Facilities of the Future and Defending Them

Simon VanDyk
Director of Business Development,
Blue Umbrella

Howard Manson
Owner, Today's Integration

Jonathan Pollet
Owner, Red Tiger Security

Topics for Discussion

- New technology for your district
  Simon VanDyk

- Physical site security – Options and their differences
  Howard Manson

- Digital and cyber security – Protecting your modern technology
  Jonathan Pollet

How Will This Talk Be Any Different?

- Active Q&A Tools
  - Questions will be collected throughout the talk
  - Text all questions to ###-####
  - The top questions will be answered at the end
  - Unanswered questions will be responded to by COB Monday

- Feedback for Future Topics
  - Participate in online survey to help improve this experience
  - Email info@blueumbrellaco.com for copy of presentation and notes

Improving Internal Communications and Efficiencies

- Separating district from personal communications
- Director devices for added security and interconnectivity
- WAN access options for secure facility monitoring

New Tools for the Modern Board to Consider

- A Possible Scenario:
  - Mainline break – clock starts ticking
  - What is your communication plan?
  - How many residents will be notified and how long will it take?
  - How will the public respond?

- Possible Solutions:
  - Plant Interconnectivity / Telemetry
  - Remote monitoring of system and security
  - SMS Text Alert System
  - Website posting – alert, instructions, and follow up

SCADA and Telemetry Benefits

- Operator
- Engineer
- Board Member
- Consultants
- Residents

Physical Site Security

- Difference between security alarm and camera recording systems
- How to deploy each in an industrial environment

Security in Your Facilities

- Critical areas to cover and what devices should monitor them
- How to interface with the operator
- Added benefits beyond security

Jonathan Pollet – CISSP, PCIP, CAP

- 20 Years of Electrical Engineering, SCADA, Industrial Controls, and IT Experience
  - SCADA Engineer for Chevron in 1990's
  - PLC Programming and SCADA System Design and Commissioning
  - Wireless RF and Telecommunications Design and Startup
  - Acting CIO for Major Oil Company for 2 years – Enterprise IT Management
  - Published industry first White Papers on SCADA Security early in 2001
  - Focused research and standards development for SCADA Security since 2002
  - Conducted over 3000 security assessments on Critical Infrastructure systems
  - Conducted over 180 International conferences and workshops on security
  - Developed safe security assessment methodology for live SCADA Systems
  - Developed the first SCADA Security 5-day hands-on training course
  - Trained over 3,000 Professionals Globally
  - Featured presenter on Fox News Live, regular featured guest on the Houston Fox News Morning Show, CBNC, Vanity Fair, Popular Mechanics, CIO Magazine, and several security publications

Digital Security
(How to Minimize Risk to Water Utility Systems)

- Definitions and Terms
- Why has the world changed today versus 20 years ago?
- Proven methodology to determine risk, close gaps, and secure utility systems based on the NIST Cyber Security Framework created under direction of the White House in 2014

Cyber Security Defined

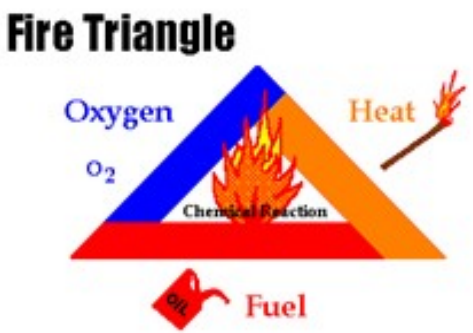
The protection afforded to an information or automated system in order to attain the applicable objectives of preserving the **integrity**, **availability** and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications)*

* NIST Special Publication 800-12

In simple terms, the purpose of computer or digital security is to ensure the systems are **AVAILABLE** with High **INTEGRITY** and **CONFIDENTIALITY** to authorized users and NOT AVAILABLE to anyone without the right to access the system.

