DATA BREACHES: THINK YOU'RE PROTECTED?

Caitlin Wiley and Kayla Watts

Target Breach:

- 41 Million debit and credit card number stolen
- Access gained to Point of Sale system via third party credentials
- Target failed to have proper network segmentation
- Target allowed third party systems to have access to its payment system
- Target paid an $18.5 million multistate settlement, the largest ever for a data breach

What is Network Segmentation?

Network segmentation is the process of dividing a network into smaller sections.

How the Target Breach Happened

Access was gained to Targets online network via stolen credentials from a third-party HVAC company.
The hackers then proceeded to upload malware to the system to harvest data such as: full names, phone numbers, email addresses, payment card numbers, credit card verification codes.
This worked because the malware would RAM (Random Access Memory) scrape the information from the systems. The malware would then place the sensitive information onto a "dump" server that was set up by the hackers. The hackers would then harvest the data from their server and place it for sale on the dark web.

Rank	State	Number
1	California	50,132
2	Florida	27,178
3	Texas	27,178
4	New York	21,371
5	Washington	13,095
6	Maryland	11,709
7	Virginia	11,674
8	Pennsylvania	10,914
9	Illinois	10,337
10	Indiana	9,746

This lists top 10 states by number of Cybercrime victims as of 2019

Capital One:

- Second largest financial company in the US
- Breach occurred March 22, 2019
- Breach in data was not detected until July 19 when the company received an email containing information leading to Paige Thompson's GitHub page.

Email Received by Capital One:

Hello there, there appears to be some leaked s3 data of yours in someone's github/gist. Let me know if you want help tracking them down. Thanks

The link in the email contained huge amounts of credit card application data, social security numbers, bank account numbers, and a file with the code used to leak this information.

Types of Cyber Fraud:

- Business email compromise (BEC)
- CEO Fraud
- Identity theft
- Phishing
- Ransomware
- Smishing
- Social engineering
- Spear phishing

Ways Cyber Fraud Can Occur:

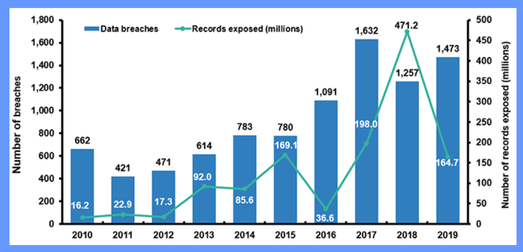
- Easy system access
- Storing data in a small space
- Negligence
- Loss of evidence
- Complex coding's

Marriott Hotels:

- September 8th, 2018
- Noticed they had been hacked when a security tool flagged an unusual database query
- Credit card numbers they stored were encrypted – but the encryption keys were on the same server
- Passport numbers were simply saved in the clear, most not encrypted
- Incurred $28 million in expenses related to this breach but cyber insurance covered most of it

What Is Cyber insurance?

- Specialty lines insurance product intended to protect businesses and individuals generally from risks related to information technology infrastructure, information privacy, and information governance liability



Cyber Fraud Prevention Tips:

- Be click aware
- Pay attention to details
- Ask questions
- Slow down and read
- Keep your computer and devices up to date
- Shop carefully
- Never use free public Wi-Fi
- Do not give out personal information

EB-5 Immigrant Investor Program Fraud:

- 3 Houston developers misused investor funds raised from 90 Chinese investors under this program
- Told the investors their funds would be used for large mixed-use real estate developments
- They took almost $50 million

Why Commit Financial Statement Fraud?

- Personal benefits (bonuses for meeting goals)
- Making the company look more profitable than it is
- Increasing investors interest in the company because revenues are high

Common Red Flags:

- Living beyond your means
- Having personal financial difficulties that suddenly are fixed
- Being unusually close with certain vendors or customers
- Having control issues in the business

Methods of Financial Statement Fraud:

- Fictitious revenue and sales
- Phantom revenue posting
- Shell companies
- Asset manipulation
- Altered accounting records and financial statements
- Inflated company valuation

How to prevent this type of fraud:

- Strong internal controls
- Independent auditors
- Have a hotline/reporting system
- Do not tie significant money amounts to bonuses based on short term goals
- Company culture involving honesty and integrity