Cyber Security Overview

4/13/2022

Gregory Pope

Cyber Security Overview

There are two types of organizations:

1. Those that know they are being attacked.

2. Those that do not know they are being attacked.

Cyber Security Factoids

- Cost of Cyberattacks $7 Trillion globally in 2021 [1]

- US Gross National Product = $20 Trillion [2]

- Average cost of an attack = $4.24 Million dollars [3]

- A cyberattack occurs every 39 seconds [4]

- During this talk 92 cyberattacks will occur (3600/32)

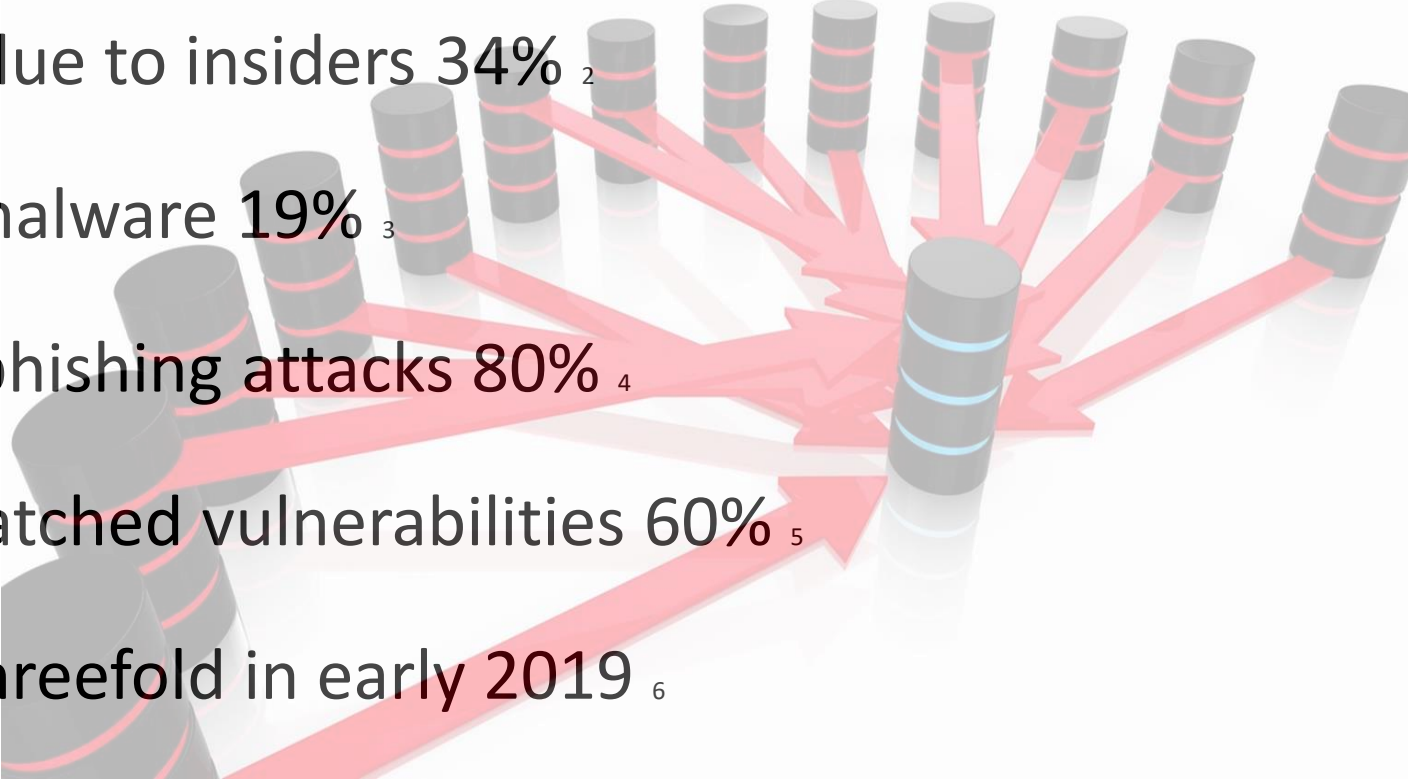1. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
2. https://www.bea.gov/news/2021/gross-domestic-product-4th-quarter-and-year-2020-advance-estimate#:~:text=Current%2Ddollar%20GDP%20decreased%202.3,(tables%201%20and%203)
3. https://www.upguard.com/blog/cost-of-data-breach .
4. https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/, How many cyberattacks took place in 2021?