Cyber Security Attack Triangle

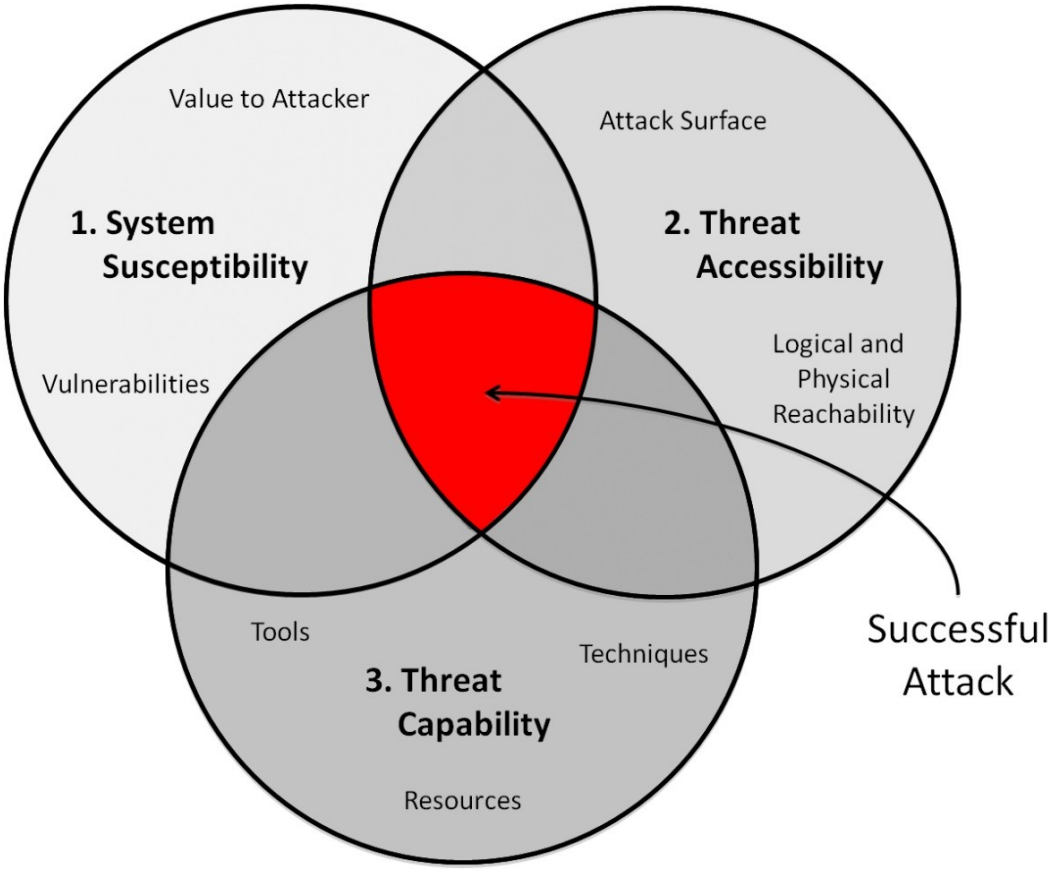
- A Cyber Attack is the result of the presence of a **Threat**, taking advantage of a **Vulnerability**, through a successful **Exploit**
  - Threats typically stem from people or organizations
  - Vulnerabilities are deficiencies in the security of a system
  - Exploits are created by Threats to take advantage of Vulnerabilities
- Think of this like the Fire Triangle





- Take any one leg out, and the Fire will be mitigated
- **This same principle applies with Cyber Security**
- The likelihood of a vulnerability getting exploited combined with the possible result / impact to the infrastructure is the **Risk**

What Do We Need to Worry About?
How to Quantify Risk?

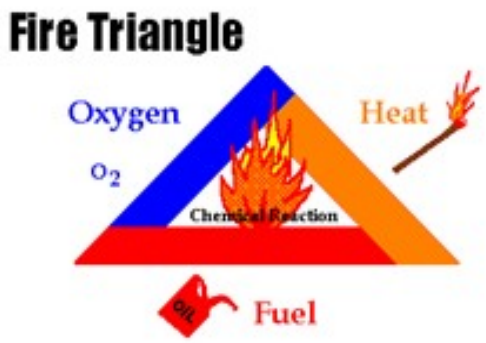


Physical / Controls Assessment
+ Technical (Digital) Assessments
+ Threat Assessment

