About the presenter:
Daniel Paillet, CISSP, CEH

- Lead Cyber Security Architect at Schneider Electric, Partner Business

- Bachelors and Masters Degrees from San Francisco State University

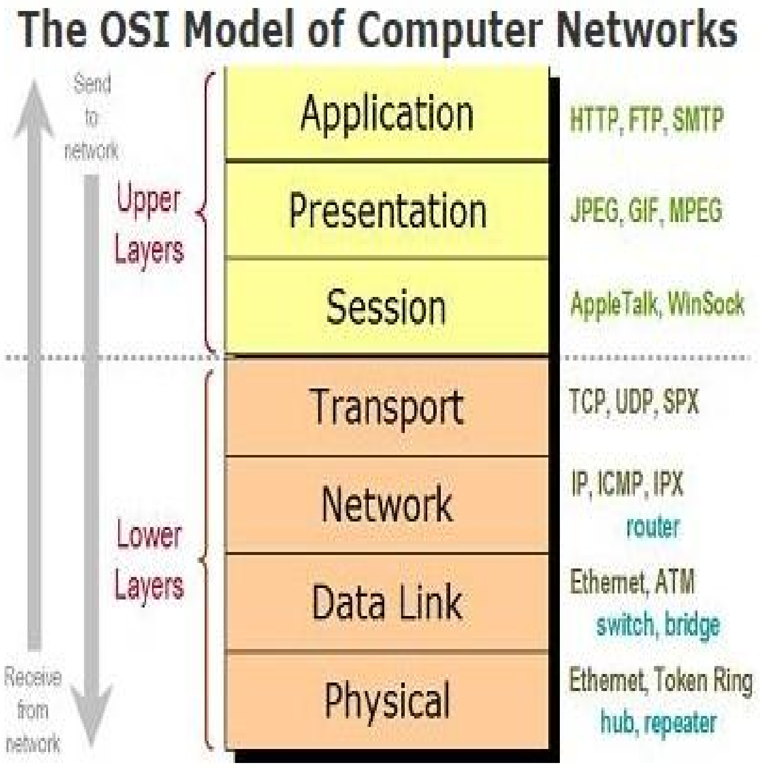
- Over 15 years experience in IT security, working in Point-of-Sale, Banking, Retail and Operational Technology

- Worked with US ARMY in Global deployment of HBSS

- Worked with US ANG in IDPS Installation and Standardization Project for all of CONUS

- CISSP, CEH and other agnostic and vendor certifications

- Current role architecting to improve and develop secure offerings within Schneider Electric



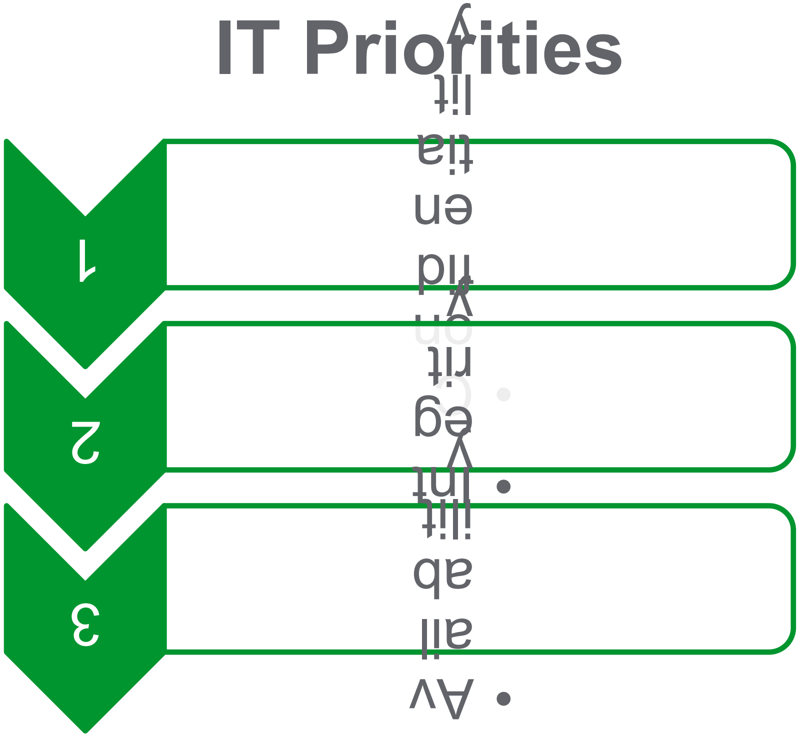
Defense in Depth and Breadth

Topics for this session

- IT vs Operation Technology (OT)
- What is Defense in Depth and Defense in Breadth?
- Key elements of both strategies in OT
- Solutions for the OT space
- The weakest link in your defense strategy

