NC STATE UNIVERSITY Industry Expansion Solutions

North Carolina State University Industry Expansion Solutions Presents: How Much Would a Cyber Breach Cost Your Business?

10/10/24

Goal of This Training Session?

This training is designed to increase awareness of the rising costs of a cyber breach to small businesses

The training will accomplish the following:

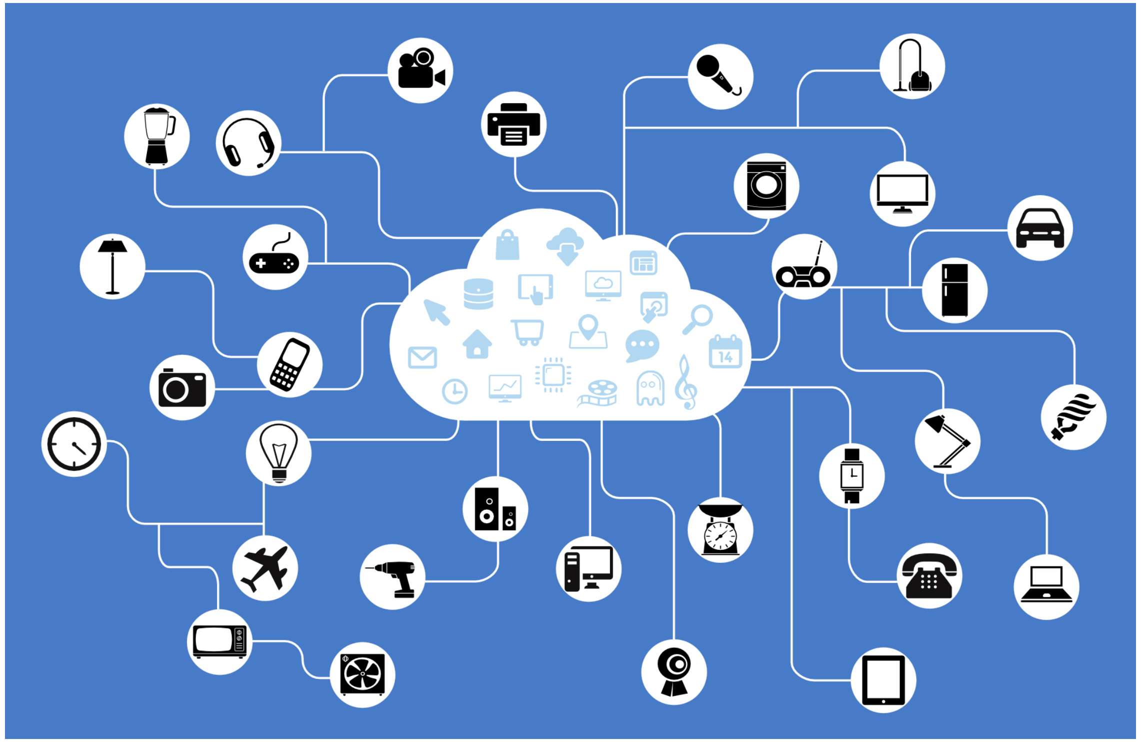
- Define threats and industry trends
- Expose the cost of being breached
- Explore the value of cyber security planning & training
- Tips for creating a culture of cyber security
- Explain methods of securing a business

Agenda

- Identifying the threat
- Cyber security trends
- **Cost of a breach in 2024**
- Building a cyber culture
- Kickstart a security program
- Resources

