Introduction to Critical Infrastructure Industrial Control System (ICS) Cybersecurity
Famed German Philosopher Friedrich Nietzsche once wrote:

“Those that were dancing were thought insane by those that couldn’t hear the music”

This is a great metaphor for the state of ICS Cybersecurity in the US today.
• My name is Randy Kirkendoll
  o Chief Operating Officer, Redi Automation, LLC
  o Registered EE PE – primarily in Control Systems (over 40 years experience)
  o Certified Cybersecurity Analyst (GIAC GSEC)
  o Steering Team Member of DHS Industrial Control Systems Joint Working Group (ICSJWG)
  o Member FBI INFRAGARD System, Denver, CO network, Energy Sector
  o ICS partner with the Arizona Cyber Warfare Range
  o ISA Member
  o Certified Rockwell Automation Systems Integrator
  o Certified Solution Partner with Bedrock Automation
  o Certified Wonderware Systems Integrator
  o Certified Inductive Automation Ignition Systems Integrator
  o SI for numerous other products
Director of the National Security Agency (NSA) 
Admiral Michael Rogers 
Has a message for industries of all kinds in the US: 
“It is not a matter of if, it is a matter of when your control system will be attacked”.

Deputy Director of the National Security Agency (NSA)
Rick Ledgett
June 2016:
“...industrial control systems and other critical infrastructure assets are vulnerable to cyber attacks as infrastructure providers fail to address security risks”.
DHS Deputy Assist Sect. for Cybersecurity and Comm’s Greg Touhill and ICS CERT Director Marty Edwards at a recent briefing with the ICSJWG team:

“Last year ICS CERT investigated 295 incidents of cyberattacks on critical infrastructure control systems in the US.”
DHS: Cyberattacks on critical manufacturing doubled in 2015

The Department of Homeland Security investigated almost twice as many cyberattacks on the
Of those, 97 were attacks against critical manufacturing sector (automobile & aircraft mfg), 46 were against the energy sector, 25 involved water/wastewater, and 23 against transportation systems.
Methodology and Survey Details

- A total of 540 online surveys were completed in the United States (165), Canada (125), Germany (125) and the United Kingdom (125) during June 2016.

- In order to qualify for participation in the survey, respondents had to be a CIO, IT manager, IT director, CISO or in a related role; and knowledgeable about security issues within their organization.

- A total of 21 questions were included in the survey.

- The mean number of employees at the organizations surveyed was 5,443; the mean number of email accounts was 3,616.

From a survey taken in June 2016 (For Malwarebytes)
Ransomware Penetration in Top Industries Surveyed

The top five industries represented in the survey are financial services, manufacturing, government, healthcare and high tech.

Ransomware penetration is substantially higher in two of the five: financial services and healthcare.
Security Attacks Over the Past 12 Months

Asked of all respondents

The largest proportion of security attacks have been against US organizations.
The reason we are here today is to convey from the Department of Homeland Security the need for critical infrastructure organizations to take Industrial Control System Cybersecurity threats seriously as it poses a potentially crippling danger to your organization. This includes dangers to the human, environmental, operational, financial, and the reputational health of your organization.
Threat Trends in ICS’s

![Threat Trends Chart]

- ICS Application Specific Malicious Code (STUXNET)
- HAVEX/Dragonfly
- Rogue VPN Tunnel Attacks
- ICS Attack Proof-of-Concept
- SCADA Enumeration Scripts
- Command and Control Distributed Attack Tools
- N.A. ONG Cyber Campaign
- Application Specific Malicious Code
- Automated Probes and Scans
- Password Cracking
- Exploiting Known Vulnerabilities
- Hijacking Sessions
- Sniffers
- Packet Spoofing
- Denial of Service
- 0-Day Vulnerabilities
- Code Injection
- Back Doors
- Disabling Audits
- Self-Replicating Malicious Code
- Password Guessing

Risk Curve Likelihood/Consequences

→ Advanced Persistent Threat (APT)
Why is it easier to attack systems today?

