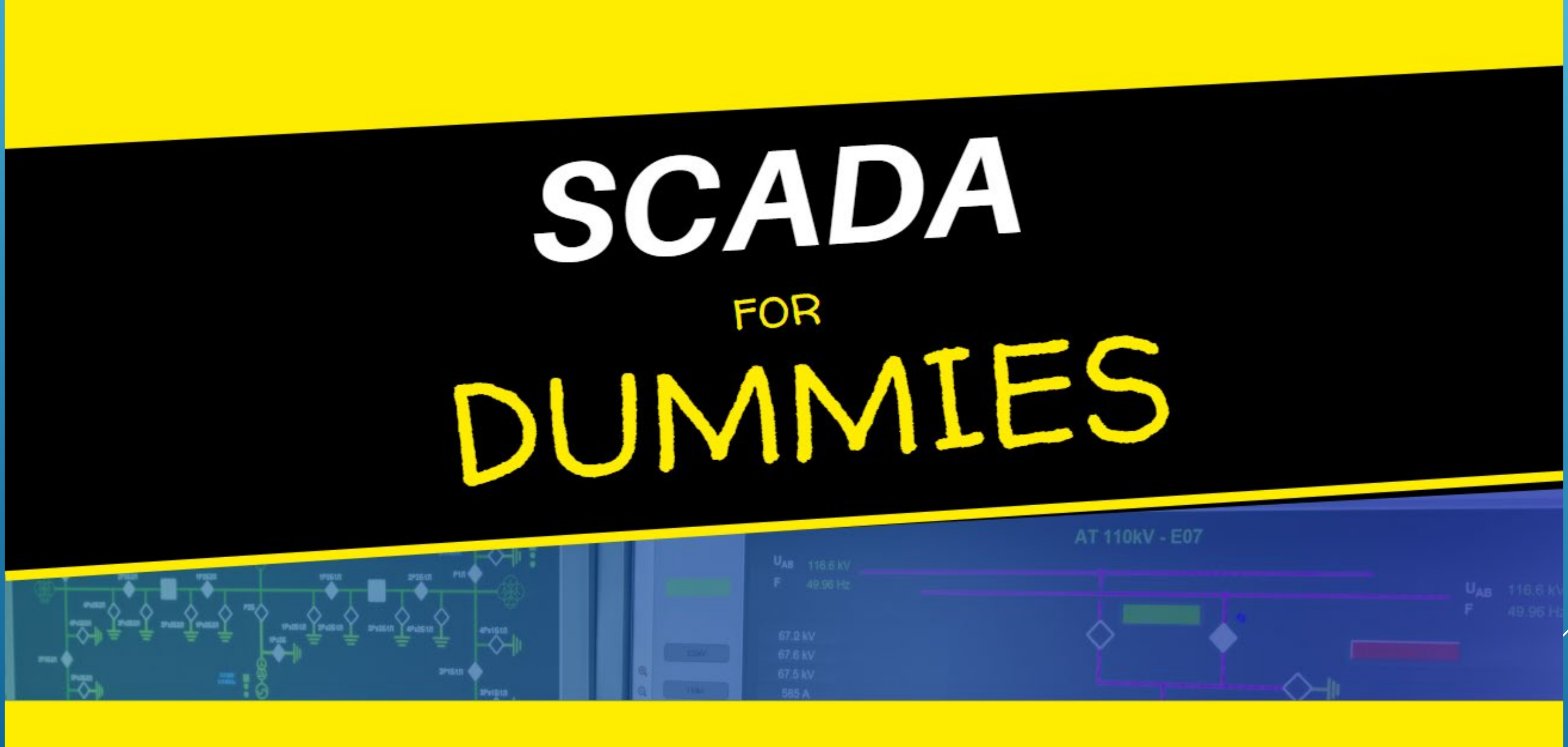
SCADA SECURITY

Florida
Rural
Water
Association

DON'T WAIT
ANOTHER DAY

- What does SCADA stand for?



