



<https://www.guardsight.com/>

GuardSight is an established provider of comprehensive cybersecurity threat detection and response, risk assessments, and professional cybersecurity services since 2009.

"We fight bad guys on the internet!"



John McGloughlin, CISSP
Founder & CEO GuardSight, Inc.
johnmac@guardsight.com

CYBERSECURITY: FOR THE INDIVIDUAL

(my pgp key) → <http://pgp.mit.edu/johnmac@guardsight.com> | <https://www.linkedin.com/in/mcgloughlin> ← (about me)

GuardSight® is a registered trademark of Guardsight, Inc. All other products and company names mentioned herein are trademarks or registered trademarks of their respective owners. ©GuardSight, Inc.



CYBERSECURITY: HISTORY OF CYBERCRIME

1900-1949

1903

Maskelyne
(magician) hacks
Marconi's
secure wireless
telegraph

1932

Enigma machine
code broken by
Polish cryptologists

1939

Turing co-develops
the Bombe making
the Enigma machine
vulnerable to brute
force attacks

CYBERSECURITY: HISTORY OF CYBERCRIME

1950-1979

1957

Hackers tie up phone lines between Harvard and MIT and make long-distance calls charged to a local radar installation

Engressia (7 yrs old & blind) discovers that whistling the fourth E > middle C interferes with AT&T's telephone systems (phreaking)

1963

Rosenbaum of Esquire magazine publishes "Secrets of the Little Blue Box" relies on accounts from Draper (Captain Crunch) and a toy whistle

1971

Draper arrested toll fraud (5yrs prob) - catalyst for Wozniak meeting and connection: *Jobs & Wozniak sold phone-phreaking tools*

