Protecting Organizations from Cyber Attack

Cliff Glantz and Guy Landine
Pacific Northwest National Laboratory (PNNL)
PO Box 999
Richland, WA 99352
cliff.glantz@pnnl.gov
guy.landine@pnnl.gov
Key Topics

- Introductions
- Cyber attacks and their consequences
- Adversary capabilities
- Types of attacks / pathways
- Cyber security myths
- Steps for implementing an effective cyber security program
- Cyber security controls
- Resilience in the face of a cyber attack
Introductions

➤ Cliff Glantz
  - Project manager/scientist with ~30 years at PNNL
  - Support various cyber security and critical infrastructure security projects
  - Chair of the Department of Energy (DOE) Subcommittee on Consequence Assessment and Protective Actions
  - Not an expert in technical security controls

➤ Guy Landine
  - Nationally recognized expert in cyber security
  - Leading cyber security expert for the nuclear power industry
  - Expert on technical security controls, defensive strategies, security assessments and forensics.
One of ten DOE national laboratories

A staff of 4,900 mostly based in Richland, WA. Facilities in Seattle, Tacoma, Sequim, and Portland.

One core mission is to “prevent and counter acts of terrorism through applied research”

Well over 100 staff members involved in cyber security projects
Why Should You Care about Cyber Security?

- Cyber attack is a major threat to critical infrastructure:
  - Electric power
  - Telecommunications
  - Water systems
  - Oil and gas (e.g., production, distribution)
  - Medical (e.g., hospitals)
  - Transportation (e.g., vehicles, aviation)
  - Chemical industry

- Have you planned for a major cyber attack that can disable multiple critical infrastructure sectors throughout your region?
- Can you operate under these circumstances?
- Do you train for this?
Cyber Security Background Information

- Scope: Computer networks $\leftrightarrow$ microprocessors
- Malware – “malicious software” designed to disrupt computer operations
- Information Technology (IT) systems – renders data
- Digital Control Systems (DCS) – real-time control of a dynamic system (e.g., machines, pumps, valves)
- Organizations use combinations of IT and control systems
- Example – Electric power utility:
  - IT: email, financial management, power demand
  - DCS: power generation, transmission, distribution
Cyber Attack

- Can be:
  - Logical/digital (e.g., malware)
  - Physical (e.g., bomb)
  - Infrastructure (e.g., power, temperature)
- May originate from either inside or outside of your organization/facility
- May be targeted specifically against your systems or may be a generic attack
- May occur as a result of malicious or non-malicious intent
- May impact one or more systems at a time
- Attacks may occur in combination with other cyber or physical attacks.
What are the Consequences?

The CIA of Cyber Attacks:

- **Loss of Confidentiality**
  - Theft of information

- **Loss of Integrity**
  - System is operational but you cannot effectively control the system or process
  - The bad guy is in the driver’s seat

- **Loss of Availability**
  - Denial of service attack
  - System becomes inoperative or ineffective
Common Perception

BRINGING CIVILIZATION TO ITS KNEES...

Goths

Vandals

Huns

Geeks

Used by permission. Kevin Siers, North Carolina – Editorial cartoons from the Charlotte Observer
Who is Your Cyber Security Adversary?

Threat Agents:
- Hackers / crackers
- Industrial Competitors
- “Insiders”
- Organized Crime
- Extremists / Terrorists
- Nation States
Insider Threat

Types of insider threats:
- Disaffected employees
- Former employees
- Current or former employees in your “industry” (e.g., they are experienced in industry operations, they have used the same hardware or software)

Inadvertent actions:
- Insecure design – Example: Control room simulator
- Productivity errors – Example: Short circuiting cyber defenses in the name of productivity
Organized Crime Threat

**Threat:** Organized crime is using cyber attacks to make billions of dollars per year through:
- Theft
- Extortion
- Commodity market manipulation
- Selling exploits to others

**Real World Example:** In 2008, cyber attacks disrupted electrical power in South America.
- **Impact:** Disrupted power in multiple cities.
- **Cause:** European organized crime syndicate


**No problems acquiring expertise:**
- Purchase expertise and exploits
- Not afraid to use coercion
Extremist/Terrorist Threat

**Threat:** Disruption or destruction of critical infrastructure, (including emergency response services), denial of service of attacks, theft of information, etc.

**Real World Examples:**
- al Qaeda called for "cyber jihad"
- “They will enter the cyber world because it's comparatively remote, comparatively safer than strapping on a bomb” said Cofer Black, former head of the CIA Counter Terrorism Center.
- In 2011, Anonymous conducted denial of service attacks and broke into “secure” computer systems operated by governments and private industry.
Threat: Over 100 countries are actively involved in acquiring cyber warfare capabilities.