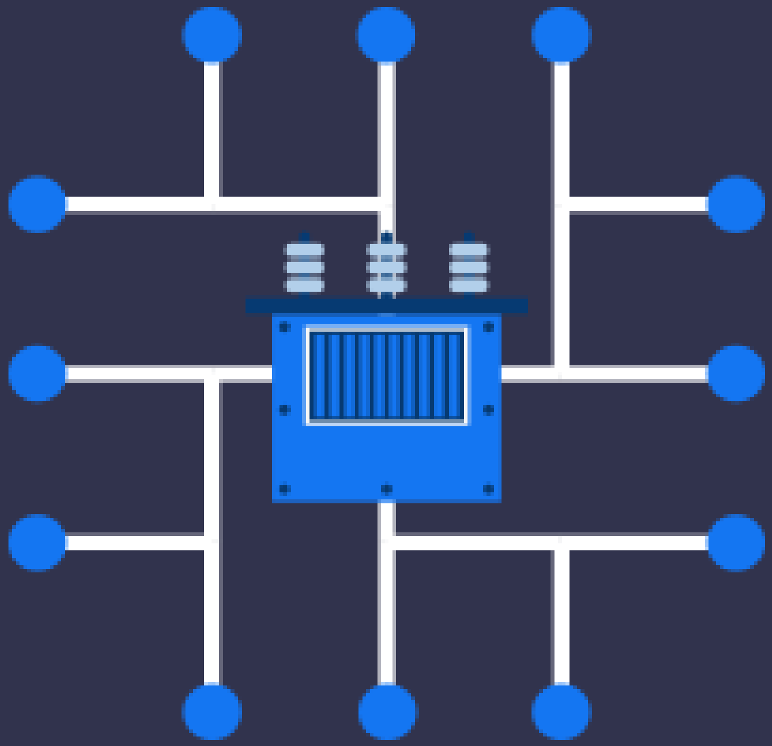
S = Supervisory

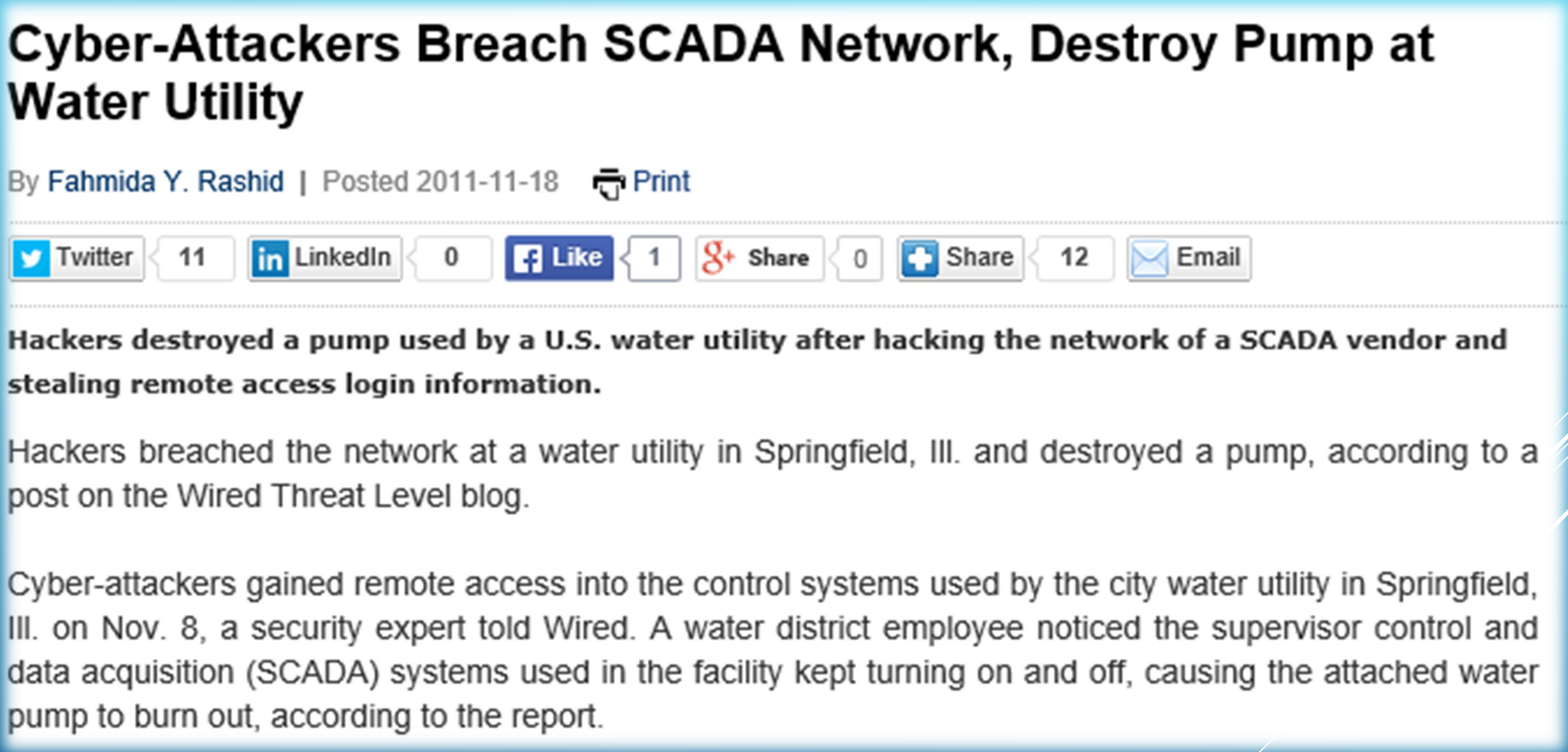
C = Control

A = And

D = Data

A = Acquisition





Cyber-Attackers Breach SCADA Network, Destroy Pump at Water Utility

By Fahmida Y. Rashid | Posted 2011-11-18 Print

Hackers destroyed a pump used by a U.S. water utility after hacking the network of a SCADA vendor and stealing remote access login information.

Hackers breached the network at a water utility in Springfield, Ill. and destroyed a pump, according to a post on the Wired Threat Level blog.

Cyber-attackers gained remote access into the control systems used by the city water utility in Springfield, Ill. on Nov. 8, a security expert told Wired. A water district employee noticed the supervisor control and data acquisition (SCADA) systems used in the facility kept turning on and off, causing the attached water pump to burn out, according to the report.

