CYMANII

the cybersecurity manufacturing innovation institute

Better Plants: Cyber Security Bootcamp 2025 - Thursday, April 17th

Cybersecurity and Manufacturing: Overview, Challenges, and Trends

Rima Asmar Awad, PhD
Cybersecurity Software Engineer // ORNL
Rima.Awad@cymanii.org // awadrl@ornl.gov

Jennifer Sims
Cyber Security Professional// ORNL
Jennifer.Sims@cymanii.org // simsja@ornl.gov

Objectives

After attending this module, you will able be to:

- Understand the Strategic Importance of Manufacturing
- Identify and Analyze Key OT Cyber Attacks
- Interpret Vulnerability Statistics and IIoT Threats
- Examine Trends in AI and Their Cybersecurity Implications
- Articulate a Cybersecurity Philosophy and Defense Strategies
- Assess Supply Chain Cybersecurity Risks
- Apply Knowledge Through Hands-On Analysis

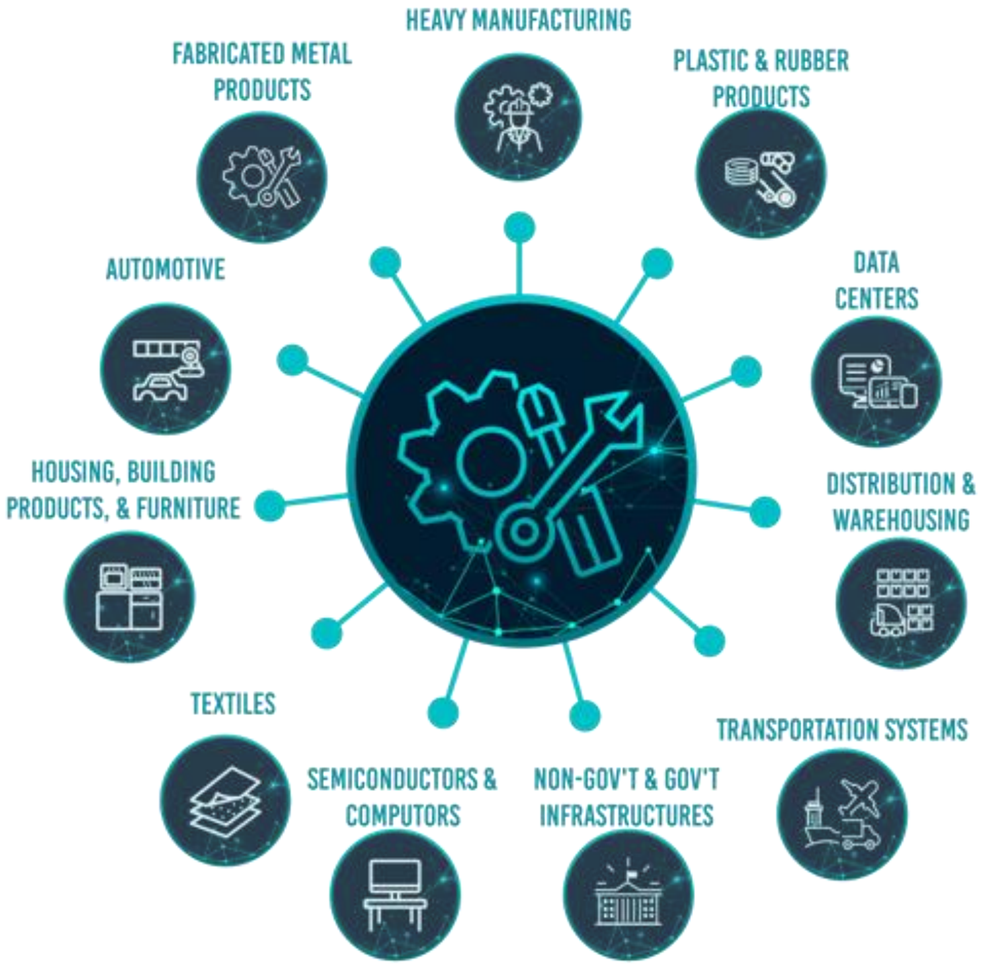
Manufacturing & National Security

Importance of Manufacturing for National and Economic Security

- Manufacturing is crucial to national and economic security
  - Economic growth and jobs
  - Domestic capability of producing goods
  - Reduces reliance on foreign nations
  - Critical infrastructure support
  - Supply chain stability

Challenge

- Manufacturing diversity
  - Varying production methods
    - Different manufacturing processes require distinct workflows, equipment, and skill sets
  - Supply chain complexity
    - Sourcing raw materials and components for different manufacturing types may involve managing multiple suppliers



OT Cyber Attacks

Phishing

- Form of social engineering where attackers attempt to acquire sensitive data through a fraudulent email
- Goal
  - To gain sensitive data (logins, passwords) from victims to access the targeted network or company
- Many different types of phishing
  - Spear phishing(whaling), smishing, vishing, quishing

Phishing Attacks Statistics

- Phishing Attacks on Manufacturing Industry Rise More Than 80%
- 24% Growth in Vendor Email Compromise Attacks on Manufacturers
  - threat actor poses as an external third party rather than an internal employee.
- Business Email Compromise Attacks Targeting Manufacturers Increase 56%
  - Threat actors masquerade as trusted parties—usually someone with whom their target has a trusted relationship or someone in a position of authority

Phishing Scenarios

Phishing Case Study – FACC (2016)

1. Malicious cyber attacker accessed FACC's email server and studied CEO's writing style
2. Malicious cyber attacker sent email (posing as CEO) to employee in finance department requesting funds to be sent to account
3. Employee wired money to the malicious cyber attacker's account

