Cybersecurity Essentials for Smart Manufacturing Professionals

Module 1: An Introduction to Cybersecurity

ESL Global Cybersecurity Institute

Rochester Institute of Technology

September 2023

Learning Outcomes

By the end of this class, you will be able to:

- Understand the importance of protecting business operations
- Identify common types of cybersecurity attacks in manufacturing
- Practice cybersecurity best practices to prevent or respond to cybersecurity attacks
- Report a suspected cybersecurity incident

Become a more skilled, more competitive machinist

Introduction to Cybersecurity

Manufacturing (Cyber)security

- What comes to mind when you think of manufacturing security?
  - How about Cybersecurity?
- What do you think about hackers' motivations?

Courtesy: https://www.trendmicro.com/en_us/ciso/22/l/cybersecurity-plan-2023.html

Security

- *"A condition that results from the establishment and maintenance of **protective measures** that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems"* — NIST
- Examples: physical security (safes, doors, fences, personnel, etc.)

[avoidance and prevention]

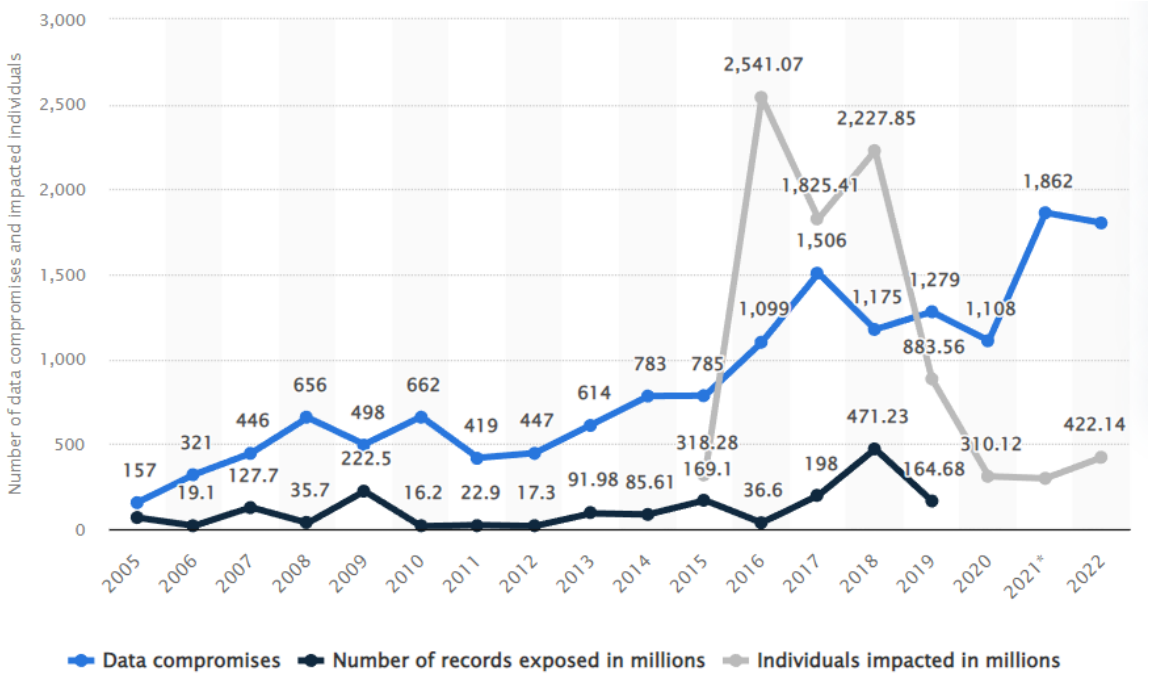

[deterrence and detection]

Cybersecurity

- *"**Prevention** of damage to, **protection** of, and **restoration** of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its **availability**, **integrity**, **authentication**, **confidentiality**, and **nonrepudiation**"* — NIST
- *"Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks"* — IBM

Why Do We Care [in Manufacturing]?