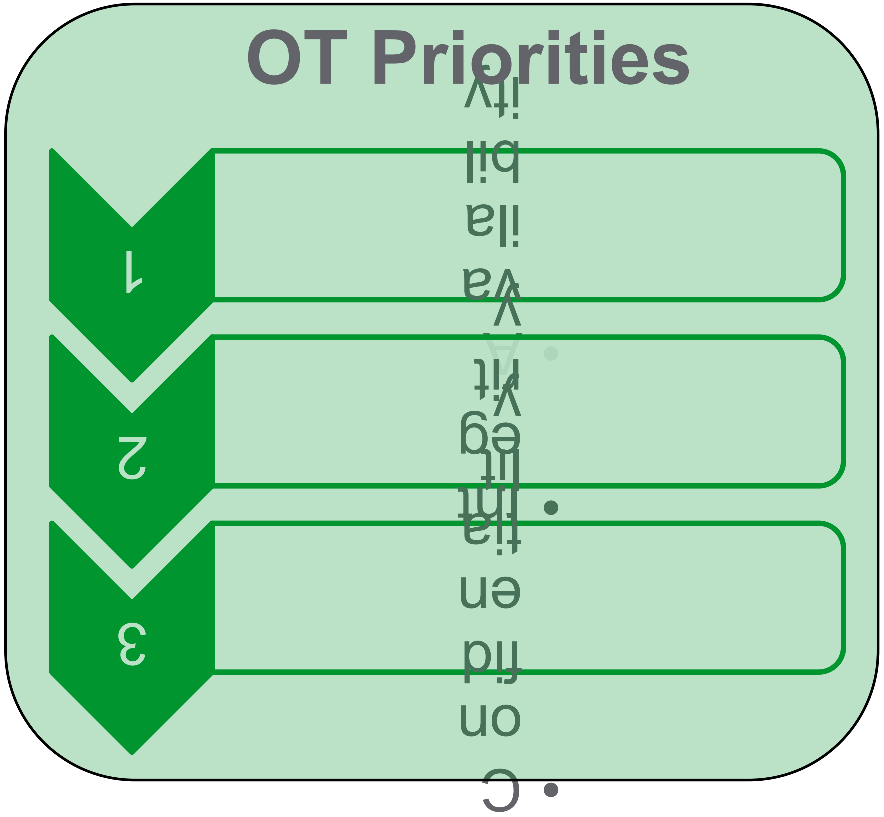
OT and IT Security Differences

Availability is key in OT



IT Priorities

Focused on Information



OT Priorities

Focused on: Operational Processes,
associated assets and configuration

Why Defense in Depth & Breadth?

No defense is absolute

Historical military strategy

- Objective is to slow enemy advance through defensive lines, wearing them down while protecting the defending resources
- Counter-attack when attackers are weakened

Defense in Depth and Breadth applied to Cyber Security

- Objective is to slow the attacker advance through defensive layers, consuming their time and resources while preventing access to system assets
- Multi-disciplinary defense approach at all level of the system
- Provides opportunity to detect and/or prevent a full breach
- Requires a cost-benefit balanced focus on three primary elements: People, Technology and Operations[1]
- Part of a comprehensive risk mitigation strategy

[1] National Security Agency; Defense in Depth

Defense in Depth

Definition

Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.[2]

[2] CNSSI 4009

Defense in Depth

Key Elements[3]

People:
- Support from senior leadership
- Trained and aware personnel
- Assign responsibilities and roles
- Establish policies and procedures

Operations:
- Create & implement the activities necessary to sustain the security position of your operations on a day to day basis

Technology:
- Assure the right technologies are procured and deployed
- Defend at multiple points
- Layer defenses
- Deploy technology to detect intrusions

[3] National Security Agency; Defense in Depth

Defense in Depth

Key Elements

People:
- Threats: Phishing, Spear Phishing, Advanced Persistent Threats (APT),
- Insiders