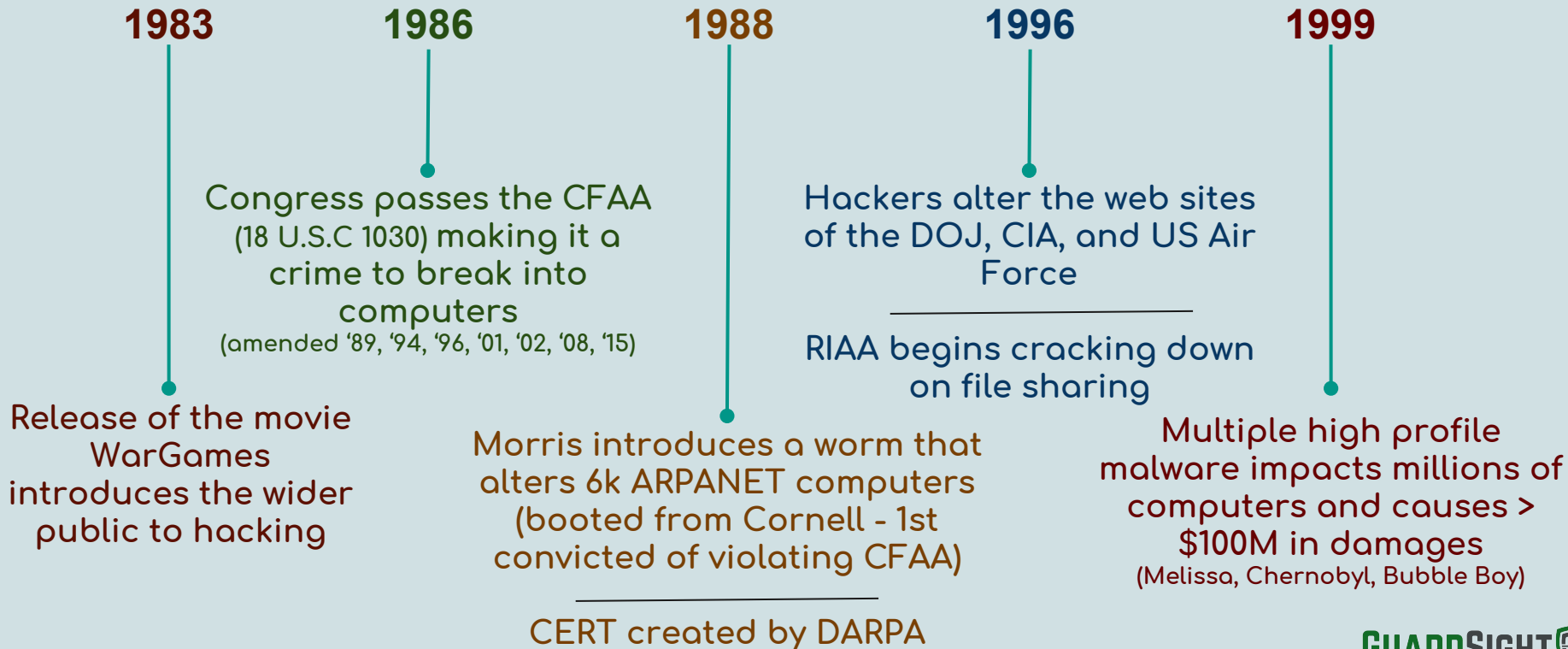
1972

Mitnick (16 yrs old) posing as Chernoff (DEC developer) breaks into the DEC ARK system used to develop the RSTS/E OS