Repercussions

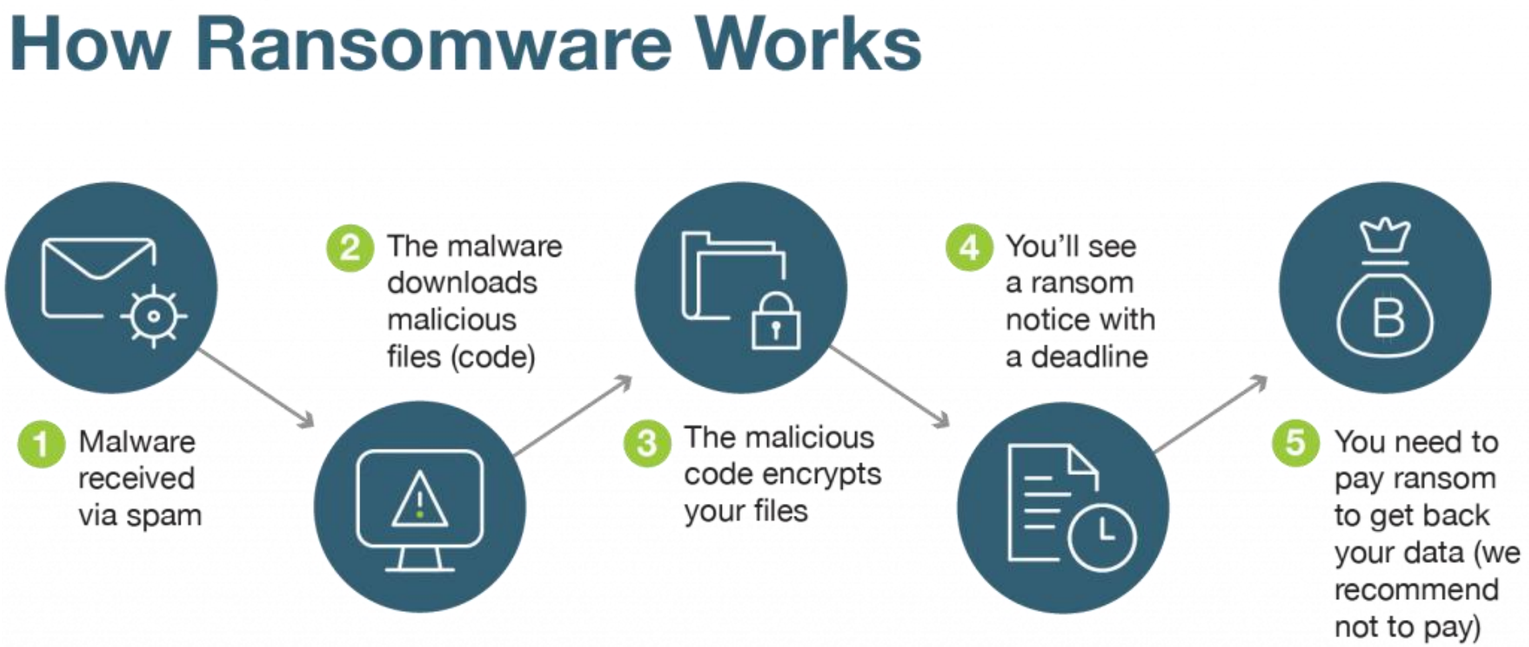
- CEO and CFO were fired
- Company stock dropped by 17%
- FACC recovered €10.9 million of stolen funds

Mitigations for Phishing

- Education
  - Train employees and raise awareness with internal phishing campaigns
- Internal Reporting
  - Companies should have an adequate and operational internal reporting procedure in place
- External Reporting
  - Report phishing attempts to competent authorities
  - Forward phishing emails to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies)

Ransomware

- A type of malware that encrypts the victim's personal data until a ransom is paid



Ransomware's Impact in Manufacturing

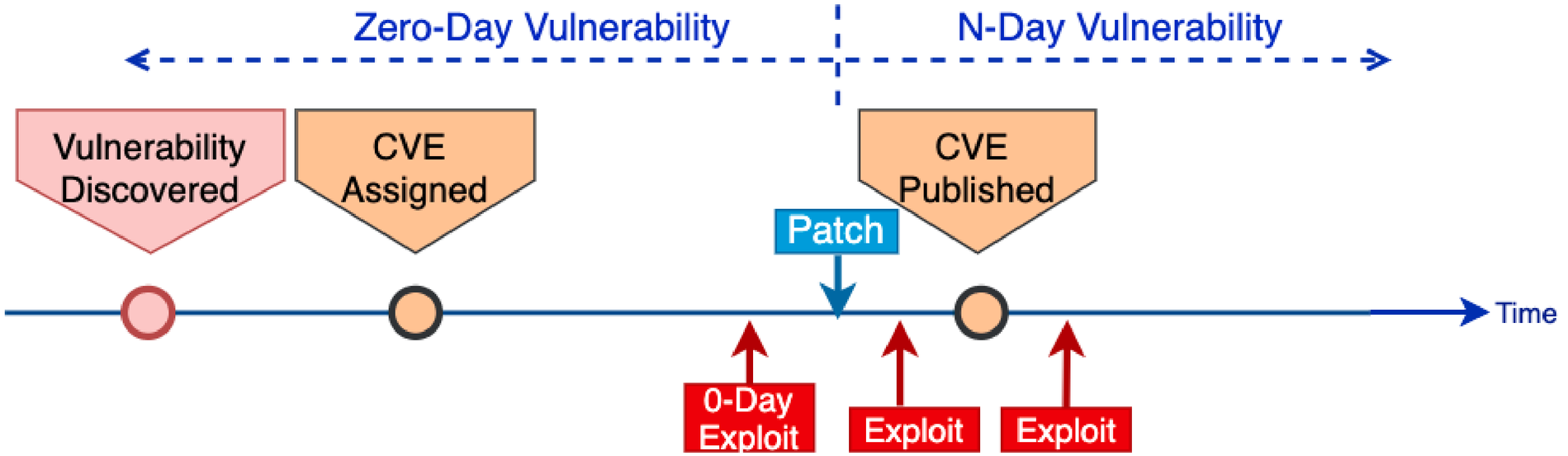
- Cybereason Study:
  - Average cost of a ransomware attack on a manufacturing company is approximately $1.85 million
- Impact:
  - Production downtime
  - Disruption to supply chain
  - Financial loss
  - Damages reputation
  - Equipment Malfunctions

Ransomware Case Study – Norsk Hydro (2019)

- LockerGoga ransomware - Attributed to APT group FIN6
  - Logs off all users, disables all network adapters, and changes the local user and administrator passwords following encryption
- The cyberattack targeted Extruded Solutions department – responsible for producing aluminum products that are pressed through a die.
- The LockerGoga strain was linked to three previous cyberattacks targeting other industrial organizations (i.e., Altran Technologies, Hexion, and Momentive) just months earlier