= True Valuation Risk

Source: http://timreview.ca/article/712

Understanding Each Element of a Cyber Attack

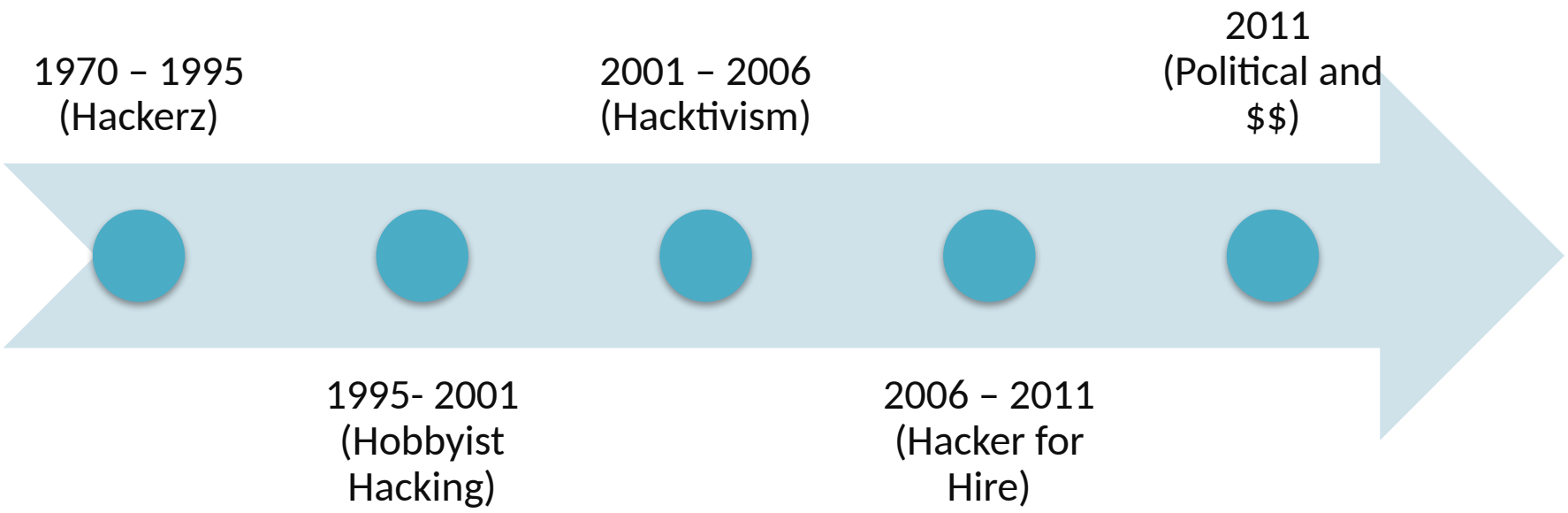




1. Threats can never fully be mitigated, so the strategy is to model or understand what the threats are and how they work
   - "Understanding the Threats"
2. Vulnerabilities Mitigated are either Eliminated, Reduced, or Managed, based on the Risk
   - "Mitigating the Vulnerabilities"
3. The chance of an Exploit being successful can also be reduced through Deterrents and Detectors
   - "Prevention, Detection, Response to Exploits"

THREATS TO UTILITY IT AND SCADA SYSTEMS

Timeline of Attacker Motivation



SQL Slammer Takes out Offshore Production Rig - $1.2 Million in losses (virus / malware)

Problem

In late April 2004, a major US Oil and Gas Producer experienced a sudden blue screen affect on all of their Windows HMI consoles running the Wonderware SCADA application. All HMI consoles crashed to a blue screen state and began to reboot randomly within 15 seconds. An infection of the SQL Slammer worm came in through a connection from a royalty-owner in the platform.

Consequences

Since the operators could not have visual feedback on the HMIs, an emergency shutdown procedure was initiated and production ceased for 8 hours while the HMI functionality was restored. Over $1.2 Million in hard financial losses were experienced from the downtime and fines from lost crude due to market hedging.

Key Control System Recommendations

Technology: Effective firewalls, UTMs, Network AV, and SEM for notification

Policy: All connections with the SCADA systems must be audited

Source: Public Record http://www.ntsb.gov/publictn/2002/PAR0202.pdf

Fired employee plants Trojan to shutdown transport site (intentional malicious insider)

Problem

In 2009, an employee disgruntled at being fired from a major Asian transport site planted a Trojan to wipe out 3 of the site's main SCADA servers. Due to a fault in the Trojan, only one server was completely wiped out.

