Cyber Future

Overview & Expected Future Trends



The History of Cybersecurity

1970

1980s Gov't Orange Book Cybersecurity Industry

1990s Polymorphic, Stealth, Macro Comp. Sec. Big Business 2000s
Internet
Explosion
Website
Infections
Hacker Groups
DDOS Attacks
Credit Card
Hacks
Gov't Sponsored
Attacks

2010s-2020s
Phishing
Personal Data Loss
Ransomware
Al and Machine
Learning



ARPANET

First Worm

















1979 Kevin Mitnick 1st Cyber Criminal 1987 McAfee VirusScan NOD AntiVirus Malware Stateful Inspection FW

1995 SSL Introduced 2000s
Forensics
MFA
Backup & mirroring
Web Application
Firewalls
Real Time
Protection
Sandboxing



The History of Security Regulation

1996 HIPAA 2002 Homeland Security Act incl. FISMA 2011
DoD Strategy for
Operating in
Cyberspace
Int'l Partnership
DFARS

2014 FFIEC expanded to incl. Cybersecuri ty NIST CSF v1

2018 NIST CSF v1.1





















1999 GLBA 2003 DHS Nat'l Strategy to Secure Cyberspace NIST est. CNS (Comp. Net. Security) 2013 DoD cybersecurity rule 78 Fed Reg. 69373 NIST IT Standards

Congress found 50 Statutes relative to Cybersecurity Compliance

FISMA (included)
ISO/IEC

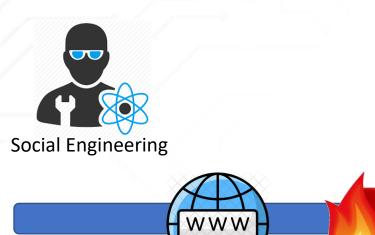
2016 CNAP – Cyber Security National Action Plan 2019 DoD - CMMC



Your Technology Resource

net-cloud.com

Threat Landscape



















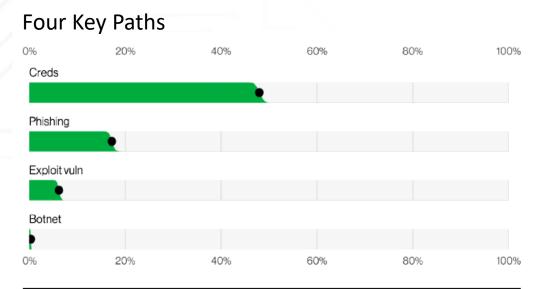
Phishing



Compromised Sites



Current State of Cybersecurity



Ransomware uptrend (13% = last 5 years)

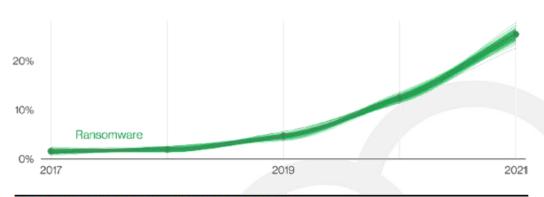


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

Figure 6. Ransomware over time in breaches

- "...many organizations continue to struggle with keeping an eye on their people and their systems."
- 82% of breaches involved the human element



Economics of Cybersecurity

- Cybersecurity now a "Sector"
 - Business, Technology, Jobs, Services
- Increase cost to business to do business
- Organized Crime Cyber-Cartels
- PII Personal Identifiable Information
 - We all have a responsibility!

Cybersecurity is not an IT issue;

Cybersecurity is a Business Risk Issue!!



Toledo (OH) Public Schools (Sep.'20)

- Maze Ransomware Cartel
- ? Extortion Demands
- 9GB of PII records
 - (2008-2017 data)
- Less than 6 months:
 - Identity Theft
 - Credit Fraud

- Dissent Doe (September 14, 2020). "Maze attacking some of the country's largest school districts." Available online at: https://www.databreaches.net/maze-cartelattacking-some-of-the-countrys-largest-schooldistricts/
- 7 Dissent Doe (October 15, 2020). "Privacy nightmare for Toledo Public Schools: Hackers dumped student and employee data." Available online at: https://www.databreaches.net/privacynightmare-for-toledo-public-schools-hackersdumped-student-and-employee-data/
- 8 Shaun Hegarty (February 22, 2021). "Toledo Public School students seeing effects of massive data breach." Toledo, OH: WTVG. Available online at: https://www.13abc.com/2021/02/22/toledo public-school-students-seeing-effects-of massivedata-breach/

Toledo (OH) Public Schools (Sep.'20)

"[One parent]... learned his son's information is in the hands of people it shouldn't be. Here are some of the messages he's received about his elementary schooler:

- The first one was for denial for a credit card.
- Another one happened when the child was denied for a car loan because it said the reason was because of his income ratio.
- One of the last ones was to have fixed electric rates.
- The family got a flier talking about the student's Toledo Edison account and the gift card he could get by switching suppliers.

'They've got our children's information and they're trying to use it,' said [the parent]."

Where I see Cybersecurity next

- More Government Regulation / "Recommendations"
- Technology measures are getting better with AI/ML
 - e.g. Endpoint Detection and Response
- Business & Cyber Insurance Policies will raise the awareness & expand the requirements.
 - Because they are needed to reduce risk.
- Cybersecurity will infiltrate every aspect of our lives & businesses.
 - All aspects of business process will be thinking security
 - IoT security risks will test our homes and businesses
- Cybersecurity labor crunch will explode exponentially
- The economic impact....



What can I do? Jim's Big Five / Six

- 1. Cyber-Education Regular & Consistent w/ Phishing
- 2. Multi-Factor Authentication
- 3. Structure Backup & Data Recovery Strategy
- 4. Endpoint Detection & Response
- 5. Regular Patch Management
- 6. Network Security (VPN Encryption / Next-Gen Firewall)

Then.....take action on a Cybersecurity Standard (e.g. NIST CSF)

NIST Cybersecurity Framework

A Roadmap for All



NETWORKING

ECHNOLOGIES
Your Technology Resource





Jim Bahm

President & CEO
Networking Technologies
[o] 814-836-0000 x103
jbahm@net-cloud.com
3910 Caughey Rd. Suite 120
Erie, PA 16506