1979

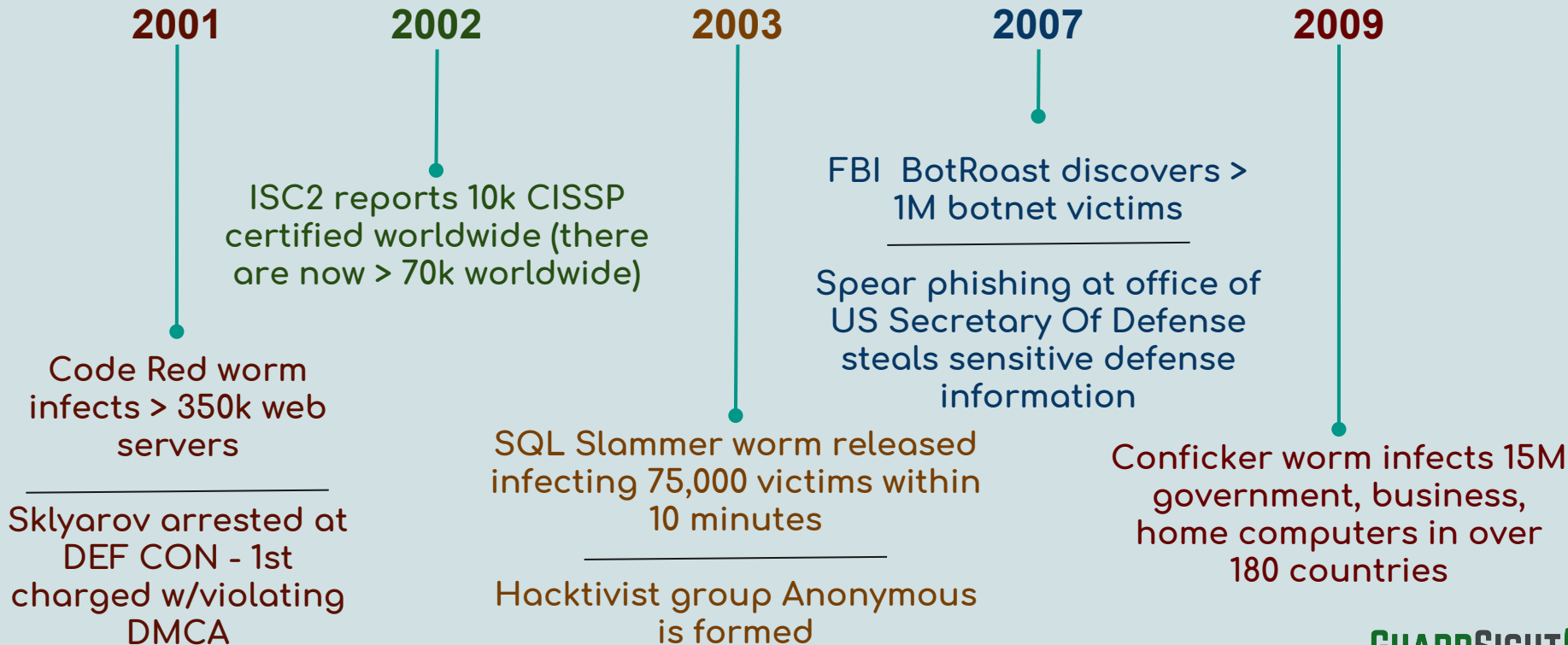
CYBERSECURITY: HISTORY OF CYBERCRIME

1980-1999



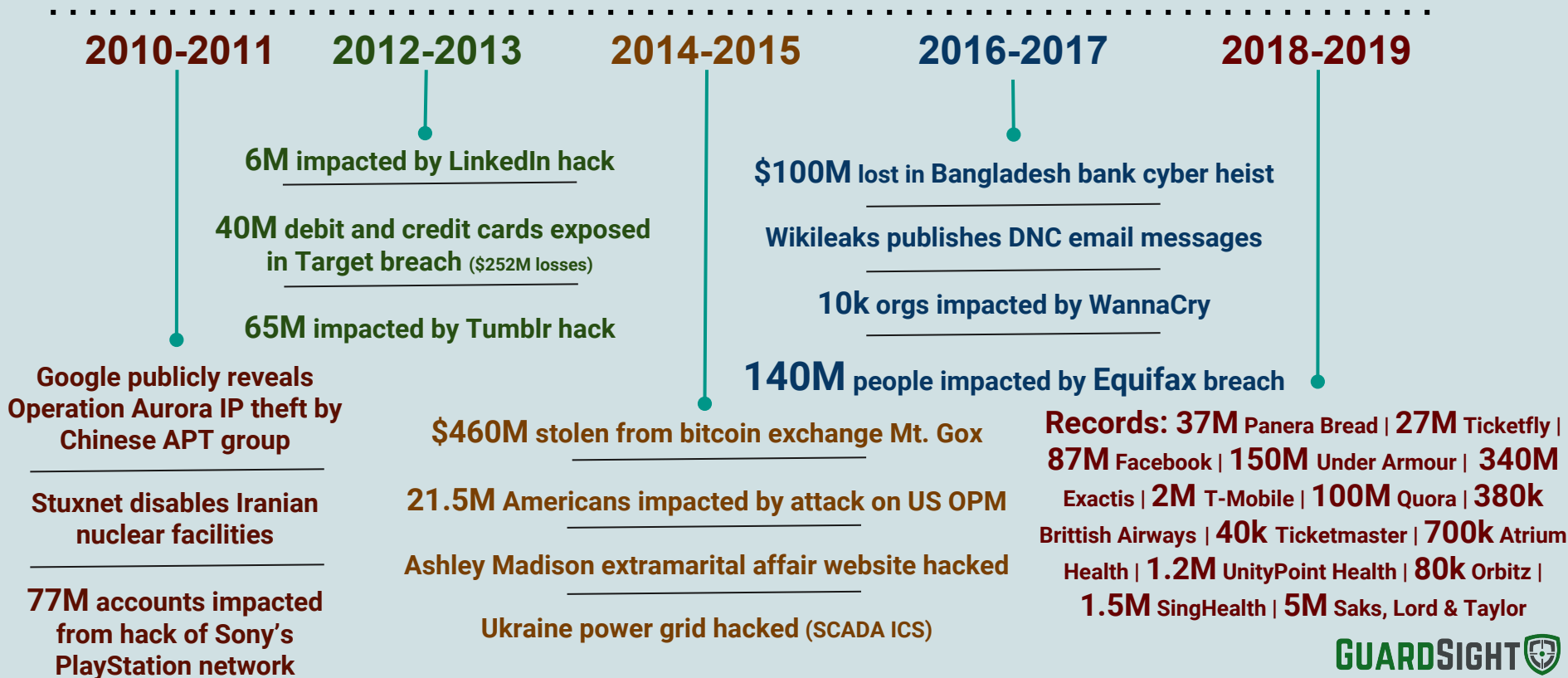
