CYBERSECURITY FOR BUILDING OPERATIONAL TECHNOLOGY (OT) VS. INFORMATIONAL TECHNOLOGY (IT)

WHITEPAPER

Proper cybersecurity posture requires an accurate inventory of the system (assets) inside buildings and the identification and activity logging of the employees and vendors that interact with those systems.

TOTEM BUILDINGS℠

1 ABSTRACT

Problem Area: Real estate cybersecurity best practices should include an accurate inventory of the building systems (assets) and identification, as well as activity logging of the employees and vendors that interact with those systems and affect their internal setup. These best practices are largely related to human behavior, which accounts for approximately 3/4 of all cybersecurity incidents* and can be divided into employee management and vendor risk management (VRM).

Awareness & Risks: The increasing number of cybersecurity breaches in building control systems (also referred to as building operational technology (OT) systems) around the world has raised the awareness of building owners and managers. These critical systems are responsible for controlling *all aspects* of the building environment: HVAC equipment, elevators, lighting, power, physical security, video surveillance, parking, and others. When these systems are compromised (either internally or externally), they create risks, including life-safety, equipment replacement, core-network intrusion, business interruption, brand damage, and regulatory / legal non-compliance.

Best Practices: According to the U.S. Government's National Institute of Standards and Technology (NIST) and the SANS Institute (a private U.S. information security and cybersecurity company), the fundamental construct for controlling risk is understanding which systems you have, who has *access* to them, what actions the users are allowed to complete once connected, and a *record* of what actions took place affecting those systems.

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.

This whitepaper draws a clear contrast between the IT and OT environments, outlines the problem created by the vast differences, and points to a solution to bridge the gap that is being introduced to the market by U.S.-based Totem Building Cybersecurity, LLC.

** 80% of breaches occur due to lack of basic processes, policies and procedures, and employee / vendor mistakes. 1/30/18 IT www.itgovernance.co.uk*

2 IT ASSET & IDENTITY MANAGEMENT

Most enterprise IT departments manage and secure their computing assets and control user access to desktops and the applications that run on them in similar ways.

Asset Management

- IT departments are able to directly **track** their computing assets, including servers, PCs, laptops, network equipment, and software through a large variety of software tools that are readily available in the market.
- Because application software is licensed, many of these tools assist in managing contract renewals, service agreements, and **patches and upgrades**.

Identity Management

- Identity management begins with connecting to your desktop, which is typically a laptop or workstation computer. Increasingly, tablets are also being used equivalently. Once powered up, employees (users) **log in** to the device by entering their username and password. Because of the exponential rise in cybersecurity breaches, most companies are now requiring **multi-factor authentication** through the use of biometrics or a text message sent to the employee's cell phone. Once authenticated, users then access and run the individual applications contained in their desktop. This is true whether the desktop has the applications installed locally or virtually.
- Users create and maintain **passwords** for their assigned desktop. Each password should comply with **company policy** around cybersecurity best practices (such as the use of strong and expiring passwords). Readily available software exists to enforce these policies.
- IT departments control both the desktop operating system (OS) and the applications used by each employee. To secure the applications and prevent unwanted software from being added to the desktop, the IT department has sole **administrative rights** and is responsible for installing / uninstalling and maintaining all of the associated applications.
- IT departments also protect each desktop with **antivirus / anti-malware** software and automatically update this software as new virus definitions are released by the vendor. Additionally, software patches are applied periodically to protect the OS and / or applications as vulnerabilities are identified and corrected.
- Once users are granted access to an application, they can interact with the application's features. For example, when using Excel, users can create, edit, and delete spreadsheets using all of the capabilities that come with the product.
- To **work remotely,** users either utilize a **virtual private network (VPN)** to communicate with the company's network, launch a browser, and connect to their **virtual desktop** over the Internet, or launch the browser and connect to a Software as a Service (SaaS) application (e.g., Office365). In all cases, user authentication is needed to establish a working session, and network traffic is typically encrypted.
- **Audit logs** of user activity are a standard feature of IT systems that make tracing user actions associated with security incidents possible for IT engineers.

