Cybersecurity Essentials for Smart Manufacturing Professionals

Module 4: Awareness, Training and Non-technical Elements

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 awareness and training
- Identify common security risks and best practices
- Understand the role of management in promoting a secure environment
- Understand the impact of human error on security

Importance of Cybersecurity Education and Training

Awareness and Training

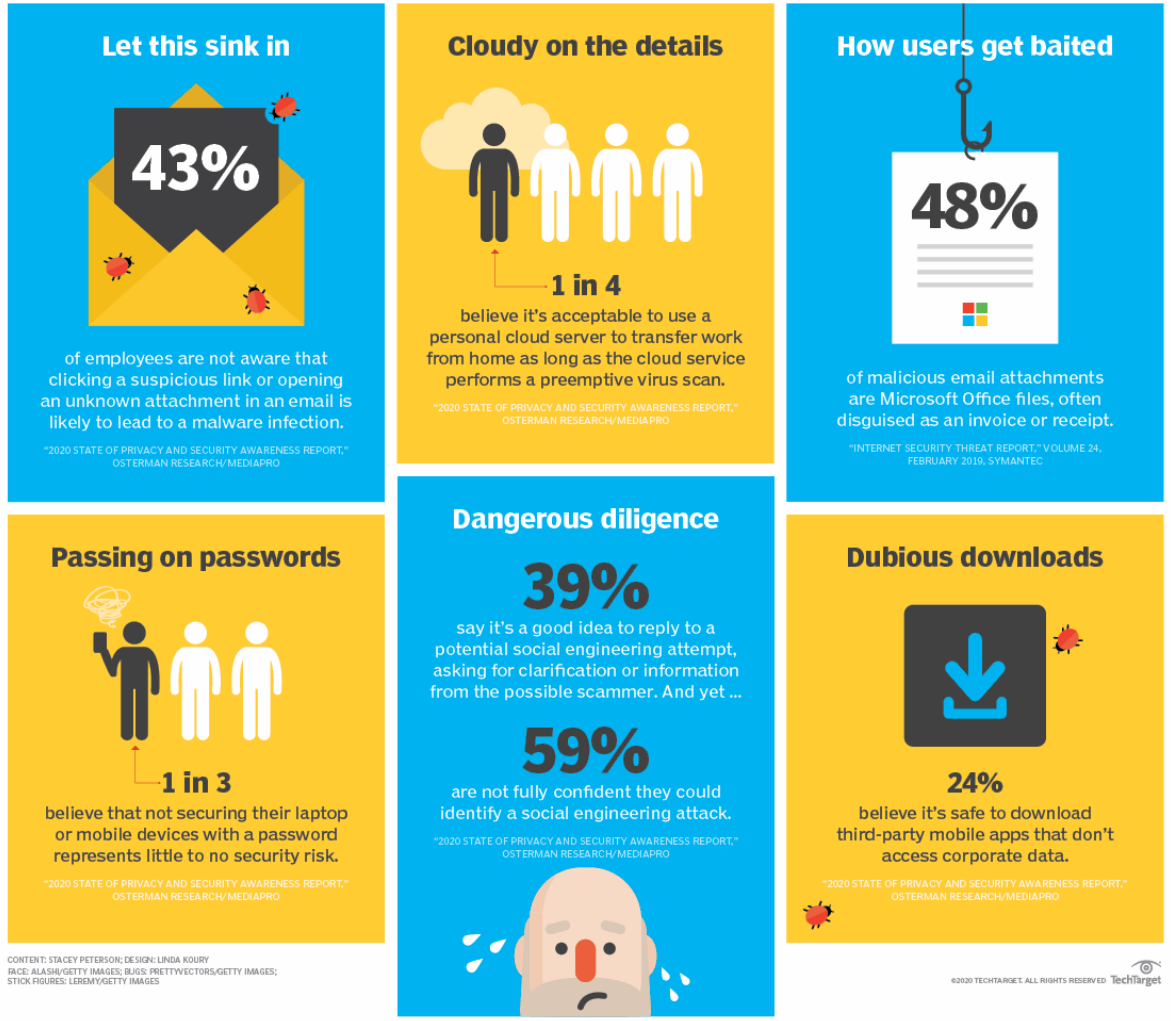
- Why do you think we need cybersecurity training?

Awareness and Training

- Awareness – spread awareness about the existence of threats
  - Awareness campaigns – emails, memos, phone calls, short meetings
  - Goal – being able to identify security threats
- Training – learning security best practices
  - Training Schools – seminars, lectures, short courses
  - Goal – learn to properly respond to security threats
    - Ensure productivity and business continuity

Impact and Importance

- Lack of can awareness lead to:
  - Password leaks – using sticky notes
  - Phishing attacks – emails/text messages not properly analyzed
  - Ransomware – attachments / USB drives not scanned
  - Insider attacks – user accounts not properly decommissioned



Prioritizing Awareness and Training

- Integrating Cybersecurity Awareness in on-boarding
  - First few weeks at a workplace
  - Quickly gain knowledge on common threats
  - Familiarize with security policies
- Cybersecurity Training should be a periodic process
  - Provided at least once a year
  - Spread awareness about new attacks
  - Keep up to date with best practices