Attack Factoids

- Malware delivered through email 94% [1]

- Data breaches that occurred due to insiders 34% [2]

- Data breaches that involved malware 19% [3]

- Security breaches a result of phishing attacks 80% [4]

- Security breaches due to unpatched vulnerabilities 60% [5]

- Attacks on IoT devices grew threefold in early 2019 [6]

1,2,3 - 2020 data breach Investigation's report, https://enterprise.verizon.com/resources/reports/dbir/
4,5,6 - Top cybersecurity facts, figures and statistics, https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Attack Surfaces (Network vs Applications)

- Cause was network vulnerabilities 80%

- Network vulnerabilities considered high or critical risk 2%

- Cause was application vulnerabilities 20%

- Application vulnerabilities considered high or critical risk 20%

source: 2019 VULNERABILITY STATISTICS REPORT, edgescan™ January 2019

Average total cost and frequency of data breaches by initial attack vector

Measured in US$ millions
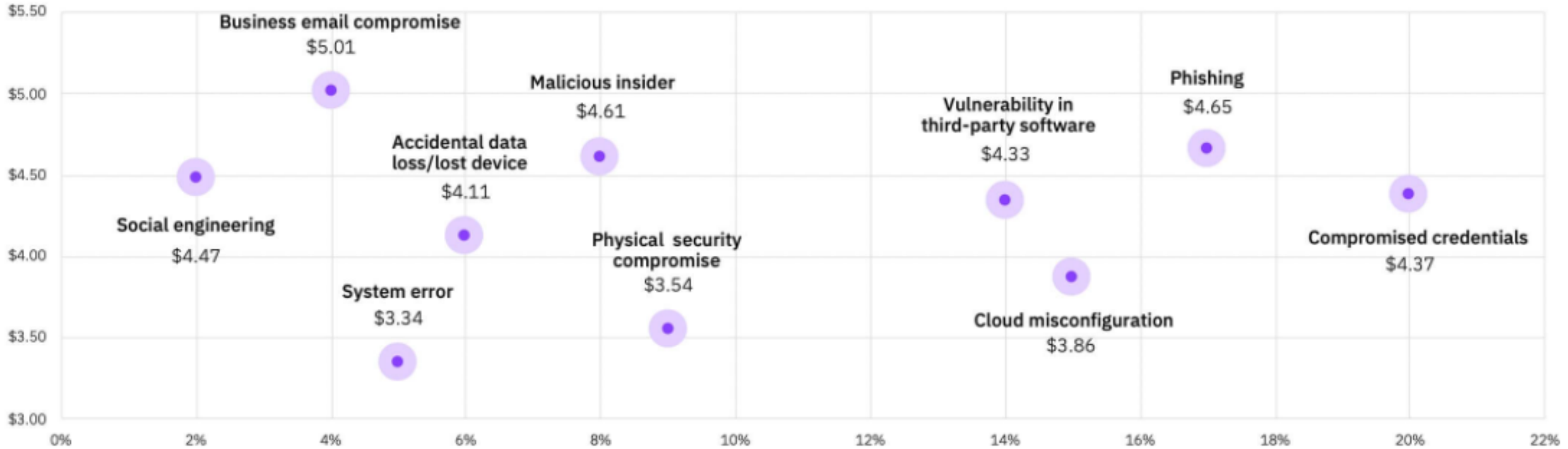
Source: Cost of a data breach report 2021 by Ponemon Institute and IBM

Methods of Cyber Attacks

- Malware

- Phishing

- Man-in-the-Middle

- Denial of Service

- SQL Injection

- Buffer Overflow

- Zero Day Exploit

Source: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~how-cyber-attacks-work