Meet “Shodan”
Shodan Search Engine for Internet Facing ICS IP Addresses (Rockwell Automation)
Multiple unspecified vulnerabilities on the Rockwell Automation AB MicroLogix 1100 and 1400 controllers allow remote attackers to obtain privileged access or cause a denial of service (RAS) via unknown vectors.

Open redirect vulnerability in the web interface in the Rockwell Automation ControlLogix 1756-ENBT/ETA EtherCAT/IP Bridge Module allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.

The FactoryTalk (FT) PNAdiagReceiver service in Rockwell Automation Allen-Bradley FactoryTalk CPSR through SRS and RSLogix 5000 17 through 28 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted packet.

Buffer overflow in RISEvd.dll in RSI-Ware.exe in the DCS Hardware Installation Tool 1.0.5.1 and earlier in Rockwell Automation RSLogix RT/Link Classic before 2.58 allows user-assisted remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a malformed .edit file.

The web interface in the Rockwell Automation ControlLogix 1756-ENBT/ETA EtherCAT/IP Bridge Module allows remote attackers to obtain "Internal web page information" and "Internal information about the module" via unspecified vectors. NOTE: this may overlap CVE-2002-1163.

Rockwell Automation ControlLogix Connected Components Workbench (CCW) before 7.00.00 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an invalid property value to an ActiveX control that was built with an outdated compiler.

Multiple cross-site scripting (XSS) vulnerabilities in the web interface in the Rockwell Automation ControlLogix 1756-ENBT/ ETA EtherCAT/ IP Bridge Module allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Unspecified vulnerability in Rockwell Automation FactoryTalk Diagnostics Viewer before V2.30.00 (CPVR 503) allows local users to execute arbitrary code via a crafted FactoryTalk Diagnostics Viewer (ftd) configuration file, which triggers memory corruption.
Shodan Search Engine for Internet Facing ICS IP Addresses (Siemens)
Shodan Search Engine Exploits For Siemens Controllers
Shodan Search Engine Exploits
For GE Controllers

Multiple stack-based buffer overflows in the KeyHelp.KeyCtrl.1 ActiveX control in KeyHelp.occ 1.2.3.1.2 in KeyWorks KeyHelp Module (aka the HTML Help component), as used in EMC Documentum Application Developer Desktop 5.4; EMC Captiva QuickScan Pro 4.6 SP1; GE Intelligent Platforms Proficy Historian 3.1

GE Proficy CIMPLICITY gefebst.exe Remote Code Execution
by metasploit

Linux HA Heartbeat <= 2.0.6 - Remote Denial of Service Vulnerability
by Yen Hong Sa

The (1) CimView and (2) CimEdit components in GE Proficy HMI/SCADA-CIMPLICITY 8.2 and earlier allow remote attackers to gain privileges via a crafted CIMPLICITY screen (aka .CMF file).

GE Fanuc Real Time Information Portal 2.6 writeFile() API Exploit (meta)
by Kevin Prizeman

GE Proficy Real Time Information Portal Credentials Leak (sniffer (meta)
by Kevin Prizeman

BITTracker <= 1.4.1 (become admin) Remote SQL Injection Vulnerability
by mudge (c0s)
Latest Known Major Attacks/Tools

• Blackenergy – RAT – Remote Access Trojan
• Havex - RAT
• Stuxnet
• Ukraine attacks shut down 40% of their power grid in December 2015 (Black Energy Trojans found throughout)
• German Steel plant cyber attack causes massive damage
• US Natural Gas Pipeline Attacked on 39 IP addresses
German nuclear plant suffers cyber attack designed to give hackers remote access

A nuclear power plant in Germany has been found to be infected with computer viruses, but they appear not to have posed a threat to the facility's operations because it is isolated from the Internet, the station's operator said on Tuesday.
Types of bad actors/attackers

- Disgruntled former employees
- Accidental hacking from poor cyber hygiene and management
- Hactivists who have a personal philosophical with your organization
- Internal threats – full time employees with a grievance, independent contractors, interns, other staff.
- External threats – third party co’s, competitors, suppliers, vendors, outsourced IT or tech support
- Organized crime from around the world
- Nation states (China, Russia, North Korea, Pakistan, Iran)
- Entire darkweb communities just like regular internet with full compliment of cyberattack tools and services that can be bought or hired.
Cybersecurity science has created a few different models for a cyber attack. The most well known models are:

- The Mandiant APT Attack Lifecycle (now FireEye)
- The Lockheed Martin Cyber Kill Chain
The Mandiant APT Attack Lifecycle
## Lockheed Martin Cyber Kill Chain

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reconnaissance</strong></td>
<td>• Harvesting email addresses, conference information, etc</td>
</tr>
<tr>
<td><strong>Weaponization</strong></td>
<td>• Coupling exploit with backdoor into deliverable payload</td>
</tr>
<tr>
<td><strong>Delivery</strong></td>
<td>• Delivering weaponized bundle to the victim via email, web, USB, etc</td>
</tr>
<tr>
<td><strong>Exploitation</strong></td>
<td>• Exploiting a vulnerability to execute code on victim system</td>
</tr>
<tr>
<td><strong>Installation</strong></td>
<td>• Installing malware on the asset</td>
</tr>
<tr>
<td><strong>Command &amp; Control</strong></td>
<td>• Command channel for remote manipulation of victim</td>
</tr>
<tr>
<td><strong>Actions on Objectives</strong></td>
<td>• With “Hands on Keyboard” access, intruders accomplish their original goal</td>
</tr>
</tbody>
</table>
## Model Comparison

<table>
<thead>
<tr>
<th>Model</th>
<th>Lockheed Martin Cyber Kill Chain</th>
<th>Mandiant APT Attack Lifecycle Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-compromise</td>
<td>Reconnaissance</td>
<td>Initial reconnaissance</td>
</tr>
<tr>
<td></td>
<td>Weaponization</td>
<td>Penetration</td>
</tr>
<tr>
<td></td>
<td>Delivery</td>
<td></td>
</tr>
<tr>
<td>Compromise and</td>
<td>Exploitation</td>
<td>Gaining a foothold</td>
</tr>
<tr>
<td>maintaining a presence</td>
<td>Installation</td>
<td>Appropriating privileges</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal reconnaissance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintain presence</td>
</tr>
<tr>
<td>Post-compromise &amp;</td>
<td>Command and Control</td>
<td>Exfiltration</td>
</tr>
<tr>
<td>external communication</td>
<td>Actions on Objectives</td>
<td>Mission accomplished</td>
</tr>
</tbody>
</table>

Increasing cost and difficulty to stop attack
Key Aspects of Cyber Attack Vectors

• C I A

  o Confidentiality – private information (credit card information, bank accounts, financial information, user names, passwords, etc) while data is in transport or rest. (Ransomware, identity theft)

  o Integrity - Is the information from who it says it is? Is the information as initially sent unchanged. (ARP Poisoning)

  o Availability – Is the information being transacted in a timely manner? Is it on time? (DOS, DDOS). Is it available at all? (control systems focus here)
Types of Attacks on ICS’s

- Viruses
- Worms
- Logic bombs
- Cloned devices
- Cloned software
- Operators
- Maintenance
- Engineering
- Bad code
- DoS & DDoS attacks

Client Management Computers

Networks

Controllers

Sensors/Actuators
US Government Support for Cybersecurity

**Technical Support**
- Department of Homeland Security (DHS)
- National Cybersecurity & Communications Integration Center (NCCIC)
  - US Computer Emergency Response Team (US CERT)
  - Enterprise Cybersecurity
  - Industrial Control System Cyber Emergency Response Team (ICS CERT)
  - Critical Infrastructure Cybersecurity
  - ICS Joint Working Group (ICS/WG)
  - Joint Government/Private Sector Org

**US Government Cybersecurity Support Organizational Structure**

**Law Enforcement**
- Department of Justice (DOJ)
  - Federal Bureau of Investigation (FBI)
    - FBI INFRAGARD System
    - Law Enforcement Arm Of Government Cybersecurity Support
Several Organizations dealing with ICS Cybersecurity Standards