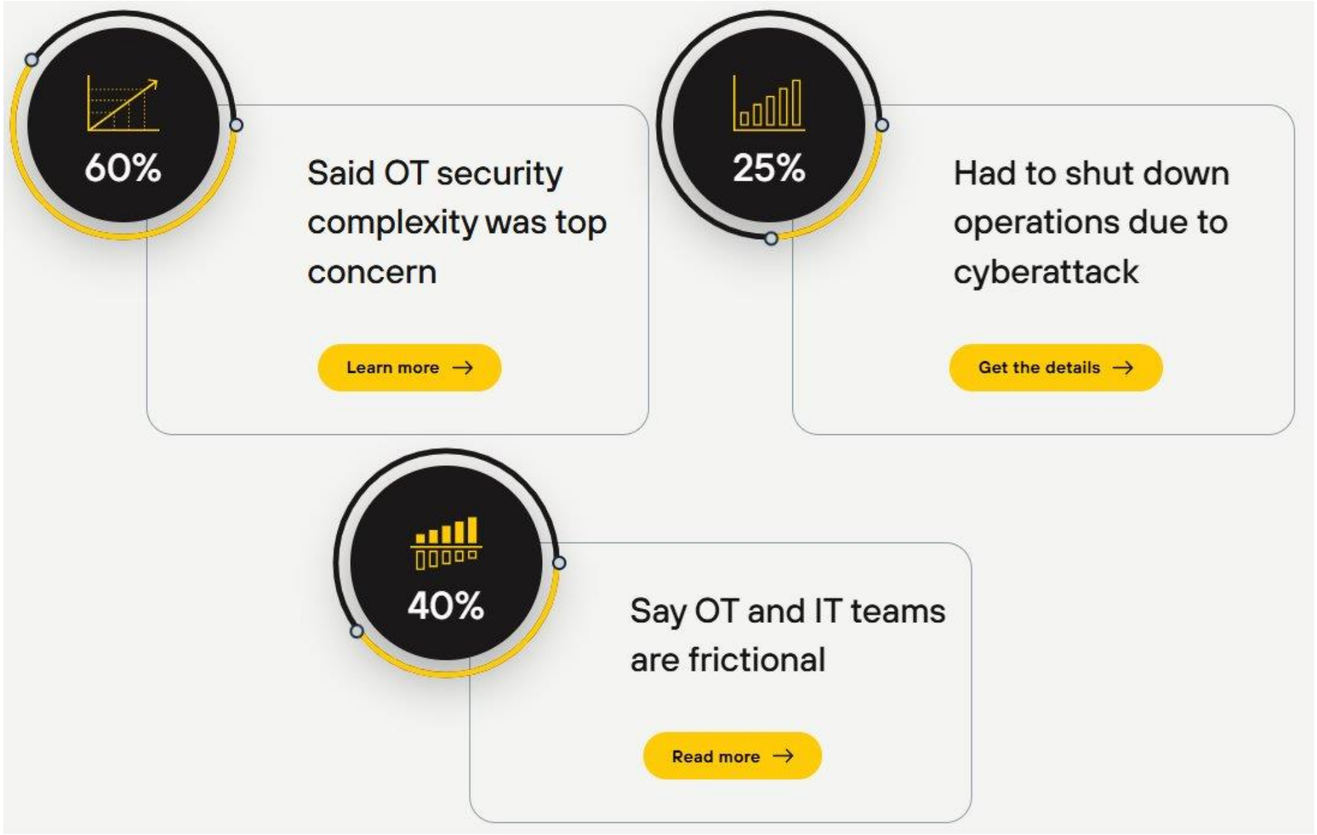
Time to Discovery

- Time to discovery of an ICS CVE can vary significantly (several months or even years)
  - Complexity of ICS systems
  - Vendor response time



Statistics on Vulnerabilities

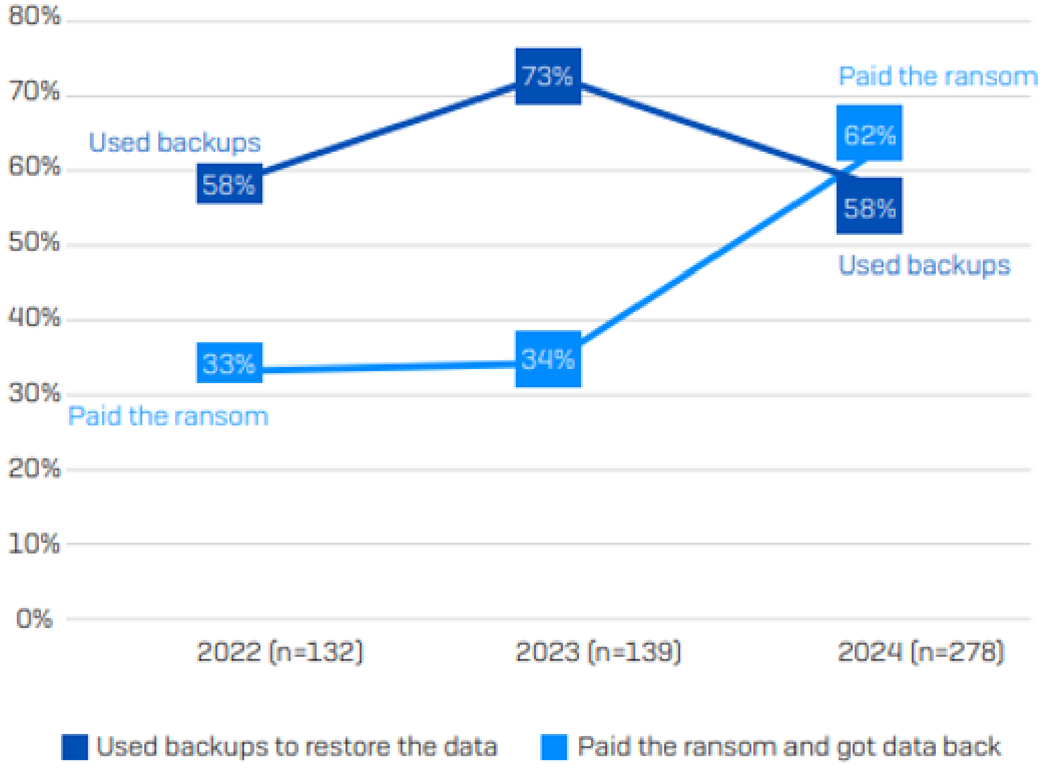
Threats to an OT Environment



Ransomware Statistics

In the last year, has your organization been hit by ransomware?
Yes. n=585 (2024), 363 (2023), 419 (2022), 438 (2021), 648 (2020)

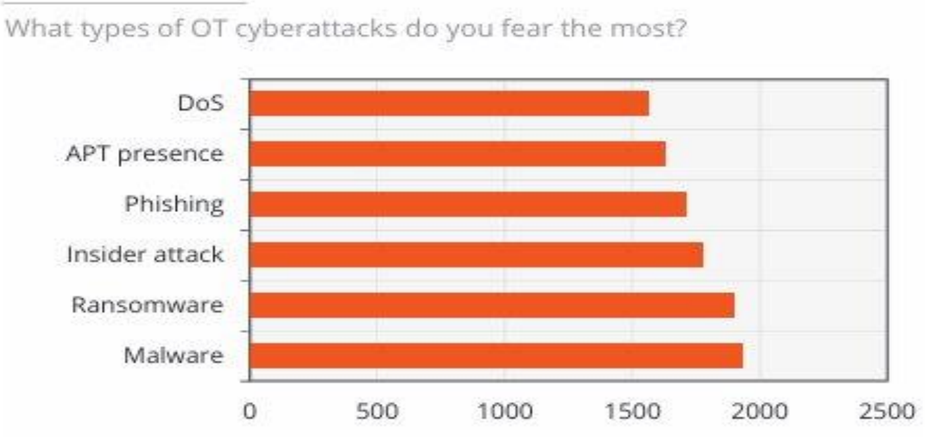
SOPHOS



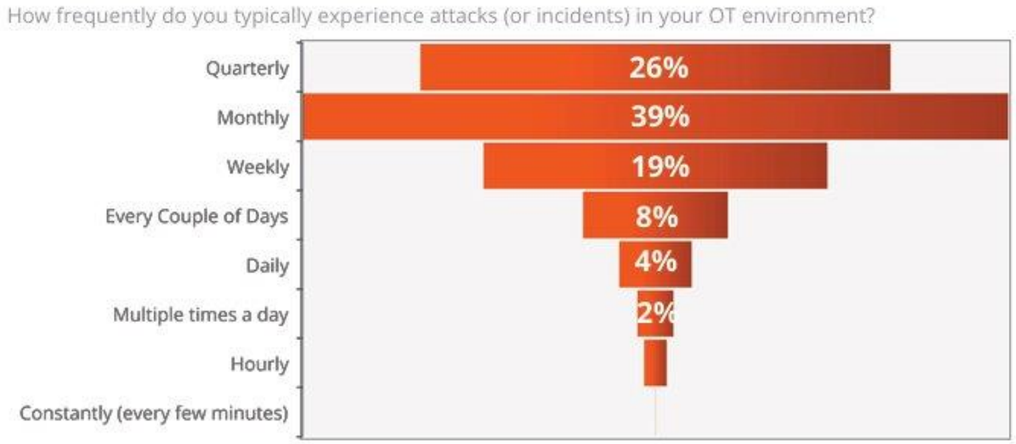
Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. Base numbers in chart.

