Cybersecurity 101

2022

Kimmell Cybersecurity

Kimmell Cybersecurity

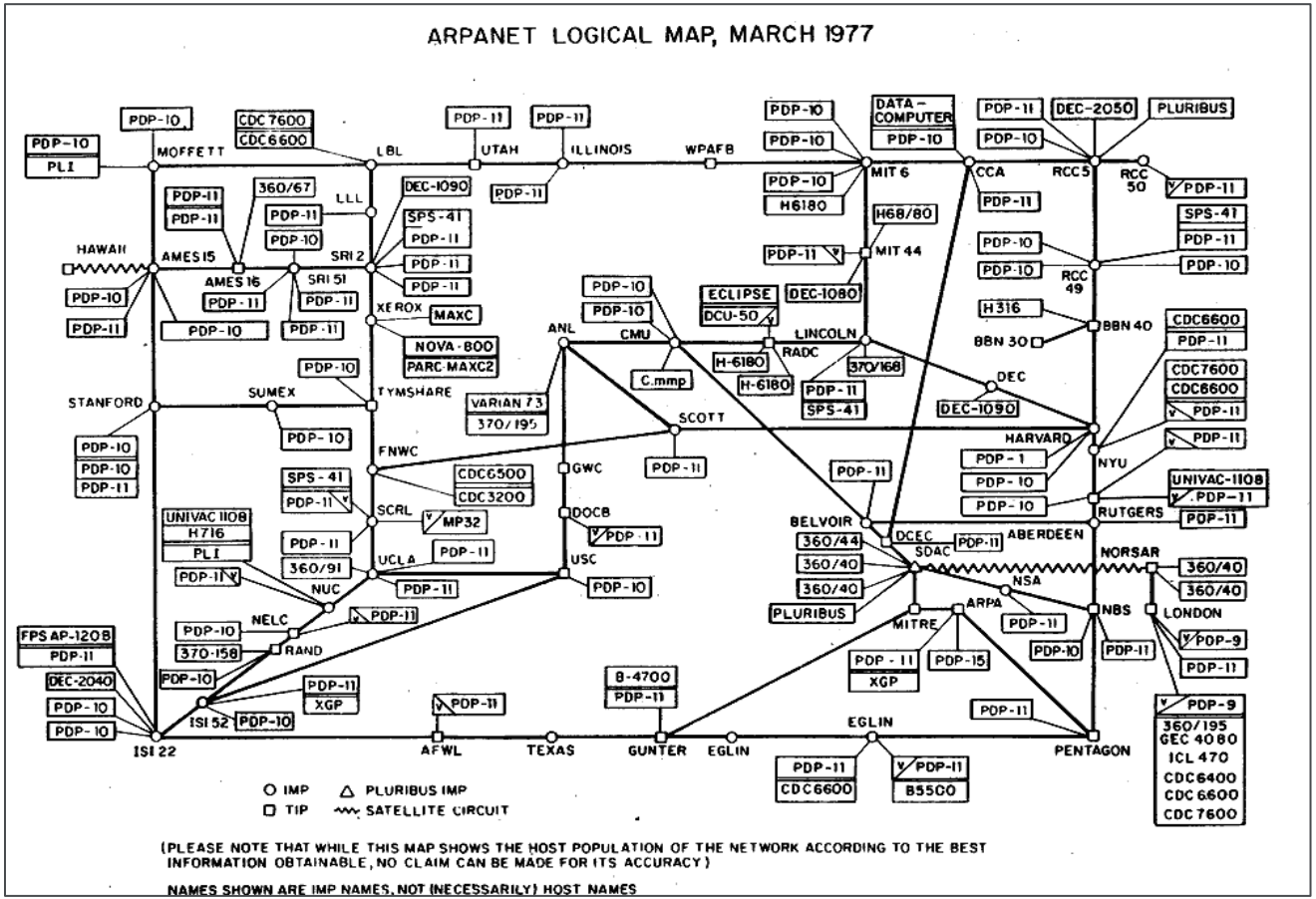
Abdullah Alkhulaiwi

- Masters in Digital Science
- Completion of DoD Mandatory Controlled Unclassified Information Training
- CompTIA: Security+
- Windows Server Administration Fundamentals
- Veeam Technical Sales Professional
- Veeam Certified Sales professional
- Sophos Certified Architect
- Sophos Certified Engineer

Kimmell Cybersecurity

Topics:

- Internet History
- What is Cybersecurity?
- Why is Cybersecurity Important?
- Why target Churches?
- Vulnerabilities
- Patching
- Threats
- Sources of Cyber Threats
- Phishing
- Passwords
- Physical Security
- How to Secure Social Media
- Your role in cybersecurity!



