Advanced Institute for Manufacturing

Cybersecurity Workshop For Manufacturers

Agenda

- Opening Remarks
- The Chain of Security
- The Who, Why, and What of Cyber Attacks
  - Who is attacking?
  - Why they attack
  - What they attack with

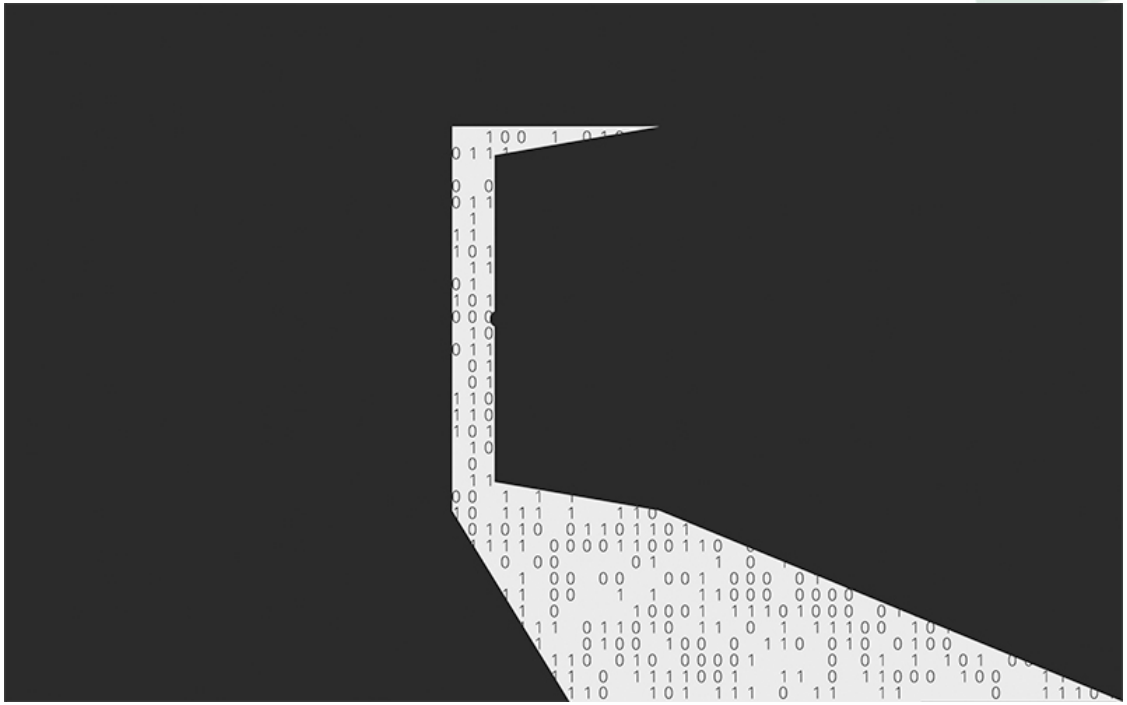
The Chain of Security

The different areas which comprise information security as a whole

- Physical
- Network
- Policy
- Training

The Chain of Security

- Physical: Can my information be accessed in the real world?