SOPHOS

OT Security Report 2024 - Palo Alto Networks

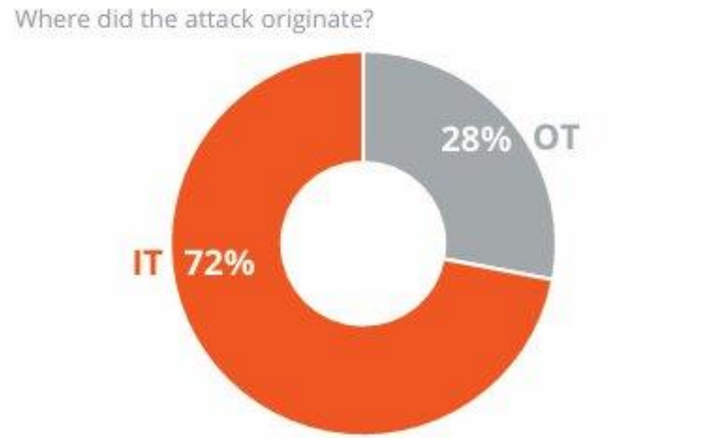


OT Security Report 2024 - Palo Alto Networks

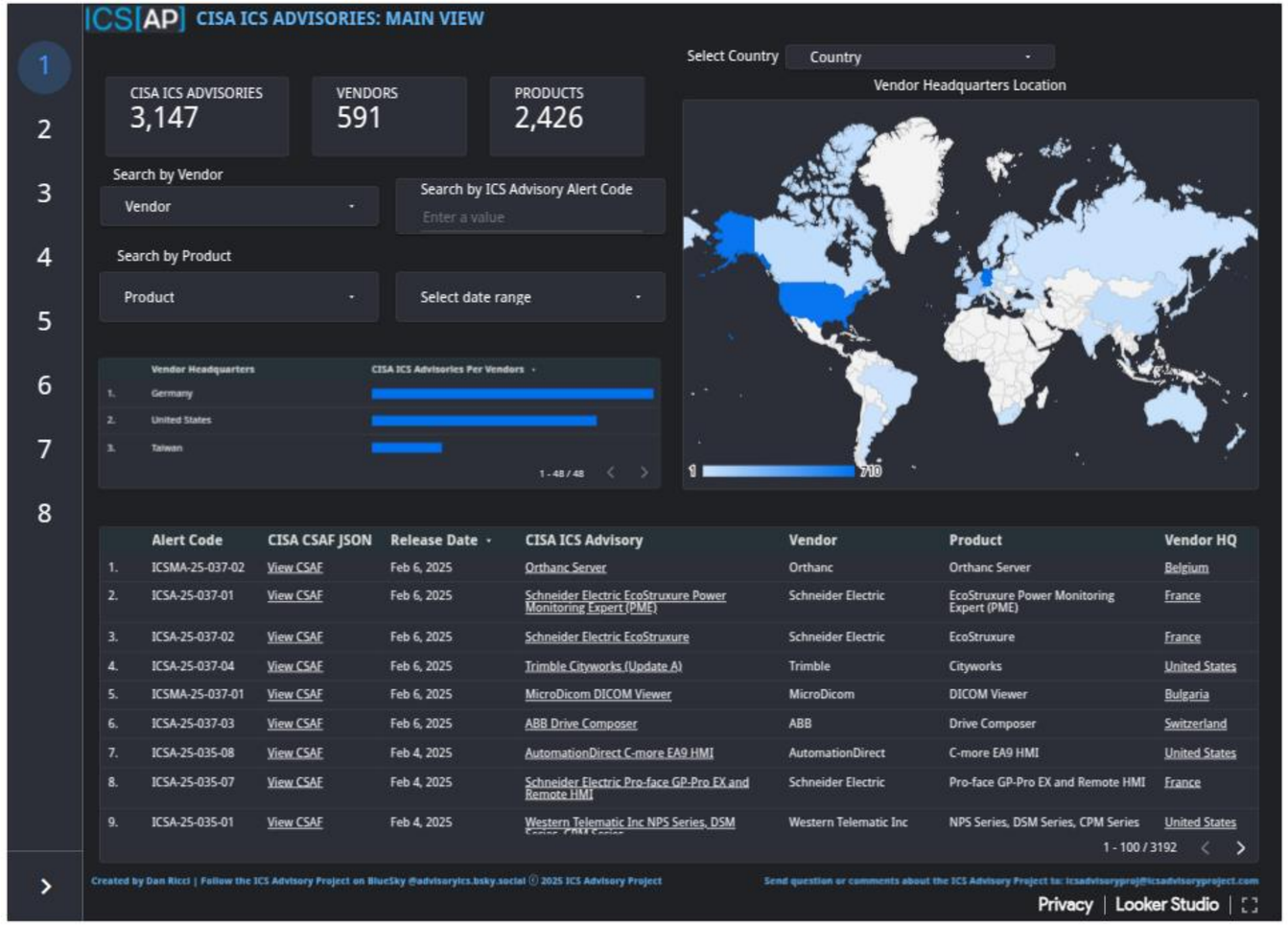


Insights from Industrial Operators

"Evaluate and validate supply chain vendors."



