Awareness of Cybersecurity for Intelligent Building Management Systems

Presented by: Adam Summers
Cybersecurity for Intelligent Building Management Systems

Agenda

• Intelligent Building Management Systems
• IP Convergence
• Threats
• Cybersecurity
• Information Security Management Methodology
Today’s Building Management Systems

• Energy Efficiency

• Intelligent Buildings and level of integration is on the increase.

• Systems are becoming more complex.

• Systems are being inter connected over an IP network. (IP Convergence)
IP Convergence: Multiple Systems, One Network
IP Convergence

Reduce CAPEX
- Lowered equipment, software and installation costs
- Common footprint
- Power over Ethernet

Lower OPEX
- Faster training deployment
- Staff reduction
- Minimized maintenance cost
- Energy reduction

Simplicity
- Standard process
- Based on job responsibilities
- Focus on key functions
- Proven IT experience
- Accessibility
Threats

Threats are real
• Deliberate
• Unintentional
• Within/Remote

Effects of an attack
• Loss of Control
• Loss of Visibility
• Loss of Data
• Disruption to Building Systems
• Disruption to Security Systems
• Disruption to Business Systems
Vulnerability can extend outside an intelligent smart building.

- Smart Cities
- Smart Grid
- Smart Homes
- Smart Public Services
- Smart Mobility
Methods of breaking in to a network

- People
  - Pretexting
  - Phishing and Spear Phishing

- Technology
  - Wi-Fi
  - Ethernet
  - USB

- Operations
  - Password Vulnerabilities
  - Impersonation attacks
The virus is placed on a USB Drive
Enters a secure internal Network
The virus scans through the network
It takes a blueprint of the network and relays it to an external server
A new updated virus targets specific computers
It sends back false messages that the plant/machines are fine
The virus subverts the software controlling specific items of plant or machinery
It subverts the computers running specific software
The virus now controls the plant or machines to damage or destroy themselves
The virus spreads to other, highly interconnected infrastructures

CRITICAL INFRASTRUCTURE COMPROMISED
REGIONAL AND NATIONAL INFRASTRUCTURES COLLAPSE
Cost of Cyber Attacks

Average cost of cyber crime to companies in 6 countries
Cost expressed in millions (US dollars)

- Australia: $3.67
- France: $5.19
- Germany: $7.56
- Japan: $6.73
- UK: $4.72
- USA: $11.56


*Understanding the economics of IT risk and reputation, “ IBM November 2014.
What is Cybersecurity

- Cybersecurity addresses attacks on computer systems and networks that can cause accidental or intentional disruptions.
- Body of technologies, processes and practices designed to protect systems.

Why it’s important

- Minimize Business Interruption
- Maximize Operational Integrity
- Maximize Operational safety
- Minimize Production down time
- Protection of intellectual property
- To be Compliant with internal regulations
- To be Compliant with international regulations
Cybersecurity

Design

Install

Operate

iBMS Lifecycle
Cybersecurity Design Phase

Physical Security
- Access to devices and networks
- Locked room or cabinet
- Access control

Network Infrastructure
- Limit access points
- Utilise Firewalls

Manage User Access
- User Access
- Remote Access
- Secure connections (VPN)
- Secure protocols (HTTPS, SSH)
- Utilise DMZ
Secure Design
Cybersecurity Installation Stage

Harden System Devices
• Remove removable media
• Enable Security Features
• Device Web interface Security
• Antivirus, OS updates

Configure User Accounts
• Replace default passwords
• Disable by default - Add permissions
• Use expiration dates
• Enforce password changes

Enable Threat Detection & Mitigation
• Monitor network, device activity
• Monitor physical and user activity
Cybersecurity Operational Stage

Monitor the System
- Utilise monitoring analysing tools
- Incident reporting

Build Security Awareness
- Security policies and procedures
- Manage User accounts
- Use Trusted Sources
- Develop plans

Perform Security Audits
- Ensure Procedures, Policies have no gaps
- Report breaches
- Effective audits
Information Security Management Methodology (ISO 27001)

- Detecting incidents
- Monitoring effectiveness
- Compliance
- Risk analysis
- Development of security measures
- Create procedures and policies
- Implementation of procedures and policies
- Training and awareness
- Take corrective and preventative actions based on information and results.
Summary

• Intelligent Buildings

• Cyber Crime Increasing

• Cybersecurity (Plan-Do-Check-Act)

Schneider Electric has always regarded the security of our customers’ systems as of paramount importance and has, for many years, had security guidelines available for its customers to ensure their systems are protected from attack.
Questions?
THANK YOU.