
CERIAS
Weekly Security Seminar Series
Wednesday, Jan. 19th, 2021 4:30p ET
"Leading Trends and Emerging Technologies for Cybersecurity in 2022"
Chuck Brooks - Georgetown University
Later..
PURDUE UNIVERSITY
https://ceri.as/seminar

Internet and Security

“

The Internet was not built for security, yet we have made it the backbone of virtually all private-sector and government operations, as well as communications. Pervasive connectivity has brought dramatic gains in productivity and pleasure but has created equally dramatic vulnerabilities. Huge heists of personal information are common, and cyber-theft of intellectual property and infrastructure penetrations continue at a frightening pace.

-Joel Brenner, former Counsel to the National Security Agency

GLOBAL CYBERSECURITY TRENDS

Trends

- **Threat actors, especially state-sponsored, and criminal enterprises will take advantage of the expanding cyber-attack surface by using their resources to employ more sophisticated means for discovering target vulnerabilities, automating their phishing attacks, and finding new deceptive paths for infiltrating malware**

- **Disruptive technologies like mobility, IoT, and cloud computing bring operational shifts that drive new security requirements. Advances in security like continuous monitoring and analytics find strong reception with agencies.**

Cost of Cybersecurity And Cyber-Threats

Threats & Stats

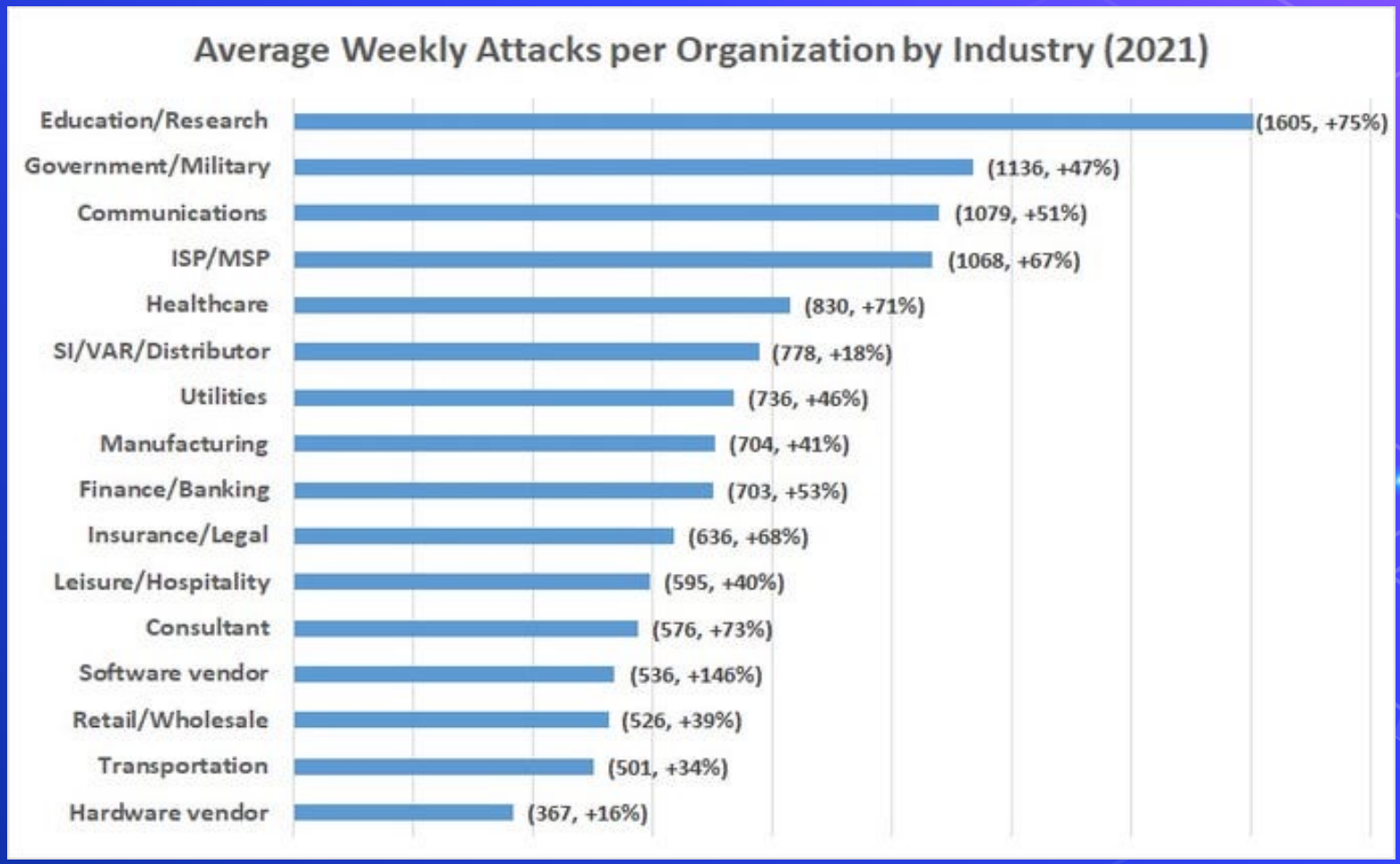
- Security investments continue to be driven by persistent threats, policy remedies, workforce shortages, and technological innovation
- Phishing attacks: Consistently Top Cyber Threat
- Ransomware is the fastest-growing cybercrime
- There are over 430 million types of malware online
- a cyber attack happens every 39 seconds
- Cybercrime will cost the world $6 trillion annually by the beginning of 2022
- Advanced Persistent Threats: Trojans can be placed wherein an attacker gains control of the computer system, creating a backdoor and obtaining access to confidential and sensitive data.
- Insider Threats difficult to thwart