ICS Advisory Project



Trends in AI

Trend in AI as a Defensive Tool

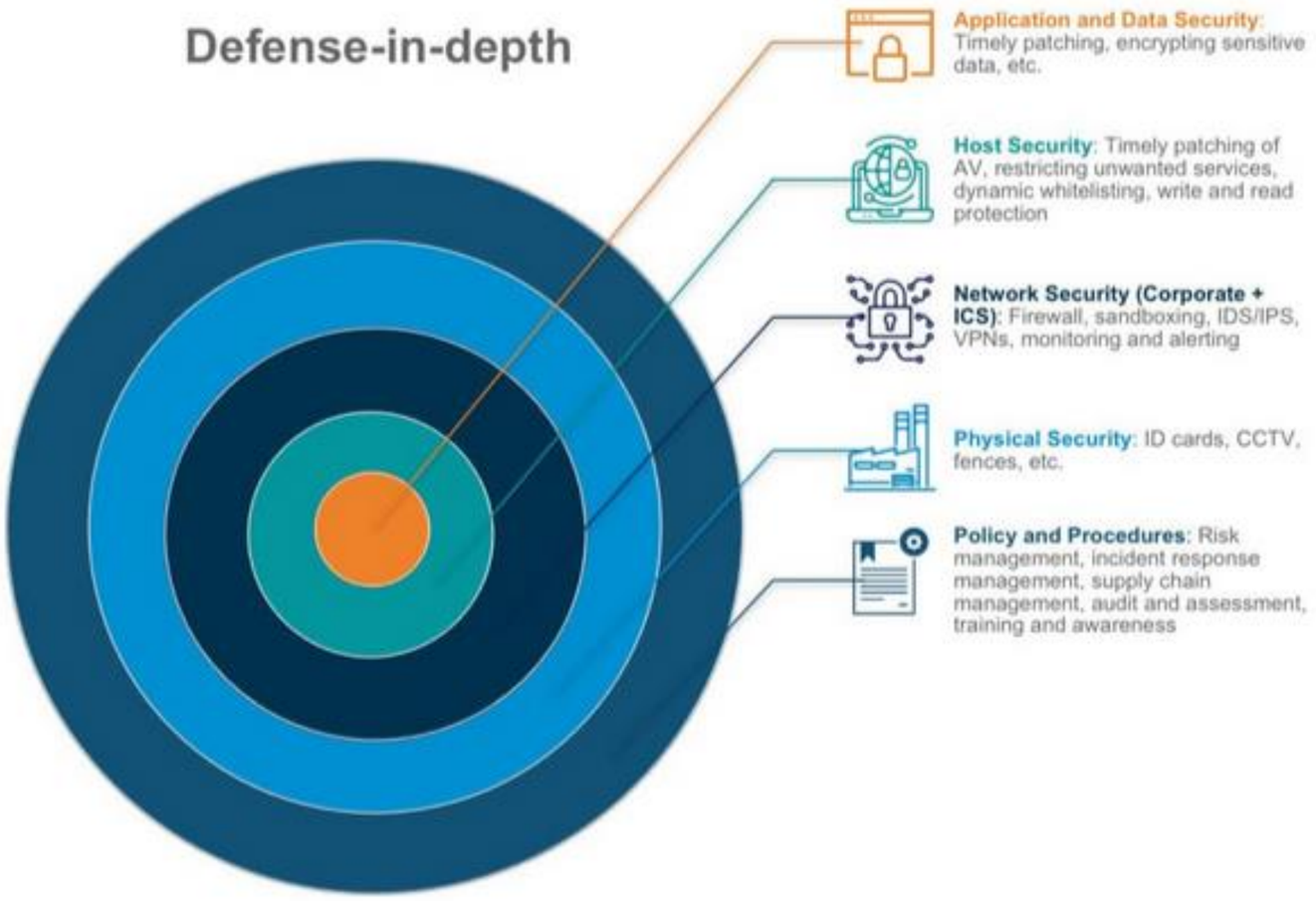
- Advanced Threat Detection
  - Proactively identify and flag potential cyber threats within a manufacturing environment
- Anomaly Detection
  - Identify unusual patterns or deviations from the expected norm in production data
- Automated Incident Response
  - Uses machine learning and automation to detect, analyze, and respond to security incidents in real-time

Trend in AI as an Offensive Tool

- Automated Malware Generation
  - Generative AI to write novel malware code, identify potential vulnerabilities in manufacturers' information systems
- Automated Social Engineering Attacks
  - AI generated realistic phishing emails, deepfake videos or voice recordings to further deceive victims

Perimeter Defenses

Perimeter Defenses



CyManII's P.U.R.E. Framework

- CyManII developed the P.U.R.E. Framework to enhance cybersecurity in manufacturing while ensuring efficiency and resilience
  - Focuses on secure, energy-efficient, and scalable cybersecurity solutions
- What is P.U.R.E.?:
  - Pervasive (P) – Cybersecurity is integrated across all aspects of manufacturing, from IT and operational technology (OT) to supply chain security
  - Unobtrusive (U) – Security measures operate seamlessly without disrupting production efficiency or manufacturing workflows
  - Resilient (R) – Strengthens manufacturing systems to prevent, detect, and recover from cyber threats such as ransomware and supply chain attacks
  - Economical (E) – Ensures cybersecurity is cost-effective and energy-efficient, reducing operational costs while maintaining strong protection

Supply Chain Cybersecurity

Supply Chain Cybersecurity Risks

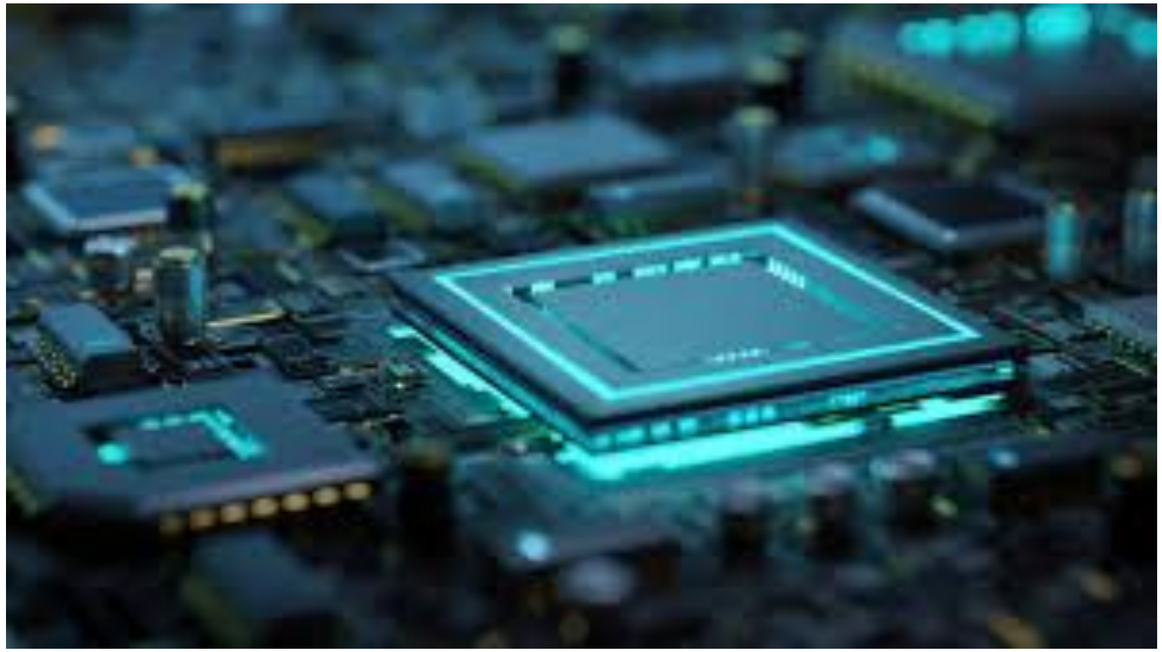
- Third-Party vendor vulnerabilities
- Compromised hardware and component integrity
- Software supply chain and open-source dependencies
- Remote access and maintenance exploits

Third-Party Vendor Risks

- Compromised firmware or software updates
- Weak security practices by third-party vendors
- Lack of security visibility and monitoring
- Data sharing and storage risks
- Cascading supply chain attacks

Insecure Product and Hardware Supply Chain

- Compromised Hardware
- Hardware-based attacks
- Lack of integrity verification
- End-of-life and legacy hardware risks
- Tampering during transit or storage



Software Dependencies and Open-Source Risks

- Vulnerabilities in open-source components
- Supply chain attacks on open-source software
- Lack of patch management
- Dependency confusion attacks