- DNS Tunneling

Malware Types

- Adware

- Bots

- Rootkits

- Viruses

- Trojan

- Spyware

- Keylogger

- Ransomware

Source: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~how-cyber-attacks-work

- Scareware

Cyber Security and Software Quality Overlap

- SAST – Static Analysis Security Testing

  Finds:

  Null Pointer Dereferences

  Buffer Overflows

  Uninitialized Variables

  Opaque Predicate

  Dead Code

  Tainted Flow

- DAST – Dynamic Analysis Security Testing

  Finds:

  Test Code Coverage

  Addressing errors

  Fuzzing

  Concolic Testing .....

- These are both software bugs and potential vulnerabilities that hacker's search for and exploit.

Sources:
IEEE (NCSU) Study ~ 33 million LOC C, C++, since 2001 NORTEL (Network Services Code
LLNL Study ~ 6 million LOC C,C++, Scientific Codes since 2006
MITRE Common Weakness Enumeration (CWE) data base http://cwe.mitre.org/

Cyber Security Standards

- ISO/IEC 27001
  - Implement an Information security management system
  - Set of procedures that states the rules and requirements which has to be satisfied in order to get the organization certified
  - Keep all the technology up to date, the servers should exist without vulnerabilities
  - Organization has to be audited after the specified interval to remain compiled to this standard

- PCIDSS
  - Payment Card Industry Data Security Standard
  - For organizations that accept credit card payments

- HIPAA
  - Health Insurance Portability and Accountability Act
  - Ensure that their patient's data are fully protected and cannot be leaked anyway

- FINRA
  - Financial Industry Regulatory Authority
  - Financial bodies that handle the funds or aggressively engaged in financial transactions

- GDPR
  - General Data Protection Regulation
  - Make sure that the user's data is secure and cannot be accessed without proper authorization
  - Large fines for not complying

Source: https://www.educba.com/cyber-security-standards/

Cyber Security Standards

- Cobit 5 Framework https://www.invensislearning.com/blog/what-is-cobit-5/
  - Ideal to start out or for small companies
  - Framework, Maturity Model, Process Descriptions, Control Objectives, Management Guidelines

- ISA 62443-2-1:2009 and 2013 https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99
  - Mostly Industrial Automation and Control Systems Security
  - Hardware and software systems such as DCS, PLC, SCADA
  - Networked electronic sensing, and monitoring and diagnostic systems

- NIST SP 800-53 Rev 5 https://www.nist.gov/cyberframework/framework

- NIST Security Framework Ver 1.1 https://www.nist.gov/cyberframework/framework

- Crosswalk https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Source: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

MITRE Enterprise ATT&CK™ Framework

More Information

- **MITRE Common Weakness Enumeration (CWE) data base**
  - Web site: http://cwe.mitre.org/

- **MITRE ATT&CK knowledgebase**
  - https://attack.mitre.org/

- **NIST National Vulnerability Database (NVD)**
  - https://nvd.nist.gov/vuln

Source: attack.mitre.org

Case Study

Overview

Organization

Governance

Causes

Mitigation Measures

Lessons Learned

Timeline Overview

- March 8, 2017 -> NIST issues alert to patch Apache Struts

- March 10, 2017 -> Attack on unpatched Equifax Customer Dispute Web Server begins

- July 30, 2017 -> Equifax discovers unpatched Customer Dispute Web Server

- September 7, 2017 -> Equifax notifies customers of a cyber-attack

- March 10 and July 30, 2017 -> 145.5 Million customer PII records exfiltrated to Chinese IP address

- September 26, 2017 -> Equifax shares down 26%

- Follow on -> $90 million in attack related costs, $525 million in class action suits

Sources: https://www.ciodive.com/news/what-caused-the-equifax-breach-failure-to-patch-a-bug/504945/
https://www.secureworld.io/industry-news/day-by-day-timeline-of-equifax-breach

Harvard Business School 9-118-031, Data Breach at Equifax. Suraj Srinivasan, Quinn Pitcher, Jonah S. Goldberg, exhibit 8, Timeline of Equifax Breach
Anders Merlin, "Three Equifax Managers Sold Stock Before Cyber Attack Reveled", Bloomberg, Sept. 7,2017.