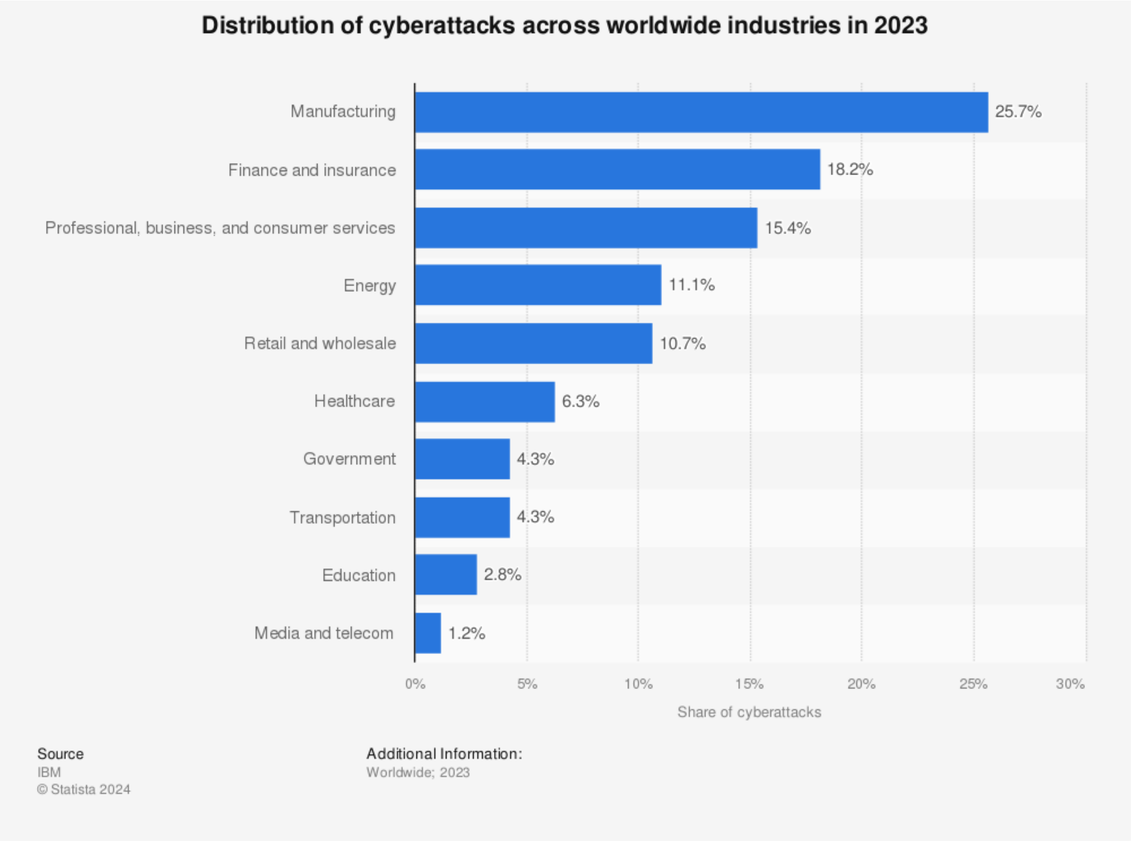
Part 1: Threat Overview

What Makes Manufacturing Such an Appealing Target?



- Low tolerance for downtime
- Servers with sensitive data
- Connections to up and downstream partners, supplier, retailers
- Lack of dedicated IT/cyber resources
- Global supply chains with increased risk of cross contamination
- Legacy IT systems/IoT devices

Top Threats to Manufacturing Industry



Distribution of cyberattacks across worldwide industries in 2023

Source
IBM
© Statista 2024

Additional Information:
Worldwide; 2023

Manufacturing was the Top Targeted Business in 2023

- Social Engineering
  - *Leading method of attack*
- Embedded Sensors, Automation & Robotics
  - *Creating new pathways for attackers*
  - *Older devices coming online*
- AI tools
  - *Enabling more sophisticated attacks*

Who Wants My Data?

- Assume **you *ARE* a target**, not the other way around!
- If you assumed a home was not valuable enough to break into (and decided not to invest in locks and security systems) are you increasing or decreasing the chance of a break in?
- The correct starting point for any cyber security program: **trust no one, verify everyone!**

Social Engineering- The People Problem

70% of data breaches involved the human element in 2023

1 in 3 data breaches involves phishing

WHY??