Remote Access and Maintenance Risks

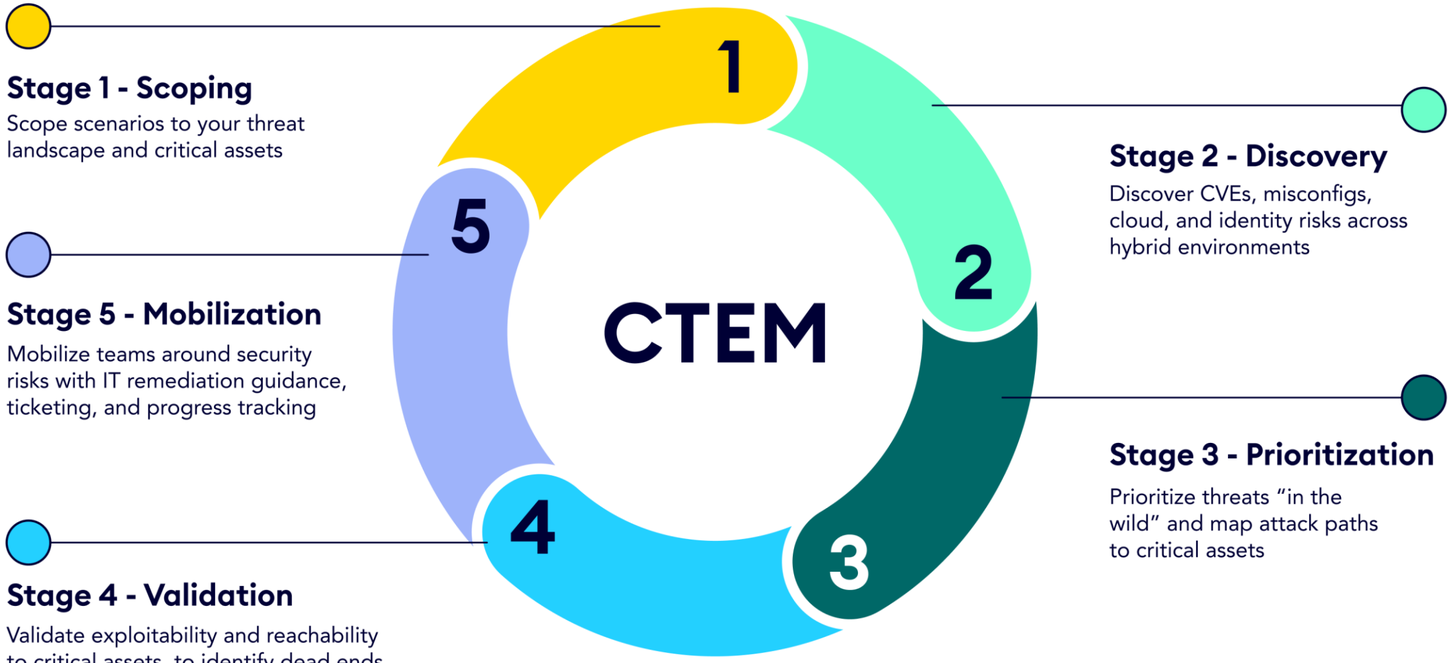
- Remote access vulnerabilities
- Inadequate monitoring of remote sessions
- Insecure supply chain communications
- Weak credential management
- Lack of Multi-Factor Authentication (MFA)
- Ransomware and malware injection via remote access

Philosophy on Cybersecurity

Cybersecurity as a Continuous Process

- Cybersecurity is not a one-time action but an ongoing cycle of protection, adaptation, and improvement. It is a dynamic field where:
  - Devices are continuously added and removed, creating an evolving attack surface
  - New vulnerabilities emerge daily due to software updates, misconfigurations, and new attack techniques
  - Complex interactions between systems and networks introduce unforeseen security gaps and dependencies

Cycle of Continuous Threat Exposure Management



Stage 1 - Scoping
Scope scenarios to your threat landscape and critical assets

Stage 2 - Discovery
Discover CVEs, misconfigs, cloud, and identity risks across hybrid environments

Stage 3 - Prioritization
Prioritize threats “in the wild” and map attack paths to critical assets

Stage 4 - Validation
Validate exploitability and reachability to critical assets, to identify dead ends and choke points

Stage 5 - Mobilization
Mobilize teams around security risks with IT remediation guidance, ticketing, and progress tracking

XM Cyber

Resilience: The "Not if, But When" Approach

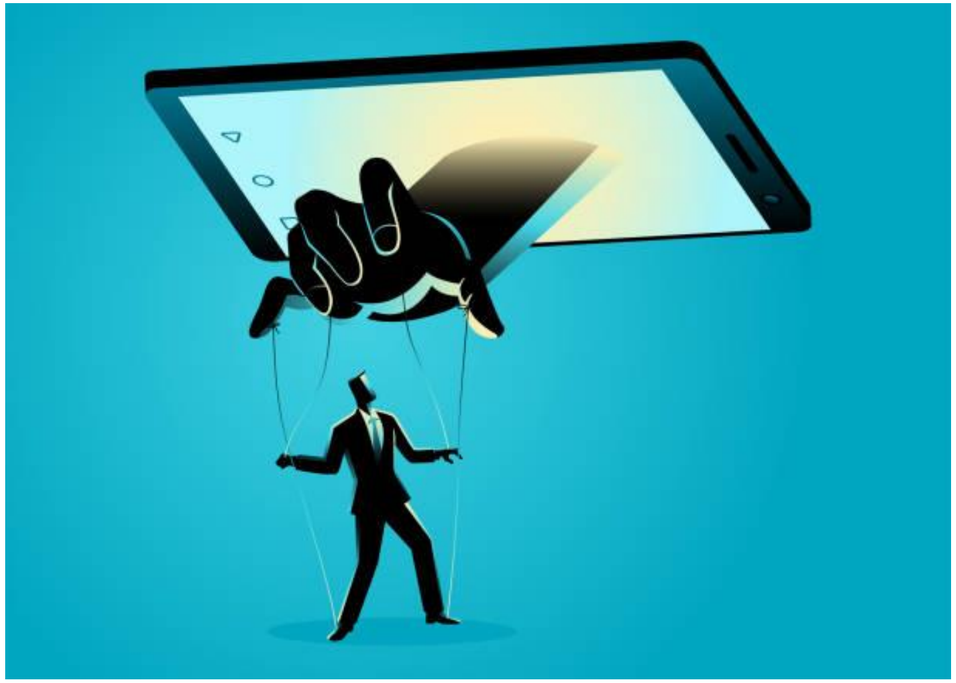
- We must operate under the *assumption* that breaches will occur.
  - **Incident preparedness**
  - **Detection and response**
  - **Business continuity and disaster recovery**
- The goal is *not just* to *prevent* attacks but **to withstand, recover from, and adapt** to cyber threats effectively