- Growing frequency of cyberattacks
  - Ransomware, phishing, theft, …
  - Can be disruptive
- Damages can be
  - Operational → Financial
  - Reputational
  - Business secrets leak
    (sensing/cutting data, employee information, trade secrets, etc.)



https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed

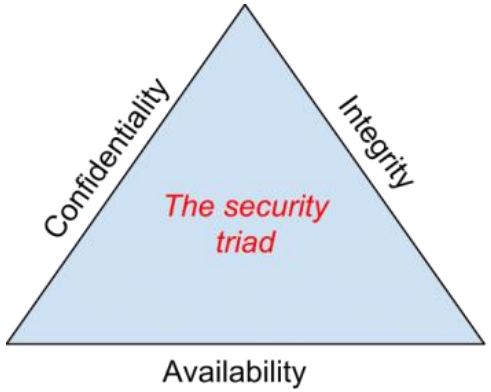
Attacks on Businesses

- Small Scale
  - Data/Identity theft
  - Extortion
  - Loss of personal data
  - Unauthorized access
- Large Scale
  - Compromising critical infrastructure
  - Significant public health/economic effects

Basics of Cybersecurity

What is the CIA Triad?

- The CIA triad: Confidentiality, Integrity, and Availability
  - A commonly used model in cybersecurity that helps organizations make sure they handle data safely when they store, send, or use it [4]
- Ensuring CIA allows companies to enhance their security



This is a reoccurring component, and we will connect back to this frequently throughout the course

Confidentiality

- To prevent unauthorized access or reading of data, it is important to ensure that only authorized parties can access data
- Encryption [using a secret known only to authorized parties] is a common mechanism to protect confidentiality
- Eg: passwords control access to user accounts

https://www.haascnc.com/service/troubleshooting-and-how-to/how-to/software-available-for-download-from-haas-portal.html

Integrity

- To keep information and systems safe from unauthorized changes. The integrity measures make sure that the data is accurate and complete, which provides assurance that it hasn't been tampered wit or altered without permission.
- Eg: machining data should be verified and checked for tampering

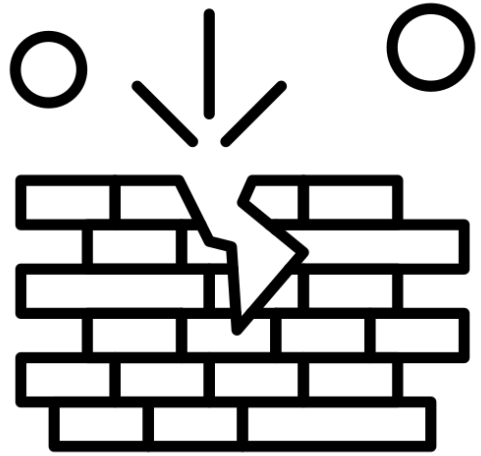
Attacker may intercept
and tamper data

Availability

- Data and systems should be available when authorized parties need them
- Attackers may attempt to deny services to authorized users – a denial-of-service (DoS) attack
- Eg: CNC machines should always be available on the network

Vulnerability

- A **weakness** or **flaw** in software, hardware, users, or any system that can be exploited by attackers to gain unauthorized access, cause damage/DoS, or steal information.
  - Software bugs
  - Misconfigurations
  - Human errors



https://thenounproject.com/icon/vulnerability-3596995/

Threat

- Any **potential danger** or **harmful event** that could exploit a vulnerability to compromise the security of a system.
  - Hackers
  - State-funded actors
  - Insider threats – former employees

