of their other accounts become at risk. Any financial account you have should not only have a unique password, but also have multi-factor authentication enabled. In my opinion, every financial institution should make multi-factor authentication non-negotiable if persons want to transact online.

- **iRobot sues logistics company Expeditors International for losses it sustained as a result of Expeditors not having a business continuity plan to execute after a cyberattack it experienced.** iRobot relied on Expeditors and was contractually engaged with them to receive and store iRobot's products and ship them within 24 hours of receipt of a customer order. iRobot claims it incurred almost $2.1 million in additional expenses as a result of having to shift to a new logistics provider and back charges from retailers during their outage.

  Tom's Takeaway: In this day and age, if you have a business, the increasing expectation is going to be that you have a cybersecurity program in place to protect data and perform the services in which the business is engaged. What is unfortunate is that many companies, both for- and not-for-profit, continue to turn a blind eye or fail to adequately understand and assess their risk and plan for the worst. Asking your IT staff if you are protected – and accepting that on blind faith – is not performing adequate due diligence or exercising due care. Third-party cybersecurity assessments or engaging with business continuity planning advisors, when conducted by qualified professionals, should serve to not only help you assess your cyber risk and strengthen your resiliency, but protect your company and its stakeholders.

- **Bridgewater-Raritan School District in New Jersey reported a cybersecurity incident.** An unauthorized individual gained access to insurance enrollment information for employees, exposing their SSNs. Letters have been sent to the impacted employees.

- **"Honor" among thieves:** The LockBit ransomware group provided a free decryptor key and issued an apology to The Hospital for Sick Children noting that one of LockBit's members violated their rules in attacking the Hospital with its ransomware. The ransomware group prohibits the attack on hospitals or any institution that could result in death from the attack due to encryption; however, stealing data from institutions is authorized.

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