Kimmell Cybersecurity

JAN 2021

DIGITAL AROUND THE WORLD

ESSENTIAL HEADLINES FOR MOBILE, INTERNET, AND SOCIAL MEDIA USE

INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE NOT COMPARABLE WITH PREVIOUS REPORTS

TOTAL POPULATION

7.83 BILLION

URBANISATION:

56.4%

UNIQUE MOBILE PHONE USERS

5.22 BILLION

vs. POPULATION:

66.6%

INTERNET USERS*

4.66 BILLION

vs. POPULATION:

59.5%

ACTIVE SOCIAL MEDIA USERS*

4.20 BILLION

vs. POPULATION:

53.6%

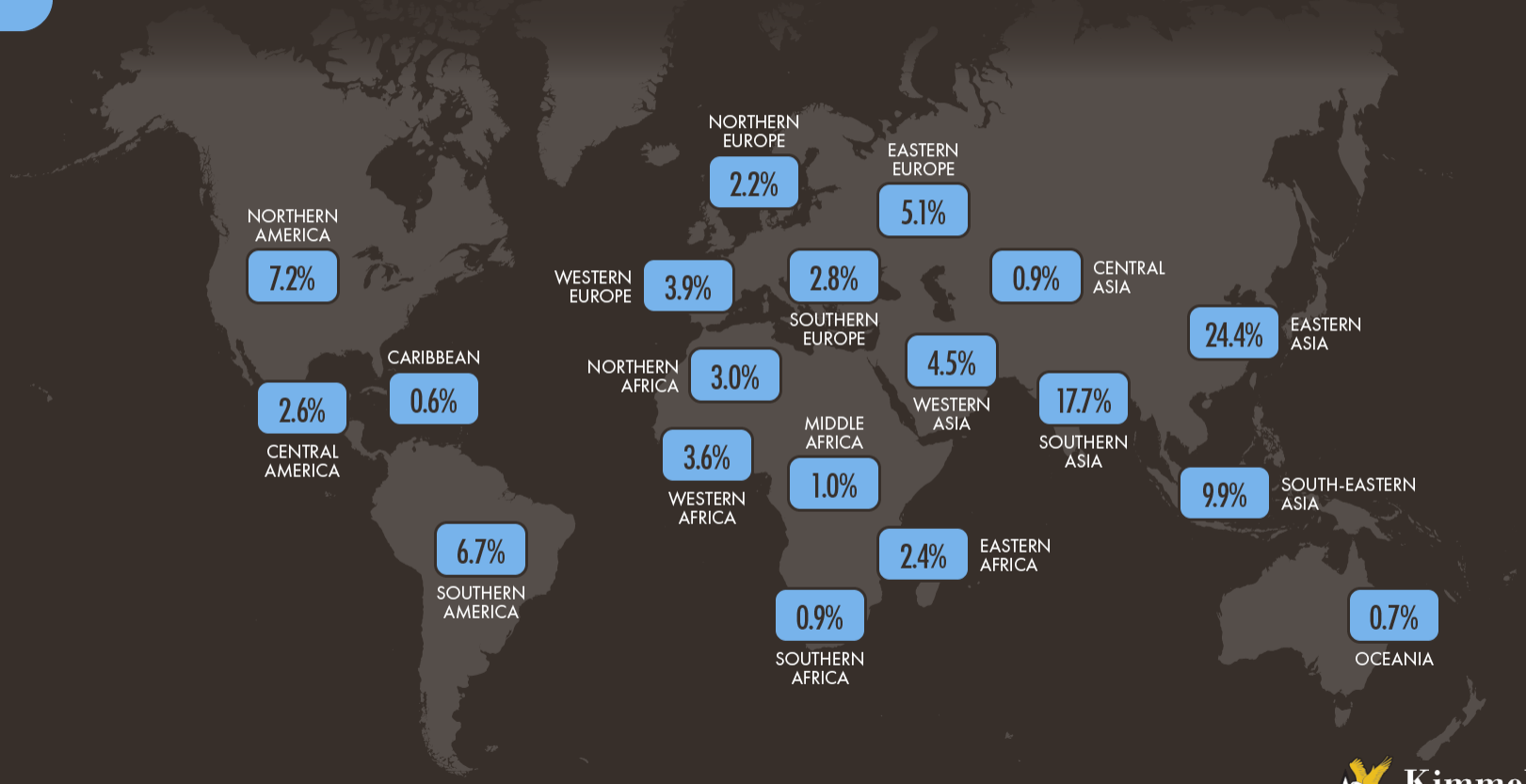
SOURCES: THE U.N.; LOCAL GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; GWI; EUROSTAT; CNNIC; APJII; SOCIAL MEDIA PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; COMPANY EARNINGS REPORTS; MEDIASCOPE. ***ADVISORIES:** INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE NOT COMPARABLE TO DATA PUBLISHED IN PREVIOUS REPORTS. SOCIAL MEDIA USER NUMBERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. ◈ **COMPARABILITY ADVISORY:** SOURCE AND BASE CHANGES.