https://thenounproject.com/icon/hacker-4993730/

Risk

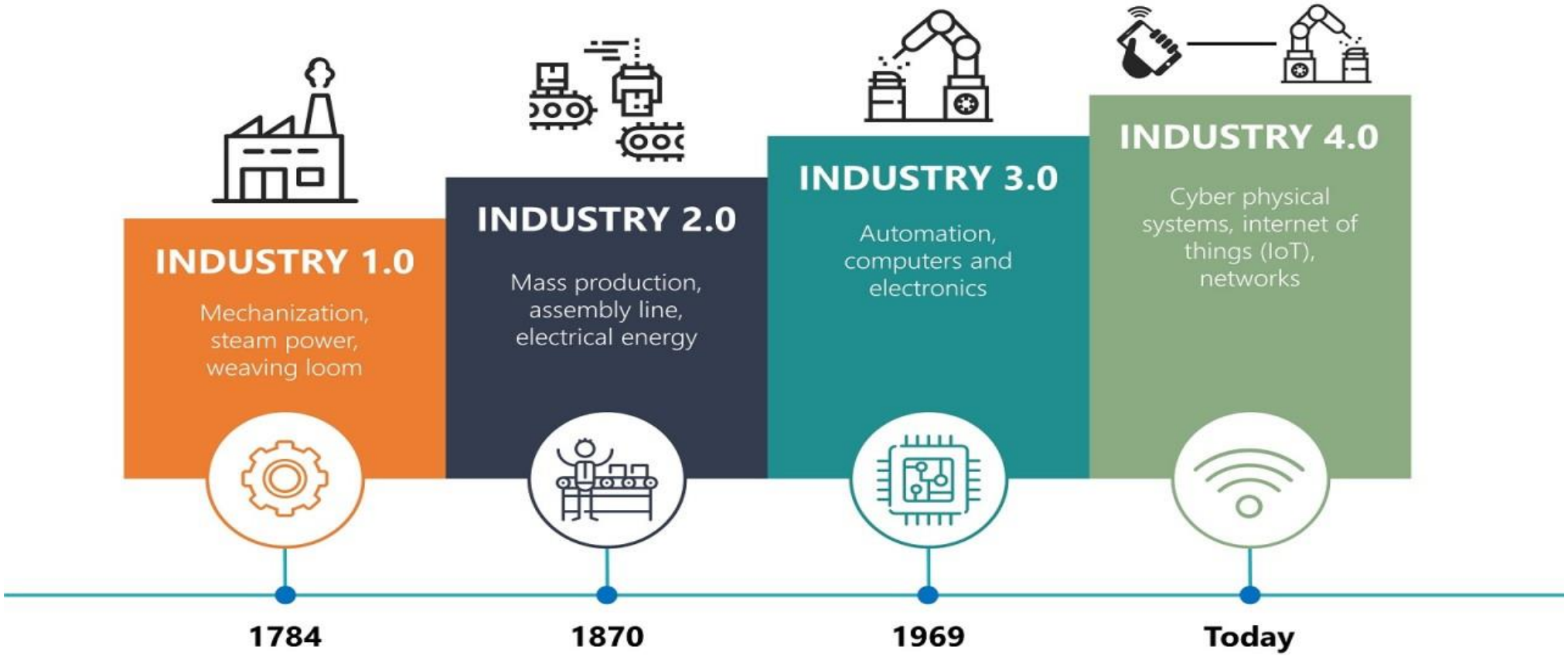
- The **probability that a threat will exploit a vulnerability**, causing harm or loss to a system or organization.
- Risk is usually calculated as a combination of the likelihood of an attack and the potential impact of that attack.

https://thenounproject.com/icon/risk-3404674/

Motivations Behind Cyber-Attacks

- Any ***additional*** motivations of an attacker?
- Motivations can vary and often fall into four main categories: **money, ideology, coercion, ego**
  - Attackers seek financial gain through money theft, data theft, or business disruption
  - Politically motivated attackers seek attention for their causes and use cyberattacks as a form of hacktivism
  - Cybersecurity experts, who are otherwise benign, may get coerced or extorted into becoming hackers
  - Personally motivated attackers, such as disgruntled employees, seek retribution or a chance to disrupt a company's system

Smart Manufacturing and Cybersecurity



[5

https://media.licdn.com/dms/image/C4D12AQF74RRejHQ3nQ/article-cover_image-shrink_720_1280/0/1565435172239?e=2147483647&v=beta&t=-TiisTEPdxI91auQODmoi0-Y06WJVEzJWDHxaRv-UGI