CYBERSECURITY: HISTORY OF CYBERCRIME

2000-2009

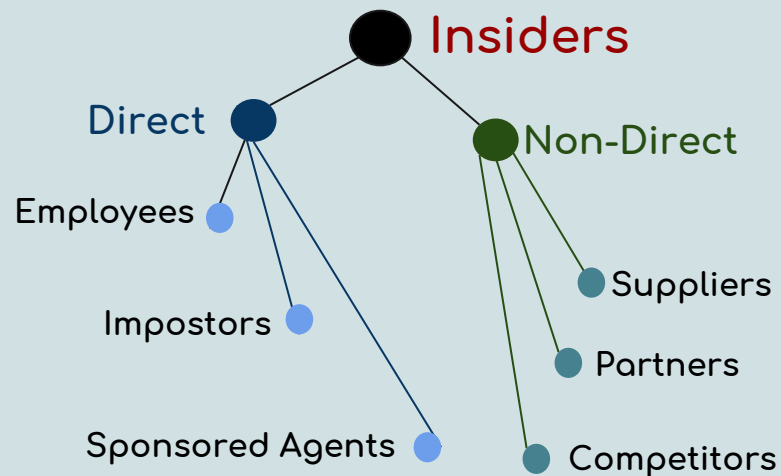
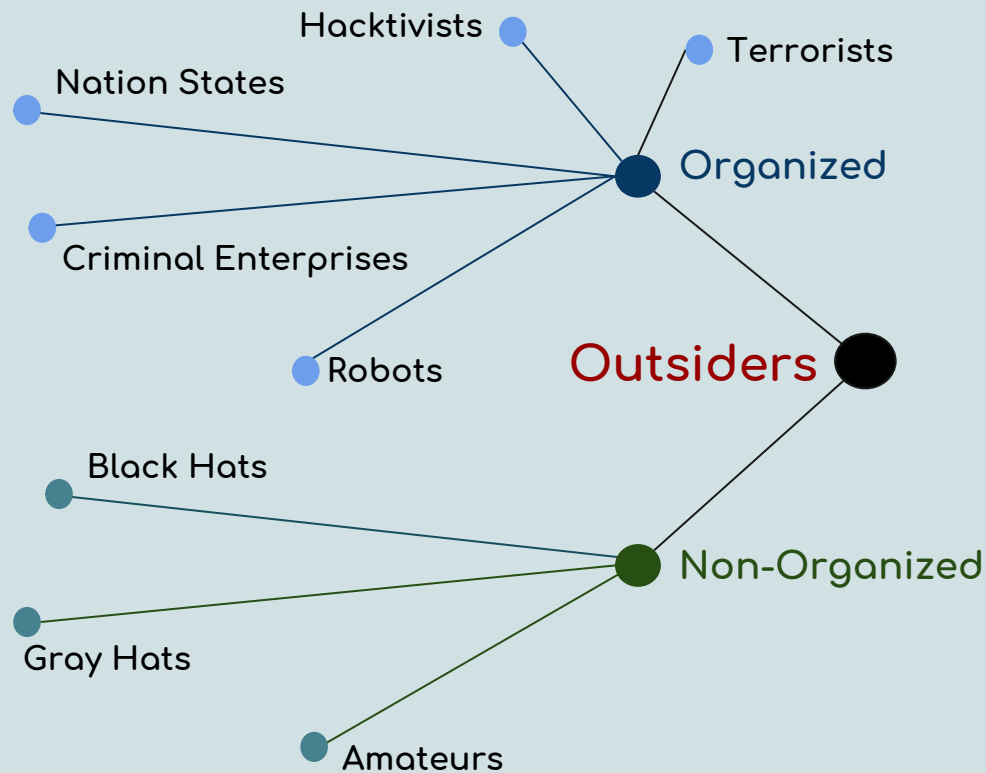