- Only 1 in 9 businesses (11%) provided a cybersecurity awareness program to non-cyber employees in 2020

2023/2024 Trends

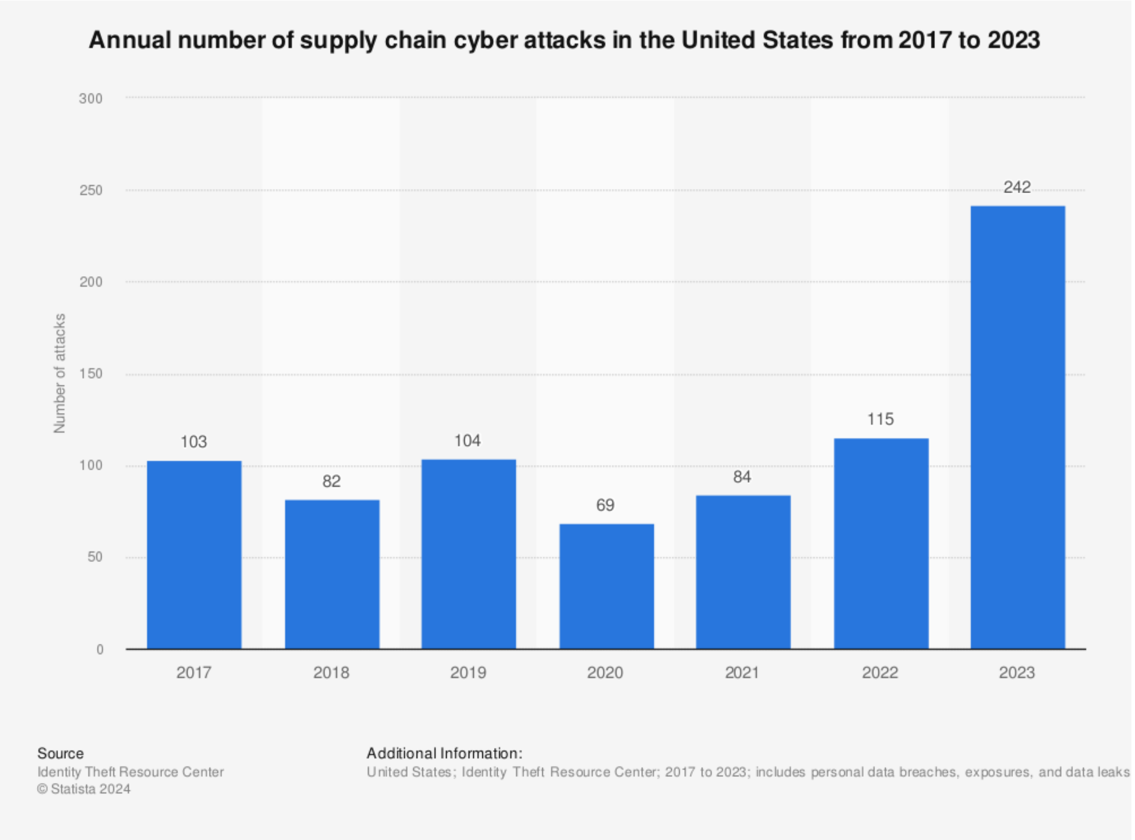
data breaches hit an all-time high in 2023 (Source: MIT)

According to 2023 IBM survey, more than 80% of data breaches involved data stored in the cloud

The global average cost of a data breach increased 10% over the previous year (Verizon Report)

Cybercriminals Search for Supply Chain Weaknesses

- Between 2022 and 2023, the number of supply chain attacks in the United States doubled
- These cyberattacks impacted 2,769 entities in the market
- Supply chain attacks create added pressure to comply with ransomware demands