Consequences

Transport services controlled by the SCADA server were stopped for several days. Several days work was also required to reconstruct the server.

Key Control System Recommendations

Technology: Missing appropriate end point security on SCADA workstations and servers

Policy: Restrict control system access as a prelude to firing employees

Attacks Originating from Asia Targeting Oil and Gas Companies (intentional malicious external agent or nation state)

Problem

In September 2010, several US-based Energy / Exploration and Production companies reported APT-style attacks against their Enterprise IT and SCADA infrastructures. The FBI also became heavily involved in alerting energy companies to these attacks. Some of the oil and gas companies were under attack for over 18 months without noticing that the attackers were stealing valuable corporate and operational data.

Consequences

Executive emails, plant blueprints, I&E one-line diagrams, network diagrams, SCADA real-time tags, DCS configuration data, and financial data were stolen over a period of 18 months. **In one case, the purchase of a Chinese Onshore Processing Facility was undercut by another company using stolen emails and financial data.**

Key Control System Recommendations

Technology : Ineffective firewall configuration, Logging not enabled, **No use of centralized logging, No use of a SEM, lack of security awareness**

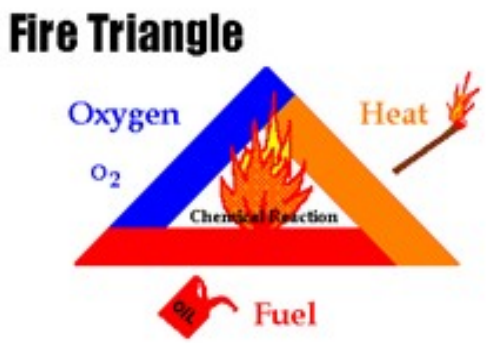
Policy: All devices produce logs and can be easily configured to send security alerts and logs to a central SEM

Source: http://www.kb.cert.org/vuls/id/138633

Threat Vectors

- Malware / Worms
- Phishing Attacks
  - Compromised Websites
  - PDF files with embedded droppers (rootkits)
- **Insecure Remote Access**
- Mobile Devices
  - USB drives
  - Stolen or lost Laptops
- **Insecure Builds or Unmanaged Systems**
  - Computers, Servers, and Routers/Firewalls that are misconfigured / unpatched

Understanding Each Element of a Cyber Attack





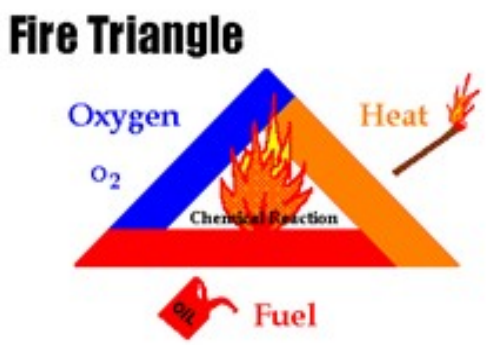
1. ~~Threats can never fully be mitigated, so the strategy is to model or understand what the threats are and how they work~~
   - ~~"Understanding the Threats"~~
2. Vulnerabilities Mitigated are either Eliminated, Reduced, or Managed, based on the Risk
   - "Mitigating the Vulnerabilities"
3. The chance of an Exploit being successful can also be reduced through Deterrents and Detectors
   - "Prevention, Detection, Response to Exploits"

TYPICAL UTILITY IT AND SCADA **VULNERABILITIES**

Actual Current Vulnerabilities Found in SCADA Environments

- SCADA Systems are often on the same corporate LAN system as other network resources, and not segmented into separate subnets.
- Once penetration is made through corporate firewall, internal SCADA computers are susceptible to same attacks (DoS, Trojans, Data Manipulation, etc…) as other internal resources.
- SCADA Systems often have modems or back doors for system support and upgrades from vendors
- Often SCADA systems are left with administrative privileges for print, alarm, and paging services to run properly.
- Computers on SCADA LAN all share common account names and passwords
- Computers and Servers are not regularly patched
- Intrusion Detection Systems and End Point Security products are typically not deployed on SCADA systems (such as Antivirus, Application Whitelisting, IDS, IPS, etc…)
- Event log is not enabled, so there is no log of any unauthorized attempts
- Password Policies either not implemented or not enforced
- Passwords often guessed, so cracking not required
- SCADA protocols are clear text with no authentication or encryption and often routed over public un-trusted 3rd party external telecom networks
- Adult video content, games, movies, music, and unauthorized applications and files found on SCADA Utility Computers