Cyberattack in Oldsmar Florida.

Even the phones went down in the government of Lake City, Fla., after hackers launched a cyberattack that disabled the city’s computer systems. For several days after computer systems were paralyzed by a ransomware attack, the staff of the small North Florida town worked with the F.B.I. and an outside security consultant to restore phone lines, email and online utility payments. But in the end, city leaders called an emergency meeting this week and reluctantly approved paying the hackers the ransom they demanded: 42 Bitcoin, or about $460,000.

It was the second city to agree to a large ransom in two weeks. Riviera Beach, in Florida’s Palm Beach County, signed off on an extraordinary $600,000 payment last week, also in Bitcoin, a cybercurrency that is difficult to trace.

As in Riviera Beach, the brunt of Lake City’s ransom will be paid by insurance. Only $10,000 will come out of the city’s coffers.

Ransomware is the most profitable type of malware in history. In the past, attackers primarily tried to steal information and maintain long-term access to their victims' systems and resources. They typically did not deny access to systems or destroy data. Ransomware has changed the game from stealthy access to extortion.

In a ransomware attack, victims pay attackers directly to recover their files. The emergence of anonymous currencies such as Bitcoin and Ripple has meant that attackers can profit easily and with relatively low risk. This makes attacks highly lucrative and funds development of the next generation of ransomware. As a result, ransomware is evolving at an alarming rate.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.
Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

What is cybersecurity all about?

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks. A unified threat management system can automate integrations across select Cisco Security products and accelerate key security operations functions: detection, investigation, and remediation.

People

Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data. Learn more about basic cybersecurity principles.

Processes

Organizations must have a framework for how they deal with both attempted and successful cyber attacks. One well-respected framework can guide you. It explains how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks.

Technology

Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyber attacks. Three main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and the cloud. Common technology used to protect these entities include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.

Why is cybersecurity important?
In today’s connected world, everyone benefits from advanced cyberdefense programs. At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning. Everyone also benefits from the work of cyberthreat researchers, like the team of 250 threat researchers at Talos, who investigate new and emerging threats and cyber attack strategies. They reveal new vulnerabilities, educate the public on the importance of cybersecurity, and strengthen open source tools. Their work makes the Internet safer for everyone.

Types of cybersecurity threats

Phishing

Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information. It’s the most common type of cyber attack. You can help protect yourself through education or a technology solution that filters malicious emails.

Ransomware

Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.

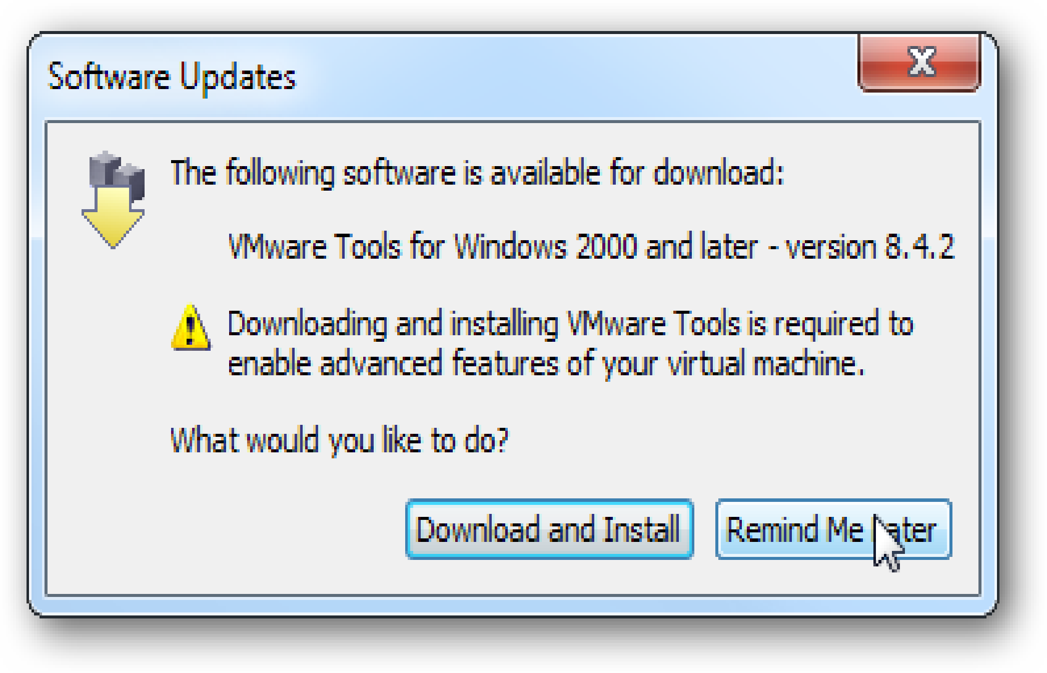
Malware

Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.

Social engineering

Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.

You're busy. You're tired. You just want to play Pokémon Go or access your company's internet. Whatever the reason, whenever you click "Remind me later" on a software update, you make your device vulnerable to ransomware. That is just one of the many ways ransomware can enter your system. Malvertising, phishing emails, and even sophisticated thumb-drive schemes are common tactics that adversaries use to compromise your system.