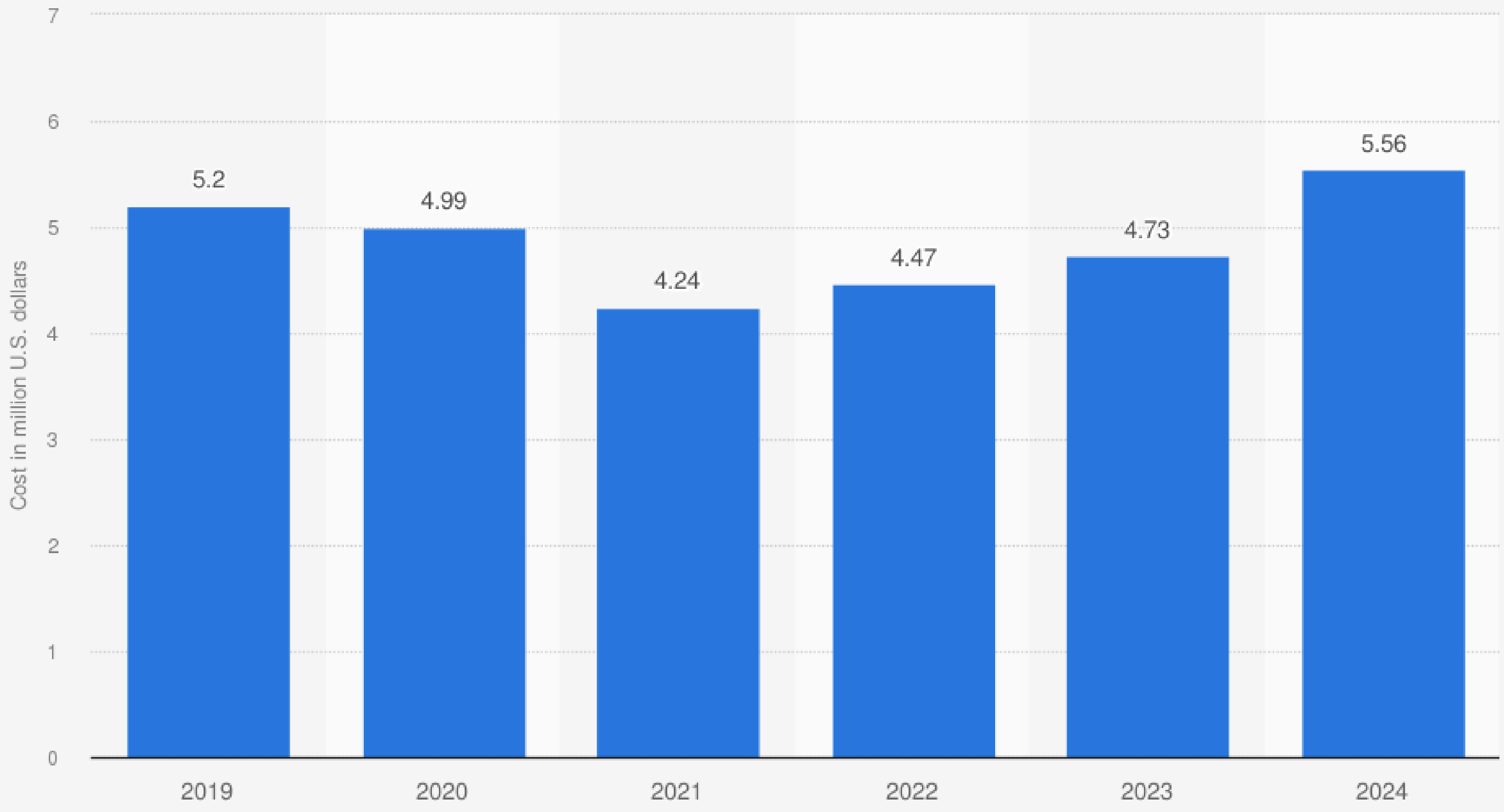
Annual number of supply chain cyber attacks in the United States from 2017 to 2023

Source
Identity Theft Resource Center
© Statista 2024

Additional Information:
United States; Identity Theft Resource Center; 2017 to 2023; includes personal data breaches, exposures, and data leaks

Part 2: The Cost of a Cyber Breach

Average total cost of a data breach in industrial sector worldwide from 2019 to 2024 (in million U.S. dollars)



Sources
IBM; Ponemon Institute
© Statista 2024

Additional Information:
Worldwide; Ponemon Institute; 2019 to 2024

Costly Mistakes

- The median cost of a manufacturing ransomware attack responded to by Arctic Wolf Incident Response is now $500,000 USD
- Average total cost of a data breach in the industrial sector was $5.56 million according to IBM 2024 Cost of a Data Breach Report
- Length of downtime is directly connected to total cost (a 2023 global survey by ABB found that one hour of downtime can cost up to $120,000 for manufacturers)

Catastrophic Cyber Incidents: Clorox

- Attack type: Unknown, but has indications of ransomware
- Location: North America
- Year: 2023
- Cost: $356 million USD
- Description: Most likely ransomware, disrupted purchasing systems, reduced output, 20% decline in sales, sharp stock price drop, $25 million spent on remediation

