Cybercrime: A Year in Review

Lizzi Esparza
eesparza@mwlaw.com
(479) 464.5660

01/25/2023

Information security will remain a top priority for all industries in 2023. Healthcare, government, and education will likely continue to be top targets for ransomware attacks, with for-profit businesses close behind. In 2022, most breaches could be traced back to compromised employee credentials and phishing attempts.

Here are ten highlights of both large- and small-scale incidents from 2022 which illustrate these cybercrime trends.

- On January 1, 2022, **Twitter** discovered a vulnerability in its network that allowed a hacker to steal data from over 5.4 million Twitter accounts, which were then listed for sale. The data stolen included email addresses and phone numbers from celebrities and companies in addition to non-famous account holders.

- In February, over 1.9 million persons had their personal and medical information exposed following a ransomware attack on debt collection company **Professional Finance Company**. The company has since employed artificial intelligence tools, 24/7 monitoring of its network, and has contracted with two cybersecurity firms to prevent future attacks.

- In March, a breach of **Marriott**'s systems allowed hackers to steal the personal information of over 5.2 million guests. In addition to contact information, such as name, phone number and email, personal information such as loyalty account information and personal hotel room preferences of Marriott's guests were stolen.

- The **State Bar of Georgia** was hit with a ransomware attack in April that affected tens of servers and workstations. The organization has not released many details regarding the incident but has stated that personal information of members and current and former employees were potentially exposed. The State Bar is offering all potentially affected persons complimentary credit monitoring and identity protection services.

- In June, a vulnerability in student loan servicer **Nelnet**'s systems allowed unauthorized persons to access the personal information of over 2.5 million users. Affected information included names, home and email addresses, phone numbers and social security numbers.

- Password locker **LastPass** discovered a compromised employee account in August, which allowed access to personal information including basic customer account information and related metadata, and encrypted password vaults. According to the company, the password vaults remain secure because only the user holds the encryption key. Still, the company recommended strengthening and

updating passwords, and to not reuse the master password for any non-LastPass account.

- The **Internal Revenue Service** discovered in September a coding error that allowed ordinarily confidential tax data to be publicly accessible on its website. Though not the result of malicious outsiders, this human error caused the disclosure of about 120,000 taxpayers' confidential tax information.

- Several of rideshare company **Uber**'s internal databases were compromised in September when a hacker gained access through employee login credentials. The hacker gained entry into the system through a technique known as "multifactor authentication fatigue" in which the hacker spammed the employee with two-factor approval requests until one was eventually accepted.

Here at home.....

- **Miller County, Arkansas** fell victim to a ransomware attack this November that spread to 54 other Arkansas counties. A virus caused outages at government buildings, some of which lasted two weeks. Officials say that no sensitive information was exposed during the attack.

- The **Little Rock School District** ended the year with a ransomware attack that occurred in December. Although the incident is still fresh and few details have been released, the district has revealed that some data was taken, but it does not know which. The district's Board approved a $250,000 payment to the threat actor (a move that goes against FBI and other agency guidance) to return the data. As of today, the district has not yet disclosed whether the data has been returned.

Although threat actors grow more sophisticated each day, there are valuable steps to take to protect systems from unauthorized access. Businesses and organizations should train all employees frequently on how to spot and report phishing attempts, implement multifactor authentication, monitor networks and repair known system vulnerabilities. Developing a breach response plan and testing the plan is vital to help your company act quickly to lock down networks and limit further damage in the unfortunate case that a breach does occur.