Kimmell Cybersecurity

JAN 2021

SHARE OF GLOBAL INTERNET USERS BY REGION

THE NUMBER OF INTERNET USERS IN EACH REGION AS A PERCENTAGE OF THE TOTAL NUMBER OF GLOBAL INTERNET USERS



SOURCES: KEPIOS (JAN 2021) BASED ON EXTRAPOLATIONS OF DATA PUBLISHED BY: THE ITU; LOCAL GOVERNMENT BODIES; GWI; GSMA INTELLIGENCE; EUROSTAT; APJII; CNNIC.
NOTES: FIGURES REPRESENT SHARE OF TOTAL GLOBAL INTERNET USERS. REGIONS BASED ON THE UNITED NATIONS GEOSCHEME.

Kimmell Cybersecurity

Kimmell Cybersecurity

What is Cybersecurity?

Cybersecurity is a set of principles and practices designed to safeguard your computing assets and online information against threats.

Kimmell Cybersecurity

Cybersecurity is necessary since it Protects your information from theft, damage, or misuse.

Why target Churches?

Kimmell Cybersecurity

- A lot of Data
- Different network users
- Online bank accounts
- Connections to other organizations
- Hacktivism
- Lack of resources

Kimmell Cybersecurity

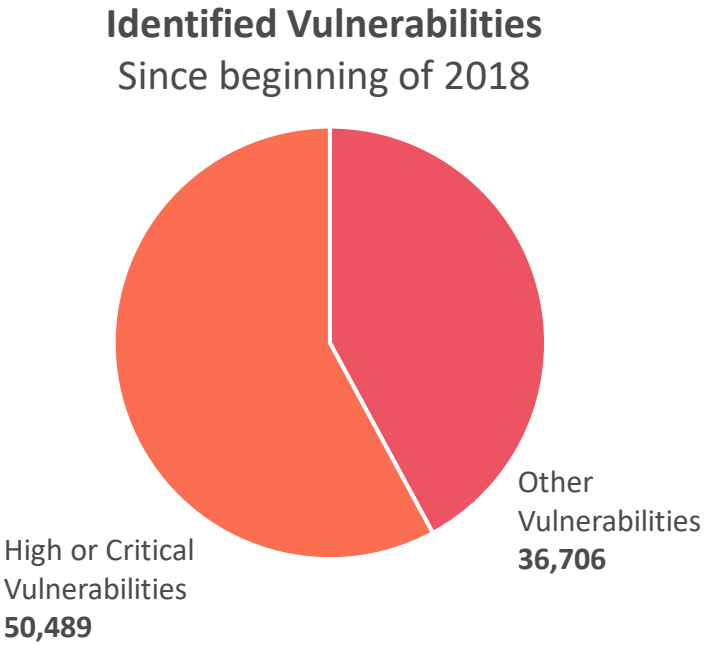
Question:

What is the cost of cyber attack?