Catastrophic Cyber Incidents: Bridgestone Americas

- Attack type: Ransomware
- Location: North America
- Year: 2022
- Cost: Unknown
- Description: Ransomware, disrupted all North and South American manufacturing operations. Both employee and customer data compromised including SSNs, names, banking and other PII

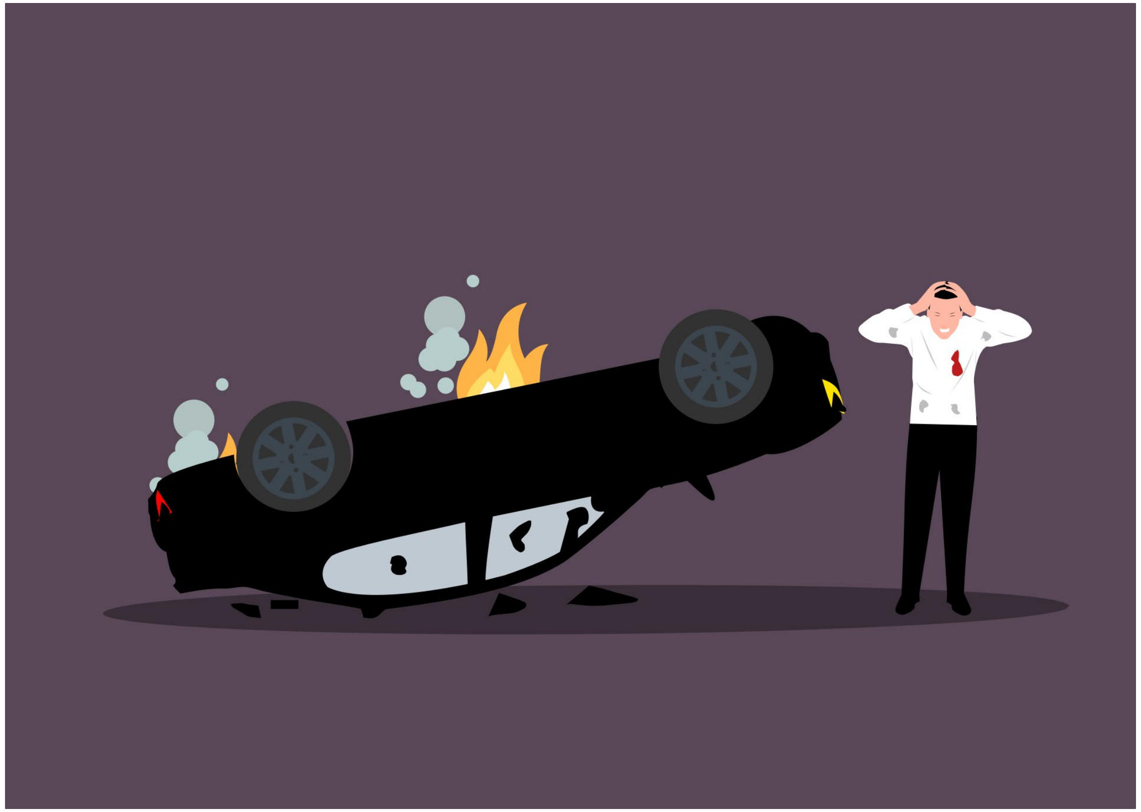
Catastrophic Cyber Incidents: Parker Hannifin

- Attack type: Ransomware
- Location: North America
- Year: 2022
- Cost: Unknown
- Description: Ransomware, attackers compromised the data of current & former employees. Compromised data included names, DOB, SSNs, addresses, passport numbers, and financial account information