- NIST – National Institute of Standards and Technology
- NERC – North American Electric Reliability Council
- AGA – American Gas Association (for gas producers and pipelines)
- API - American Petroleum Institute (for oil producers and pipelines)
- US Department of Transportation (for transportation systems and pipelines)
- ISA – International Society of Automation (ISA/IEC 62443 Standards)
- Department of Homeland Security – ICS CERT (Industrial Control Systems Cyber Emergency Response Team)
- Council On Cybersecurity – Created the “Critical Security Controls”
DHS ICS CERT & the FBI subdivides into 16 Critical Infrastructure Groups

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy

- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems
The Council On Cybersecurity was formed by:

- DoD (Department of Defense)
- US- CERT
- DoD Cyber Crime Center (DC3)
- Military Investigators (Cyber)
- The FBI and police units
- DoE Laboratories
- Dept. of State
- Army Research Labs
- DHS
- Forensics Experts (DoD and private)
- The SANS Institute
- Civilian Penetration Testers
- Federal CIOs and CISOs
- Plus more than 100 other collaborators
They have identified 20 Critical Security Controls

1. Inventory of auth. & unauth. devices
2. Inventory of auth & unauth software
3. Secure configurations H & S on laptops, W/S’s, and Servers
4. Continuous Vulnerability Assessments and Remediation
5. Malware Defenses
6. App software security
7. Wireless Device Control
8. Data Recovery Capability (validated manually)
9. Security Skills Assessment and Training to fill the gaps
10. Secure configurations on network devices (firewalls, routers, and switches)
They have identified 20 Critical Security Controls

11. Limitation of Control on network ports, protocols, serv’s
12. Controlled use of admin privileges
13. Boundary Defenses
14. Maintenance, monitoring, and log analysis
15. Controlled access based on need to know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response Capability
19. Secure Network Engineering
20. Penetration Testing and Red Team Exercises
1. Application Whitelisting (38%)
2. Ensure proper configuration/patching (29%)
3. Reduce your attack surface (17%)
4. Build a defendable environment (9%)
5. Manage Authentication (4%)
6. Monitor and Respond (2%)
7. Implement Secure Remote Access (1%)
Redi Automation Recommended Additions To ICS CERT Minimums

1. **Must** implement a fully layered “Defense In Depth” strategy.
2. **Must** have accurate asset identification on all system hardware and software (system audit).
3. **Must** have real change management processes at all times.
4. **Should** perform vulnerability assessments and remediate all high priority risks. Without this you won’t know what to protect or how.
5. **Should** have ICS Cybersecurity Incident Response Plan for the facilities that have been well thought out and tested.
6. **Should** have ICS Cybersecurity Policies and Procedures
Redi Automation has created a program to implement the 7 minimum essentials identified by the DHS called:

“The Redi Automation Defense in Depth Program”

We have assembled a complete set of tools for our clients to use that meets the intent of the 7 Essentials recommended by the Department of Homeland Security.
1. App Whitelisting – Servers, Clients, Hosts
2. Proper Configuration & patching – Servers, clients, & hosts
3. Reduce Attack Surface – Isolate untrusted networks, lock down unused ports, turn off all unused services, use one way data diodes where possible.
4. Build a Defendable Environment – Divide networks into logical enclaves. Restrict peer to peer comms to only those needed.
5. Manage Authentication – Use multifactor authentication. Implement secure password policies, separate corporate and control system networks, reduce use privileges to only those needed.
7. Implement Secure Remote Access – Only allow remote access if needed. Use secure means if possible (e.g. VPN tunneling). Limit access, implement strict access controls (timed access, etc), use multifactor authentication
ICS Defense In Depth Strategies

Table 2. Defense-in-Depth strategy elements.

