

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)

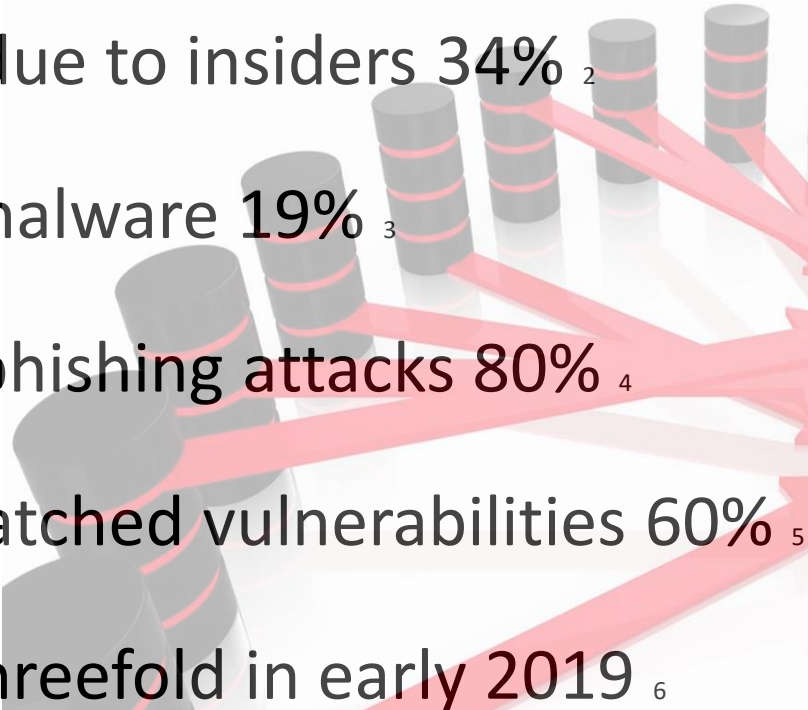
1. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>

2. [https://www.bea.gov/news/2021/gross-domestic-product-4th-quarter-and-year-2020-advance-estimate#:~:text=Current%2Ddollar%20GDP%20decreased%202.3,\(tables%201%20and%203\)](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
- DNS Tunneling

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

Malware Types

- Adware
- Bots
- Rootkits
- Viruses
- Trojan
- Spyware
- Keylogger
- Ransomware
- Scareware

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

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>

More Information

- MITRE Common Weakness Enumeration (CWE) data base

<http://cwe.mitre.org/>

- MITRE ATT&CK knowledgebase

<https://attack.mitre.org/>

- NIST National Vulnerability Database (NVD)

<https://nvd.nist.gov/vuln>

	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Forced Authentication	Hooking	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification	Password Filter DLL	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts	LLMNR/NBT-NS Poisoning	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking	Securityd Memory	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture		Remote File Copy
AppCert DLLs	File and Directory Discovery	System Information Discovery	Distributed Component	Dynamic Data Exchange	Automated Collection	Scheduled Transfer	Multi-Stage Channels
Hooking	Private Keys	Keychain	Object Model	Mshta	Clipboard Data	Data Encrypted	Web Service
Startup Items	Hidden Files and Directories	Input Prompt	Pass the Ticket	Local Job Scheduling	Email Collection	Automated Exfiltration	Standard Non-Application Layer Protocol
Launch Process	Launchd	Security Software	Exploitation through Remote Command	Trap	Screen Capture	Exfiltration Over Other Network Medium	Communication Through Removable Media
Application Shimming	LC_MAIN Hijacking	Two-Factor Authentication	Windows Admin Shares	Launchctl	Data Staged	Exfiltration Over Alternative Protocol	Multilayer Encryption
AppInit DLLs	HISTCONTROL	Interception	Remote Desktop Protocol	Space after Filename	Data from Network Shared Drive	Data Transfer Size Limits	Standard Application Layer Protocol
Web Services	Clear Command History	Account Manipulation	Pass the Hash	Execution through Module Load	Data from Local System	Data Compressed	Commonly Used Port
Service Registry Permissions Weakness	Gatekeeper Bypass	Replication Through Removable Media	Exploitation of Vulnerability	Regsvcs/Regasm	Data from Removable Media		Standard Cryptographic Protocol
Scheduled Task	Hidden Window	Input Capture	Shared Webroot	Logon Scripts			Custom Cryptographic Protocol
New Service	Deobfuscate/Decode Files or Information	Network Sniffing	Remote Services	Regsvr32			Data Obfuscation
File System Permissions Weakness	Credential Dumping	Credentials in Files	Application Deployment Software	PowerShell			Custom Command and Control Protocol
Port Monitors	Regsvcs/Regasm	Exploitation of Vulnerability	Application Deployment Software	Rundll32			Connection Proxy
Screensaver	Access Token Manipulation	Access Token Manipulation	Remote System Discovery	Scripting			Uncommonly Used Port
LSASS Driver	Bypass User Account Control	Bypass User Account Control	Permission Groups Discovery	Graphical User Interface			Multiband Communication
Browser Extensions	Process Injection	Process Injection	Process Discovery	Command-Line Interface			Fallback Channels
Local Job Scheduling	SID-History Injection	Component Object Model Hijacking	System Service Discovery	Scheduled Task			
Re-opened Applications	Component Object Model Hijacking	Component Object Model Hijacking		Windows Management Instrumentation			
Rc.common	Code Signing	Code Signing		Trusted Developer Utilities Service Execution			
Login Items	Redundant Access	Redundant Access					
LC_LOAD_DLLS	File Deletion	File Deletion					
Launch Agent	Timestamp	Timestamp					
Hidden Files and Directories	NTFS Extended Attributes	NTFS Extended Attributes					
.bash_profile and .bashrc	Process Hollowing	Process Hollowing					
Trap	Disabling Security Tools	Disabling Security Tools					
Launchctl	Rundll32	Rundll32					
Office Application Startup	DLL Side-Loading	DLL Side-Loading					
Create Account	Indicator Removal on Host	Indicator Removal on Host					
External Remote Services	Indicator Removal from Tools	Indicator Removal from Tools					
Authentication Package	Indicator Blocking	Indicator Blocking					
Netsh Helper DLL	Software Packing	Software Packing					
Component Object Model Hijacking	Masquerading	Masquerading					
Redundant Access	Obfuscated Files or Information	Obfuscated Files or Information					
Security Support Provider	Binary Padding	Binary Padding					
Windows Management Instrumentation	Install Root Certificate	Install Root Certificate					
Event Subscription	Network Share Connection Removal	Network Share Connection Removal					
Registry Run Keys / Start Folder	Rootkit	Rootkit					
Change Default File Association	Scripting	Scripting					
Component Firmware							
Bootkit							
Hypervisor							
Logon Scripts							
Modify Existing Service							