Software Updates

The following software is available for download:

VMware Tools for Windows 2000 and later - version 8.4.2

Downloading and installing VMware Tools is required to enable advanced features of your virtual machine.

What would you like to do?

SCADA Security

- SCADA Subsystems
- SCADA Threats
- SCADA Security
  - Management
  - Physical
  - Connectivity
  - Configuration Mgmt.
  - Authentication
  - Disaster Recovery

SCADA Now

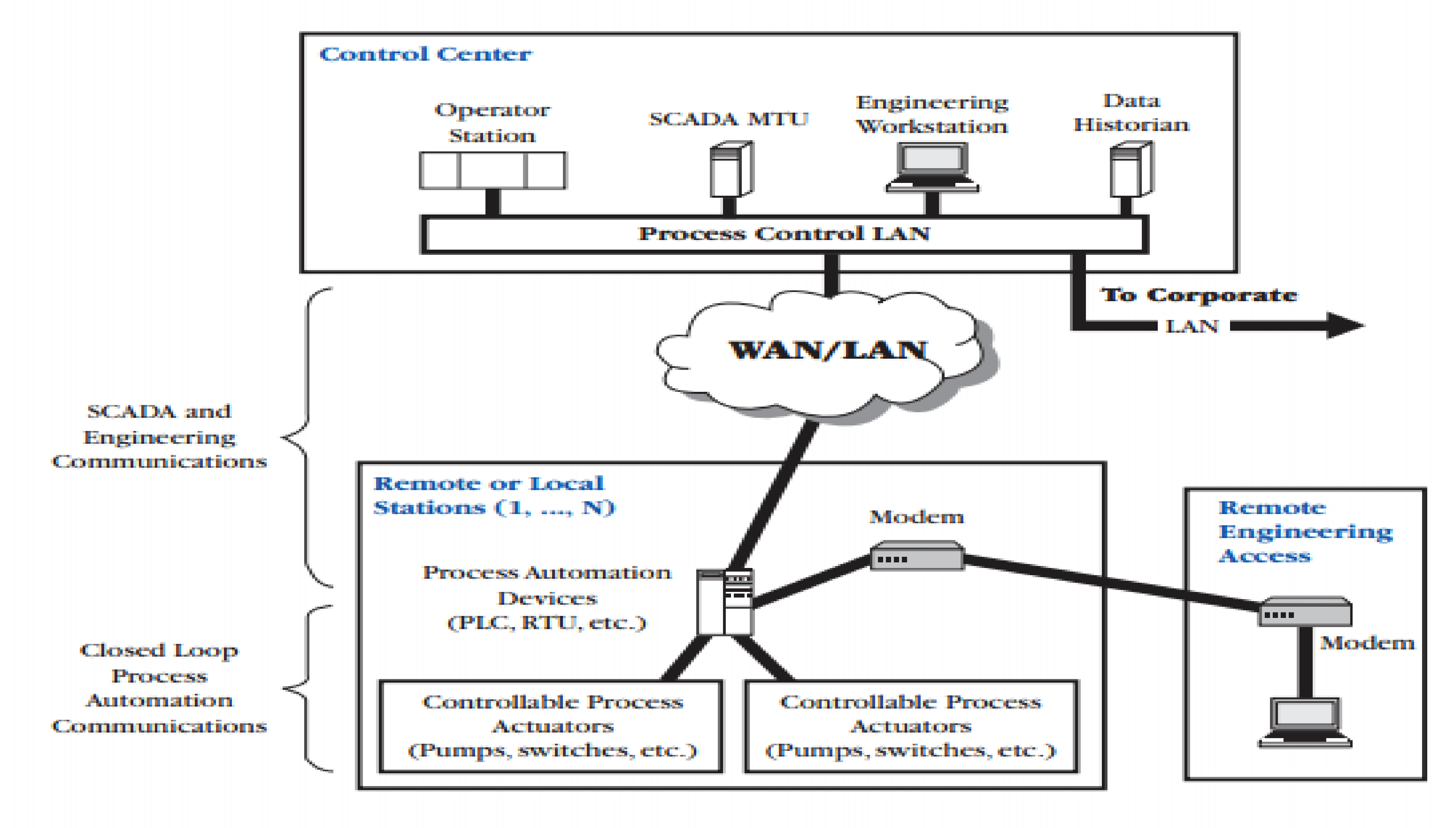
- The major challenge for governments is the inclusion of protection for these critical components in their cyber strategies
- There are many systems deployed with factory settings, pre-set standard configurations
- Almost every SCADA performs well. They’re reliable and flexible, but often lack security.

SCADA Subsystems

Attackers could target each of the components to compromise a controlled process.

For example, any supervisory system is usually a computer based on a commercial OS for which it's possible to exploit known vulnerabilities or zero-day vulnerabilities.

SCADA systems could be infected exploiting attack vectors via mobile support (e.g. USB sticks) or the network connections.

