SECURITY TRANSFORMATION
FOR INDUSTRIAL CONTROL ENVIRONMENTS

FEBRUARY 2015
Summary

- Traditionally, information technology (IT) and operation technology (OT) are managed as siloed domains.
- Underlying technology of OT systems is swiftly beginning to resemble IT systems.
- There is a need to establish integrated enterprise policies for OT and IT solutions.
- An integrated environment enables a data driven value chain to better convert real time data into actionable intelligence.
CONVERGED TECHNOLOGY AND SECURITY
ICS Evolution

1970-1980
• Isolated subsystems with proprietary protocols

1980-1990
• Interlinked subsystems with proprietary protocols

1990-2000
• Fully embedded systems with open protocols utilizing COTS technology

2000-beyond
• Increased interconnectivity
• Demand for operational data outside OT environment
• Active research on ICS System vulnerabilities

What are the challenges?
Siloed Domains

- Ever increasing automation
- Technology advancements, increasing efficiency and productivity, while reducing human errors
- Increased use of common IT platforms within the PCD (e.g. Windows OS, SAP, etc.)
- Increased interconnectivity between the Enterprise IT and PCD domains
- The need for faster decision making through trending, advanced analysis and analytics
**Key Differences**  
(ICS Security vs. Information Security)

- **Availability:**  
  Availability and uptime is the most important (focus is on systems rather than information/data)

- **Integrity:**  
  Health and Safety has the highest priority (heavy engineering culture)

- **Confidentiality:**  
  ICS are (historically) more isolated than IT systems and sophisticated protective mechanisms are not the norm

- **Availability:**  
  ICS typically remain relatively static for years and are maintained manually

- **Integrity:**  
  ICS are tightly integrated proprietary systems that are generally custom built and foreign to IT
Lessons from IT

Over the years, enterprise IT has developed a number of architecture patterns, security controls, and technologies for information security. These approaches can provide excellent security and mitigate cyber risk. However, they often have difficulties translating to the OT world because:

- Uptime requirements dictate very little downtime for OT environments, including for tasks such as patching;
- IT assets are often retired after less than 5 years while OT environments last for decades;
- OT vendors and vendor relationships are often developed without inclusion of security requirements, and many OT vendors are not mature in security capability;
- OT is heavily decentralized with standalone systems in each asset while IT lives within specific datacenters.
New Risk Dimensions

TRADITIONAL RISKS
- Theft of assets
- Critical equipment failure
- Health and safety
- Compliance and Regulatory
- Environment
- Human error
- Misuse of assets and facilities
- Physical Espionage

ANALOG ICS

EMERGING RISKS
- Cyber Espionage
- Cyber attack, including national state attacks
- Privacy risks
- Unavailability of critical systems
- Critical systems failure
- Interconnectivity risks
- Loss of critical data
- Automation errors and mis-configurations
- Leakage of confidential information
- Misuse of systems and equipments
- Data Integrity risks

DIGITAL ICS

CURRENT RISK LANDSCAPE IS MORE COMPLEX

TIME
- 1990
- 2000
- 2010
- 2020

RISK SIZE
What is needed is a structured, strategic approach to designing in security to an organization so that it can be blended into everyday activities in a sustainable way.
Impact of a Strategic Approach

Increasing Capabilities Over Time

Your security spend

- Lost to Friction
- Strategic
- Tactical

Cyber Security Risk Over Time
Risk of Inappropriate Spend Over Time

Pressure to “reduce risk NOW”
Dynamic areas of change

---

### Business Delivery “Stack”

- **Business Layer**
  - Industry Leading Practices
  - Geopolitical Drivers
  - Business Process
  - Corporate Objectives

- **Enablement Layer**
  - Application
  - Data

- **Infrastructure Layer**
  - Servers/Hosts
  - Networks
  - Physical Environment

---

### Areas of Dynamic Change

- Slow Economic Recovery
- Driving Growth & Profitability
- New Products/Services
- Mergers/Acquisitions
- Globalization
- Strategic Sourcing
- Competitive Differentiation
- Increased Regulatory Scrutiny

- Mobile & Cloud Deployments
- “Big Data,” BI & Analytics
- Self-service & Consumerization

- Virtualization & Cloud Platforms
- Internetworking/VPNs
- New Operating Systems
- Low-cost Computing Models
- Changing Data Center Models
Approach

Governance

People

Processes

Technology

Portfolio, Program and Project Management

Vendor & Supplier Management

Risk Management

Compliance

Business Strategy and Goals

Assets

Intelligence

Regulatory Environment

Ownership

Accountability

Policy

Funding & Sponsorship

Implementation

Planning and Control

Understanding

Foundations

Planning and Control

Understanding

Foundations

Implementation

Governance

Portfolio, Program and Project Management

Vendor & Supplier Management

Risk Management

Compliance

Business Strategy and Goals

Assets

Intelligence

Regulatory Environment

Ownership

Accountability

Policy

Funding & Sponsorship
An organization has some concerns in regards to how it’s Operational Technology [OT] cybersecurity risk is being addressed.

First steps would be to undertake a current state assessment - Identify key stakeholders and understand organizational risk appetite, governance processes, compliance requirements, risk and control frameworks and their implementation.