CYBERSECURITY: HISTORY OF CYBERCRIME

2010-2019



CYBERSECURITY: THREAT ACTOR ATTRIBUTION



CYBERSECURITY: THREAT ACTOR INTENT

- Identity Resources (Impersonate)
 - o PII
 - o PHI
 - o Credentials
- Intellectual Resources (Dominate)
 - o Brand
 - o Property
 - o Knowledge
- Physical Resources (Perpetuate)
 - o Energy
 - o Strength
 - o Persistence
- Logical Resources (Violate)
 - o Speech
 - o Reputation
 - o Communication

Motives & Objectives

- Profit
- Wealth
- Prestige
- Assets
- Warfare
- Defense
- Espionage
- Mobilization
- Ideal[ogy | ism]
- Elimination
- Extortion
- Destruction

CYBERSECURITY: BLACK MARKET LOOT (US BASED)

ONLINE BANKING CREDENTIALS

\$2k-\$20k+ Balance **\$100 - \$1,000+**

ATM CARD WITH BALANCE & PIN

\$2k-\$10k+ Balance **\$500 - \$1,000+**

CREDIT CARD NUMBER "Fullz"

Major Cards **\$7 - \$50**

SOCIAL MEDIA ACCOUNT ACCESS

1k-10k Accounts **\$15 - \$60**

PERSONALLY IDENTIFIABLE INFORMATION

SSN, DOB, Histories **\$40 - \$200**

PERSONALLY IDENTIFIABLE INFORMATION

Bundle (DL, Green Card, Visa, Passport, Insurance) **\$2000-\$3000**

AIRLINE REWARDS POINTS ACCESS

50k-150k Miles **\$100 - \$200**

HOTEL REWARDS POINTS ACCESS

50k-150k Points **\$75 - \$140**

1.4 BILLION

US \$\$ LOSSES EXCEEDED IN 2017

214 MILLION

CALIFORNIA \$\$ LOSSES
EXCEEDED IN 2017

230 THOUSAND

NEW MALWARE VARIANTS
DETECTED EVERY DAY

24 THOUSAND

MALICIOUS MOBILE APPS
BLOCKED EVERY DAY

66 PERCENT

MALWARE INSTALLED USING
EMAIL ATTACHMENTS

CYBERSECURITY: PROTECT YOUR ASSETS



- Reduce the attack surface
 - ◆ Own your assets & data
 - ◆ Inventory your assets & data
 - ◆ Prune apps not being used often
 - ◆ Prune accounts not being used often
 - ◆ Prune upload / download residue
 - ◆ Unplug it when you're not using it
 - ◆ Always on location services != friendly
 - ◆ Beware of the "benevolent"
 - ◆ READ the "Terms of Service"
 - ◆ You are the product when it is FREE
 - ◆ FREE == alternative arrangement
 - Apply real world protection strategies to your online persona[s]
 - If you think something is suspicious and could cause you harm that's your limbic system talking - listen to it!
 - The US Congress is not going to fight for you anytime soon - foreign and domestic technology firms own them and lobby the major parties *equally* - own your assets and fight to protect yourself!
- Use multifactor authentication
 - Avoid using the same passphrase for multiple services
 - Use a pass-[word|phrase] manager
 - Update hardware & software regularly
 - Use automated security patching
 - Use anti-virus / endpoint protection software
 - Routinely backup critical assets
 - Use content-filtering / white-listing / ad-blocking
 - Avoid opening email from unknown senders
 - Avoid opening attachments from unknown senders or senders that normally do not send attachments
 - Refrain from accessing sensitive online accounts when using public Wifi networks
 - Use available alerting from online services
 - Think layered defense-in-depth