Industry 4.0

- Uses advanced technologies like artificial intelligence, Internet of Things (IoT), and robotics to automate manufacturing
- Involves smart (and potentially) wireless devices
  - Intelligent IoT devices may use artificial intelligence (AI)
  - They may use Wi-Fi or Bluetooth for connectivity

Automated drilling

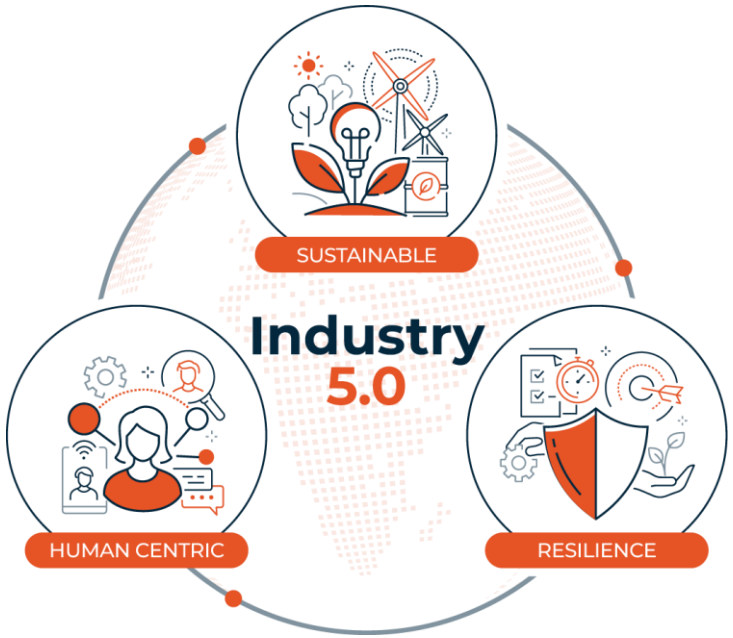
- Industry 4.0 would connect different parts of the manufacturing process, from suppliers to customers, through a network of intelligent devices; connecting physical world to digital world

Manufacturing Cyber Threats: Today

- Vulnerabilities identified by *American Machinist*
  - Unsecured CNC machines and ransomware
  - Poor password management
  - Lack of commitment to cybersecurity (cybersecurity training)
- CyberX risk analysis of smart machining networks worldwide
  - 62% have outdated Windows OS
  - 64% have unencrypted passwords
  - 54% have devices that are remotely accessible
- Manufacturing industry fell victim to 33% of all data theft attacks!

From Industry 4.0 to Industry 5.0

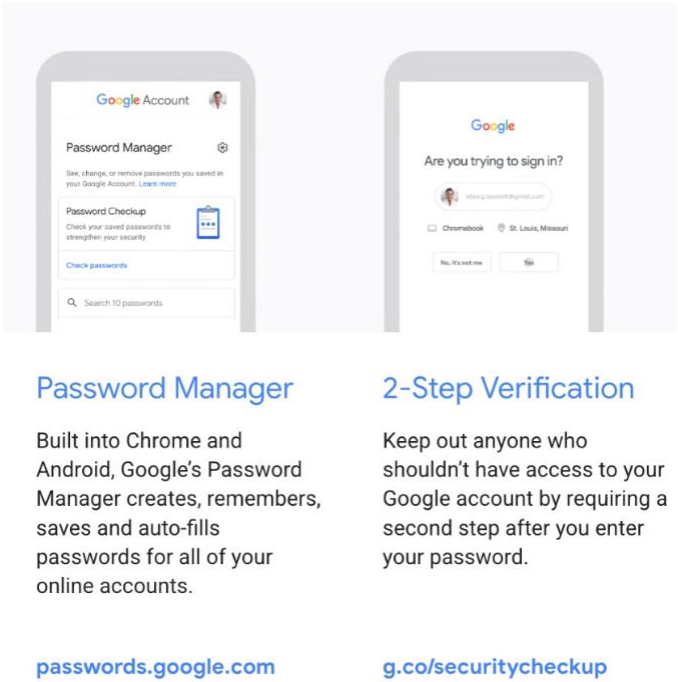
- Industry 4.0 – today
  - Industrial IoT
  - AI and Automation – intimidating for workers
- Industry 5.0 – 2030 and beyond
  - Focus manpower back to factories
    - Human working on site and from remote (AR/VR/XR)
  - Distributed production
  - Intelligent supply chain
  - Cyber safe data transmission, storage, and analysis
  - Trustworthy autonomy