"Hard on the Outside, Soft on the Inside" Dilemma

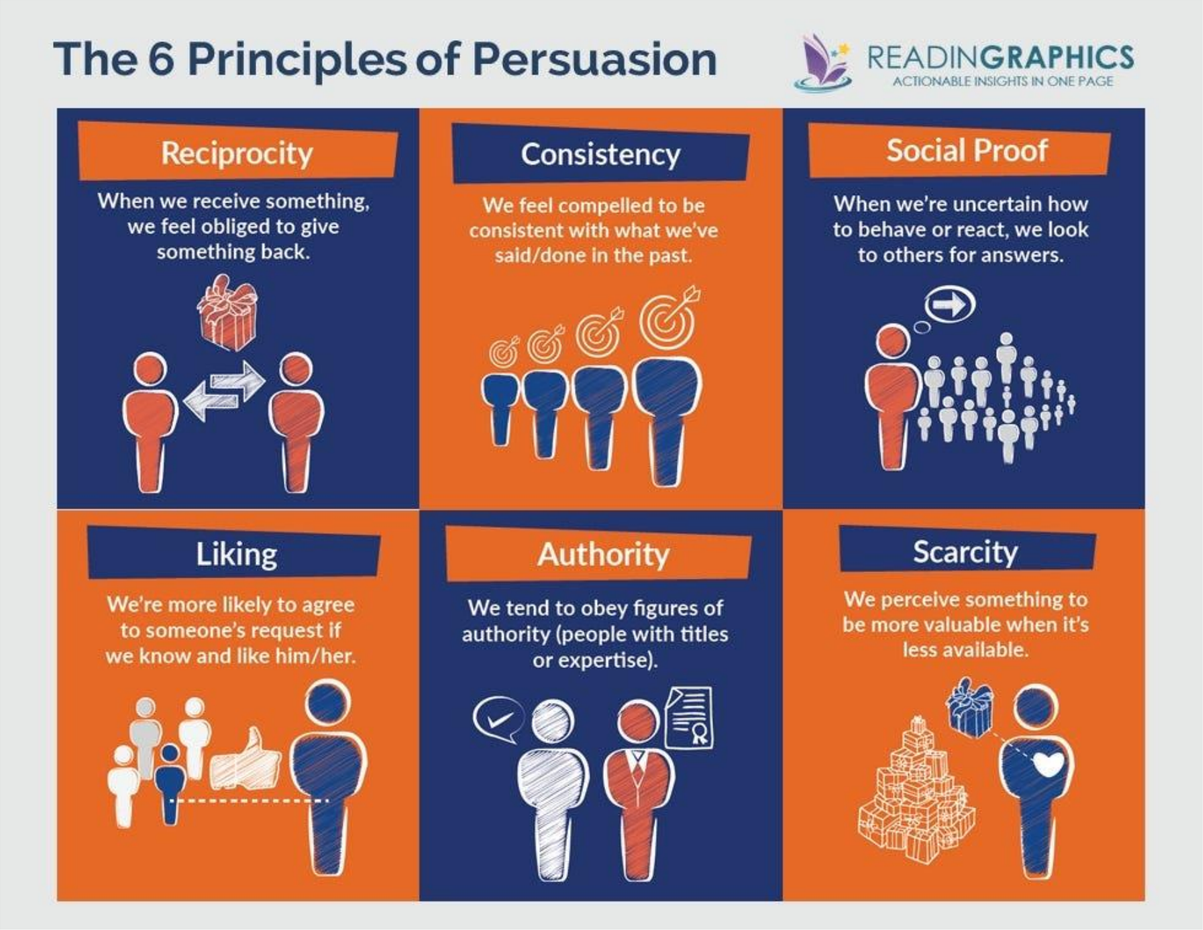
- Many organizations invest heavily in robust perimeter defenses (firewalls, IDS) but once an attacker breaches this perimeter, there is often weak internal security
- To mitigate, organizations should:
  - Implement a zero-trust architecture
  - Enforce strong segmentation
  - Adopt multi-factor authentication (MFA)
  - Continuously monitor for anomalous behavior

Cialdini's Principles of Persuasion & Phishing Attacks

- Social engineering exploits human psychology to manipulate victims into revealing sensitive information
- Dr. Robert Cialdini’s Six Principles of Persuasion explain how cybercriminals craft convincing phishing scams
  - Reciprocity
  - Scarcity
  - Authority
  - Consistency
  - Liking
  - Social Proof



Cialdini's Six Principles of Persuasion



Cialdini's Principles of Persuasion & Phishing Attacks

- How to defend against Cialdini’s tactics
  - Verify the Source – Check sender details and URLs before clicking
  - Think Before You Click – Avoid reacting emotionally to urgent messages
  - Enable Multi-Factor Authentication (MFA) – Adds extra protection even if credentials are stolen
  - Educate Employees & Users – Awareness training helps recognize persuasion-based phishing tactics

Conclusion

- Cybersecurity requires continuous adaptation, resilience, strong internal security, and awareness of social engineering tactics
- Manufacturing plays a key role in national security, making OT environments a critical target for threats like phishing, ransomware, and supply chain attacks
- Emerging AI-driven threats and defenses demand adaptive security strategies
- Frameworks like CyManII's PURE and defense-in-depth approaches enhance resilience
- Integrating proactive measures, organizations can safeguard both digital and physical assets against evolving cyber risks

Activity: OT Cyber Attack Attack Scenario Exercises

- Phishing email
- Ransomware impact report
- Network diagram
- Supply chain risk assessment

Cybersecurity Attack Scenario: Ransomware at GhostBuilt Manufacturing

- GhostBuilt Manufacturing, a critical supplier in the semiconductor industry, has fallen victim to a ransomware attack that originated from a phishing email. The attack has severely impacted the company's operations, leading to system encryption, production downtime, and potential data exfiltration.

  - **Analyze the incident, identify vulnerabilities, and propose solutions.**

Incident Analysis - Email

Sample Email Invoice Payment Required – Invoice #INV-8573

Subject: Invoice Payment Required – Invoice #INV-8573

Email Body:
Dear Valued Vendor
Please find attached Invoice #INV-8573 for the recent services rendered. Our records indicate that this invoice is overdue. To prevent any interruption in your service, we require immediate payment.
For your convenience, review the attached invoice and update your bank details using our secure payment portal:
Update Payment Details:
If you have any questions, please contact our billing department at billing@companyservice.com.
Thank you for your prompt cooperation.
Best regards,
Accounts Receivable

What are the flags?

Sample Email Invoice Payment Required – Invoice #INV-8573

Subject: Invoice Payment Required – Invoice #INV-8573

Email Body:

impersonal

disguise malicious content (executable code)

Dear Valued Vendor

Please find attached Invoice #INV-8573 for the recent services rendered. Our records indicate that this invoice is overdue. To prevent any interruption in your service, we require immediate payment.

For your convenience, review the attached invoice and update your bank details using our secure payment portal:

Update Payment Details:

http://updated-payment.net/
Ctrl+Click to follow link

Domain doesn't match expected company

If you hav contact our billing department at billing@companyservice.com.

Sender's email address and domain should be cross-checked

Thank you for your prompt cooperation.