In summary, in managing IT assets and providing secure access to the desktops and applications that run your business, IT departments should:

- Use commercially available software to track and manage IT assets
- Have administrative control over desktop user access
- Determine the requirements for authenticating desktop users
- Control which applications are installed for each user
- Provide secure remote connections
- Protect the desktop from viruses and malware
- Regularly patch the OS and applications to protect against known security vulnerabilities

3 OT ASSET & IDENTITY MANAGEMENT

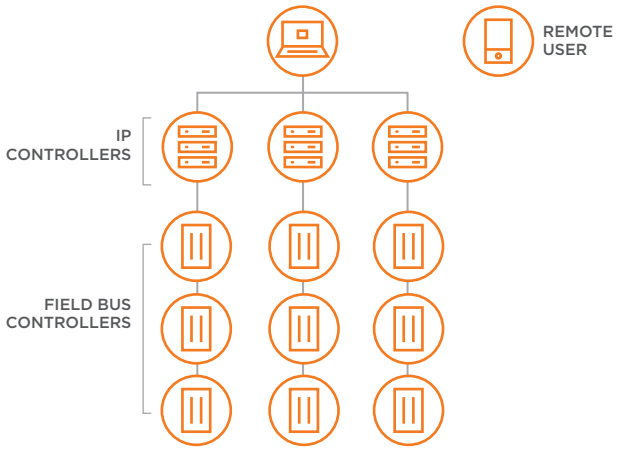
In order to compare the current IT systems environment to the OT systems environment for asset and identity management, the following lays out two (2) types of architecture that are typical for OT systems, namely server-based and serverless..

Server-Based Systems

- This architecture (see Figure 1) involves the use of a server connected to a network of IP-based controllers. Each controller may, in turn, have a connected sub-network of smaller controllers operating over a field bus (non-IP serial communications) network. Operators normally communicate directly with the server, which often doubles as the workstation for the vendor's host application. This architecture is typical for building automation systems (BAS), access control, video surveillance, and fire systems. It can also be found in chilled water plants, elevator banks in large office buildings, and lighting systems.
- In addition to the local operator, it is common for these systems to be accessed remotely via a standard unsecure **internet connection** installed by the system's contractor (who often has limited IT knowledge).
- The server normally runs a commercial OS, such as Windows or Linux. The installed application from the OT manufacturer is used to administer, configure, program, and operate the connected IP devices and their associated subnetwork controllers. **If an IT policy exists, the tools are not in place to manage such a policy**.
- There are separate user accounts to the OS versus the vendor's application software.
- In many cases, the IP controllers are also designed to have direct user access, thereby bypassing the server.
- There are no third-party products that can electronically interrogate and compile **asset data** on the wide variety of systems in the market. Currently, the only option is to manually collect the information and save it in a spreadsheet or asset management software package.
- There is no standard in the industry for **authenticating users**. The set of available options (e.g., strong passwords, expiration dates, auto-logoff features, etc.) varies by vendor.
- The **vendor** (with limited IT knowledge), through either their local office or an authorized contractor, is normally given the job of installing software on the server (and, in many cases, providing the hardware), as well as setting up all users (company and vendor employees alike).
- When service is needed, the vendors typically communicate to the systems remotely over an unsecure internet connection. Unless special care is taken to control remote access through the use of firewalls, VPNs, or virtual desktops, many OT systems have their IP addresses exposed to the Internet.
- In addition to creating users, roles for each user must also be created. Typical roles include operators, programmers, and system administrators:
  - **Operators** view the status of all connected devices or people (as in the case of access control) and, in some cases, adjust setpoints or manually grant access to an employee who has forgotten their pass card.
  - **Programmers** create and modify control algorithms and modify system configuration.
  - **System administrators** have full system access rights, which include tasks such as upgrading firmware and performing system backups. Contrast this to the lack of limitations imposed on users of business software, such as Excel or Salesforce.
- Identity management security policies that are often in place for the IT environment are rarely applied or enforced for OT systems. This is true in large part because the worlds of **OT and IT are both technically and culturally different**. Responsibility for OT systems usually falls with the facilities staff, not the IT department.
- It is very common for OT servers to be used by the facilities staff to run other types of software, including email and internet browsers.
- OT servers should also have antivirus / anti-malware software installed, but providing **automatic updates can be problematic** to some applications, meaning that a manual process is required to respond to updates that can cause the application to malfunction when updates are applied.
- Security patches to OT applications are typically installed by the vendor's local contractor, who usually has limited IT experience. OT manufacturers are typically unaware where their systems are installed and are therefore unable to directly notify building owners when a security patch has been released to the marketplace. OT manufactures rely on the local contractor to inform the building owner and arrange for the upgrade, yet the local contractors have no economic incentive to do so.

- Audit logs are often available in OT systems but are minimally configured and rarely archived, meaning that a historical record of activity is unavailable should a security investigation ensue.