Common Types of Cyber Attacks

Password Attacks

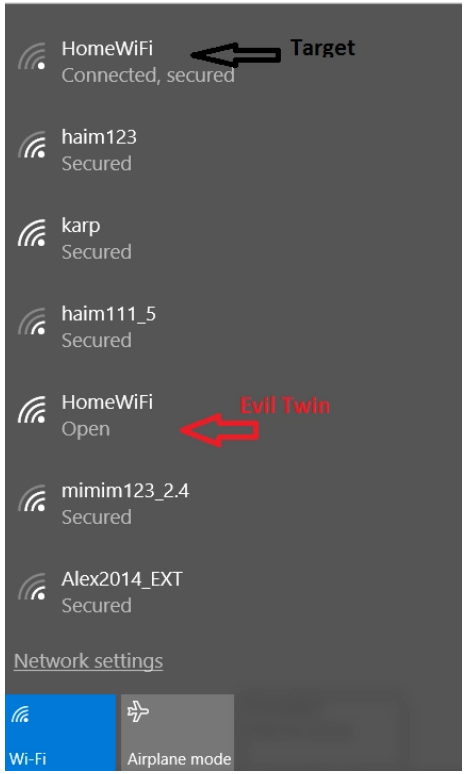
- Passwords are a form of **access control**
  - Personal computers, Wi-Fi networks, control systems
- Password attacks are very common in manufacturing
  - Post-it notes; looking over your shoulder!
  - Brute force attacks
  - Social-engineering / Phishing
- Best practices of defense
  - Don’t reveal passwords in the open!
  - Use long phrases that are easy to remember
  - Multi-factor authentication



Password protections suggestions by Google

Wi-Fi Attacks

- Wi-Fi is used for both personal and work-related tasks
  - Wirelessly connect manufacturing resources
- Security attacks on Wi-Fi
  - Password attacks
  - Fake Wi-Fi networks
- Best practices
  - Verify Wi-Fi network names
  - Strong passwords



Malware

- **MAL**icious soft**WARE** used to exploit a vulnerability and gain unauthorized access.
- Often spreads through email attachments, malicious ads, fake software installations, phishing, and infected devices (e.g., USB)
- Types of malware
  - Ransomware
  - Spyware
  - Adware
  - Virus, and many more!

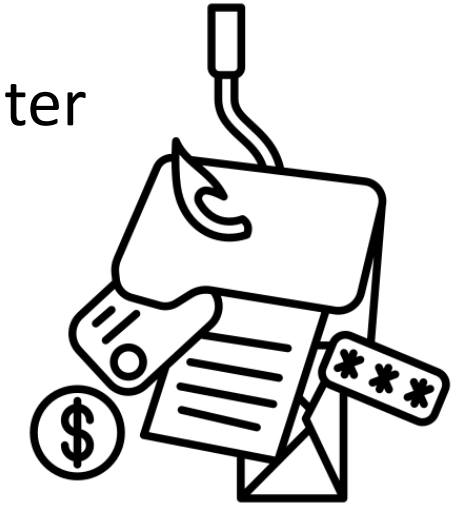
https://www.bbc.co.uk/bitesize/topics/zv63d2p/articles/zcmbgk7

Ransomware

- A type of malware that encrypts files stored on the victim's system — a common attack affecting the manufacturing industry
- The malware then demands that the victim company pays a ransom in return for the decryption key.
- Example best practices to avoid malware and Ransomware
  - Avoid unknown links and websites
  - Never connect unauthorized USB devices
- How to respond?
  - Leave the infected computer and contact IT