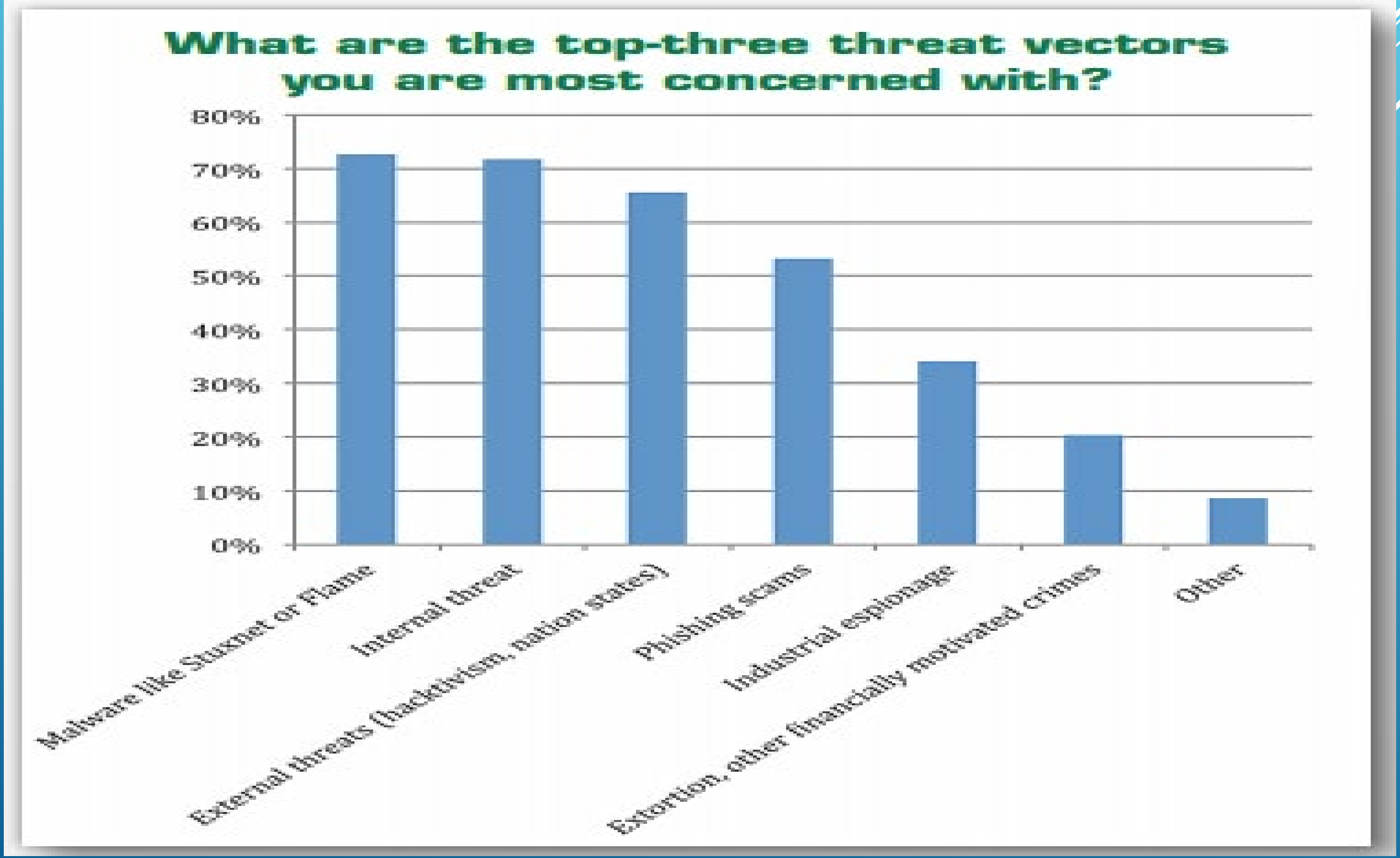

Control Center
Operator Station
SCADA MTU
Engineering Workstation
Data Historian
Process Control LAN
To Corporate LAN
WAN/LAN
SCADA and Engineering Communications
Closed Loop Process Automation Communications
Remote or Local Stations (1, ..., N)
Modem
Process Automation Devices (PLC, RTU, etc.)
Controllable Process Actuators (Pumps, switches, etc.)
Controllable Process Actuators (Pumps, switches, etc.)
Remote Engineering Access
Modem

SCADA Threats

"… the awareness of cyber threats and the perception of the risks related to a cyber attacks are high. Nearly 70% of respondents believe the threat to be high.