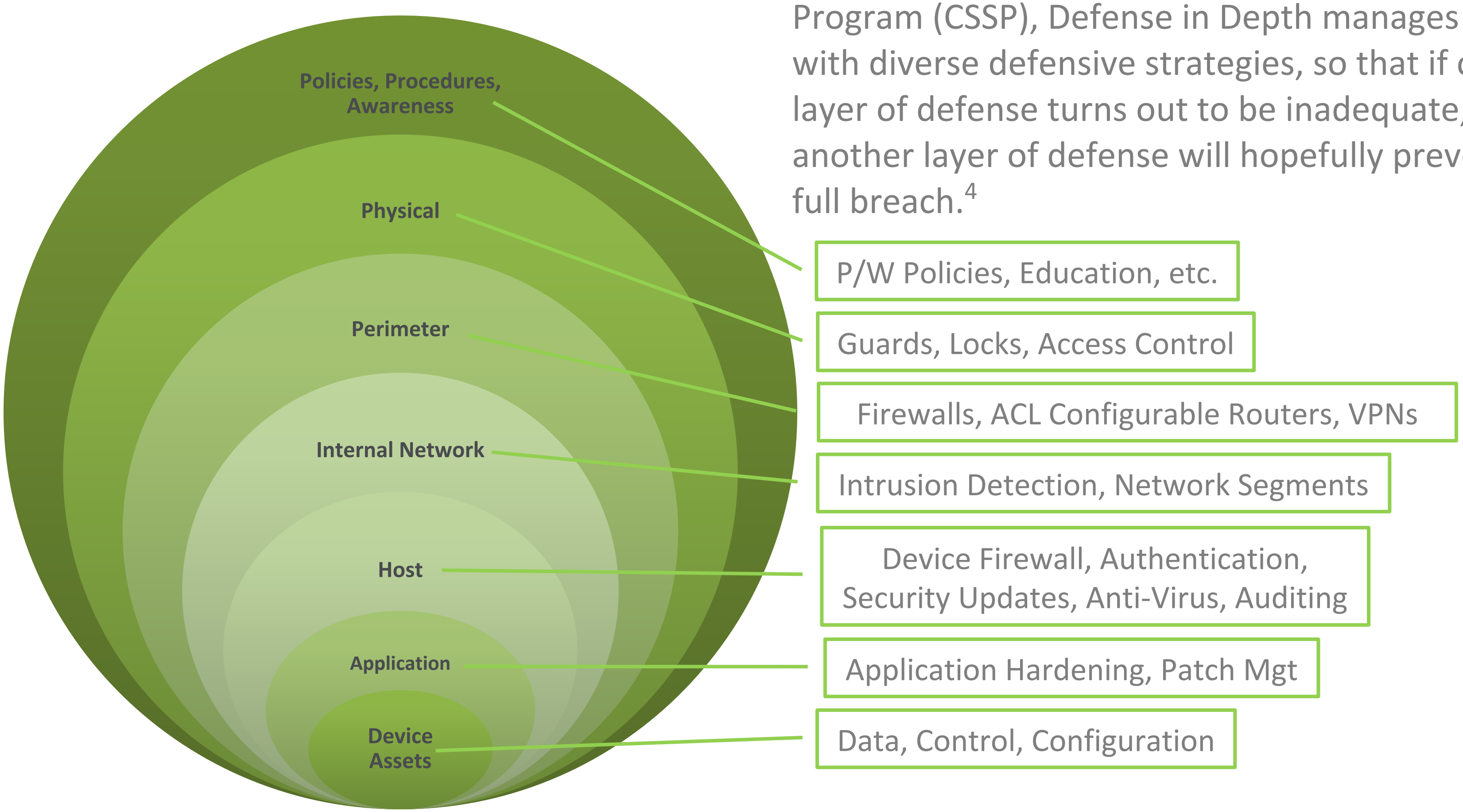
Technology:
- Threats: Malware, Key Logger, USB Key Drop, Pwnie Plug, Pineapple,…

Operations:
- Threats: Password / Authentication Vulnerabilities

Defense in Depth

A Layered Approach to Defense

Developed by the U.S. Control Systems Security Program (CSSP), Defense in Depth manages risk with diverse defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense will hopefully prevent a full breach.[4]



Policies, Procedures, Awareness	P/W Policies, Education, etc.
Physical	Guards, Locks, Access Control
Perimeter	Firewalls, ACL Configurable Routers, VPNs
Internal Network	Intrusion Detection, Network Segments
Host	Device Firewall, Authentication, Security Updates, Anti-Virus, Auditing
Application	Application Hardening, Patch Mgt
Device Assets	Data, Control, Configuration

[4] Viega and McGraw [Viega 02] in Chapter 5, "Guiding Principles for Software Security," in "Principle 2: Practice Defense in Depth" from pages 96-97