- ✓ Economic Cost
- ✓ Reputational Costs
- ✓ Regulatory Costs

VULNERABILITIES

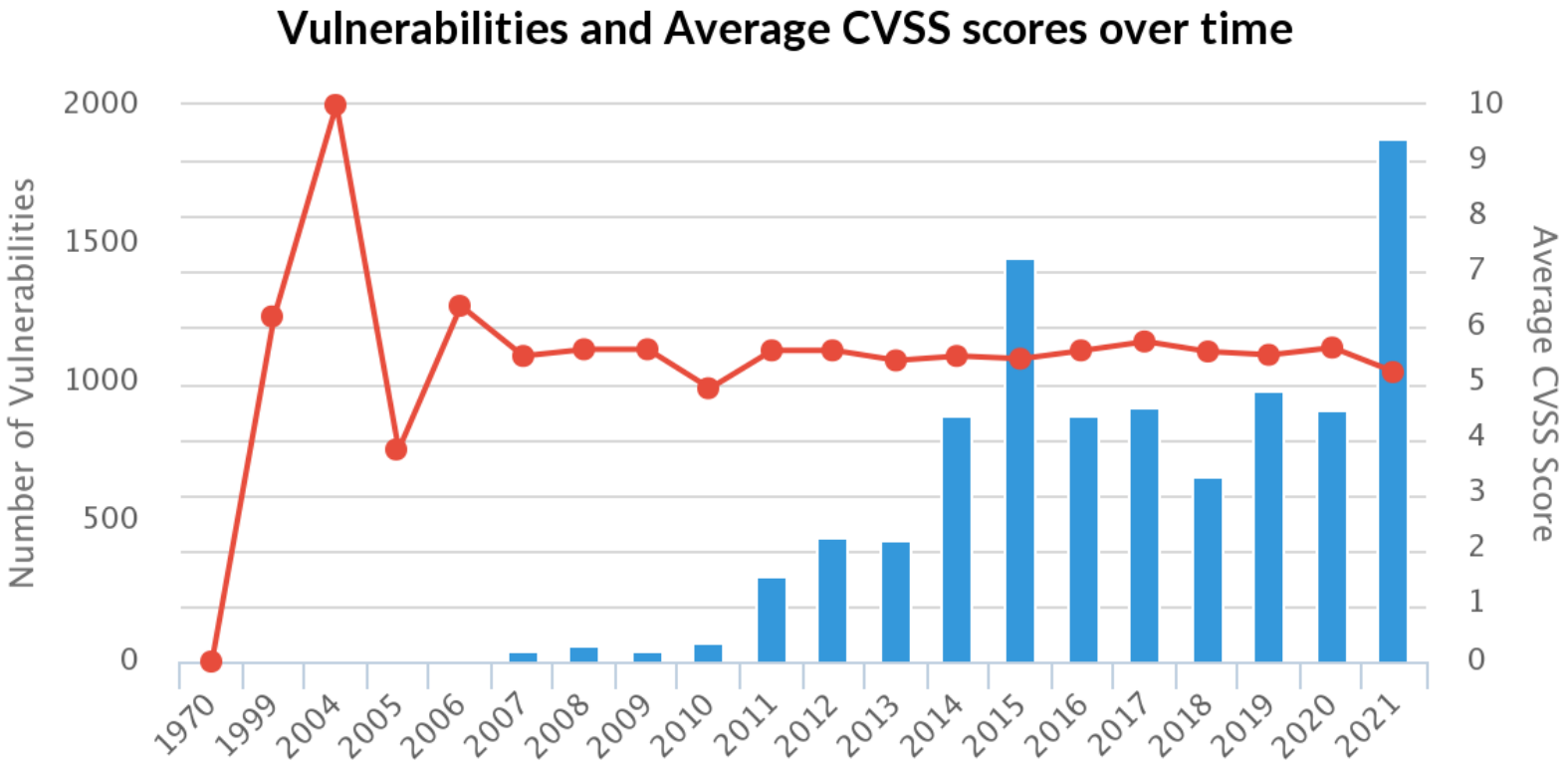
Kimmell Cybersecurity



- A ***vulnerability*** is a weakness in software or program that makes it susceptible to a threat.
- Every Operating System, Application and hardware/firmware have/had vulnerabilities that can be exploited