Understanding Each Element of a Cyber Attack



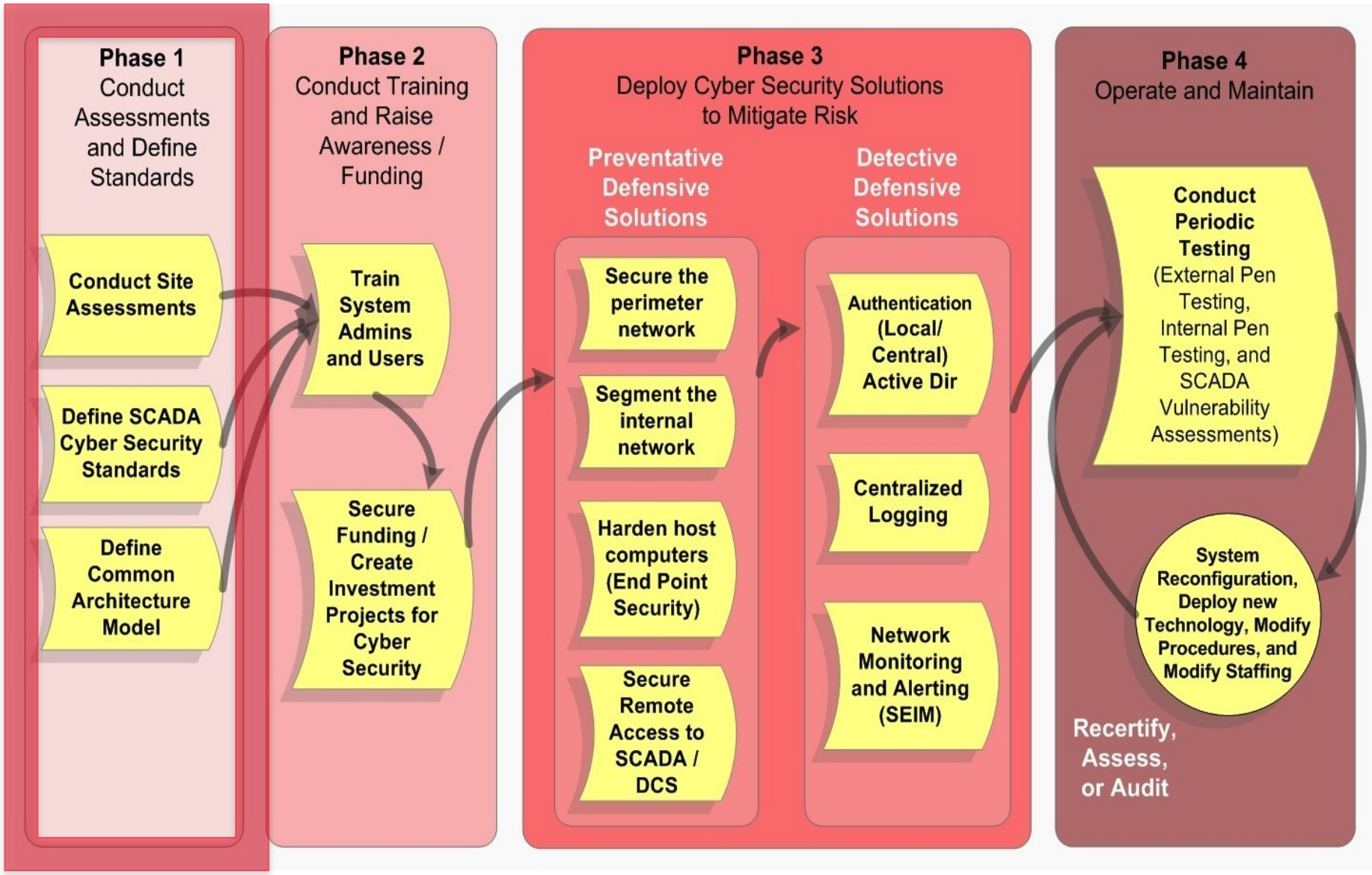


1. ~~Threats can never fully be mitigated, so the strategy is to model or understand what the threats are and how they work~~
   - ~~"Understanding the Threats"~~
2. ~~Vulnerabilities Mitigated are either Eliminated, Reduced, or Managed, based on the Risk~~
   - ~~"Mitigating the Vulnerabilities"~~
3. The chance of an Exploit being successful can also be reduced through Deterrents and Detectors
   - "Prevention, Detection, Response to Exploits"