Ransomware

According to the World Economic Forum's new annual report, *The Global Cybersecurity Outlook 2022,* 80% of cyber leaders now consider ransomware a "danger" and "threat" to public safety

WEF notes that cybercrime - ransomware attacks rose 151% in 2021. There were on average 270 cyberattacks per organization during 2021, a 31% increase on 2020, with each successful cyber breach costing a company $3.6m. After a breach becomes public, the average share price of the hacked company underperforms the NASDAQ by -3% even six months after the event.

Businesses Suffered 50% More Cyberattack Attempts per Week in 2021



Cyber Threat alties

ACTOR	MOTIVE	TARGETS
Nation States	Economic or Military	IP or Infrastructure
Organized Crime	Financial Gain	IP, Banks, PoS
Terrorists / Extremists	Cause Support	Highly Visible Targets
Hackers / Hacktivists	Publicity, Watch it burn	Anything and Everything
Trusted Insiders	Revenge, Financial Gain	Your Data and/or Networks

- Every connected device is a potential entry point for hackers (IoT is often connected to critical infrastructure)
- ternet-of-Things (IoT) devices face 5,200 attacks a month, while one in every 36 mobile devices has high-risk apps installed on it, according to Symantec's 2019 Internet Security Threat Report insights.
- Attackers can also turn IoT devices into a bot and infect other connected devices

IoT Attack Surface / Vulnerabilities

50 billion will be wirelessly connected via a network of sensors to the internet by 2021 (Cisco)

By 2023, there will be 3X more networked devices on Earth than humans

By 2025, an average connected person anywhere in the world will interact with connected devices nearly 4,800 times per day

–

Basically one interaction every 18 seconds. (IDC)

Security incidents involving IoT devices have impacted 67% of enterprises. (Forrester)

50% IoT devices on corporate networks security organizations don't maintain basic security measures beyond default passwords

98% of all IoT device traffic is unencrypted - exposing personal and confidential data on the network

Critical Infrastructure Cybersecurity Challenges

- IT-OT convergence. IoT technology is a part of both IT data and OT operations. Operational technology (OT) vulnerabilities increased 30% year-over-year.