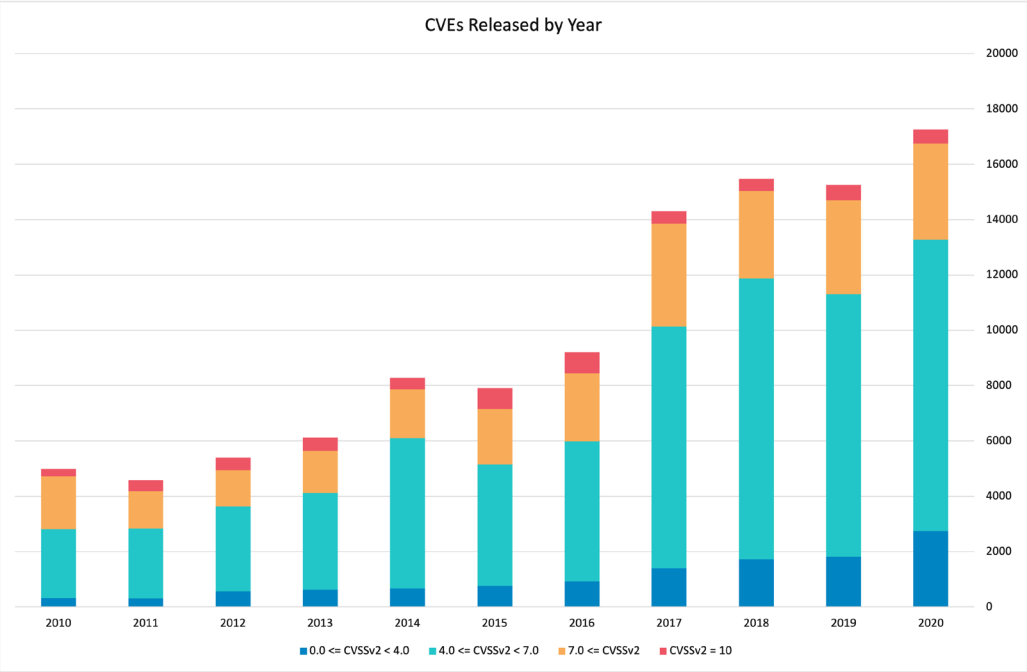
Kimmell Cybersecurity

2021 OPERATING SYSTEM VULNERABILITIES



Not All Vulnerabilities are Equal

Kimmell Cybersecurity



CRITICAL severity

if they have a CVSS base score of 9.0-10.0

HIGH severity

if they have a CVSS base score of 7.0-8.9

MEDIUM severity

if they have a base CVSS score of 4.0-6.9

LOW severity

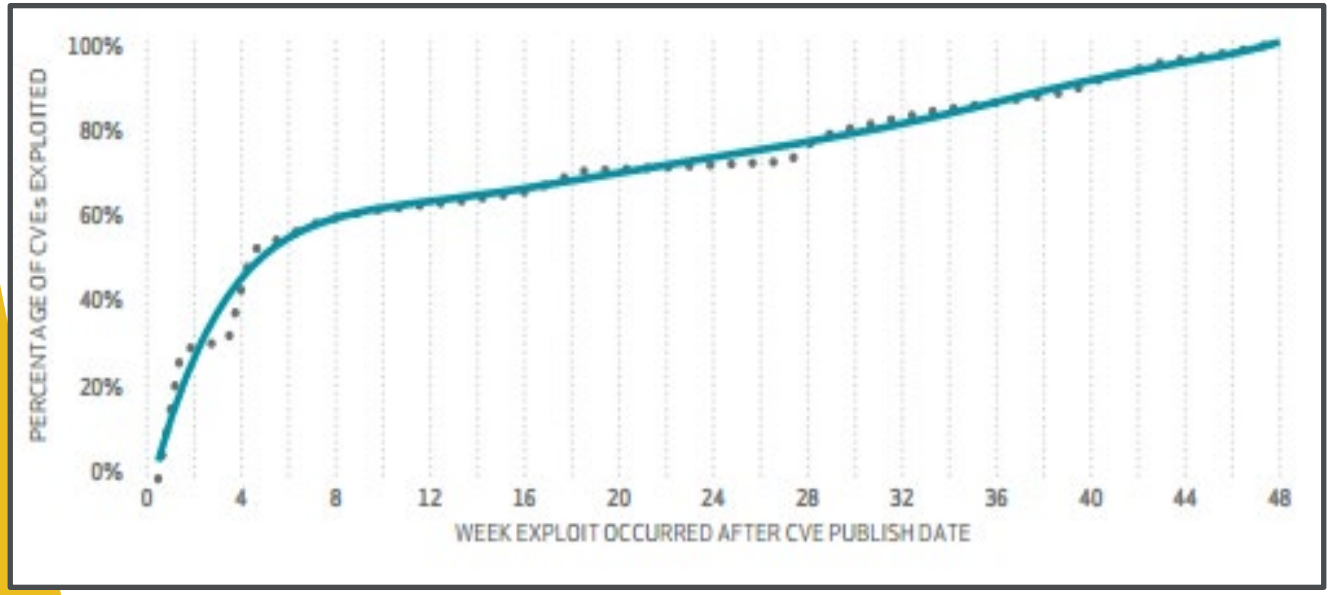
if they have a CVSS base score of 0.0-3.9

PATCHING

- Patching is a huge part of managing IT infrastructure. It can consume a large part of IT operation's time and energy.
- However, this is one area where automation and automated processes can really shine when it comes to keeping patches and other software up-to-date.
- If you have many servers, there is no question that automation is going to be your friend.