The outputs from this stage would be assessed to understand how comprehensive the program / projects / functions vision is.
Typically we find: **No** ICS involvement in the security governance process
Create a structure that includes appropriate ICS stakeholder involvement the definition of roles and responsibilities and the delivery of ICS specific policies and metrics.

Note: Each organization is unique and cultural and political issues must be addressed if any new governance regime is to operate effectively.
Typical Findings
Understanding

Typically we find:

**Business Strategy and Goals:** Security strategies not aligned with the production business strategies. Existing strategies tend to focus strongly on Confidentiality assurance with lesser emphasis on Integrity and Availability.

In the OT domain the focus should be reversed with supply/production chain assurance being a key driver - in sectors where there are safety risks integrity may take precedence.

**Assets:** Nature of ICS Assets are poorly understood. Only parts from when the ICS systems were first installed are only elements in inventory. Network diagrams are usually not available or are wildly inaccurate and there is no recording of the information assets, or their security attributes.

**Intelligence:** No real threat monitoring in the ICS space or ability to take action if imminent threats are discovered.

**Regulatory:** Heavily regulated industries tend to focus on compliance in the reliability of service, Environmental monitoring and HSSE space. Security requirements tend to have a lesser focus unless an incident has occurred.
Typical Findings
Planning & Control

Typically we find:

Risk: Engineers do not “buy in” to IT security risk management techniques. We use a mechanism known as the Risk Bowtie. This is a threat-oriented and qualitative assessment methodology that aligns with the Process Safety Bowtie. Its uptake in the engineering community is good because these techniques are normally organizationally relevant and understood.

Compliance: Deploying the appropriate mechanisms to protect ICS assets needs to be tested. This is especially true in regulated industries. We typically find that if they do exist compliance checks are performed manually and implemented poorly.
How to Get Started

1. Determine Risks
2. Create Standards
3. Assess Gaps
4. Implement

ICS

Create Program Plan

- Americas
- Europe
- APAC
- Middle East
- South America
- Africa

- Facility
- Q1 Rating
- Q2 Rating
- Score

- Key
- Score: 1=poor performance
- Score: 2=fair performance
- Score: 3=good performance
- Score: 4=excellent performance

- Threats
- Consequences
- Barriers

- Business Unit
- Site
- Performance Rating
- Score
Determine Risk

- Decrease Likelihood of Top Event
- Decrease Impact of Top Event
Create Standards

Portable media is key – enforcing A/V in advance of media entering the ICS environment. Patching will require close MAC involvement.

Event logs should be generated and analysed considering bandwidth and latency impacts of centralised analysis; A/V should be evaluated for implementation on HMI / historians / OPC.

Network architecture should maintain containment between ISA-99 zones. IR plans should focus on isolating events and escalating correctly.

Documentation is key, however IT-style tests of effectiveness are unlikely except in large, green field capital projects.

Prepare
- Governance and Risk Management
- Workforce Development
- Management of Change
- Asset Inventories

Prevent
- Access Control
- Portable Media & Portable Computers
- Operating System Security Patches
- System Hardening

Detect
- Event Log Management
- Anti-Virus

Respond
- Network Architecture
- Incident Response

Recover
- Backup and Restore
Assess Gaps
Create Program Plan

Understanding
- Define ownership, accountability, funding and sponsorship, business goals, asset environment, threat environment, regulatory demands

Assess Current Capabilities
- Assess your current state and your understanding model against these capabilities to produce a future state, resulting in a gap list

Portfolio Gap Assessment
- Compare gaps in current state versus future state against existing projects, producing a list of projects to execute
EMERGENCE OF DISRUPTIVE TECHNOLOGIES
Future Trends in ICS

• Increased use of advanced process control software
• Further integration with IT communication protocols
• Increased use of mobile applications and web infrastructure
• Integrated sensor networks with embedded IT
• Growing use of industrial wireless for process control
• Adoption of virtualization for improved availability
• **Advanced, Standardized, Integrated & Connected**
Future Trends in Information Security

- Increased move to threat-centric security management
- Increase in quality and dispersion of smart sensor adding more process information AND more security event information
- Automation in configuration management and asset discovery
- Big data techniques becoming more prominent as a way of detecting highly sophisticated attacks and anomalous behaviour

Level of deviation and system critically drives automated response

GRC defines roles for users to access key systems

Structured Data

Unstructured Data

Social Media

Images

Video

Email

Active Directory

Human Resource

SIEM

GRC

IAM

Adjust Policy

Inform Management

Lockdown

Anomaly Detection based "pattern of life" derived through machine learning
DRIVEN BY BUSINESS
We work with our clients to move their business forward. Positively managing cyber risk not only helps take control of uncertainty across business; it can be turned into a genuine strategic advantage.

RAZOR SHARP INSIGHTS
In a fast-moving digital world of constantly evolving threats and opportunities, you need both agility and assurance.

Our people are experts in both cyber security and our priority sectors, which means we give our clients leading edge insight, ideas and proven solutions to act with confidence.

SHOULDER TO SHOULDER
We work with our clients as long term partners, giving them advice and challenge to make decisions with confidence. We understand that this area is often clouded by feelings of doubt and vulnerability so we work hand-in-hand with them to turn that into a real sense of security and opportunity.