"SANS SCADA and Process Control Security Survey"
The SANS Institute

SCADA Threats

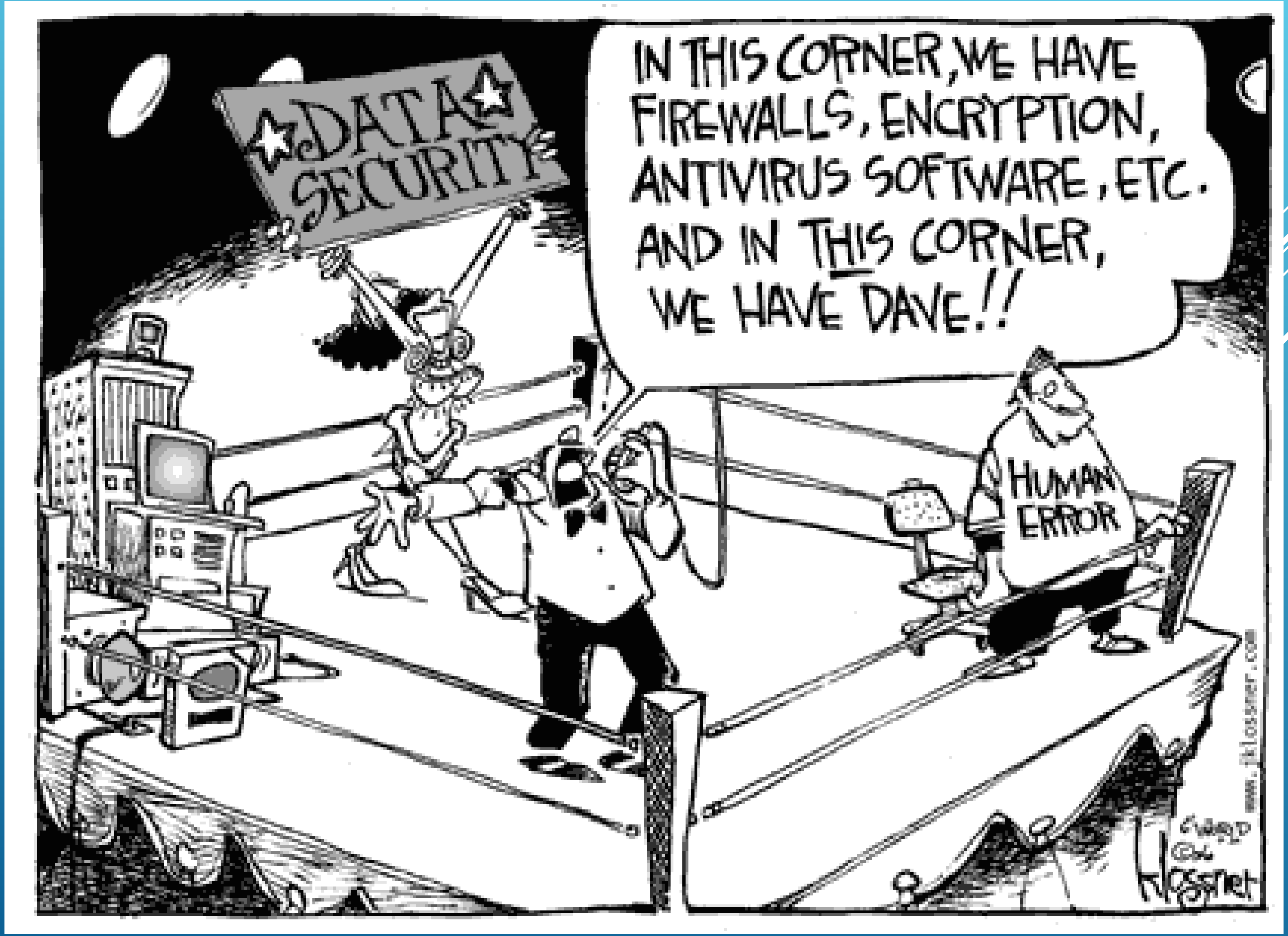


SCADA Threats

A list of principal vulnerabilities that have been identified for control systems environments:

- ☹ Increased Exposure
- ☹ Interconnectivity
- ☹ Complexity
- ☹ Common Computing Technologies
- ☹ Increased Automation

SCADA Threats


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©WORLD ©06
Klossner

SCADA Threats

FBI director James Comey said about cyberterrorism:

“There must be a collective effort by all governments to produce continuous report on the security status of critical infrastructures and related SCADA systems.”

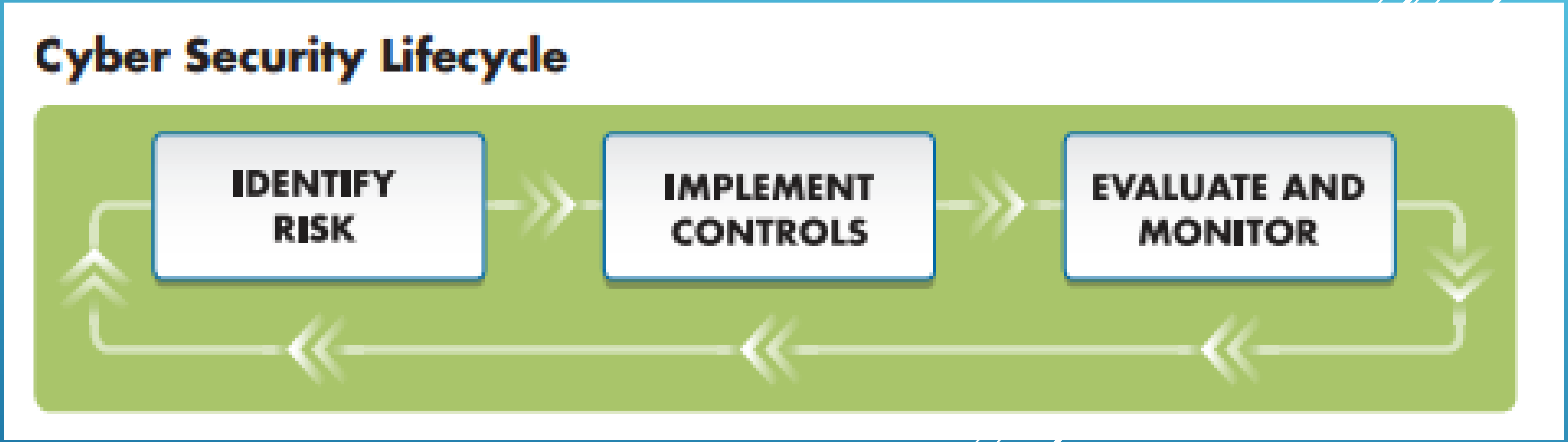
“The security component must become part of the project of an industrial system. It must be considered a specific requirement. The overall security of critical infrastructures must be audited during the entire lifecycle of its components.”