Defense in Breadth

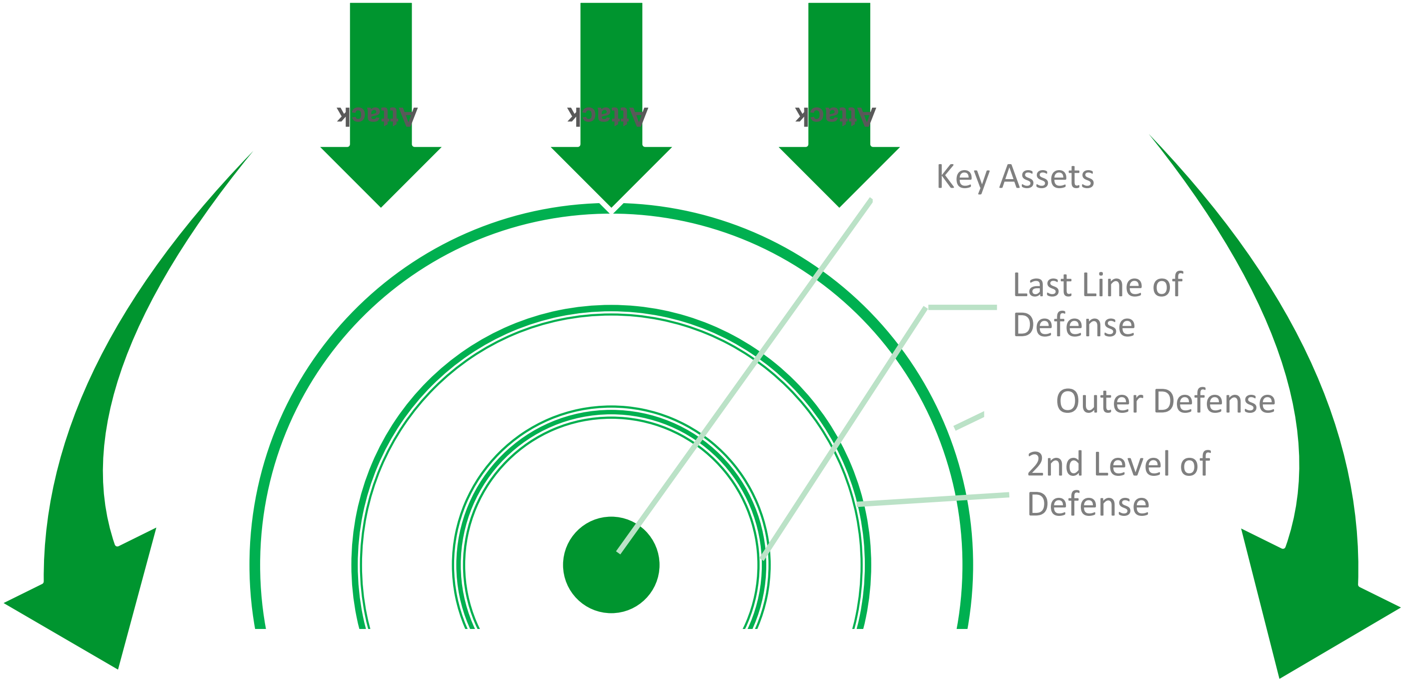
Definition

A planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). [5]

[5] CNSSI 4009

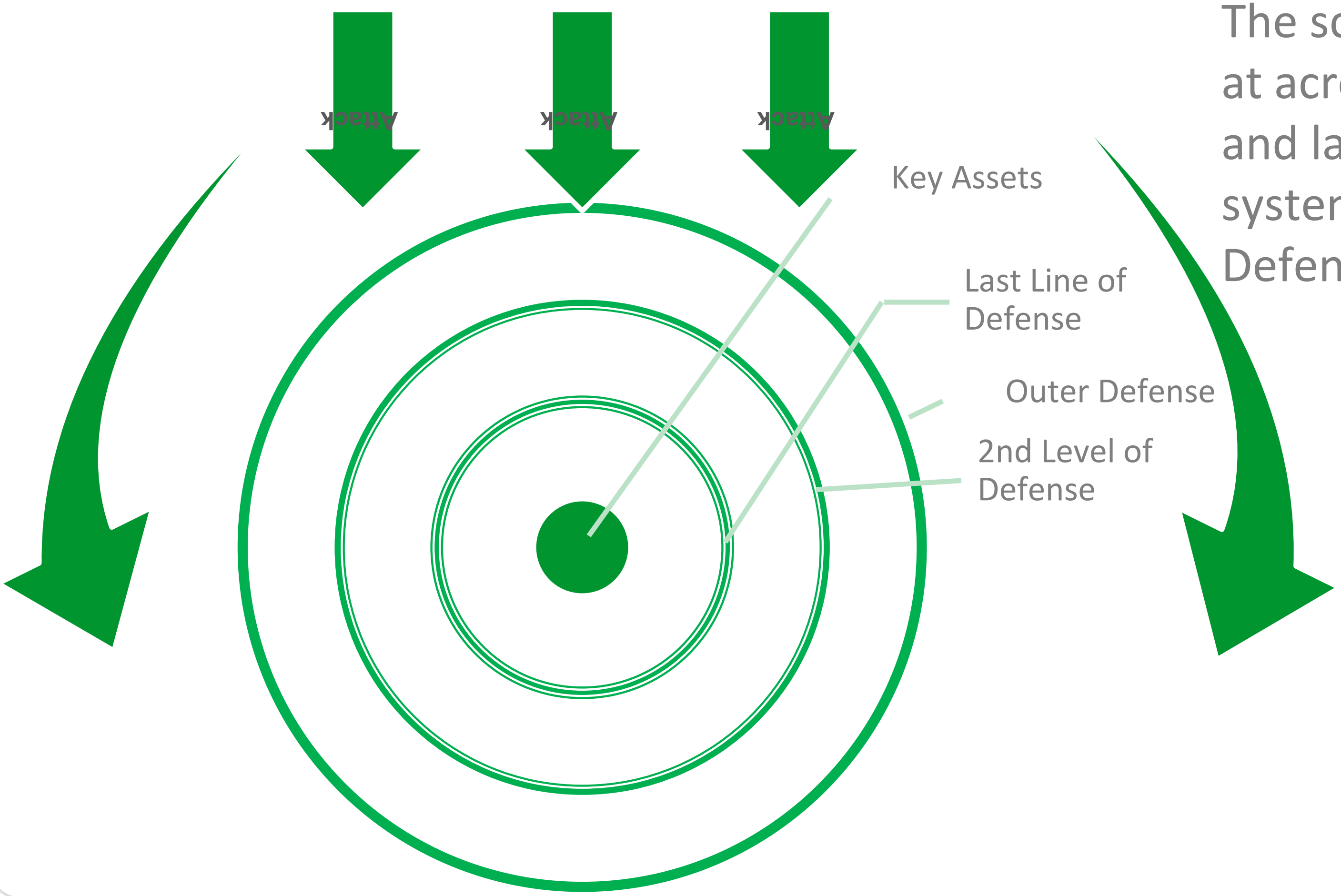
Defense in Breadth

Scaling the Extent of Defense Across Multiple Disciplines



Defense in Breadth

Scaling the Extent of Defense Across Multiple Disciplines



The scope of coverage at across each stage and layer of the system is the focus of Defense in Breadth