Hidden Costs of Cyber Breaches

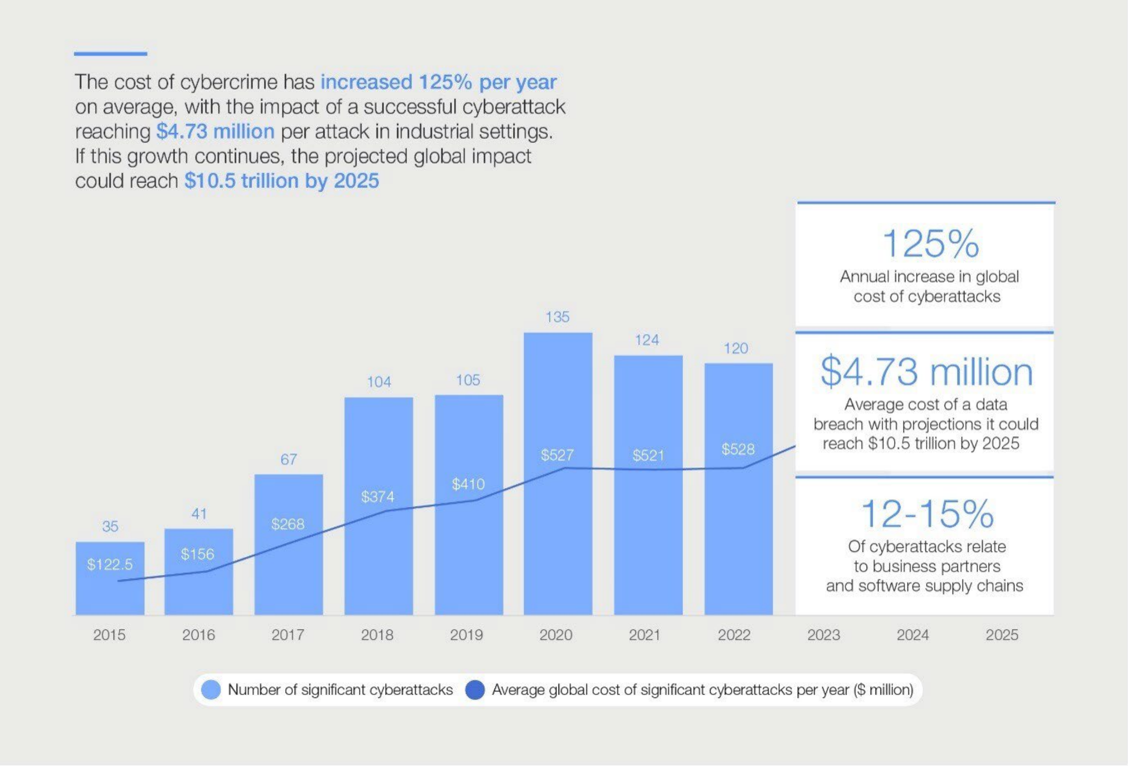
- Legal and regulatory fines
- Customer trust
- Partner/supply chain reputation
- Employee downtime
- Recovery and remediation costs

What Makes Cyber So Tough to Nail Down?



- There is no “cybersecurity gold standard” for manufacturers across different sectors, states, sizes, etc.
- Most manufacturers don’t have a legal or regulatory requirement
- Vendors rarely build cyber solutions for manufacturing industry
- Technology advances (IoT, digital twins, AI, robotics, cloud computing) have outpaced cybersecurity investment

Getting Worse Before it Gets Better



The cost of cybercrime has increased 125% per year on average, with the impact of a successful cyberattack reaching $4.73 million per attack in industrial settings. If this growth continues, the projected global impact could reach $10.5 trillion by 2025

125% Annual increase in global cost of cyberattacks

$4.73 million Average cost of a data breach with projections it could reach $10.5 trillion by 2025

12-15% Of cyberattacks relate to business partners and software supply chains

35
$122.5
41
$156
67
$268
104
$374
105
$410
135
$527
124
$521
120
$528
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
● Number of significant cyberattacks
● Average global cost of significant cyberattacks per year ($ million)

- The data is clear- the number of breaches is rising year over year, and the cost is getting higher every year
- Until manufacturers take note- and invest in cybersecurity- the problem will almost certainly get worse before it gets better
- Without a strong government incentive, most businesses will continue to make the minimum investment in cyber