Security Risks and Best Practices

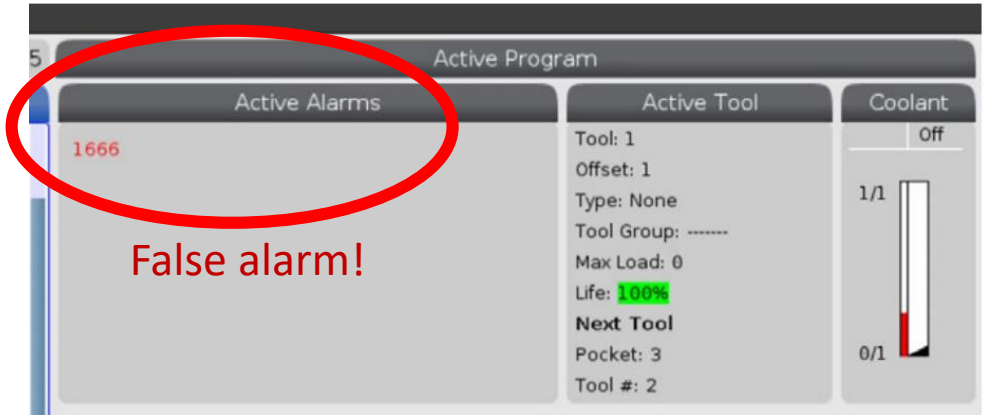
Minimizing Security Risks

- Security Risk – probability that a threat will exploit a vulnerability
  - Lack of awareness ⇒ higher probability of successful attack
  - Lack of Training ⇒ more loss to company
- Proper Awareness and Training minimizes risk
  - Awareness – quickly detect attacks ⇒ reduce attack success rate
  - Training – quickly respond to attacks ⇒ reduce attack effectiveness

Latest Threats in Machining 4.0

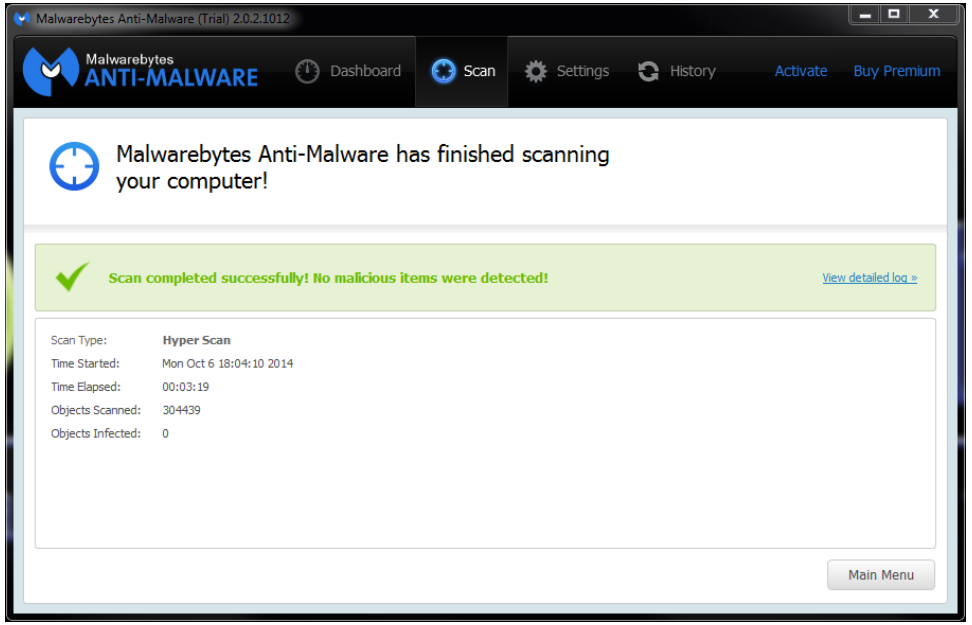
- Phishing attacks
  - Emails/phone calls/text messages
- Data theft and privacy breaches
  - User account compromise
  - Exposure of sensitive data
- Hijacking/device compromise
  - Tampering job settings
- Denial-of-service attacks
  - Triggering alarms
  - Limiting internet connectivity

Tampering due to attack



Awareness – Detecting Threats

- Phishing Attacks
  - Analyzing emails/text messages
- Data theft and privacy breaches
  - Scanning unknown/unvetted USB drives
- Hijacking/device compromise
  - Regularly scan device for malware
  - Check machine configuration before activation



Training – Best Practices for Response

- How to best respond if you're a victim of an attack?
- Phishing attacks
  - Notify IT/Security departments of user account compromise
- Data theft and privacy breaches
  - Hand over malicious USB drives to IT/Security
- Hijacked CNC Machine – usually due to malware
  1. Immediately deactivate machine
  2. Attempt to retrieve sensitive data – contact IT/Security
  3. Reset machine to factory defaults – remove all traces of malware

Non-technical Elements Impacting Security

Impact of Human Error

- Human error is a major source of threats
  - Benign mistakes can lead to unintended leakage of confidential data or improper configuration of security mechanisms
  - Lack of oversight can cause misconfigurations to be left unchecked
- Examples of human error
  - Typing password in username field – password is then recorded in logs and becomes visible and readable by others
  - Emailing confidential data to all employees instead of select recipients
  - Forgetting to disable Administrator account on a workstation

The Role of Management

- Perform cybersecurity gap analysis
  - Analyze and discover vulnerabilities in company
- Prioritize security awareness and training
  - Create tasks for subordinates to regularly attend awareness sessions
- Design tasks with cybersecurity in mind
  - Sub-tasks include cybersecurity checks that conform with best practices
- Design Security Policies and Procedures

Security Policies and Procedures

- Importance – policies and procedures:
  - Help formalize cybersecurity best practices
  - Describe how to securely use machining tools, perform and deliver tasks, and maintain records
  - Describe how to best respond to security threats
- Policies and procedures are essential to reduce security risk
  - Policies, when properly implemented, reduce the likelihood of an attack
  - Properly following incident response procedures help reduce the disastrous impact of an ongoing attack

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