Low cost / high impact

Real-World Example: Stuxnet

- Stuxnet worm targets nuclear industry software and equipment in Iran. Stuxnet impacts only clandestinely obtained Siemens control systems.
- Damages plant infrastructure causing extended shutdowns at Iranian nuclear facilities.
- Speculation is that a worm of such complexity could only be developed by a nation-state.
Ways of Launching a Cyber Attack

- Malware coming from the internet (e.g., viruses, worms)
  - compromised websites
  - email attachments
- Malware coming from a trusted source
  - commercial hardware and software
  - vendor access / upgrade packages
- Wireless break-ins
  - Signal range is much greater than most suspect
  - Attacker can monitor wireless signals for extended periods
  - Attacker can overpower legitimate traffic.
Ways of Launching a Cyber Attack (cont)

- Social engineering
  - Phishing attacks
  - USB Storage devices (e.g., parking lot test)
  - Threats/intimidation
  - Take advantage of people’s goodness
- “Inappropriate” connections
  - Inappropriate links between business/corporate networks and plant control system networks
  - Overuse of administrative privileges
- Compromise data storage (e.g., records, cloud computing)
Attacking Tools
Threat to Emergency Managers

- Loss of confidential information
- Loss of availability or integrity:
  - Communications
  - situational awareness
  - computational and information resources
  - command and control functions.
Myth: “We have security by obscurity”

- “My systems are too old and obscure to be interest to attackers.”
- “No one can understand what my system is doing – they can break in but they could not figure out how to abuse the system”
- System, language, and control information is readily available on the Internet.
- Exercises have shown that given enough time and interest, a hacker can crack and take over most systems.
Myth: “Our firewalls and anti-virus software protect us from attack”

- Provide protection from what?
  - Known viruses/worms
  - Some attack pathways
- A firewall is only as good as its configuration
- Purpose: **Deter, delay, detect, & deny**
- Are firewall logs being monitored to detect an ongoing attack?
- Anti-virus tools only protect you from known viruses. Zero-day viruses cannot be stopped.
- There may be multiple pathways around (or through) firewalls and anti-virus products.
Myth: “We have no insider threat!”

- Even the most secure organizations cannot discount the threat posed by insiders (current or former staff members)
- Co-workers tend to protect colleagues
- Managers tend to protect their team members. “John/Jill is having a tough time right now, but they will pull through this.”
- It is psychologically easier to mount a cyber attack than a physical attack.
- Non-malicious activities or the failure to follow security policies can turn out to be the insider threat that poses the greatest risk.
Steps for Instituting an Effective Cyber Security Program

- Examine organization- or corporate-wide cyber security practices
- Identify important computer/digital assets
- Conduct table top reviews
- Conduct walk-through inspections and validation testing
- Assess potential threats, attack vectors, and vulnerabilities
- Determine the consequences of compromise
- Perform simple risk assessments
- Evaluate “new” security controls and make risk-based decisions on security enhancements
- Maintain an ongoing cyber security program
Effective cyber security requires a recognition of the threat, vulnerabilities, consequences, and defensive measures.

Requires an organizational response at the management, operational, and technical levels.

National Institute of Standards and Technology (NIST) defines a suite of security controls in NIST-800-53.

**Management Class of Security Controls**
- Program Management
- Planning
- Security Assessment and Authorization
- System and Service Acquisition
- Risk Assessment
Security Controls (cont)

- **Operational Class of Security Controls**
  - System and Information Integrity
  - Awareness and Training
  - Configuration Management
  - Maintenance
  - Media Protection
  - Contingency Planning (Continuity of Operations)
  - Incident Response
  - Personnel Security
  - Physical and Operational Environmental Protection
Security Controls (cont)

- Technical Class of Security Controls
  - Access Control
  - Audit and Accountability
  - Identification and Authentication
  - System and Communications Protection

- The three classes of security controls are divided into 19 families, which contain close to 140 security controls. Each security control has a number of required elements.
20 Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines

Critical Controls Subject to Automated Collection, Measurement, and Validation:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations of Network Devices Such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based On Need to Know
Top 20 Critical Security Controls (cont)

10. Malware Defenses
11. Continuous Vulnerability Assessment and Remediation
12. Account Monitoring and Control
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

Controls not directly supported by automated measurement and validation:
16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Training
Top Four Mitigation Strategies To Protect Your IT System

1. Rigorously conduct system patching
   • Do not let known vulnerabilities persist for extended periods of time

2. Restrict administrative privileges
   • Accounts with these privileges are prime targets for attackers
   • Limit and tightly control accounts with these privileges

3. Perform and enforce application whitelisting
   • Only allows authorized applications to run

4. Implement defense in depth
   • Do not rely on one single technology or defensive measure; have multiple security controls in case one approach fails.
Implement a Defensive Architecture

Define a series of concentric defensive levels (or layers) of increasing cyber security to protect critical systems
Define acceptable types of communications occurring between assets that are maintained at different security levels.
Resilience is the ability of systems to resist, absorb, and recover from an attack.
Components of Resiliency

- **Resistance** is the ability to limit damage. Identify a successful attack/incident and mitigate negative impacts before they happen. *Defensive controls are in place to stop an attack/incident from reaching a computer system; resistance controls only come into play after malware reaches the computer system.*

- **Absorption** is the ability of the system to experience an attack, sustain damage, and compensate to recover from the attack. This may involve a slow and graceful failure -- providing time for mitigating actions.

- **Restoration** is the ability to rapidly repair, reconstitute, or replace damaged/disabled services and return to an acceptable level of functionality.
Scoring Resilience

Scoring the Components of Resilience (10 Point scale)

Net Resilience Score (0 to 1)
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?

YO! DUDE... BACK HERE

CYBER SECURITY
A New Age of Cyber Security is Dawning

- There are a lot of adversaries looking for easy routes for cyber attacks
- An effective cyber security program will:
  - Enhance overall security
  - Take time and resources to implement
  - Provide a level of risk you can live with.
- Resilience is an important component in any cyber security program.
- Don’t get caught with your pants down! Be proactive in your planning!
Questions, Concerns, Comments?

Cliff Glantz
PNNL
PO Box 999
Richland, WA  99352
509-375-2166
cliff.glantz@pnnl.gov