<table>
<thead>
<tr>
<th>Defense in-Depth Strategy Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Management Program</strong></td>
</tr>
<tr>
<td>- Identify Threats</td>
</tr>
<tr>
<td>- Characterize Risk</td>
</tr>
<tr>
<td>- Maintain Asset Inventory</td>
</tr>
<tr>
<td><strong>Cybersecurity Architecture</strong></td>
</tr>
<tr>
<td>- Standards / Recommendations</td>
</tr>
<tr>
<td>- Policy</td>
</tr>
<tr>
<td>- Procedures</td>
</tr>
<tr>
<td><strong>Physical Security</strong></td>
</tr>
<tr>
<td>- Field Electronics Locked Down</td>
</tr>
<tr>
<td>- Control Center Access Controls</td>
</tr>
<tr>
<td>- Remote Site Video, Access Controls, Barriers</td>
</tr>
<tr>
<td><strong>ICS Network Architecture</strong></td>
</tr>
<tr>
<td>- Common Architectural Zones</td>
</tr>
<tr>
<td>- Demilitarized Zones (DMZ)</td>
</tr>
<tr>
<td>- Virtual LANs</td>
</tr>
<tr>
<td><strong>ICS Network Perimeter Security</strong></td>
</tr>
<tr>
<td>- Firewalls/ One-Way Diodes</td>
</tr>
<tr>
<td>- Remote Access &amp; Authentication</td>
</tr>
<tr>
<td>- Jump Servers/ Hosts</td>
</tr>
<tr>
<td><strong>Host Security</strong></td>
</tr>
<tr>
<td>- Patch and Vulnerability Management</td>
</tr>
<tr>
<td>- Field Devices</td>
</tr>
<tr>
<td>- Virtual Machines</td>
</tr>
<tr>
<td><strong>Security Monitoring</strong></td>
</tr>
<tr>
<td>- Intrusion Detection Systems</td>
</tr>
<tr>
<td>- Security Audit Logging</td>
</tr>
<tr>
<td>- Security Incident and Event Monitoring</td>
</tr>
<tr>
<td><strong>Vendor Management</strong></td>
</tr>
<tr>
<td>- Supply Chain Management</td>
</tr>
<tr>
<td>- Managed Services/ Outsourcing</td>
</tr>
<tr>
<td>- Leveraging Cloud Services</td>
</tr>
<tr>
<td><strong>The Human Element</strong></td>
</tr>
<tr>
<td>- Policies</td>
</tr>
<tr>
<td>- Procedures</td>
</tr>
<tr>
<td>- Training and Awareness</td>
</tr>
</tbody>
</table>
Other Redi Automation’s ICS Cybersecurity Services

- Asset identification through network passive scanning and system audits
- Network audit for traffic analysis & risk assessments
- ICS Cybersecurity project management
- Full Defense in Depth Planning

- ICS Incident Response plan development
- Cyber PHA facilitation (we also facilitate full PHA’s)
- ICS Cybersecurity Policies, Procedures, & Specifications
- ICS Cybersecurity Training
- We are also a full services systems integrator for a variety of systems
Redi Automation’s ICS Cybersecurity Systems

Redi Automation is working with several equipment and system suppliers at the leading edge of ICS cybersecurity technology:

• Bedrock Automation – the most advanced and cyber secure control platform on the planet.
• Radiflow – Leading the way with cyber secure industrial control routers, switches, gateways, intrusion detection systems, and intrusion protection systems
• Using a variety of hardware and software tools to assist clients in mapping their ICS networks and assuring their systems are secure and locked down
We are a partner with the Arizona Cyber warfare Range (AZCWR.org), one of the most advanced and respected training organizations in Cybersecurity in the US. In partnership with the AZCWR we are setting up the only live fire cyber warfare range for control systems in the US.
Redi Automation

Redi Automation is working with Federal Authorities to get the message out to the industrial community as to the significance of the ICS Cybersecurity problem.

If you own a computer, you are at war right now! You do not have a choice in the matter.

The choice you do have is what you are going to do about it. If you are in a war zone and you have no defense, no plans, and do not know what the attackers plans and tools are, how can you possibly defend yourself? What will be YOUR outcome?
Redi Automation would like to thank you for the opportunity to speak with you today. We are also prepared to help your organization to create a defense that makes sense for your facilities and assets. We have the tools and training to help you to create a “Defense in Depth” strategy that will work for you.

Questions?