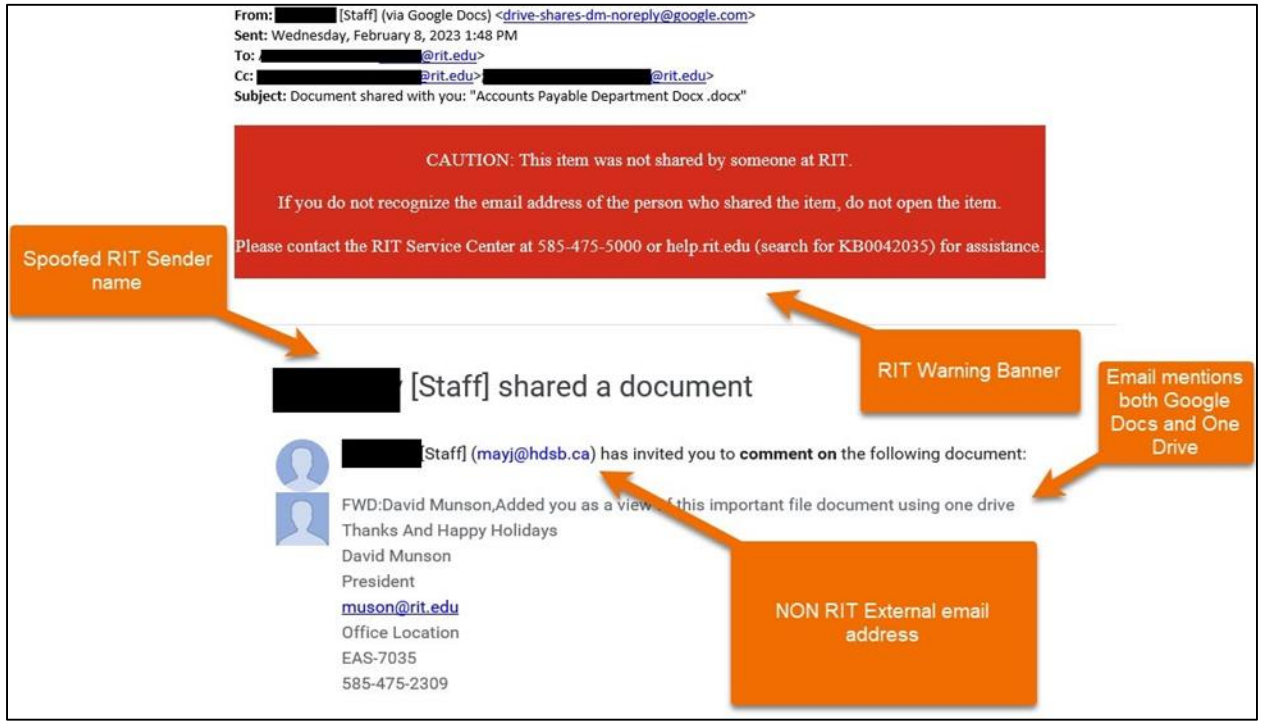
Phishing

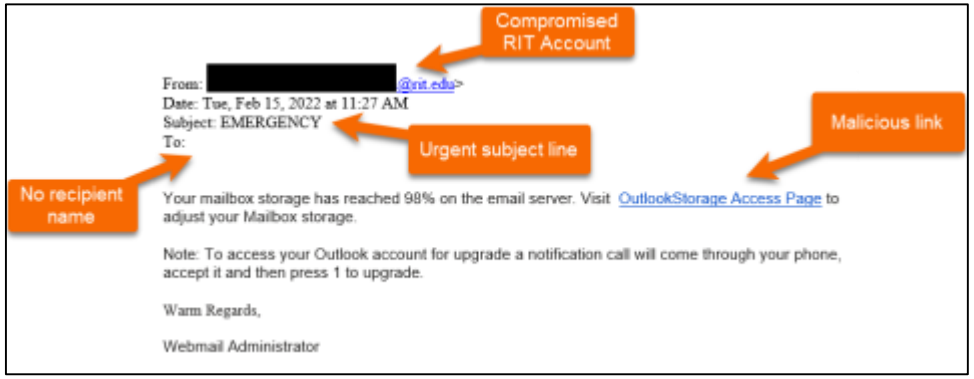
- A type of cyber-attack where an attacker attempts to trick people into revealing sensitive information such as login credentials, credit card numbers, or personal details
  - Eg: a deceptive email or message that appears to be from a trustworthy source, exploiting your emotions and your willingness to trust and believe
  - Insider threats – beware of former employees!
  - Contains links to malicious websites that can infect your computer
- Number 1 concern in [manufacturing] industry!



https://thenounproject.com/icon/phishing-4284052/

Phishing Exercise





Examples of phishing emails

Phishing Exercise – What Did We Learn?