the exploit market is booming



- Nation States
- Underground
- Commercial market
  - ZDI (HP)
  - iDefence
- Bug bounty programs
  - Luigi Auriemma sold GE vulns to ZDi after GE refused to pay
  - In March 2011, disclosed 34 SCADA specific vulnerabilities all at once… then in September released another bundle of vulnerabilities and exploit code for 6 more SCADA vendors
- Brokers
  - Researchers and Buyers
  - ExploitHub


Phase 1
Conduct Assessments and Define Standards
Conduct Site Assessments
Define SCADA Cyber Security Standards
Define Common Architecture Model
Phase 2
Conduct Training and Raise Awareness / Funding
Train System Admins and Users
Secure Funding / Create Investment Projects for Cyber Security
Phase 3
Deploy Cyber Security Solutions to Mitigate Risk
Preventative Defensive Solutions
Secure the perimeter network
Segment the internal network
Harden host computers (End Point Security)
Secure Remote Access to SCADA / DCS
Detective Defensive Solutions
Authentication (Local/ Central) Active Dir
Centralized Logging
Network Monitoring and Alerting (SEIM)
Phase 4
Operate and Maintain
Conduct Periodic Testing (External Pen Testing, Internal Pen Testing, and SCADA Vulnerability Assessments)
System Reconfiguration, Deploy new Technology, Modify Procedures, and Modify Staffing
Recertify, Assess, or Audit

Active Defense vs. Passive Detection

- **Deterrence** > Firewalls and Secure Remote Access Systems with Strong Authentication are like locks - they are technologies that actively "LOCK" out unauthorized attempts.
  - Like Locking Doors on Your Car
  - In most cases, just **locking the doors** will create enough hassles to deter most people from even attempting to break in.
  - The alarm light blinking on the dash or stickers on the car doors are additional deterrence.
  - Having banners on all digital access that indicate that any unauthorized access will be prosecuted, and IDS systems in place let cyber criminals know that you mean business.

- **Detection** > IDS and Monitoring Systems are like Alarm Systems
  - Monitors the health and performance of the network, host systems, and even applications and devices, and send out alerts when anything is abnormal.
  - Provides notification if someone or something get through the defense
  - Allows historical trending of system performance and security

NIST CYBER SECURITY FRAMEWORK (CSF)

10 Commonly Identified Critical Infrastructure Sectors

1. Food
2. Government
3. Manufacturing
4. Transportation
5. Finance
6. Communications
7. **Water**
8. Safety
9. Energy and Utilities
10. Heath Care