Defense in Depth & Breadth

Application

What Should Cyber Security Address?

"Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but ***also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters.*** *Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways."* [6]

[6] ***NIST Smart Grid Interoperability Panel ; Cyber Security Working Group***

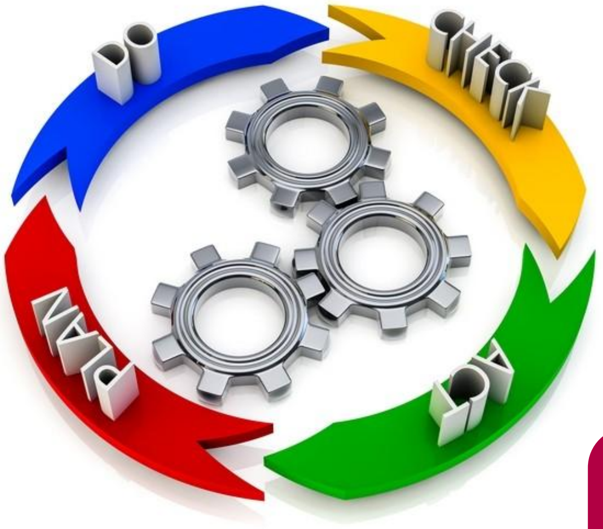
Availability & Reliability

Process & Procedures

- Processes
  - Following standards and regulations
  - Password Management
  - Server Administration
  - Patch Management
  - Incident Response

- Procedures
  - Personnel Training
  - Regular Assessments

- Benefits
  - Prevent inadvertent malware introduction
  - Avoid social engineering breaches
  - Compliance with norms



Manage the Security System

Application

Reliability and Availability go hand-in-hand.

Cyber Security today in OT must focus on the key elements of the process at all stages and levels, for example:

- Access Controls
  - Fences, Security locks, card readers, video cameras
  - Firewalls, VPN, Uni-Directional Gateways
- Hardening
  - Installation processes and procedures
  - HIPS/Application Whitelisting
- Authentication, Authorization
  - Centralized Account Management
  - Role-Based Access Control
- Monitoring and Auditing
  - Centralized Security Event Logging
  - IDS + Real-time alerting and 24/7 Monitoring

Conventional IT Security Solutions Must Be Challenged in an OT Environment

The Weakest Link in Your Defenses - People

"If terrorists ever orchestrate a cyber attack against the U.S., the odds are 9 in 10 that spear-phishing will be the first step of their assault."

– *Tom Chapman, former Navy intelligence officer, now serving as director of cyber operations at cybersecurity firm Edgewave*

The Weakest Link

Your People & Their People

- Un-intentional
  - Unsecured Laptops, Workstations, Work Areas, etc.
  - Not following process and procedures
    - ➢ Password management
    - ➢ Not revoking credentials/access
  - Fall Victim to Social Engineering
    - ➢ (Spear) Phishing, Watering Holes,
    - ➢ USB Key Drop
    - ➢ Over the phone; “Pretexting”
    - ➢ …

- Intentional
  - Insider Threats[7]
    - ➢ Sabotage
    - ➢ Fraud
    - ➢ Theft: Stealing/Leaking Classified/Confidential Information & IP