Organization

- Chief Security Officer (CSO) reports to Chief Legal Officer (CLO) who reports to Chief Executive Officer (CEO)

- CSO is a math major, former software engineer

- CLO is a lawyer, no IT or Security Experience

- CEO, CIO, CSO forced to resign

- Three managers indited for insider trading

Source: https://www.nbcnews.com/business/consumer/equifax-executives-step-down-scrutiny-intensifies-credit-bureaus-n801706

Equifax Organization Chart

CSO not part of senior staff ➡ Susan Mauldin CSO

Patching accountability spread over three organizations ➡ Vulnerability Assessment Team / Countermeasures Team / Global Threat and Vul. Management Team

Org chart:
- Richard Smith, CEO
  - John Kelley, CLO
    - Susan Mauldin, CSO
  - David Webb, CIO
    - Graeme Payne, CIO Global Platforms
      - Vulnerability Assessment Team
      - Countermeasures Team
      - Global Threat and Vul. Management Team

Governance

Had been given a failing grade for security in prior audits

Was ranked last compared to peers for security

Had been criticized for not maintaining accurate inventories

Was not using a nationally accepted standard for security

Had not acted on recommendations from prior audits

Source: United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach", Staff Report March 2019, p36-43.

Causes

- Software with identified vulnerability not patched for 5 months

- Hundreds of SSL certificates not current, the SSL visibility appliance not working

- File integrity monitoring (FIM) was not operative

- Software inventory not up to date

- Application scanner not detecting Apache Struts on customer dispute web Server

- Patching customer dispute web site was involved manual process (took 11 days)

United States House of Representatives Committee on Oversight and Government Reform, "The Equifax Breach", Majority Staff Report, December 2018, p 71-72

Regular Red Team exercises

Use of white hat hackers or bounty program

Regular pen testing of applications

Would have exposed FIM and visibility appliance inoperative

Red team exercise would have been able to identify vulnerability

Ongoing reconnaissance of industry threats

Mitigation Measures That

Could Have Prevented the Attack

Sources: Professional Certificate in Cyber Security, MIT
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
https://www.fcc.gov/cyberplanner

Mitigation Measures That Could Have Prevented the Attack

- Use of defense in depth and Segmentation
- Use of least privilege
- Use of zero trust
- Isolate PII data bases from other systems
- Encryption of PII at rest
- Retain Logs longer than 30 days
- Accurate Inventory of Resources
- Security Culture from the top down
- Single Point of Accountability, Reports to CEO
- Automated Patching
- SIEM/SOAR
- Act on prior audit findings
- Adoption of Security Standard

Lessons Learned

- This attack was preventable

- The importance of valuing cyber security

- Value of comprehensive risk assessment and mitigations

- Value of mitigation measures

- Value of having a Response Plan

- Value of acting on Audit and Assessment findings

- High cost of cyber attacks

Source: The Equifax Breach of 2017, MIT Cybersecurity Capstone, Gregory Pope, March 2022
https://www.wired.com/story/how-to-stop-breaches-equifax/

Why? Speculation on my Part

- The 145.5 million records of stolen PII has never been seen since. It has not been offered for sale on the dark web.

- The list of names of consumers, where they work, and that they have credit problems could be of great use to espionage agents.

- The Equifax data combined with the 2015 OPM attack data of 24 million records of security clearance holders allows espionage services to recruit from cleared staff with credit problems.

What Can I Do:

- Recognize phishing emails, just say no to clicking the link

- Use strong passwords, change frequently

- Do not leave default passwords

- Do not use the same passwords for personal and business

- Don't open Word or Excel attachments with Macros

- Update and patch systems ASAP

- Limit your job description on social media accounts (sound unimportant)

- Limit mentioning security tools names used on job postings

- Know who you are talking too on the phone, especially help desk

- Report stolen or lost credentials

Source: Professional Certificate in Cyber Security, MIT, Modules 4,11,13,14