SCADA Threats

“Recently the heads of the Federal Bureau of Investigation (FBI), DHS, and National Counterterrorism Center have declared cyber attacks are the most likely form of terrorism against the United States in the coming years.”

“That’s where the bad guys will go. There are no safe neighborhoods. All of us are neighbors [online].”

SCADA Security



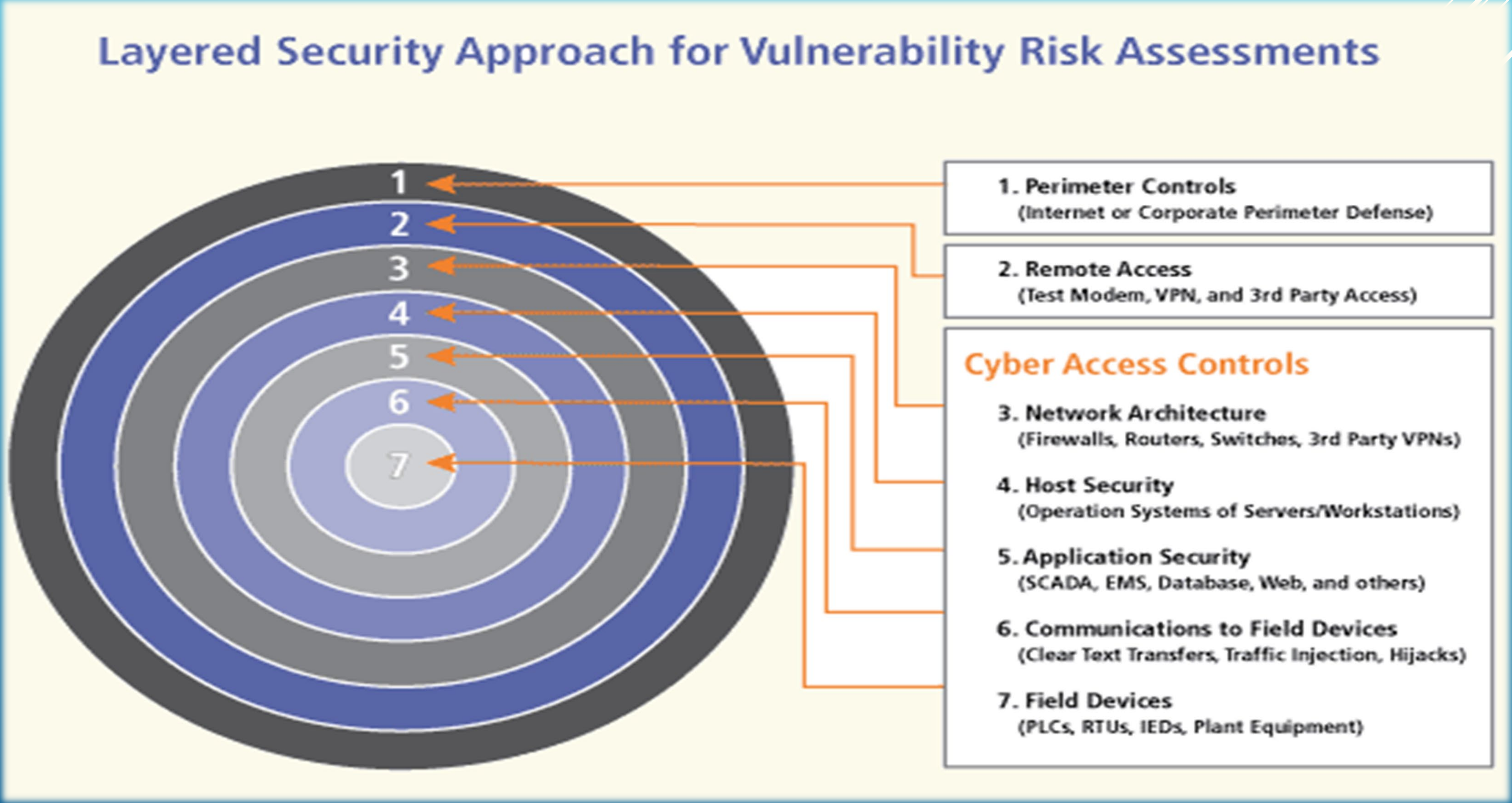
Cyber Security Lifecycle

IDENTIFY RISK

IMPLEMENT CONTROLS

EVALUATE AND MONITOR

SCADA Security



Layered Security Approach for Vulnerability Risk Assessments

1. **Perimeter Controls**
   (Internet or Corporate Perimeter Defense)