[7] The CERT Guide to Insider Threats

Social Engineering a.k.a Hacking the Human

Definitions

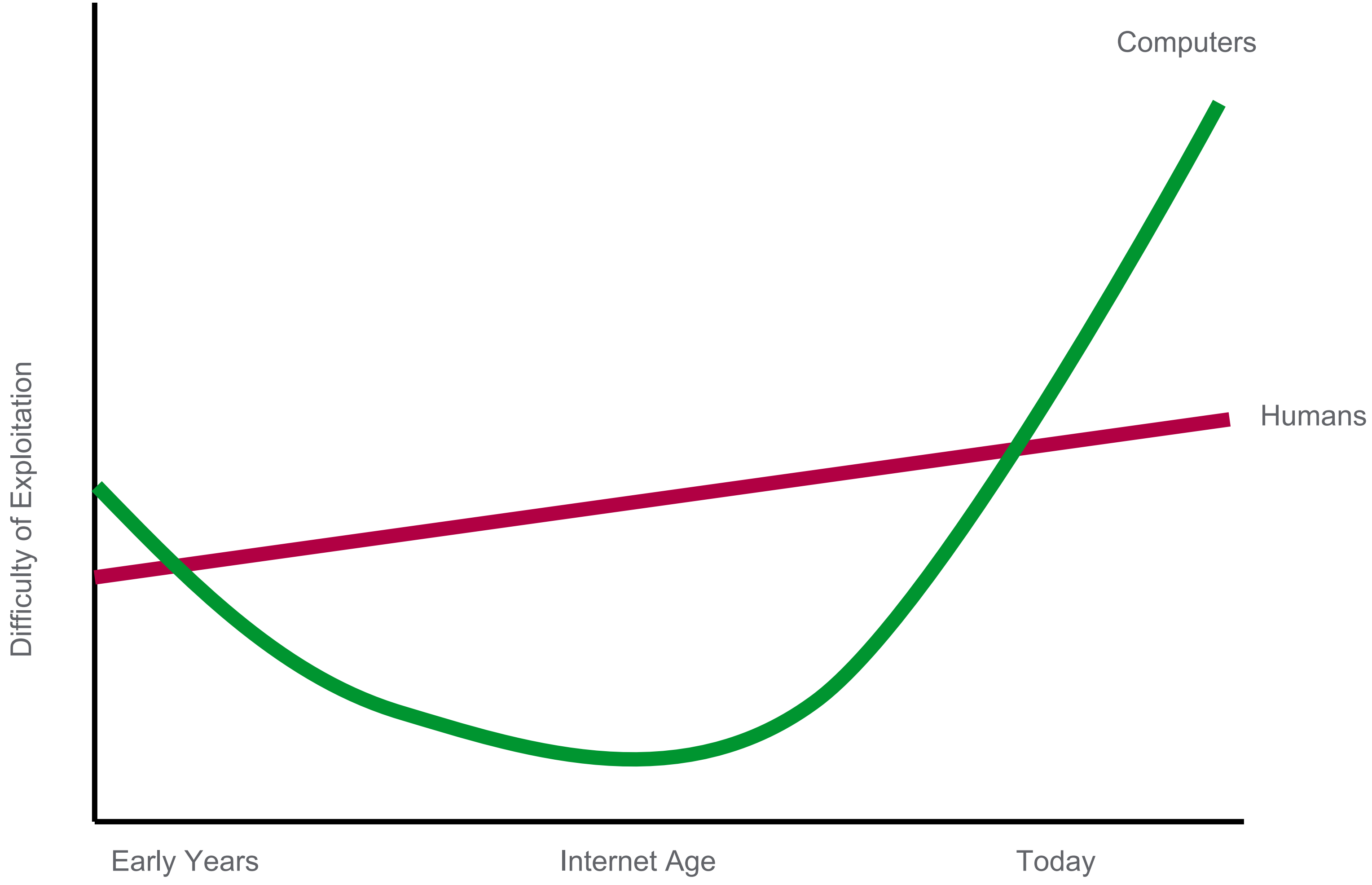
"We define it as, Any act that influences a person to take an action that may or may not be in their best interest."

– *Social-Engineering.org*

"social engineering is the art and science of getting people to comply to your wishes."…
… (it) "concentrates on the weakest link of the computer security chain. It is often said that the only secure computer is an unplugged one. The fact that you could persuade someone to plug it in and switch it on means that even powered down computers are vulnerable.

– *Harl, 1997*

Social Engineering



Based on verbiage from: Beyond HOPE Social Engineering Panel (1997)

Social Engineering

Generally the easiest path in to your OT network

How do we defend?

- Train your organization, contractors and business partners
  - Your entire organization must be trained, aware and at the ready – Verify, THEN Trust
  - Make Social Engineering Awareness Training a part of the on-boarding process
  - Reinforce awareness annually
- Threat model your organization
  - What are the easily accessible entry points? e.g. Receptionist, admin, support center,…
  - What vendors have what access?
  - Other high value targets for social engineering from an OT perspective
- Establish policies and processes and special training
  - Act on the threat model findings
  - Implement principle of least privilege
- Require the same of your vendors

Insider Threat

Definition

> “A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.”
>
> – *Software Engineering Institute, Carnegie Mellon University*

Insider Threat

Consequences

“Malicious insiders can inflict incalculable damage. They enable the enemy to plant boots behind our lines and can compromise our nation's most important endeavors.”

