Security Challenges and Governance for Smart Manufacturing

Digital Technology Service Group
Haier Group

Archer Cao
Mar 4, 2017
Archer Cao

**Current Role:**
Director, Information Security

**Background & Experience:**
- 14+ years experiences in IT industry by taking various roles across design/plan and global operations management functions
- Oversea working experience in US, Germany, Russia, Philippine
- Worked for world classed multi-national companies such as TrendMicro, Mars/Wrigley, Nielsen
- Rich experience in information security strategic planning, roadmap, business engagement and service delivery, etc.
- Familiar with International security standards, Privacy and data protection laws and regulations
Agenda

1. Transforming Traditional Industry – Industry 4.0
2. Evolving Threat Landscape for Manufacturers
3. Building Effective Information Security Program
4. Future of Information Security
5. Summary
Transforming Traditional Industry – Industry 4.0

- Smart Buildings
- Smart Homes
- Social Web
- Internet of Data (IoD)
- Internet of Things (IoT)
- Internet of Services (IoS)
- Smart Mobility
- Smart Grid
- Smart Logistics
- Business Web
- CPPS
- Smart Factory
Smart Manufacturing Solution Portfolio

1. Vertical networking of Smart production systems
2. Horizontal integration via a new generation of global value chain network
3. Through engineering across entire value chain
4. Acceleration through exponential technology

- IT Integration
- Analytics and data management
- Cloud-based applications
- Operational efficiency 2.0
- Business model optimization
- Smart Supply Chain
- Smart Logistics
- IT Security Management
- New IP management

- Corporate Venturing
- The Learning Organization
- Innovation
- Efficient management of innovation
- Efficient life cycle management
- Innovation
- Efficient management of innovation
- Efficient life cycle management
- Business model optimization
- Smart Supply Chain
- Smart Logistics
- IT Security Management
- New IP management
Evolving Threat Landscape for Manufacturers

- Insecure product and app design
- Lack of Patching
- Lack of monitoring and response

- Complex technology environment
- Lack of defense in-depth design

- Corporate espionage (theft of IP and trade secret)
- Lack of security awareness

6 Dell Annual Threat Report
The Business Model for Information Security

Systematic Thinking

- Business-oriented approach
- Four elements
- Six dynamic Interconnections
- Independent of any technology
- Applicable across industries, geographies, regulatory and legal systems

Source: USC Marshall School of Business Institute for Critical Information Infrastructure Protection.
Information Security Governance Framework

Consists of Security Drivers, Security management (Policy, Process, Technology, Metrics & People)
Adaptive Cybersecurity Framework

1. Identify
   - Business Context
   - Asset Management
   - Governance
   - Risk Assessment
   - Risk Management Strategy

2. Prevent
   - Access Control
   - Awareness and Training
   - Data Security
   - Information Protection Processes and Procedures
   - Protective Technology

3. Detect
   - Anomalies and Events
   - Security Continuous Monitoring
   - Detection Process

4. Respond
   - Response Planning
   - Communications
   - Analysis
   - Mitigation
   - Improvements

5. Recover
   - Recover Planning
   - Improvements
   - Communications

Improvements
- Communications
- Analysis
- Mitigation
- Improvements
Defense-in-depth Model

Organize security reporting around the stack
For each prepare current, target state analysis and roadmap
Transforming information security driven by,

1. rapidly evolving technology
2. rapidly changing business environment
3. and threat environment

Supporting context layer includes environmental, community, process, content, identity, application, etc.
Summary

- Information security challenges in manufacturing
- Building effective information security management program
- The future of information security
Thank you!