Some of the ways to identify a phishing email

- Carefully read the sender email address
- Notice if the email prompts urgency, or some emotion
- Check for suspicious links/attachments
- Check if it requests any personal information
  - Passwords, SSN, driver's license, etc.

Cloud Computing and Security

- Accessing computing resources online (as opposed to local)
  - Reduces infrastructure costs
  - Improves setup times
- Cloud Manufacturing – online access to manufacturing resources
- Security challenges in cloud manufacturing
  - Insecure configurations
  - Confidentiality
  - Lack of cloud security training

- Example best practices to secure cloud accounts
  - Use strong passwords!

Protecting Sensitive Information

- In manufacturing, many forms of data can be considered sensitive
  - Personal – addresses, phone numbers, health data
  - Business – intellectual property, trade secrets, sensing data
- These can be used maliciously to gain unfair advantage
  - Data smuggling – selling personal data
  - Corporate espionage – revealing trade secrets
- Best practices
  - Never reveal personal/business data in unsecure channels
  - Use strong passwords for files containing sensitive data

Existing Standards for Secure Smart Manufacturing

CMMC and NIST

- Cybersecurity Maturity Model Certification (CMMC)
  - Required for U.S. Dept. of Defense contracts
  - Mandates regular government-led assessments
- National Institute of Standards and Technology (NIST)
  - Specifies best practices and requirements for protecting controlled unclassified information

Critical NIST Requirements

- Specific requirements from NIST Special Publication 800-171 are critical to mitigating the most common attacks and vulnerabilities in smart manufacturing industry

Vulnerability	NIST Requirement Family
Poor password management	Access Control, Identification and Authentication
Unsecured CNC machines	Configuration Management and Maintenance
Unsecured internal devices (flash drives, etc.)	
Lack of commitment to cybersecurity	Awareness and Training

- In the following modules, we will look at each of these in detail.

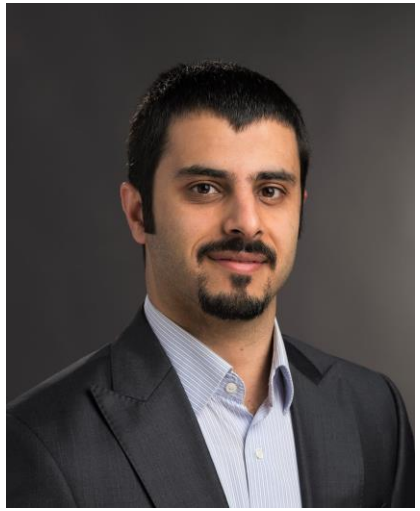
https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Resources

[1] NIST Security Definition
[2] NIST Cybersecurity Definition
[3] What is Cybersecurity: Cisco
[4] CIA Triad
[5] NIST: Industry 4.0 and Cybersecurity
[6] Threats, Vulnerabilities, and Risks
[7] NIST Malware Definition
[8] Report: Importance of Cybersecurity in Smart Machining and Industry 4.0
[9] IBM: X-Force Threat Intelligence Index 2021
[10] NIST Phishing Definition
[11] IBM: Cyber-Attacks
[12] Smart Manufacturing Security Challenges
[13] Data Privacy

Thank you!

Contact: hanif.rahbari@rit.edu
Wireless and IoT Privacy (WISP) Lab (rit.edu/wisplab)
ESL Global Cybersecurity Institute
Rochester Institute of Technology



Hanif Rahbari

Sid Dongre