Cybersecurity Decade in Review

A Year-by-Year Romp through the Biggest Events of the Teens

2021 Security Awareness

Stewart Bruner, COT Staff

1

Year: 1903

- Magician Nevil Maskelyn hacks a wireless telegraph communication
- Built 50-meter antenna, located Marconi's frequency, sent own message
- Backed by wired telegraph owners to discredit wireless and protect market

- What we learned
  - Function always precedes security
  - Practical obscurity isn't security
  - Technology breeds vested interests
  - Hacking is far older than "*War Games*!"

- Reaction: Magicians are human hackers; no widespread publicity

2

Year: 2010

- Stuxnet worm destroys data on Iranian SCADA… and elsewhere
- Google sees China differently after Operation Aurora, exits country
- Stolen unreleased news stories net huge market profits

- What we learned
  - Cyber offensives can have unintended consequences for years
  - Nation states carry out active offensives using private companies
  - Hacking the right things is extremely profitable and it's becoming a coordinated enterprise – organized cybercrime

- Reaction: Nation-state actor wariness

3

Year: 2011

- Lulzsec "50 Days of Lulz" hacktivism campaign targets big names
- DigiNotar certificates takeover ups ante on browser trust
- Sony PlayStation hack – 77 million accounts, 23-day shutdown

- What we learned: When companies don't invest in security, everybody pays, hackitivism is a thing

- Reaction: Your personal data is getting stolen and used

4

Year: 2012

- *Shamoon*, Iran's cyber weapon, wipes 35,000 PCs at Saudi Aramco
- *Flame* sophisticated malware attributed to NSA

- What we learned
  - Stuxnet pays negative dividends
  - Cyber warfare is a thing
  - The US was/is involved

- Reaction: Wariness about US Gov't; prepare for the backlash

5

Year: 2013

- Snowden leaks expose global surveillance network
- Target POS hack collects data on 40 million payment cards
- Adobe 153 million credentials stolen; passwords cracked
- Dark Web marketplaces and "card shops" see first publicity after *SilkRoad* takedown

- What we learned
  - All those stolen credentials have black market value!

- Reaction: *Have I Been Pwned* website from Troy Hunt ('abc123' appears 2,670,319 times while 'acl567' only once)

6

Year: 2014

- North Korea hack of Sony Pictures to stop *The Interview* nets US sanctions
- 40M Home Depot customers' data stolen by POS system hack (lawsuit settled for $17.5 million in 2020)
- *Celebgate* iCloud account takeovers via phishing "exposes" various stars' private video/photos
- Carbanak (FIN7) organized crime group steals $1B from 10 banks worldwide
- Heartbleed exposes OpenSSL vulnerability, takes years to close

- What we learned: Hacking is lucrative!; social engineering works; every technology has weaknesses exploitable by someone
- Reaction: Don't just rely on tech; get some training to lower risk
  - AOC issues first cyber awareness video, *Don't Be the Weakest Link!*

7

Year: 2015

- Ashley Madison database release and wide publicity leads to extortion attempts and suicides
- Chinese OPM hacks affect 21.5M US government records, esp. background check information
- Industrial controls hacking on rise; Russia - Ukraine power grid attack drops power to significant portion of country
- DDoS attacks with extortion demands increase as IoT increases

- What we learned: China is a major player; SCADA attacks can cripple countries; you leave behind a trail of your Internet activities
- Reaction: "Hack fatigue" sets in – nobody freaks out anymore…

8

Year: 2016

- North Korea's botched Bangladeshi bank heist revises money transfer system; they switch to targeting cryptocurrency exchanges
- *Panama Papers* hacktivism embarrasses the rich & famous
- Russian Podesta/DNC hack: the hack heard round the world!
- Yahoo's multiple hacks revelation – 2.2+ billion accounts dumped on Dark Web for sale
- Mirai botnet DDoS attack of Dyn name servers brings down several largest Internet businesses using baby monitors – "Pearl Harbor for IoT"
- What we learned: things on the Internet are inherently insecure; providing personal data is a form of payment for services; Google knows about me!
- Reaction: AJC ratified 44 security standards for courts; consumers keep buying open IoT devices and keep giving their data away

9

Year: 2017

- Ransomware is everywhere: WannaCry, NotPetya, Bad Rabbit
- WikiLeaks reveals NSA arsenal of malicious cyber weapons
- MongoDB Apocalypse shows perils of misconfigured cloud databases
- Equifax hack exposes personal details of 145.5M consumers
- Cryptojacking replaces ransomware as #1 scourge (temporarily)
- What we learned: It's no longer IF you get hit, but WHEN; matching passwords are the cloud's Achilles' heel (think Office 365)
- Reaction: Continue to increase security awareness, push for 2FA!

10

Year: 2018

- E-Mail spoofing breakthroughs put ransomware back on top
- Cambridge Analytica abuses Facebook profile data; Facebook appears to have let them, causing backlash
- Spectre/Meltdown vulnerable code on Intel chips worldwide
- Magecart skims payment info from online commerce sites
- Marriott leaks personal info on 383 million guests

- What we learned: It's not just your habits but those of your vendors and suppliers and outsourcers -- people you can't control or train
- Reaction: Start buying cyber insurance policies

11

Year: 2019

- Ring doorbell / Nest thermostat hack publicity – IoT remains security free!
- Business e-mail compromise (BEC) goes exponential; losses skyrocket
- Government ransomware attacks reach crisis level (104)
  - Attacks focus on entities in same proximity (schools/county/cities/healthcare -- 948)
  - At least 13 cloud providers hit by ransomware
- CapitalOne and 30 other DB leaks traced to lone AWS cloud employee
- China's comprehensive Uighur surveillance revealed; facial recognition controversy heightens

- What we learned: Insider threats are real and very hard to detect; security getting so complex only AI can manage it; nobody is willing to pay for IoT security yet
- Reaction: Upgrade anti-malware; begin phish testing employees; buy more cyberinsurance; figure out how to get Bitcoin ransom money in a hurry

12

Year 2020

- Attack surface and chaos multiply exponentially with WFH / BYOD in wake of COVID-19 pandemic
  - Massive increase in phishing, spoofing, shipping scams related to COVID-19
- Ransomware adds new twist – data extortion down to individual level (post Vaastamo)
  - 11 government entities hit in WFH transition, incl TX and GA AOCs
  - Managed.com ransomware event affects court web resources incl AZPOINT
- Twitter "blue check" account takeovers ($120,000 within hours) show insider threat painfully real
- First human death attributed to medical ransomware event
- Social media in crosshairs over disinformation and polarization
- IoT Security legislation passes! Gov't must purchase items having security…
- 15 Billion credentials now available for cheap in Dark Web marketplaces!
- What we learned: Home networks are now work networks; pace of change is accelerating; vendors and insiders are the unexamined weakest link
- Reaction: Zero-trust networks, require 2FA everywhere, increase security training beyond work situations alone as WFH extends

13

Future Predictions

Attackers will continue to discover and exploit zero-days. Companies large and small will continue to lose data and money to the usual attacks, often because they didn't take basic security precautions. Individuals will continue to lose money in the usual ways, often because they lack basic knowledge of Internet safety. Manufacturers will continue to produce Internet-connected devices with no security, or easily by-passable security, enabling attackers to hijack them. More laws will mandate that new Internet of Things devices have security, but those laws will be unenforceable and impossible to apply retroactively. No one will deploy a better authentication system than passwords, even though everyone talks about 'passwordless' computing. Consumers will continue to trade away very valuable data about themselves in exchange for free software and convenience.

14