Kimmell Cybersecurity

Exploit code published within weeks



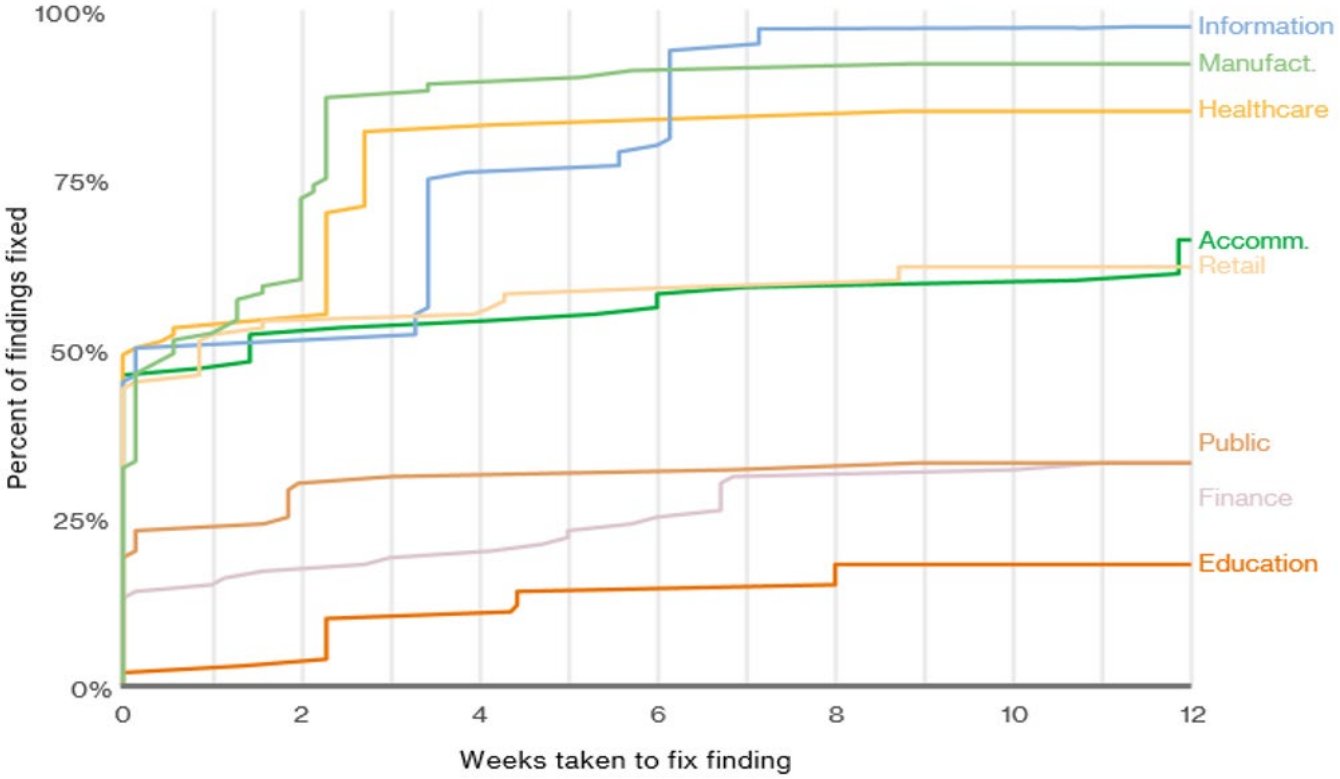
Kimmell Cybersecurity

99.9%

OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED

- Almost 100 % of the breaches were on vulnerabilities reported over a year ago.
- This is why we need to patch our systems on a regular basis

Kimmell Cybersecurity



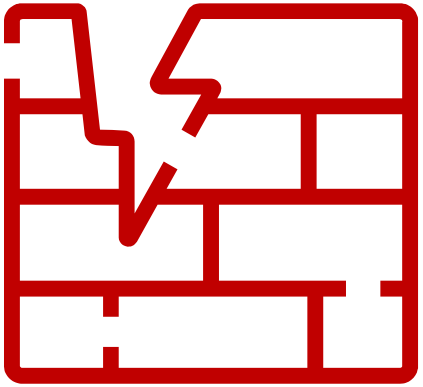
THREATS

A possible danger that might exploit a vulnerability to breach security and cause harm.

Types of Cybersecurity Threats

Kimmell Cybersecurity

- Intrusion
- Virus, Worm, Trojan Horse (Malware)
- Phishing
- Spyware
- Spam
- Man in the Middle Attack
- Denial of Service Attack
- Ransomware



- 2018 -53,000 incidents
- 2,216 confirmed data breaches
- 2019 -- 41,686 security incidents, of which 2,013 were confirmed data breaches

Sources of Cyber Threats

Kimmell Cybersecurity

- Nation States
- Criminal Groups
- Hackers
- Terrorist Groups
- Hacktivists
- Malicious Insiders
- Corporate Spies

Breaches by the numbers

Kimmell Cybersecurity

71% of breaches were financially motivated

25% of breaches were motivated by the gain of strategic advantage

32% of breaches involved phishing

29% of breaches involved the use of stolen credentials

56% of breaches took months or longer to discover

What else is common?