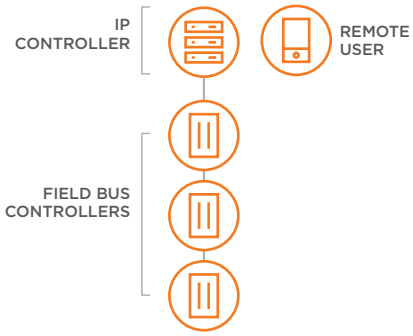
Figure 1.



Serverless Systems

- In the second architecture (see Figure 2), there is no server—just an IP-based controller and possibly a sub-network of secondary controllers. This architecture is typical of smaller BAS systems, lighting control, elevators, intrusion systems, HVAC equipment, parking lot controllers, fire panels, and more. In this architecture, users connect to each system from a remote desktop either through a browser or an application that has been installed on the user's desktop or laptop.
- In all other respects, identity management is achieved in the same fashion as described for the server-based systems, with the exception that the options available for user authentication are often even more limited.

Figure 2.



In summary, there are multiple challenges organizations face in managing their OT inventory and the identity of OT users:

- There is no third-party product available today for **automatically retrieving and updating the assets installed** at each location across the many OT manufacturers in the market.
- Each OT system is administered, configured, and operated **individually, system by system**. There is no concept of creating a desktop where one (1) or more OT application(s) are installed for each user.
- The OT industry has not adopted a standard for **authenticating systems** and the methods available are often limited in functionality.
- Users of OT systems need to be segregated into **roles that limit which functions** they can perform on any given system.
- Vendors play a big role in the installation and servicing of OT systems, yet they **lack basic knowledge of IT best practices** while routinely gaining access to these systems on a remote basis.
- Unless care is taken to provide remote connections on a secure basis, many OT system IP addresses are **exposed to the public Internet**.
- Standard **company-wide security policies** for managing identity and access are often **lacking or are unenforced** for OT systems.
- Few organizations have decided **where the accountability falls for securing OT systems**. The default is usually the facilities staff, who often lack the training and knowledge for implementing and managing access to industry best practices.

4 IT / OT CONTRAST TABLE

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.

5 TOTEM BUILDING CYBERSECURITY, LLC (TBC) SOLUTION

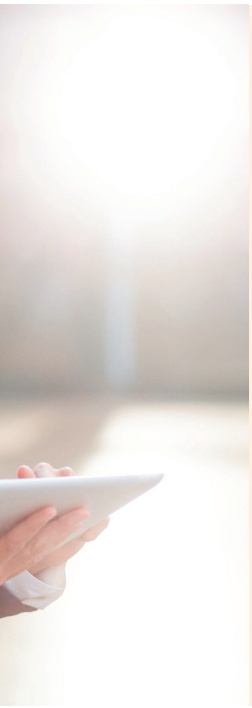
TBC is launching Totem, a cloud-based software platform that takes direct aim at the core challenges of human behavior and VRM that create significant cybersecurity risks in the OT environment.

With Totem's cloud platform securely connected to your building, your organization has an automated approach to getting information about:

1. **Inventory & Access:** A complete and verified inventory of the OT assets (both hardware and software) for each building, a listing of who has access to each system and at what permission level (both inside and outside of your organization), and a log of what was done by whom and when.
2. **System Configuration:** Ongoing view of any system setup changes that create both inside and outside vulnerabilities, including careless and malicious changes in setup.
3. **Reporting & Backup:** Instant access to a risk dashboard and full process, controls, and compliance reporting on a building, site, or portfolio, along with a customer-accessible backup of system data to aid in the recovery of a corrupted or compromised system.

The key to achieving this result is our ability to extract the necessary asset and identity information from the databases contained within each OT system via a library of parsers, industry standard protocols, manual entry, and the web services application programming interface (API). This information shows the "fingerprints" of vendor and employee behavior for assessing and monitoring policy compliance and risk indicators. Totem can also auto-discover new devices as they are added to your OT networks and inspect the traffic for anomalies that could represent security threats to your organization.

For more information, please visit our website at **totembuildings.com**.



Totem Buildings Provides Critical Information for Risk Management

- **ACCESS:** Who has access, what levels or permissions, and a record of use
- **ASSETS:** Inventory of systems, devices, and software versions
- **BACKUP:** Current backup of the system for easier, faster restoration
- **PATTERNS:** Unusual traffic in the building, portfolio, or externally (optional)
- **ORGANIZATION:** Documentation and reporting for SOC 2 processes and practices

TOTEM BUILDINGS℠

For more information, please visit our website at **totembuildings.com**

72-2020