Lighting Systems and Cybersecurity

Presented By: Ken Modeste, UL LLC
ulcyber@ul.com
www.ul.com/cybersecurity
What We All Are Seeing
Continuous Security Breaches

Threats beyond IT to connected products / systems
- Known / Unknown
- Across market verticals
- In all regions
- Business continuity, financial, privacy, safety risks

What is expected of the
• **Producer,**
• **Vendor** and
• **Purchaser?**
What UL Is Seeing

Lack of Market Confidence

- Inconsistently Requirements
- Invalidated Security Claims
- Supply Chain Vulnerability
- Increased Liability
- Breaches Everyday

Cyber Assurance Needs:

- Standardization
  - Transparent Agreed Upon Expectations
  - Adaptable / Scalable to New Product
  - “Interoperable” With Marketplace Frameworks
- Privacy / Security
- Compliance
- Availability of Skilled Staff

Do you think cyber-attacks are among the three biggest threats facing organizations today?

- 83%
- 11%
- 5%

46% expected cyber-attack, 38% thought they were ready*

*Source: ISACA, 2015, Global Cybersecurity Status Report
<table>
<thead>
<tr>
<th><strong>Marketplace Drivers (Standards / Compliance)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>President Obama:</strong> Executive Order -- “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities”</td>
</tr>
<tr>
<td><strong>Michael Daniel</strong> (Special Assistant to the President and Cybersecurity Coordinator): “An Underwriters Laboratories-type safety certification could serve as a basic model for driving Internet of Things product security …”</td>
</tr>
<tr>
<td><strong>Günther H. Oettinger</strong> (EC Commissioner Digital Economy &amp; Society): “…support international standardization efforts that ensure high levels of security, proven by certification where necessary…”</td>
</tr>
<tr>
<td><strong>ENISA:</strong> “…contribute to national and EU efforts (e.g. SOGIS) related to better alignment of certification policies and strategies at EU level…”</td>
</tr>
</tbody>
</table>
What’s Already Available to the Marketplace?

ISO 27001 or Cybersecurity Framework
Common Criteria

IEC Standards
IEC 62443

UL Standards
UL 2900

IEC Standards
IEC 62443

UL Standards
UL 2900

https://webstore.iec.ch/home
http://www.commoncriteriaportal.org/
http://www.ul.com/cybersecurity/
So What Is Missing?

- **One Framework**
  - Multiple frameworks with invested constituencies
  - Frameworks are broadly written without a clear path to compliance

- **Relevant Standards**
  - Standards written primarily for IT applications
  - Standards are broadly written leaving too much to judgment

- **Compliance Scheme**
  - Cybersecurity rating system to manage expectations
  - Focus not only on product/ software but also on process

To fill the gaps, what needs to be considered?
Security objectives

- **Availability** – disruption of access to information
- **Integrity** – unauthorized modification of information
- **Confidentiality** – unauthorized disclosure of information

Differentiation According to Objective

- Penetration Testing
- Vulnerability Assessments
- Forensic Analysis
- SIEM
- Monitoring
- Infrastructure Testing
- Active Defense
- Crisis Response
- IAM
- Security Process Audit
- Audits
- Advisory Services
- Standard Development
- Threat Intelligence
- Binary Analysis
- Solution Assessment
- Biometric Identification Solution
- Audits
- Training
- Test Tools
- Hardware Analysis
- Counterfeit Checking
- Advisory Services
- Standard Development
- Threat Intelligence
- Binary Analysis
- Solution Assessment
- Biometric Identification Solution
- Audits
- Training
- Test Tools
- Hardware Analysis
- Counterfeit Checking
Manage / Assess Risk According to Objective

What is the asset at risk?
- Essential function
- Administration / control (local or network)
- Equipment / facility integrity and personal safety
- Private / personal data…

The Vulnerability / Weakness?
An exploitable defined flaw in security measures (design or how the product / service implemented. Includes:
- Unpatched published vulnerabilities
- Remote control protocols
- Web services
- Buffer overflows
- Weak or improper Authentication mechanisms
- Improper Authorization (access control)
- Credential control
- Messaging manipulation and injection
- SQL injection into data historians

The Threat?
Any action (intended or not) to infiltrate the workings of a system. Perpetrators include:
- Nation-States
- Professional – Usually performing theft, espionage or malicious activity
- Hobbyist – No intent to perform criminal or malicious activity outside the hacking act itself.
- Employees / Insiders
- Malware – automated attack software
Standardization Working Plan

Questions…

Who would rely on the outcome?

What do the vendors want the marketplace to expect?

Does this adequately support a certification or assurance scheme?

General Requirements

- Documentation
  - Identify Product
  - Vendor’s Cybersecurity Objective
- Validate Risk Management
- Assess Risks
  - Vulnerability / Exploitation
  - Software Weakness
- Control Risks

Industry / Product Particular Requirements

Are there marketplace best practices that should be default requirements?

Can relevant requirements of existing standards be tailored to specific applications?

Will the requirements make a difference?

…and more questions…
How Might This Apply To Lighting?