Best regards,

Accounts Receivable

Ransomware Impact Report – Incident Summary

- **Incident Summary**
  - 8:00 AM – An employee unknowingly clicked on a phishing link, triggering the download of malicious ransomware
  - 8:30 AM – The ransomware rapidly spread across the network, encrypting critical files and locking production systems
  - Ransom Demand – Attackers issued a $5 million ransom in cryptocurrency for decryption keys
  - Operational Impact – Manufacturing operations came to a complete halt, disrupting semiconductor production and supply chain logistics

Ransomware Impact Report – Impact

- Loss of $500,000 per hour in downtime
- Third-party suppliers delayed shipments by two weeks
- Public trust damaged due to a cybersecurity breach headline in major news outlets

CyManII News

Volume 10, Issue 3 April 2103

GHOSTBUILT MANUFACTURING STRUCK BY RANSOMWARE

DELAY IN SEMICONDUCTOR PRODUCTION

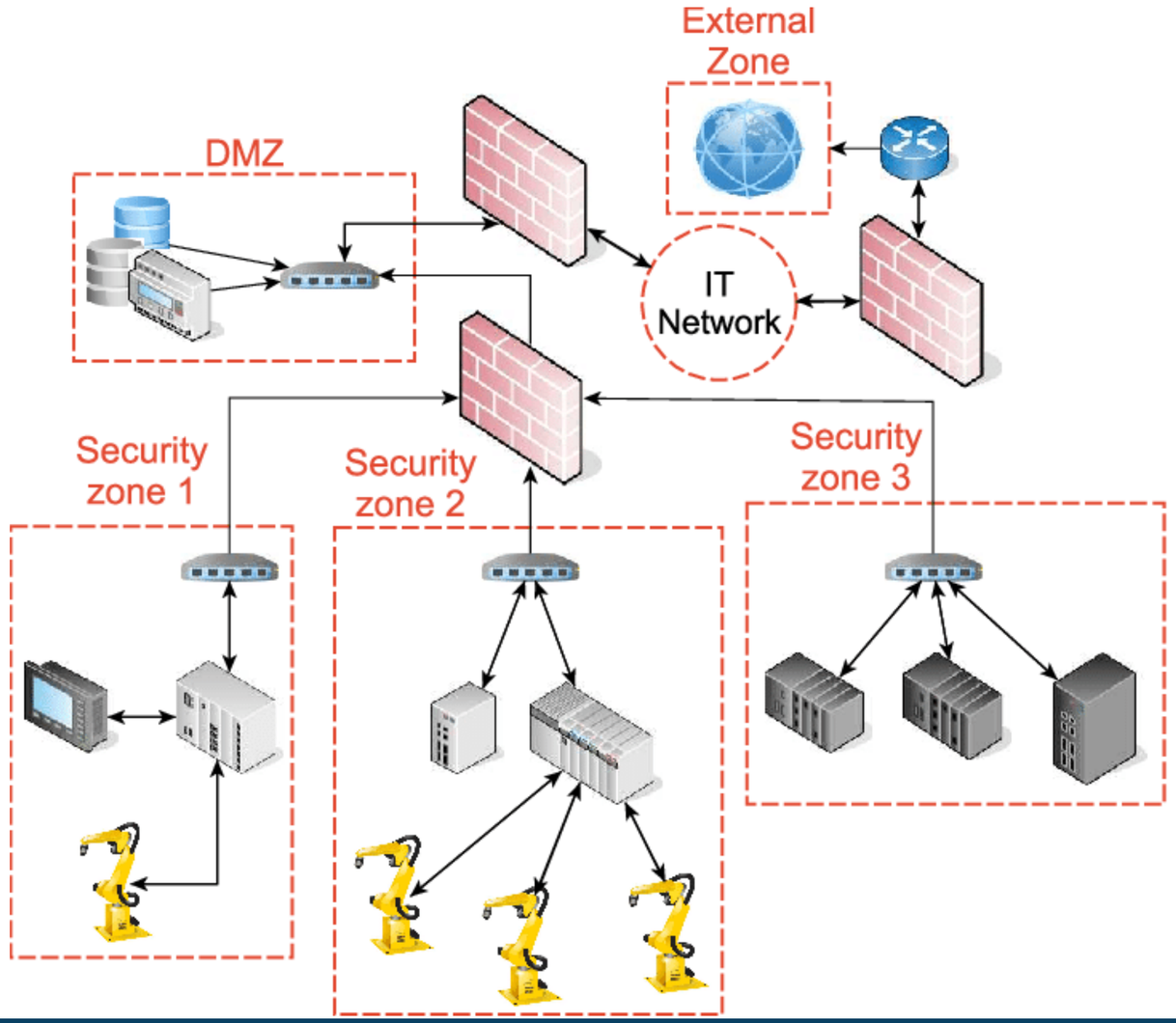
$500,000 per hour lost!!

$ 5 Million Ransom

GhostBuilt Manufacturing was hit with a ransomware on Sunday morning. Their production manager was victim to a phishing email. This attack is just one of many that have been happening globally. The need for stronger, resilient critical infrastructure security and social engineering awareness is needed greatly.

Howard Grimes' key takeaway is " Take cybersecurity seriously and develop proactive, defense-first

Network Diagram



Supply Chain Risk Assessment

Rank the vendors in order of potential cybersecurity risk.

Vendor A

Supplies raw materials, has outdated security protocols

Vendor B

Cloud-based logistics software, recently reported a data breach

Vendor C

Maintenance contractor for IIoT devices, uses remote access tools

Supply Chain Risk Assessment - Sorted

Vendor B

Cloud-based logistics software, recently reported a data breach

Highest risk because they have recently reported a breach. Attackers might still have access or stolen credentials. If this vendor integrates with company's supply chain, compromised credentials could lead to another ransomware attack.

Vendor C

Maintenance contractor for IIoT devices, uses remote access tools

Second highest because remote access is a common attack vector in OT environments. If not properly secured, attackers can gain direct access to OT systems and deploy malware. Colonial Pipeline attack stemmed from compromised credentials for a VPN without MFA.

Vendor A

Supplies raw materials, has outdated security protocols

If vendor's weak security leads to compromised communication channels, or tampered shipments, it could introduce risk. Doesn't have direct access to IT/OT systems so risk is lower.

Phishing Email Quiz

Let’s take a phishing email quiz:

https://phishingquiz.withgoogle.com/

QUESTIONS?

Contact Us

https://cymanii.org/cymanii-training/

Follow us on social media:

Content Partners and Training Provided By:

CYMANII Officially Endorsed Educational Content

UTSA Cybersecurity for Manufacturing

INL Idaho National Laboratory

NIST

References

- https://www.zoho.com/workplace/articles/facc-ceo-fraud.html
- https://news.sophos.com/en-us/2024/05/28/the-state-of-ransomware-in-manufacturing-and-production-2024/
- https://www.powermag.com/securing-industrial-control-systems-a-holistic-defense-in-depth-approach/
- https://www.paloaltonetworks.com/resources/research/state-of-ot-security-report?utm_source=bing-jg-amer-cdss-smco-sent&utm_medium=paid_search&utm_campaign=bing-cdss-ot-amer-multi-lead_gen-en-eg&utm_content=7014u000001eHHTAA&utm_term=ot%20threats&cq_plac=&cq_net=o&msclkid=b266f1d0ee911eb1123f965e75b45290%20%E2%80%8B
- https://www.foley.com/insights/publications/2024/09/cybersecurity-industry-4-part-1/
- https://link.springer.com/article/10.1007/s10462-024-10973-2#:~:text=Overall%2C%20using%20automation%2C%20attackers%20can,potential%20damage%20of%20those%20attacks.
- Cialidni, Robert B. Influence: The Psychology of Persuasion (2006.).