– *National Counterintelligence & Security Center*

Insider Threat

Sabotaging your OT process and assets

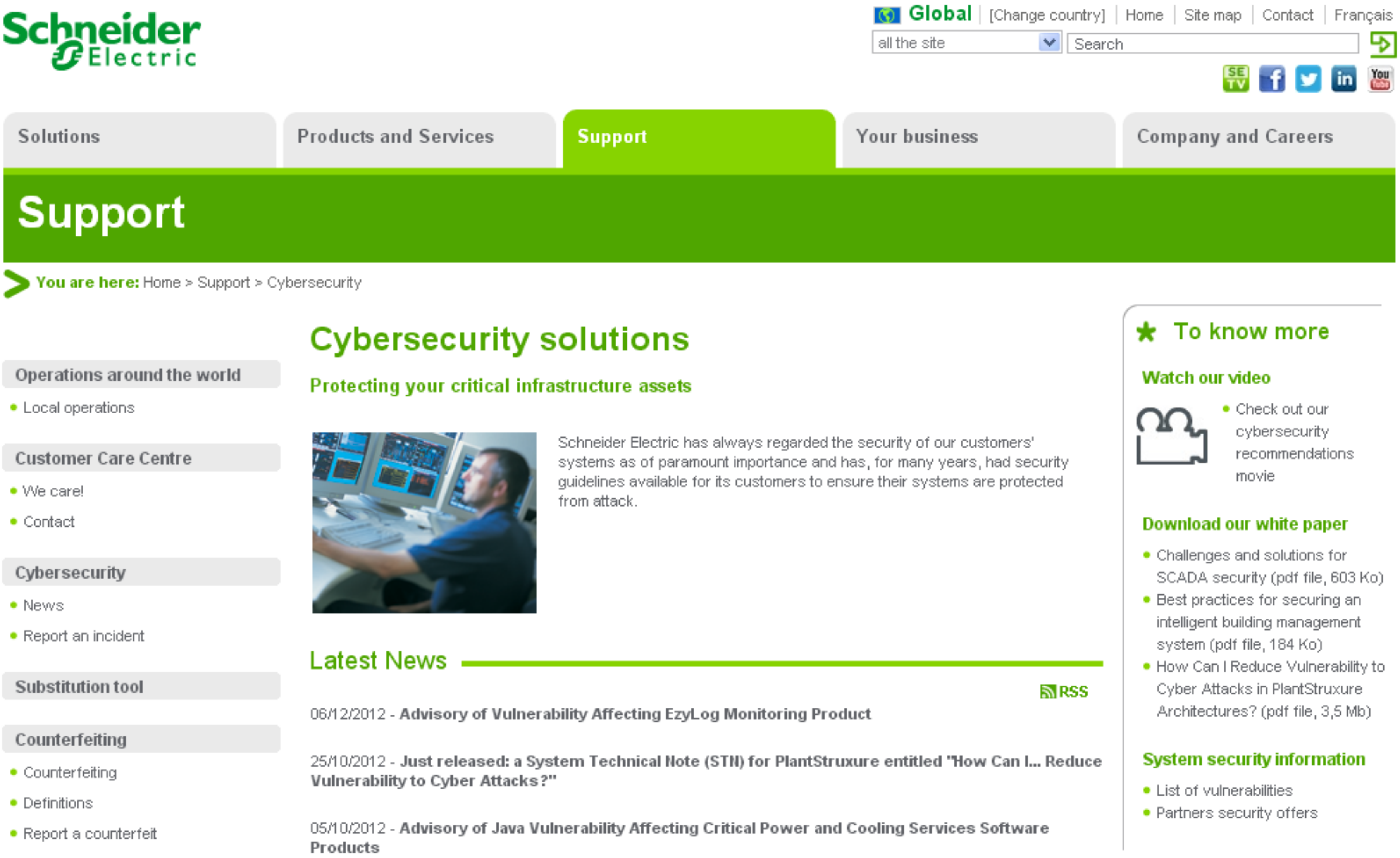
How do we defend?[8]

- Train your organization, contractors and business partners
  - Special training for managers and Human Resources
  - Reinforce awareness annually
- Address the Human Resource Aspects
  - Start with the hiring process, deactivate access on termination
  - Log & monitor activities
  - Look for and anticipate issues leading to malicious activity
- Establish & consistently enforce policies and processes
  - Implement principle of least privilege, separation of duties, strict password management rules, change controls
  - Back up and recovery
  - Establish and communicate deterrents for noncompliance
- Layered protection against remote attack
- Require the same of your vendors

[8] Summarized form "The CERT Guide to Insider Threats", Cappelli, Moore & Trzeciak, 2012 Addison Wesley

For More Information

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page



Support

You are here: Home > Support > Cybersecurity

Operations around the world
- Local operations

Customer Care Centre
- We care!
- Contact

Cybersecurity
- News
- Report an incident

Substitution tool

Counterfeiting
- Counterfeiting
- Definitions
- Report a counterfeit

Cybersecurity solutions

Protecting your critical infrastructure assets

Schneider Electric has always regarded the security of our customers' systems as of paramount importance and has, for many years, had security guidelines available for its customers to ensure their systems are protected from attack.