- Design Vulnerabilities in products
- Implementation Vulnerabilities in use of products
- Availability and Integrity
- Secure Communication
- Internal Infrastructure Attacks
- External Infrastructure Attacks

- Primary building lighting
- Secondary building lighting (e.g. emergency lighting)
- Communication lighting (e.g. signaling)
- Building automation integration

- Smart Devices
- Hubs / Routers
- Luminaires / Lamps
- Drivers
- Sensors
- Transfer Equipment

- Applications
- Data
- Communication Protocols
- Operating Systems
- ...

Hardware
Software
Network

- Access
- Authentication
- Detection
- Recovery
- Asset Management
- ...
Risk Mitigation Framework

Define the system

- Lighting + Building Automation + IT
- Boundaries of the system
- Resources of the system – people, processes, technology components
- Primary functions of the system
- Information in the system – classify the data
- How is the data used – stored, transmitted and accessed

NIST SP800-30, Risk Management Guide for Information Technology Systems

http://csrc.nist.gov/publications/PubsSPs.html
Risk Mitigation Framework

Define the system

Lighting + Building Automation + IT

Identify Critical Cyber Assets

Lighting Equipment
Building Automation Equipment
HVAC Systems
IT infrastructure equipment

NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations.
ISO 27000 series of information security and management international standards.

http://csrc.nist.gov/publications/PubsSPs.html
Risk Mitigation Framework

Define the system

Lighting + Building Automation + IT

Identify Critical Cyber Assets

Control Equipment, Devices, Sensors

Classify the data

Public Data – Free to distribute
Restricted Data – Known to some staff
• policies and procedures
• Layout schematics and naming conventions for devices
• Access to reports etc
Confidential Data – Absolutely necessary for safe and secure operations
• Encryption keys and passwords
• Security config information
• Personal Identifiable Data

NIST SP800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information

http://csrc.nist.gov/publications/PubsSPs.html
Risk Mitigation Framework

Define the system

Lighting + Building Automation + IT

Identify Critical Cyber Assets

Control Equipment, Devices, Sensors

Classify the data

Passwords, keys, names and email addresses

Vulnerability Assessment

Evaluate the perimeter security controls
- Firewalls, VPN, Proxy servers
- Penetration testing of critical cyber assets and infrastructure
- Operations and physical security assessment
- Policies and Procedures

NIST SP800-97, Establishing Wireless Robust Security Networks:
NIST SP800-115 Technical Guide to Information Security Testing and Assessment
NIST SP800-42, Guideline on Network Security Testing

http://csrc.nist.gov/publications/PubsSPs.html
Risk Mitigation Framework

Define the system
- Lighting + Building Automation + IT

Identify Critical Cyber Assets
- Control Equipment, Devices, Sensors

Classify the data
- Passwords, keys, names and email addresses

Vulnerability Assessment
- Pen Testing, Security Controls

Security Control Mitigation
- Estimate risk occurrence and reduce the risk
- Impact assessment
- Purchase Insurance
- Compliance, Privacy
- Contingency Planning and Incident Response
- Continuous Monitoring

NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations
NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

http://csrc.nist.gov/publications/PubsSPs.html
Risk Mitigation Framework

1. Define the system
   - Lighting + Building Automation + IT

2. Identify Critical Cyber Assets
   - Control Equipment, Devices, Receivers

3. Classify the data
   - Passwords, keys, names and email addresses

4. Vulnerability Assessment
   - Pen Testing, Security Controls

5. Security Control Mitigation
   - Impact Assessment, Continuous Monitoring
## Assess and Control Risks

### Common Design Vulnerabilities
- Sensors/actuators have no inherent security.
- Control panels have limited untested security.
- Remote accessibility to control panels and server software.
- Non-secure firmware updates.
- Open ports on devices and services.
- Tamper detection and/or resistance is minimal
- Web services
- Poor coding practices

### Implementation Vulnerabilities
- Limited patching and testing of new patches
- Use of default passwords
- Incorrect configuration use
- Connected systems
  - video surveillance
  - Building automation
  - access control systems

### Common Counter Measures
- Disable unused physical and logical ports.
- Fuzz testing on all ports.
- All ports should require authentication.
- Test factory defaults while in operation.
- No “hard coded” passwords.
- Firmware upgrades must be secure - digital signatures.
- Include tamper detection technologies.
- Enforce secure coding practices.
- Independent security source code audit.
- Obfuscation

### Common Counter Measures
- Patch management
- Secure workstations, servers with known IT practices and policies
- Whitelisting and blacklisting
- Auditing trails with alerts
- Network penetration testing
- Review of audit logs, security policies
- Independent vulnerability and cyber-security assessments
- Intrusion detection and prevention reviews
### Assess and Control Risks

#### Communications
- Communication lines allow for:
  - Line Sniffing (Eavesdropping)
  - Man in the middle injection
  - Denial of Service
  - Spoofing/Masquerading
  - Record and replay
- Credentials that are not secured

#### Common Counter Measures
- Cryptography and Credential security
- Test and implement against known standards
  - FIPS 140
- Secure Authentication/Non Repudiation
- Data filtering and discarding
- Secure Firmware upgrade process

---

How much or how little of the foregoing are necessary to fill the cybersecurity need for an emergency lighting system or any other system or parts thereof are yet to be determined.
Vendor’s declaration of their cybersecurity objective.

Organization Designing for Security Process Review

Product (System) Testing

Implementation Assessment (user environment)

Indication that the product meets the declared cybersecurity objective or some standardized assurance expectation.