Cybersecurity Framework, Categorization & Classification

Rob Murchison

Intelligent Buildings, LLC

2019 Haystack Connect

Smart Data. Smart Devices. Smart Buildings. Smart Business.

What's the problem (IT View)?

Figure 1. IT Data Priorities

CIA

- **Confidentiality**
  RBAC dictates that this information is on a "need to know" basics.
- **Integrity**
  The integrity of the data is also priority and must be protected through confidentiality.
- **Availability**
  As stated in Confidentiality, data is on a need to know basis and should only be granted after the user proves the need to know.

Join the CONVERSATION: https://project-haystack.org/forum/topic/667

What's the problem (OT View)?

Figure 1. IT Data Priorities

CIA

- **Confidentiality**
  RBAC dictates that this information is on a "need to know" basics.
- **Integrity**
  The integrity of the data is also priority and must be protected through confidentiality.
- **Availability**
  As stated in Confidentiality, data is on a need to know basis and should only be granted after the user proves the need to know.

Figure 2. OT Data Priorities

AIC

- **Availability**
  The majority of communication is Machine-to-Machine (M2M) and happens in milliseconds. Without high availability sequences of operations can be impacted and the system will not function as designed.
- **Integrity**
  The data passing between machines must be correct in order for the system to design as functioned. Additionally the human operator needs to know the correct responses of the system to diagnose and operate the system.
- **Confidentiality**
  Historically has had little to no consideration. Confidentiality must always be viewed through the operational risk lens.

Join the CONVERSATION: https://project-haystack.org/forum/topic/667

The Challenge!

Challenges: Acquiring and maintaining an accurate record of this OT information, as well as ongoing monitoring of the information, is difficult for a variety of reasons:

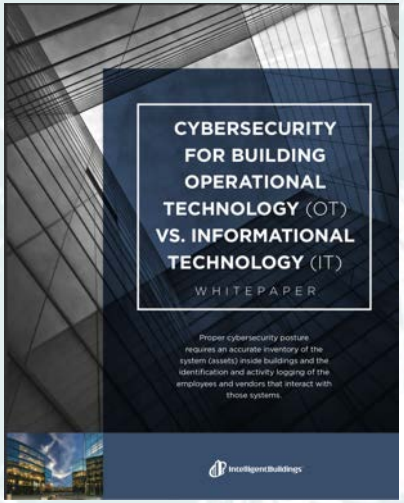
a) **OT is not IT:** Building control systems function in ways that are fundamentally different from traditional information technology (IT) systems and have a lifecycle three to five (3–5) times longer than a typical enterprise IT system, notwithstanding a very different culture, procurement process, and maintenance environment.

b) **Vendor Fragmentation:** OT vendors and contractor services are fragmented and experience turnover both within a building and across a portfolio, which makes standards, consistency, and compliance monitoring very difficult.

c) **Issue Ownership:** Most organizations have been caught flatfooted by this risk, and there are usually not clear roles regarding responsibility for assessing, remediating, and monitoring vendor and system risks.

Join the CONVERSATION: https://project-haystack.org/forum/topic/667

What's the problem (side by side)?



Free Whitepaper

Requirement	IT	OT
Asset Management	Many third-party products are available to automatically retrieve, update, and manage IT as-sets, including OS and application software.	Off-the-shelf solutions do not exist for managing OT assets, because there are no industry standard methods for extracting this information from each system.
Identity Management	IT departments administer and enforce identity management policies for all users.	In many cases, it is the installing OT vendor that provides identity management. Also, it is common for users to have shared accounts.
Desktop Access	Once a user successfully logs in to their desktop, they can access all of their installed applications.	OT systems are accessed system by system, and each requires a different authentication method.
Application Functionality	Once logged in to a desktop, users can perform all functions of the software except for system ad-ministration.	OT applications require restrictions by role, such as operator, programmer, and system administrator.
Vendor Access	IT vendors are rarely given access after systems and applications are installed and, when needed, access is tightly controlled.	OT vendors are the primary service providers and routinely interact with the installed system with virtually no policy enforcement.
Remote Access	IT departments place great emphasis on access into and out of the company's network. Multiple technologies are applied to control access, including firewalls, intrusion detection systems (IDS) / intrusion prevention systems (IPS), VPNs, and virtual desktops.	Minimal precautions are more typical in the OT industry, resulting in many systems having their IP addresses exposed to the public Internet.
Security Policies	IT departments in conjunction with the company's security officer define and implement security policies to mitigate threats and comply with regulations where applicable.	OT systems are rarely included in the scope of the company's security framework, and it is unclear who in the organization is responsible for compliance.
Security Training	Security management and threat prevention are essential to general purpose IT systems. Since much of the risk is associated with user behavior, training is routinely offered to employees.	Facility personnel and the vendors that support the OT systems are rarely subject to policy and procedure training or educated on the risks associated with social engineering threats. Given the many differences, customized training is needed.

Join the CONVERSATION: https://project-haystack.org/forum/topic/667

What's the answer, TAGS!

Step 1: Password age, password strength, auto lockout, etc. are part of the configuration information and therefore need to be analyzed..

Step 2: These items that are not readily available or access at all but a requirement of enterprise IT..

- Criticality Level
- External Communicator
- Include in Forensics
- ID'd as Life Safety
- Risk Level Compensating Control
- Applied Okay to Isolate
- Physical Location (they may have this one already)
- Data Flow Direction (one way/two way/multi)

Join the CONVERSATION: https://project-haystack.org/forum/topic/667