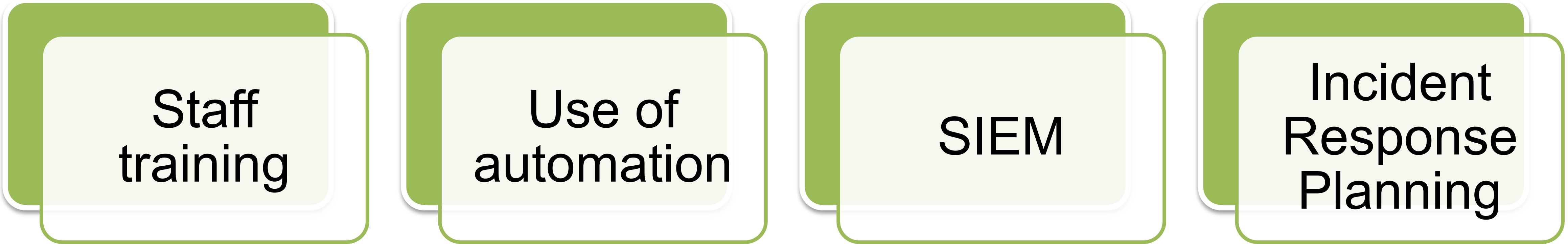
What Makes a Cyber Breach Worse (More Costly)?

Complexity of the system and security

Lack of staff

Number of external connections

What Makes a Cyber Breach Less Impactful (Less Costly)?



Staff training

Use of automation

SIEM

Incident Response Planning

Part 3: Building a Cyber Culture

Picture this Scenario

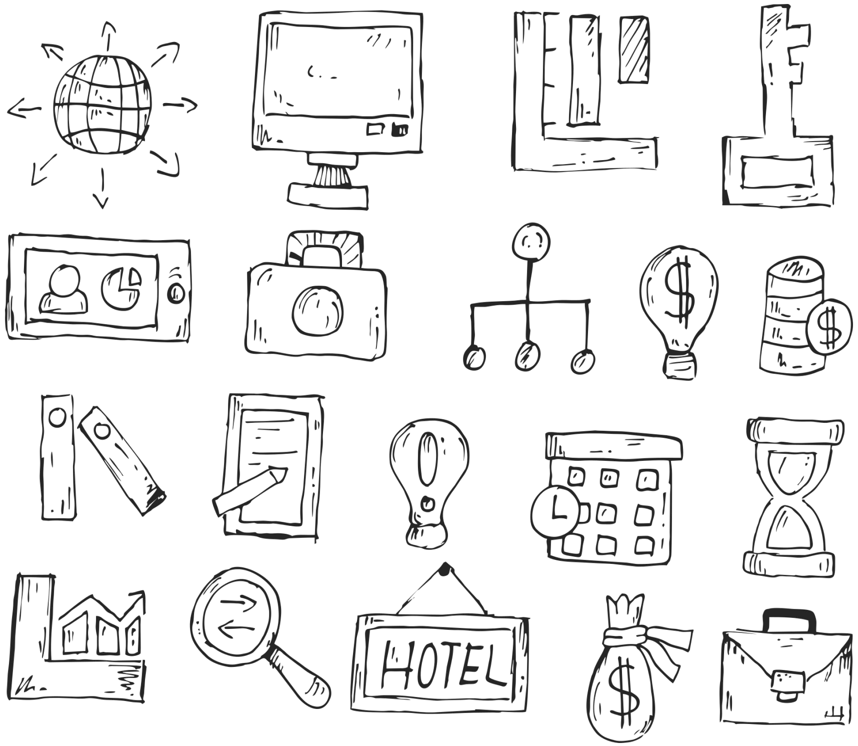
- A person comes to the front door of your office/building
- They have tools and say they are here to work on the electrical inside the building
- **How does this scene play out?**

The People-centric Approach to Security

- Most breaches are a result of human error, leading to the assumption people can only be a weak link
- The assumption is wrong! People can be trained and supported in becoming cybersecurity strengths of an organization
- When we refuse to educate and encourage our employees to be a part of the fight against hackers, we signal that it is not their role or responsibility to protect the organization

Treating Cyber Like Other Business Threats

- We invest in the physical security of our business
- We invest in the employees with benefits
- We invest in advertising to gain more business
- We invest in utilities to keep the lights on
- We invest in insurance to protect the business
- **WHY DON'T WE INVEST IN CYBER?**



Part 3: Kickstarting a Cyber Program

Benefits of Investing in Cyber

- Reduce chances of an expensive breach
- Improve customer confidence
- Differentiate from less secure competitors
- Lessen impact of breaches
- Small upfront investment vs larger expense if breached

Building a Cyber Program from Scratch

- Understand goals and risks of the organization
- Identify key systems and data
- Create and implement controls to protect assets
- Develop risk mitigation practices
- Create incident response plan
- Test controls and practices via simulation and training

Building a Cyber Program from Scratch (continued)

- Continuous monitoring to detect attacks
- Regular employee training and discussion of cyber risk and response
- Fine grain control of third-party vendors and software
- Senior leadership communicating regularly with IT/cyber staff

What are Security Controls?