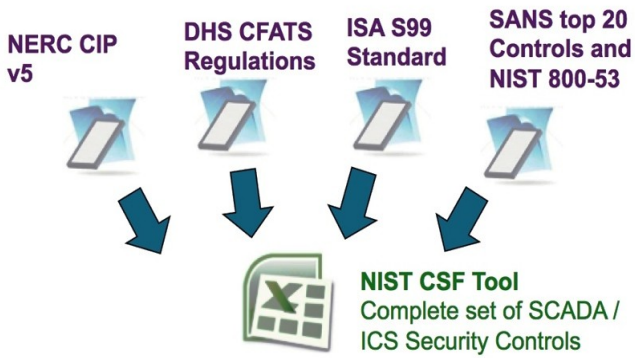


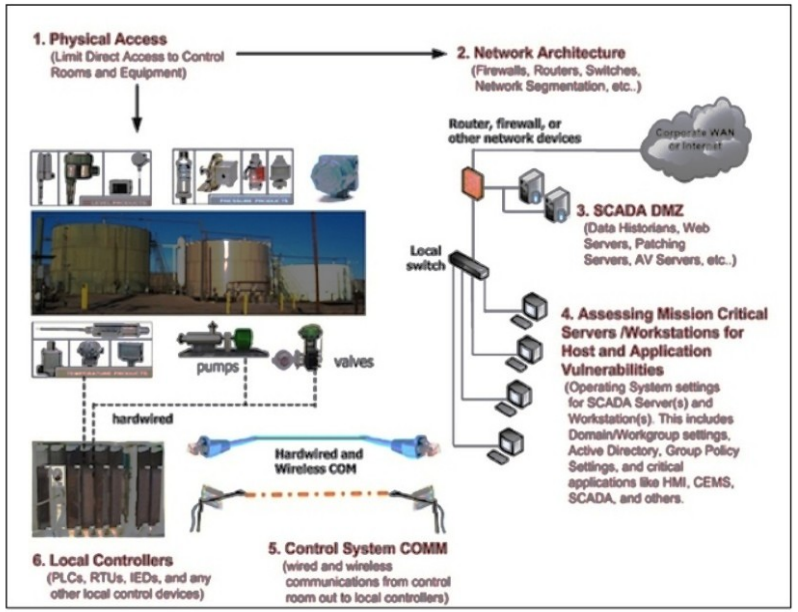



Alphabet Soup of Standards – NERC CIP, CFATS, API, TSA, AWWA, FTA, etc…

- NERC CIP: Electric Power
- CFATS: Chemicals
- API 1164 / AGA 12: Oil and Gas
- TSA Pipeline: Pipelines
- Water/Waste Water AWWA (limited guidelines available)
- HIPPA: Health Privacy Concerns
- PCII: Credit Card Privacy
- FISMA/FIPS: US Federal / Military Systems
- ISO 270001: ISO Framework
- SANS Top 20: Top 20 Controls Mapped to NIST 800-53
- **NIST CSF for Critical Infrastructure >> NEW COMMON FRAMEWORK**

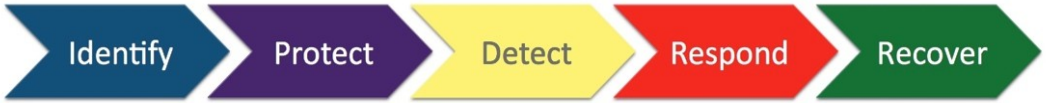
NIST Cybersecurity Framework for Improving Critical Infrastructure





1. Physical Security (preventing physical access to ICS / SCADA components)
2. Network Infrastructure (firewalls, and network segmentation)
3. ICS / SCADA DMZ host systems (Historians, Web-enabled HMIs, and Informational Systems
4. Control Room Host Systems (HMI Workstations, I/O Servers, and Applications)
5. Telemetry Communications (IACS Protocols)
6. Field Devices (PLCs, RTUs, and embedded devices)

Cyber Security Framework Capabilities



http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

Function	Category
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

(Sample) High Risk Gaps from a Controls Framework Assessment

- The controls assessment exposes High, Medium, and Low risk from a Policy/Procedures/Controls perspective. In this sample case, High risk areas included:
  - Defining Cybersecurity Roles and Responsibilities for the Entire Workforce
  - Establishing an Organizational **Information Security Policy**
  - Establishing and Maintaining a Cybersecurity Risk Management Process
  - Protecting Critical Systems with Network Access Controls and **Secure Remote Access**
  - Establishing an **Enforcing the Restriction of Removable Media** on Servers and Workstations

Conclusion

- This proven process has been applied to over 300 Critical Infrastructure clients with IT / SCADA / Automated Industrial Control Systems:
  - 1. Define the **Target State** for the Cyber Security Program
  - 2. **Conduct a Security Assessment** to compare the Current State of the systems to the Target State to uncover technical risk and any missing controls, physical, or technical vulnerabilities
  - 3. **Prioritize the remediation and correction of these security findings** to bring the system up to the desired Target State

Securing Modern District Technology

“If you do it, do it right!”

- Best Practices for Online Remote Access
  - How?
  - Why?

- The Art of the Code
  - Why is it an art?
  - How to find your artist?

Foreign Threats – The Difference Between Paranoia and Actuality

- Point One
- Point Two

How to Make Sure Your Facilities are Digitally Secure

- Penetrations Testing
- Annual Security Audit – Physical and Cyber
- Hacking Prevention / Segregating Personal from District Accounts