Protecting Critical Infrastructure Poses Unique Challenges

- of trained skilled workforce is a continual issue in OT cybersecuri
- *t works in Cybersecurity IT may pose risk to OT cybersecurity. For example where patching may not be an option as each update disrupts time system operations and requires some downtime*
- cts of a breach can be calamitous operationally and economically
- y organizations do not know if an attack has occurred or lack syste onitor or detect breaches in controls systems
- e case of energy systems infrastructure, many of the OT systems lve legacy systems over 25 years old (no security built in) and are in stages of digital transformation
- ers seeking out unsecured ports and systems on industrial system ected to the internet. IT supply chains are particularly vulnerable

Cyber-Risks Gaps

- gacy Systems
- oed organizations
- iance on bolted-on point products
- k of contextual awareness of threats and solutions
- alified worker shortage

Cybersecurity Framework: Summary

Risk Management (identifying, assessing and responding to threats-

NIST Framework: Identify, Protect, Detect, Respond, Recover

SECURITY BY DESIGN, DEFENSE IN DEPTH, ZERO TRUST

- Security by design – build agile systems with operational cyber-fusion to be able to monitor recognize, and respond to emerging threats. Install intrusion prevention systems (IPS) or intrusion detection systems (IDS) to monitor malicious activity on your industrial network. Also enable security settings on energy system networks

- Defense-in –Depth; technologies, processes, air-gapping, hardening, Encryption of data flowing from sensors and segmentation of OT and IT.

- Zero Trust is a security model that uses strict identity verification for every person or entity attempting to access network resources, regardless of whether the person or entity is in the office bound by the network perimeter or accessing the network remotely

Security strategies are evolving. Strive for a multilayered approach in cybersecurity.

- Multifactor authentication
- yered with risk-based access
- havioral biometrics
- driven anomaly detection
- End-to-end encryption.

Bake in security design & processes from the beginning

- Emerging technologies that help automate cybersecurity detection d response, including machine learning, artificial intelligence, and ockchain

How To Approach Risk:

Cyber-breaches are not a static threat and is always evolving in tactics and capabilities

- **Identify and Classify Assets**
- **Prepare Vulnerability Assessment**
- **Confirm the Security Protocols of All Parties in Your Data Chain:**
- **Do Vulnerability Assessments With Penetration Tests**
- **Test Incident Response Plan**
- **Create Cyber Resilience Plan**

Nuts & Bolts of Risk Management Strategy

Vulnerability Assessments need to be instilled up front in the process. Also mapping of the control systems, communication flows, and all connected devices in the network should be prioritized.

- **Modernizing security architectures**
- **Mobile and BYOD Security**
- **Incident Response**
- **Policy: Best Practices, Compliance**
- **Protecting critical infrastructure through rapid proto-typing of technologies and Public/Private cooperation**