Physical

Administrative

Technical

Operational

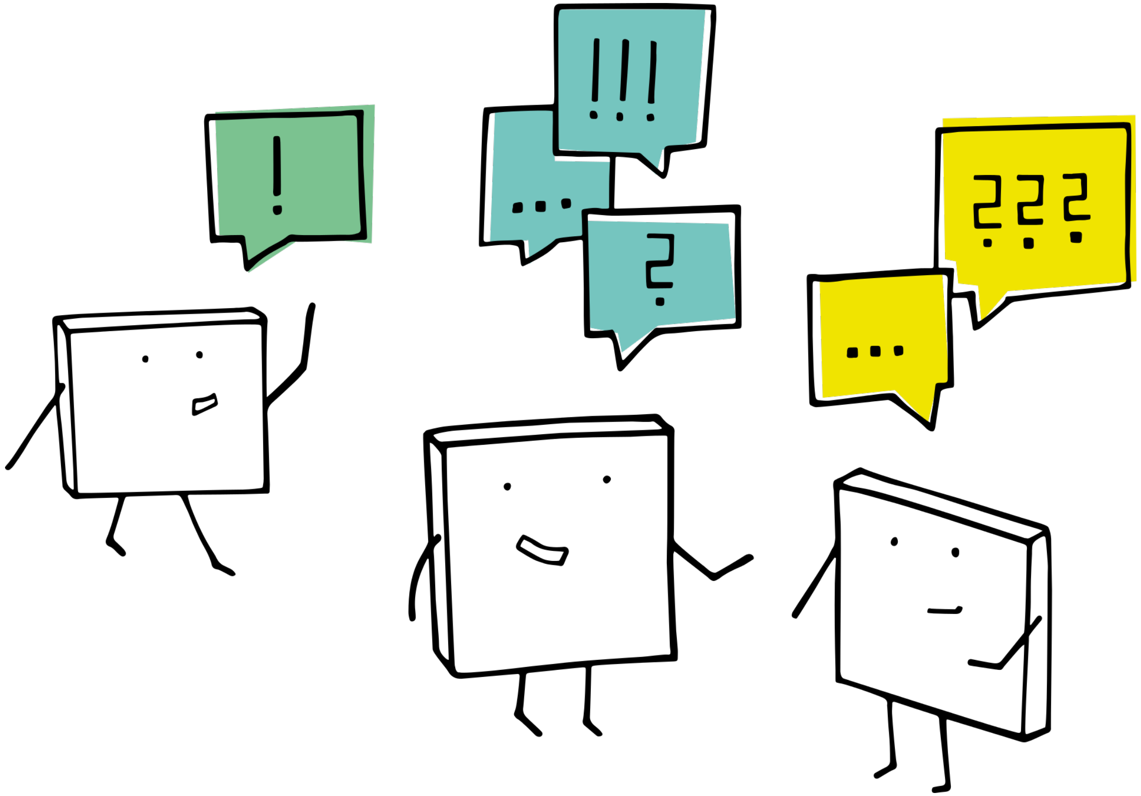
Basic Cyber Hygiene: 6 Top Tips

- People, process, technology
- Clear policies
- Multifactor authentication
- Security enclaves
- Patch software
- Backup & test

Cyber Training

- Humans are involved in the majority of cyber breaches
- Focus on our people MORE than systems
- Commit to cyber awareness training at time of hire, annually, as well as creating opportunities for discussion at regular intervals like monthly meetings

Q & A



- https://ies.ncsu.edu/cybersecurity/
  - Free training
    - CSET
    - Mission Possible Microlearning
    - Center for Development of Security Excellence
    - CISA Tabletop Guides
  - Online courses
  - Contact us today for a no cost consultation!

THANK YOU