Kimmell Cybersecurity

66% of malware was installed via malicious email attachments

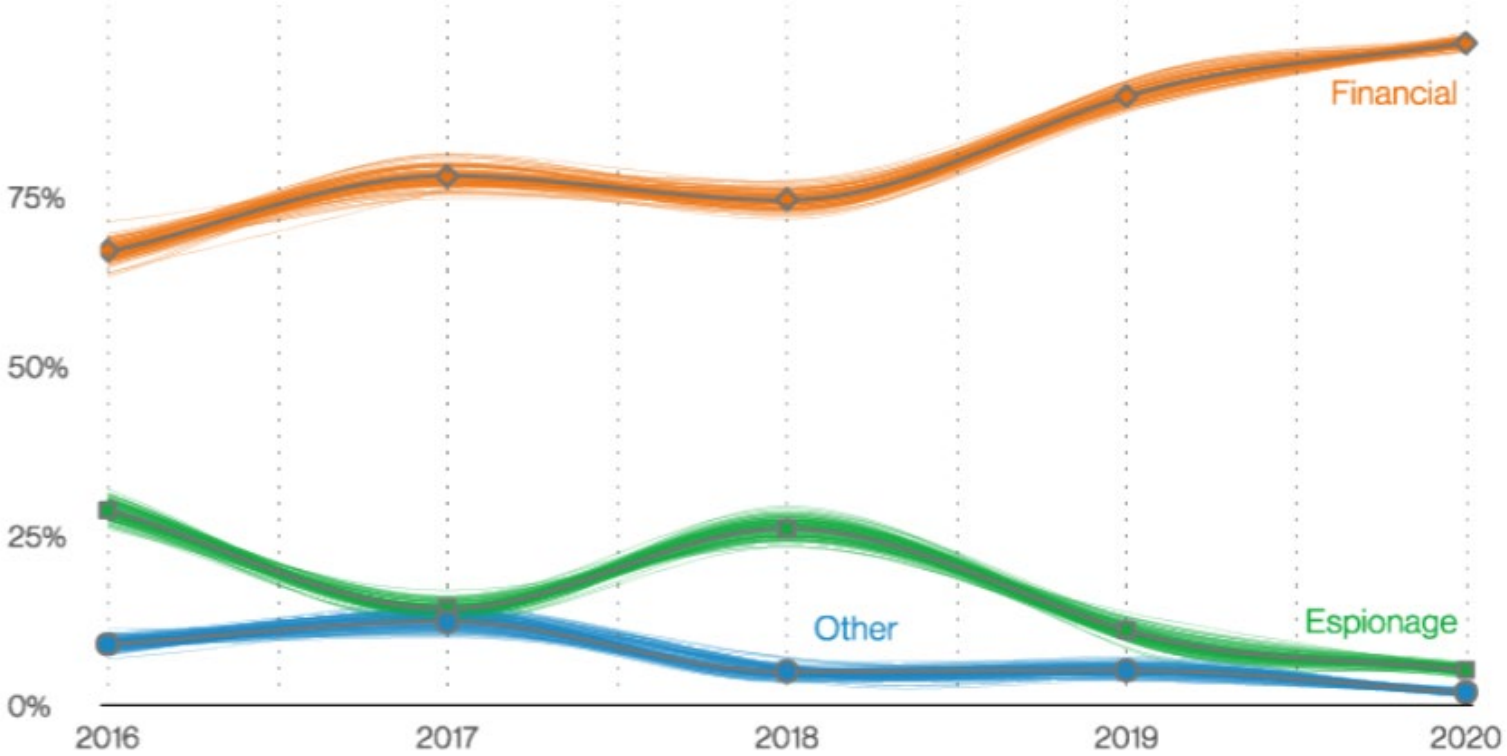
73% of breaches were financially motivated

21% of breaches were related to espionage

27% of breaches discovered by third parties

Kimmell Cybersecurity

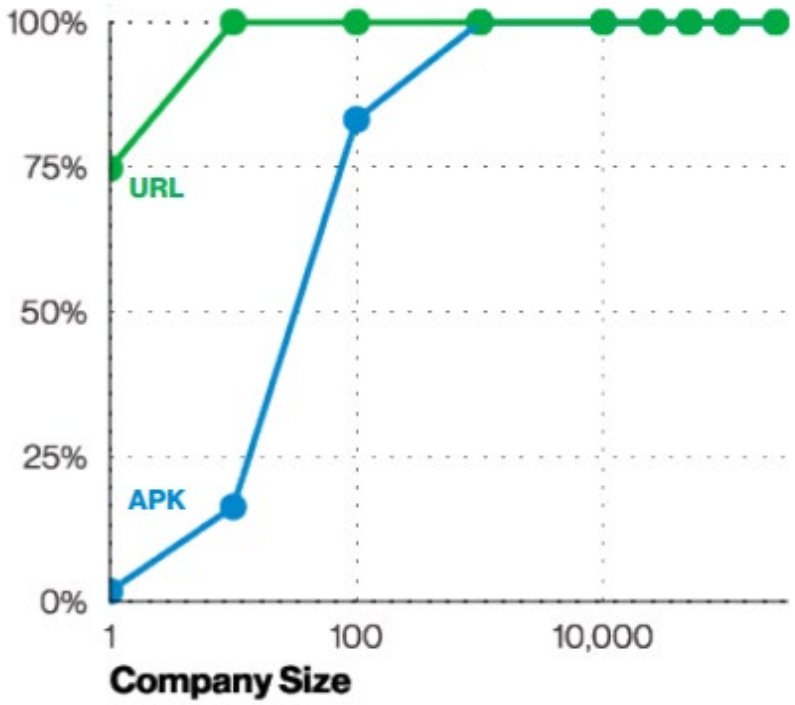
Top threat actor motive over time in Breaches