Cybersecurity Tools & Protections

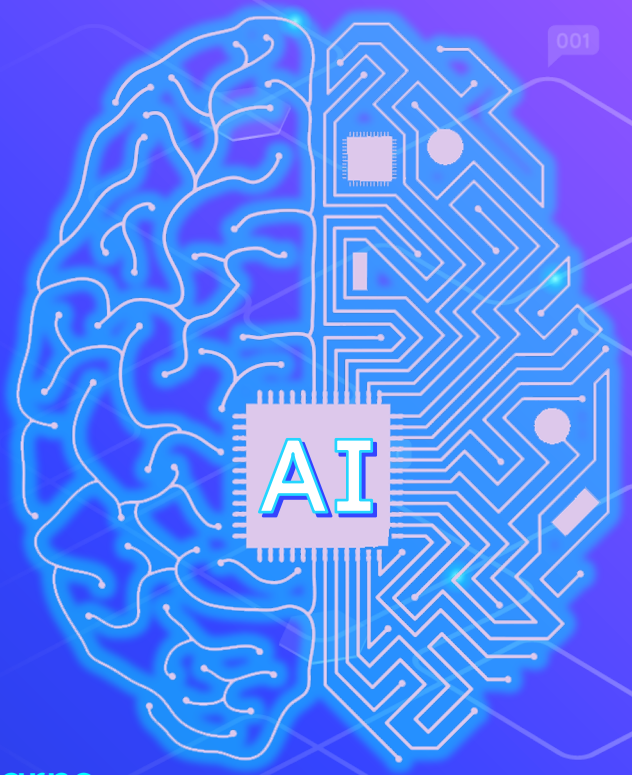
- Cybersecurity Hygiene
- Multi-factor authentication
- Advanced Firewalls
- Intrusion Prevention
- Anti-Virus/Anti-Malware
- Anti-Spam
- Encryption
- Web Application Controls
- Patching
- Data Loss Prevention.
- Vulnerability Scanning
- Security Information Management
- File Integrity Monitoring
- Air-gap compatible solutions which can keep infrastructure isolated and protected from the open environment
- Red Team/Blue Team
- Employee Awareness Training
- Incident Response

Emerging Technologies of The 4th Industrial Revolution

- Automation and Adaptive Networks
- Artificial intelligence (human/computer interface)
- Machine Learning
- Cryptography/Encryption (Identity based encryption)
- Blockchain
- Simulation Virtualization & Gaming
- Cloud computing and Edge Computing
- Biometrics and Authentication Technologies
- Software (anti-virus)
- Hardware Separation/Hardening
- Photonics/sensors
- Big Data: Real-time analytics and predictive analytics
- Super-computing and Quantum-computing

AI/ML AND CYBERSECURITY

- Threat Detection (Spam and Phishing)
- Malware Identification
- Autonomous Patching
- Categorize Attacks
- Adapt To Evolving Risks
- Both Offensive and Defensive Cyber



Cyber attackers use of offensive AI is becoming more sophisticated with the capability to self-mutate as it learns from its environment while hiding in the background by leveraging existing data flows and human behavior to remain undetectable amid the noise across networks

CLOUD COMPUTING AND CYBERSECURITY

- Cloud Computing consists of moving and storing data and applications over the Internet from remote servers.
- Generally it offers users cost flexibility, mobility, and increased productivity. For cybersecurity it allows for firewalling and managed security.
- An advantage of the cloud is you know where the data resides and who is managing its security.

Internet of Things

- IDC predict that spending on IoT will reach nearly $1.4 trillion in 2021. This coincides with companies continuing to invest in IoT hardware, software, services, and connectivity
- Cisco estimates 50 B devices are now connected to IoT
- Dr. Janusz Bryzek, vice president of MEMS and Sensing Solutions at Fairchild Semiconductor, predicts there will be 45 trillion networked sensors 20 years from now. This will be driven by smart systems, including IoT, mobile and wearable market growth, digital health, context computing, and artificial intelligence (AI)

BLOCKCHAIN

- Blockchains are immutable digital ledger systems implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority.
- At its most basic level, they enable a community of users to record. transactions in a ledger public to that community such that no transaction can be changed once published.”
- Blockchains are immutable digital ledger systems implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority.

Brooks Consulting International

Government Relations, Marketing, BD

https://www.linkedin.com/in/chuckbrooks/

Chuck Brooks

President

Cybersecurity, Tech, Risk Management

Thought Leadership, Security Influencer

GEORGETOWN UNIVERSITY

Chuck Brooks

Professor

Applied Intelligence and Cybersecurity Graduate Programs

cb1519@georgetown.edu

https://www.linkedin.com/in/chuckbrooks/

Thanks!

Any questions?

You can find me at:

- Twitter: @ChuckDBrooks
- Linkedin: Chuck Brooks