GUARDSIGHT

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)

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

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

1963

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

1971

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

1972

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

1979

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

GUARDSIGHT

CYBERSECURITY: HISTORY OF CYBERCRIME

1980-1999

1983

Release of the movie WarGames introduces the wider public to hacking

1986

Congress passes the CFAA (18 U.S.C 1030) making it a crime to break into computers
(amended '89, '94, '96, '01, '02, '08, '15)

1988

Morris introduces a worm that alters 6k ARPANET computers (booted from Cornell - 1st convicted of violating CFAA)

CERT created by DARPA

1996

Hackers alter the web sites of the DOJ, CIA, and US Air Force

---

RIAA begins cracking down on file sharing

1999

Multiple high profile malware impacts millions of computers and causes > $100M in damages
(Melissa, Chernobyl, Bubble Boy)

GUARDSIGHT

CYBERSECURITY: HISTORY OF CYBERCRIME

2000-2009

2001

Code Red worm infects > 350k web servers

Sklyarov arrested at DEF CON - 1st charged w/violating DMCA

2002

ISC2 reports 10k CISSP certified worldwide (there are now > 70k worldwide)

2003

SQL Slammer worm released infecting 75,000 victims within 10 minutes

---

Hacktivist group Anonymous is formed

2007

FBI BotRoast discovers > 1M botnet victims

Spear phishing at office of US Secretary Of Defense steals sensitive defense information

2009

Conficker worm infects 15M government, business, home computers in over 180 countries

GUARDSIGHT

CYBERSECURITY: HISTORY OF CYBERCRIME

2010-2019

2010-2011

Google publicly reveals Operation Aurora IP theft by Chinese APT group

Stuxnet disables Iranian nuclear facilities

77M accounts impacted from hack of Sony's PlayStation network

2012-2013

6M impacted by LinkedIn hack

40M debit and credit cards exposed in Target breach ($252M losses)

65M impacted by Tumblr hack

2014-2015

$460M stolen from bitcoin exchange Mt. Gox

21.5M Americans impacted by attack on US OPM

Ashley Madison extramarital affair website hacked

Ukraine power grid hacked (SCADA ICS)

2016-2017

$100M lost in Bangladesh bank cyber heist

Wikileaks publishes DNC email messages

10k orgs impacted by WannaCry

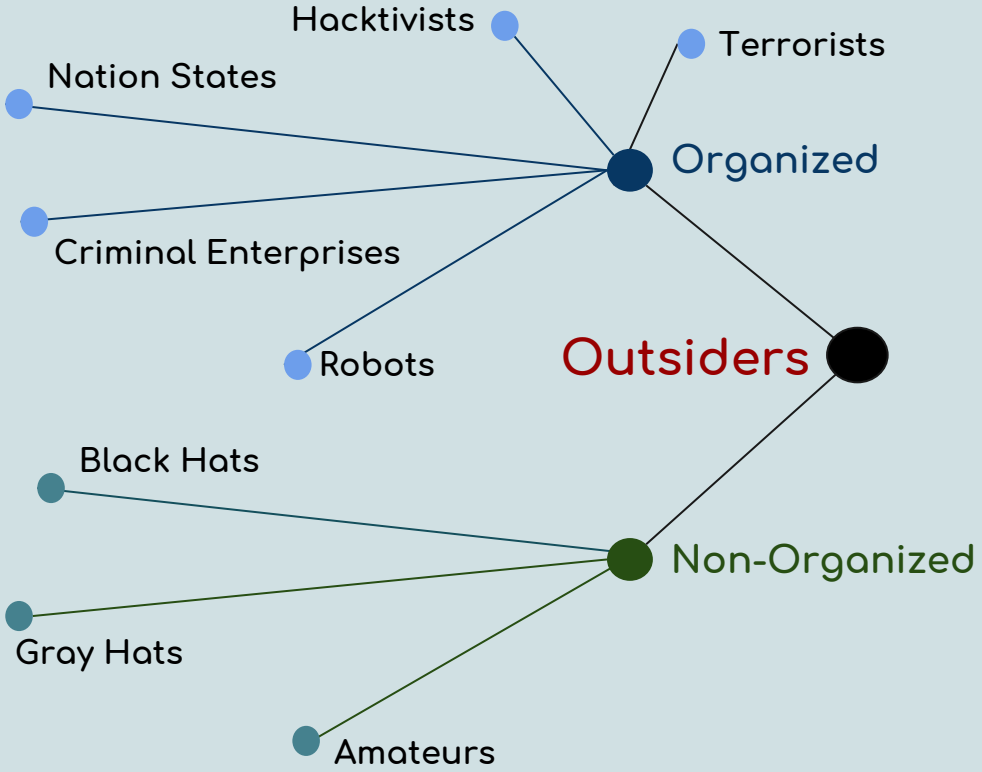
140M people impacted by Equifax breach

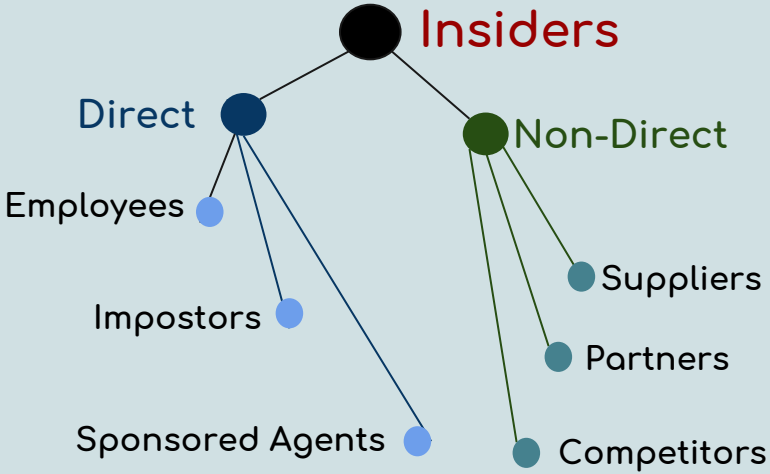
2018-2019

Records: 37M Panera Bread | 27M Ticketfly | 87M Facebook | 150M Under Armour | 340M Exactis | 2M T-Mobile | 100M Quora | 380k Brittish Airways | 40k Ticketmaster | 700k Atrium Health | 1.2M UnityPoint Health | 80k Orbitz | 1.5M SingHealth | 5M Saks, Lord & Taylor

GUARDSIGHT

CYBERSECURITY: THREAT ACTOR ATTRIBUTION





GUARDSIGHT

CYBERSECURITY: THREAT ACTOR INTENT

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

Motives & Objectives

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

GUARDSIGHT

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

GUARDSIGHT

CYBERSECURITY: PROTECT YOUR ASSETS

~~RUN~~ ~~HIDE~~ **FIGHT!**

- ➔ 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 Wifl networks
- ➔ Use available alerting from online services
- ➔ Think layered defense-in-depth

GUARDSIGHT