PHISHING

Kimmell Cybersecurity

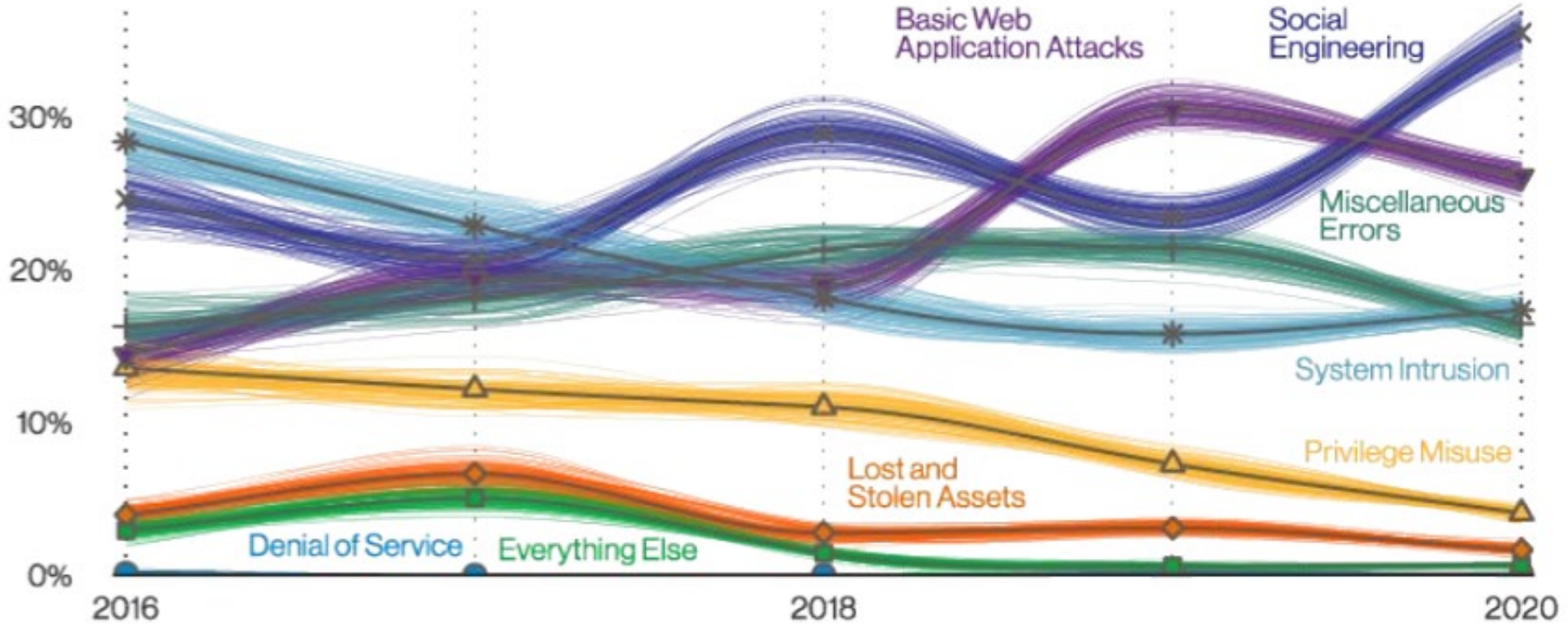
The practice of using email or fake website to lure the recipient in providing personal information



Probability that someone in the company will receive a malicious URL or install a malicious APK based upon organization size (n=5,444,000).

Kimmell Cybersecurity

Patterns over time in Breaches



Everyone is a risk….

Why?

- Not because you're bad
- We are human
- We need training
- We need to be reminded

PASSWORDS

Kimmell Cybersecurity

…in some cases, your **only** line of defense

- Guessed
  - Defaults
  - Easy
- Malware and Key Loggers
- Wi-Fi network traffic capture
- Dictionary Attack
- Brute Force Attack
- Shoulder Surfing
- Post-it Notes
- Stored in an Excel or Word file

Kimmell Cybersecurity

- Typical Password Policy
  - 7 or 8 characters
  - Upper Case, Lower Case, Numeric
- Examples
  - Fall2015 8 Characters <1 day
  - ClevelandBrowns14 17 Characters– <1 day
  - Intrecv8b 9 Characters < 1 day
  - uTrC1*E# 8 Characters < 8 hours
  - T&2fw1O0b$x9 12 Characters 34 thousand years

Randomness and length are essential to a good password

https://www.security.org/how-secure-is-my-password/

Safely Manage your Password

Kimmell Cybersecurity

- Create and maintain a strong password
- Consider using a passphrase
- Avoid sharing your password with any one
- Avoid reusing the same password for multiple accounts
- Avoid storing your password where others can see it, or storing it electronically in an unencrypted format (e.g. a clear text file, Word, Excel)
- Avoid reusing a password when changing an account password
- Do not use automatic logon functionality
- Multi-Factor Authentication

PHYSICAL SECURITY

Kimmell Cybersecurity

Physical Access is everything

Can do a lot of damage to a system with physical access

How to Secure Social Media?

- Get Alerts on Suspicious Activity
- Login Securely With a Password Manager
- Control Access to Your Social Accounts
- Manage Account Privacy Settings
- Be selective with third-party applications
- Enable two-factor authentication

Your Role in Cybersecurity!

Kimmell Cybersecurity

- End-users are the last line of defense. As an end-user, you;
- Create and maintain password and passphrase
- Manage your account and password
- Secure your computer
- Protect the data you are handling
- Assess risky behavior online
- Equip yourself and your organization with the knowledge of security guidelines, policies, and procedures

Kimmell Cybersecurity

Questions?

Thank You