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>

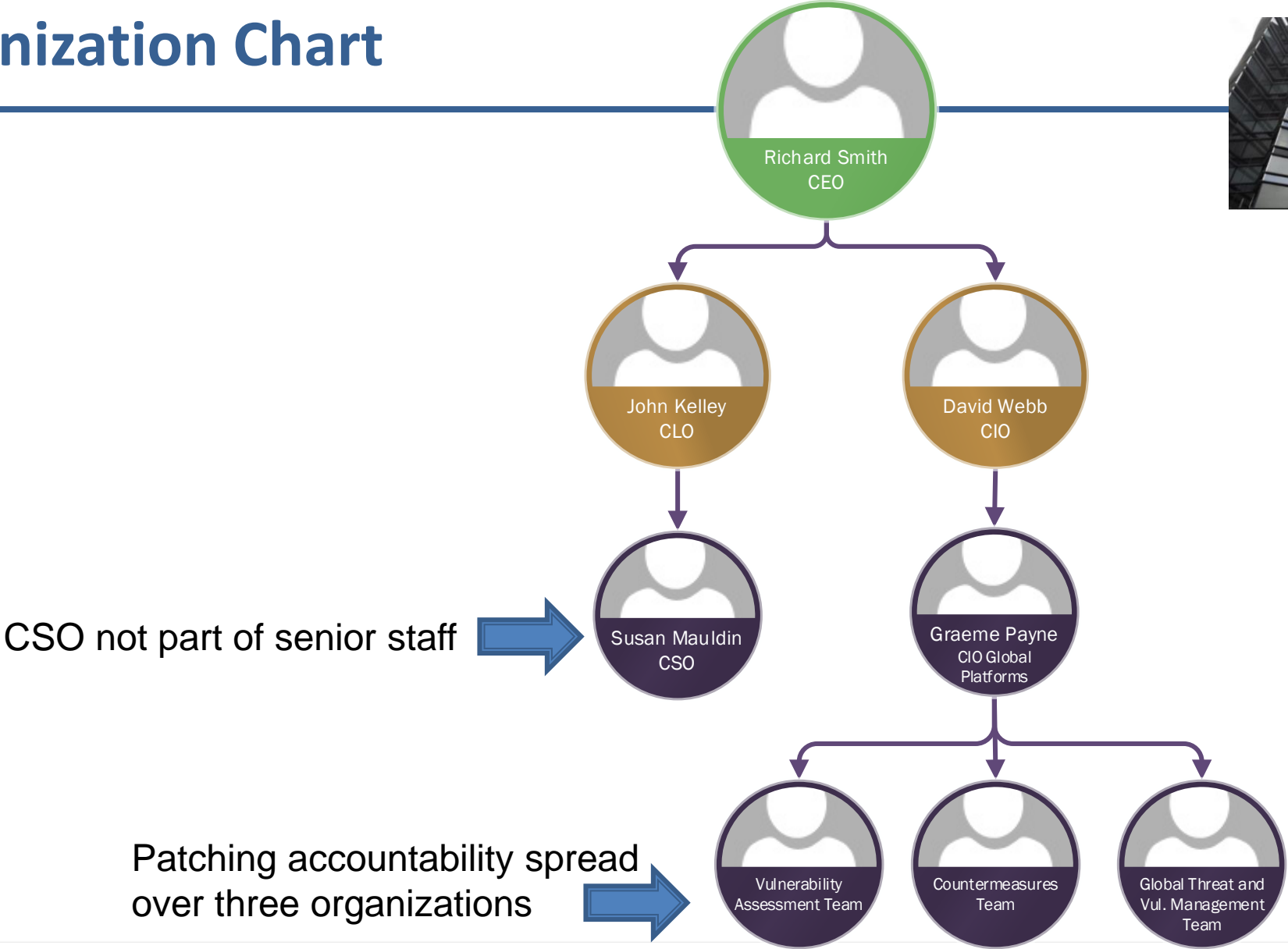
Harvard Business School 9-118-031, Data Breach at Equifax. Suraj Srinivasan, Quinn Pitcher, Jonah S. Goldberg, exhibit 8, Timeline of Equifax Breach
Anders Merlin, "Three Equifax Managers Sold Stock Before Cyber Attack Reveled", Bloomberg, Sept. 7, 2017.

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 indicted for insider trading

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

Equifax Organization Chart



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

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

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