Latest News

RSS

06/12/2012 - **Advisory of Vulnerability Affecting EzyLog Monitoring Product**

25/10/2012 - **Just released: a System Technical Note (STN) for PlantStruxure entitled "How Can I... Reduce Vulnerability to Cyber Attacks?"**

05/10/2012 - **Advisory of Java Vulnerability Affecting Critical Power and Cooling Services Software Products**

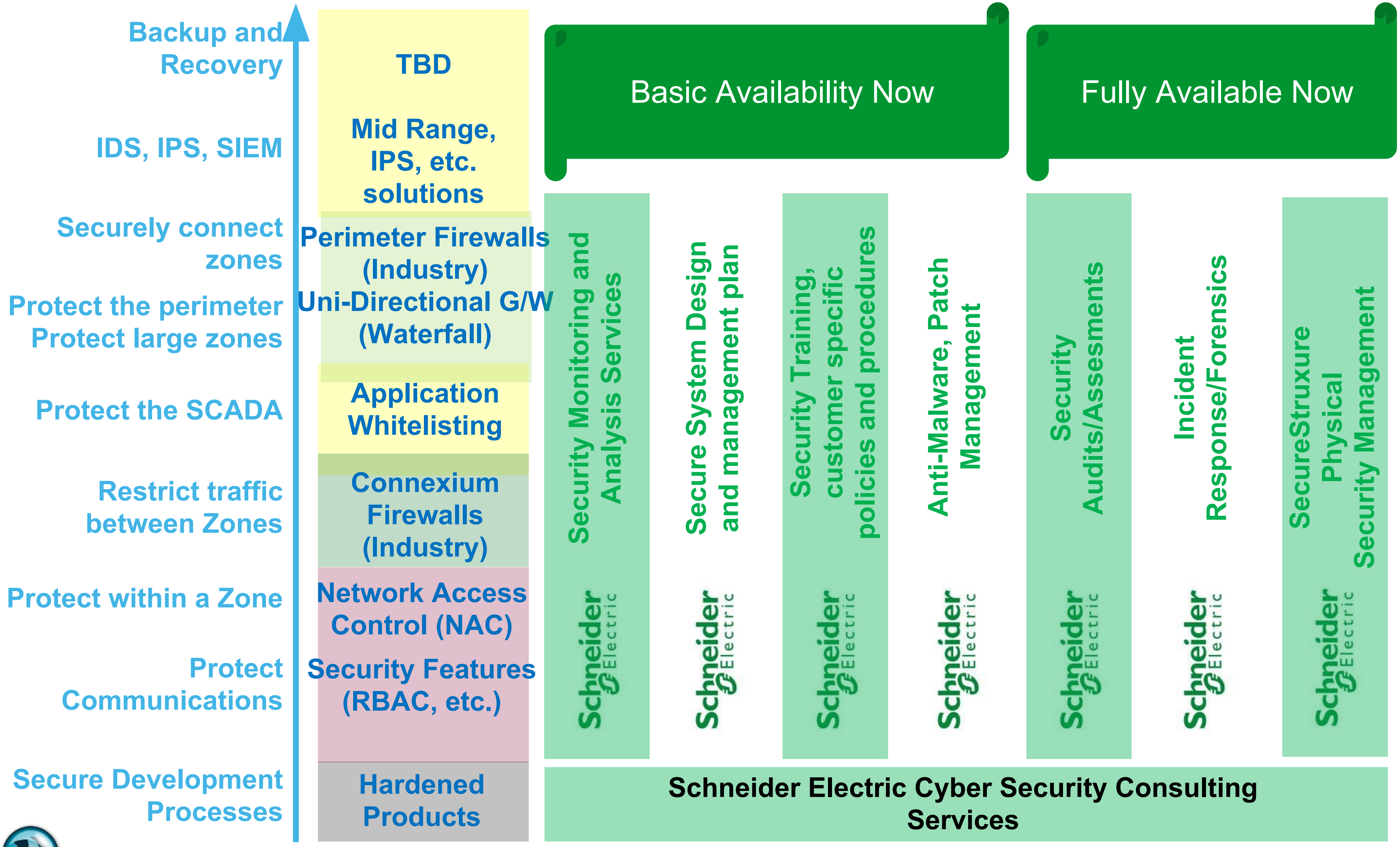
To know more

Watch our video
- Check out our cybersecurity recommendations movie

Download our white paper
- Challenges and solutions for SCADA security (pdf file, 603 Ko)
- Best practices for securing an intelligent building management system (pdf file, 184 Ko)
- How Can I Reduce Vulnerability to Cyber Attacks in PlantStruxure Architectures? (pdf file, 3,5 Mb)

System security information
- List of vulnerabilities
- Partners security offers

Comprehensive Cyber Security Offer



Backup and Recovery

IDS, IPS, SIEM

Securely connect zones

Protect the perimeter
Protect large zones

Protect the SCADA

Restrict traffic between Zones

Protect within a Zone

Protect Communications

Secure Development Processes

TBD

Mid Range, IPS, etc. solutions

Perimeter Firewalls (Industry)

Uni-Directional G/W (Waterfall)

Application Whitelisting

Connexium Firewalls (Industry)

Network Access Control (NAC)

Security Features (RBAC, etc.)

Hardened Products

Basic Availability Now

- Security Monitoring and Analysis Services
- Secure System Design and management plan
- Security Training, customer specific policies and procedures
- Anti-Malware, Patch Management

Fully Available Now

- Security Audits/Assesments
- Incident Response/Forensics
- SecureStruxure Physical Security Management

Schneider Electric Cyber Security Consulting Services

Make the most of your energy *business*

Schneider Electric

Thank You