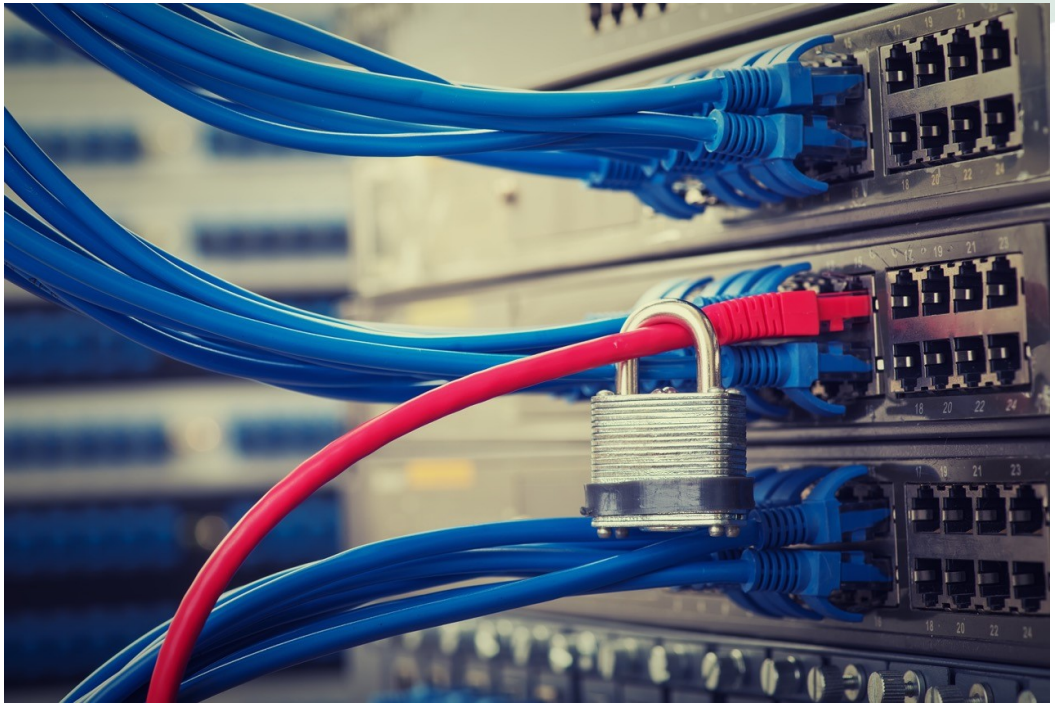


The Chain of Security

- Physical Security
  - Rarely associated with Cyber Security at all.
  - Determines how easy it is for attackers to physically access information or devices
  - Physical security devices include: Locks, doors, walls, fences, guards, security systems, etc.

The Chain of Security

- Network: Can my information be accessed by an outside computer?



The Chain of Security

- Network Security
  - What people traditionally think of when they think “Cyber security”
  - Protects information and devices on network
  - Network security devices include: Routers, firewalls, anti-virus programs, etc.

The Chain of Security

- Policy: Does my company have policies in place to keep my information safe?

The Chain of Security

- Policy Security
  - Rules set by management to determine how devices and information are handled.
  - Policies can determine how company handles usage of cell phones, thumb drives, password lengths, etc.
  - Implementation of policies help support other areas of security.

The Chain of Security

- Training: Are my employees properly trained to protect my information?

The Chain of Security

- Employee Training
  - Allows employees to safely and properly handle company devices and information.
  - Helps employees protect themselves and others from cyber security attacks.
  - The more knowledgeable a staff is, the more secure the company will be.

The Chain of Security

A chain is only as strong as its weakest link

Anatomy of An Attacker

- Considering the people who attempt to launch attacks against people and businesses

Three factors to consider:

Who is attacking
Why they attack
What they attack with

Who is attacking?

- Who causes the biggest threat to your information?
  - The “S.K.R.A.M.” score.
    - Skills
    - Knowledge
    - Resources
    - Access
    - Motivation
  - The higher an attacker’s “S.K.R.A.M.” score, the more likely they are accomplish their goal
  - Acronym acts as ranking system for attributes

Who is attacking?

- The “foreign hacker”
  - Security specialist from another country
  - Usually choose big, profitable targets
  - What everyone thinks of when they think of a cyber attack
  - High in skill and resources, but not usually a big threat to small/medium businesses if basic precautions are taken

Who is attacking?

- Corporate espionage
  - Attack committed within operating area
    - Competing business
    - Angry customers
    - Someone resolving a personal grudge
  - Trying to do business/employees/owners direct harm
  - High in motivation and knowledge of target
    - Considerably more dangerous than “Foreign hacker”

Who is attacking?

- Inside attack
  - Attacks committed by someone employed by the company
  - Disgruntled employees
  - Someone running a “parasite business” off company information or IP
  - Blackmail
  - Harm being caused by accident
- Far and away the most dangerous
  - Motivation is the attacker’s only real limit
  - Incredibly high access and knowledge
  - The most difficult to prevent.

Why They Attack

- Not all attackers have the same goals when committing an attack

The three “P”s

- Profit
- Politics
- Practice

Why They Attack

- Profit
  - Attacks committed in an attempt to make money
  - Identity theft, directly or through reselling of information
  - Intellectual property theft
  - Ransom Attacks
  - Main goal of most highly skilled attackers
  - Can also come from low-paid employees or those not being “paid what they’re worth”

Why They Attack

- Politics
  - Attacks committed by someone opposed to the business
  - Personal and ideological reasons
  - Goals can be vandalism, denial of service, theft of information for blackmail

Why They Attack

- Practice
  - Attacks made on small, weak targets by inexperienced attackers, or ones using the target as a “dry run”
  - Low skill and motivation, generally easy to defend against
  - Typically “prank” vandalism, denial of service or “Look and leave”
  - Can still be very damaging if left unchecked

What They Attack With

- Virtually all the software attackers use is free
  - Most can be run on very low-quality machines
- Techniques and information on committing attacks is easily accessible and free on the internet
- The barrier for entry into the hacking world is very low
  - Limited only by a person's motivation
- Specialized tools make once complex attacks extremely simple

In Conclusion

- The “Chain of Security”: Physical, Network, Policy, Training
- The entire chain of security must be strong
- Not All Attackers Have The Same Motivations
  - Consider Who, Why, What

For More Information

- Discussion Panel (10:45 AM)
- NIST 800-171 Workshop (11:35 AM)

Thank you!