2. **Remote Access**
   (Test Modem, VPN, and 3rd Party Access)

Cyber Access Controls

3. **Network Architecture**
   (Firewalls, Routers, Switches, 3rd Party VPNs)

4. **Host Security**
   (Operation Systems of Servers/Workstations)

5. **Application Security**
   (SCADA, EMS, Database, Web, and others)

6. **Communications to Field Devices**
   (Clear Text Transfers, Traffic Injection, Hijacks)

7. **Field Devices**
   (PLCs, RTUs, IEDs, Plant Equipment)

SCADA Security - Management

Management has a crucial role in security. Its primary task is to provide a strong commitment for the implementation of an efficient cyber strategy.

That includes:

- the assignment of cyber security roles, responsibilities, and authorities for personnel.
- A detailed security policy must be in place that describes how management defines roles and responsibilities.
- Each employee must be informed of all
- procedures adopted to keep architecture secure.

SCADA Security - Management

The goal of management is to:

- define a structured security program with mandated requirements to reach expectations
- provide personnel with formalized policies and procedures.
- Senior management must establish expectations for cyber security performance and hold individuals accountable for their performance.

SCADA Security - Management

Dr. Phyllis Scheck, Vice President and Chief Technology Officer, Global Public Sector, McAfee said:

"Achieving security by design is essential in securing critical infrastructure. Cybersecurity must be embedded in the systems and networks at the very beginning of the design process so that it becomes an integral part of the systems functioning."

SCADA Security - Physical

All plants that host SCADA systems and networks must be assessed.

Due to the fact that SCADA systems are usually distributed over large distances in multiple locations with different physical security measures their protection must be carefully evaluated.

SCADA Security - Physical

Physical restrictions that could be applied to improve security to prevent incidents are:

- Restricted access to the site
- Restricted number of technicians responsible for maintenance
- No use of mobile support
- Segregated control network, no connection to other networks
- Each computer is locked in a restricted room or cabinet

SCADA Security - Connectivity

- Configure network appliances avoiding the use of default configurations
- Adopt firewalls, intrusion detection systems (IDSs), and other appropriate defense systems at each point of entry.
- implementation of all security features proposed by SCADA vendors, in the form of updates or product patches
- Audit network connectivity and record the results clearly and accurately about every networked asset.

.

SCADA Security – Config. Mgmt.

The NSA document titled “Securing SCADA and Control Systems (CS)” introduces the following suggestions for configuration management:

- Map out and document the entire CS network, including CS and infrastructure device configurations
- Prepare and configure new equipment off-line
- Sanitize old equipment before disposal
- Keep CS infrastructure security features current with device moves, additions, and decommissions
- Enable auditing features and periodically examine the resulting logs for signs of unusual activity
- Synchronize to a common time reference, so audit logs become more useful during incident response
- Develop a Disaster Recovery Plan (DRP) for the CS

SCADA Security – Authentication

- Strong passwords must be implemented
- Identify and assess any source of information, including remote computer networks, phone lines, and fiber optics.
- Implement internal and external intrusion detection systems.
- Audit system logs

SCADA Security – Disaster Recovery

System backups are an essential to the rapid reconstruction of any network. Recovery plans usually include:

- Adoption of redundant hardware and fault tolerant systems
- Fallback mechanisms
- System backup procedure
- Routinely exercised disaster recovery
- Every change to the overall architecture triggers a review of the plan

SCADA Security – Disaster Recovery

Governments and private companies must be able to run simulations of attacks during exercises that have the intent of identifying potential attack scenarios and evaluating potential system vulnerabilities. The exercises must also consider the impact of accidental errors, and the effect of malicious insiders.

References

http://resources.infosecinstitute.com/improving-scada-system-security/

http://securityaffairs.co/wordpress/19604/malware/stuxnet-russian-nuclear-facility.html

http://www.sans.org/reading-room/analysts-program/sans-survey-scada-2013

http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

http://news.bbc.co.uk/2/hi/7583805.stm

http://www.tsips.com/SCADA.htm

http://www.mcafee.com/us/resources/reports/rp-energy-sector-industrial-control.pdf

http://www.nsa.gov/ia/_files/factsheets/scada_factsheet.pdf

http://www.fortinet.com/sites/default/files/whitepapers/WP_SCADA.pdf

https://www.honeywellprocess.com/library/marketing/whitepapers/HoneywellIndustrialCyberSecurity_IncreasetheSecurityofScadaNetworks_WP691.pdf

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

http://www.security-assessment.com/files/presentations/SCADA%20-%20Fear,%20Uncertainty,%20and%20the%20Digital%20Armageddon.pdf

http://www.nsa.gov/ia/_files/factsheets/scada_factsheet.pdf

http://www.sans.org/reading-room/whitepapers/warfare/security-critical-infrastructure-scada-systems-1644

Questions?

Florida Rural Water Association