WHITE PAPER

BUILDING RESISTANCE

A LOOK AT OT, IT AND MITIGATING RISK

Part 5 | **Smart buildings: Basic NIST Cybersecurity Framework integration into operational technology**

Applying Standards to Secure Your Organization

Building control systems have traditionally not followed any form of formalized standards. For the most part, vendors have installed systems as they saw fit, and installations varied from designer to designer, programmer to programmer. Even now, there are no set standards for installing building control systems. But for these critical systems to be secured, standards must be implemented to form basic best practices that will need to come from the end user / owner of the system.

What Is NIST?

When it comes to cybersecurity, there are several standards available, such as the National Institute of Standards and Technology (NIST), the Center for Internet Security (CSC), the International Organization for Standardization (ISO) or the Factor Analysis of Information Risk (FAIR). This paper focuses on NIST, the most well-known in the industry.

NIST was founded in 1901 and is a nonregulatory federal agency within the U.S. Department of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology that enhance economic security and improve our quality of life.[1] NIST is not mandatory but rather a purely voluntary practice to a mandatory standard for federal agencies.

Cybersecurity standards are important because they enhance security and contribute to risk management in several ways. Standards help establish common security requirements and the capabilities needed for secure solutions.

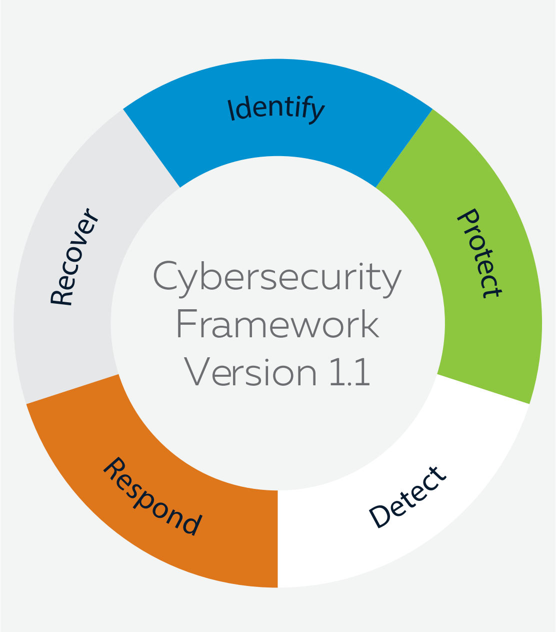
What Is a Security Framework?

A security framework is a series of documented, agreed-upon and understood policies, procedures and processes that define how information is managed to lower risk and vulnerability, as well as increasing confidence in an ever-connected world.[2]

Why NIST Cybersecurity Framework?

"The NIST Cybersecurity Framework is a set of best practices, standards and recommendations that help an organization improve its cybersecurity measures … The NIST Cybersecurity Framework seeks to address the lack of standards when it comes to security."[3] When it comes to combating hackers, data pirates, ransomware and other threat tactics, companies are using technologies, language and rules in a variety of ways.

Figure 1



What Is NIST Cybersecurity Framework?

The NIST Cybersecurity Framework covers a wide range of security controls and also breaks down security into five functions (*Figure 1*) that are easy to understand.[4] These functions are as follows:

FUNCTION	DEFINITION
IDENTIFY You can't protect what you don't know you have	The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data and capabilities.
PROTECT Once you know what you have, how do you secure it	The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.
DETECT Once you are protected, you have to monitor for threats	The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables the timely discovery of cybersecurity events.
RESPOND What you need to do once you are attacked	The Respond Function includes appropriate activities to perform regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.
RECOVER How to get back to an operational state and learn to protect against future events	The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Source: NIST

Figure 2

FUNCTION	CATEGORY	ID
IDENTIFY	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
PROTECT	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes and Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
DETECT	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
RESPOND	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
RECOVER	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

A variety of categories fall within each function (*Figure 2*).

How Can It Be Used in the Building Control World?

Cybersecurity for building control systems is in its infancy. We must look at it from a "crawl–walk–run" perspective. Most companies are in the "crawl" stage but may be on the verge of attempting to start in the "run" phase. This can often be overwhelming. The NIST Cybersecurity Framework is extremely complex; attempting to adopt it in its entirety from the beginning often results in having to start from scratch.

However, the foundational concepts—the five functions mentioned above—are simple and offer an excellent starting point.

When thinking about each function, there are some basic best practices to consider and implement that will make your systems less attractive to hackers and bad actors.

IDENTIFY

The Problem: Building owners often don't know what is connected to the building control network. Those who claim to know are often surprised by the number of unknown devices uncovered during assessments. In one example, a vendor told the assessor that there were only four devices on their network. A scan revealed that there were 32 devices on the network, including a Raspberry PI. This low-cost, credit-card sized device plugs into a computer monitor and is controlled via keyboard and mouse.[5] It enables people to explore computing and to learn how to program in languages like Scratch and Python. Although seemingly innocuous, this device poses a significant security risk.

A Raspberry PI was installed on NASA's Jet Propulsion Laboratory (JPL) network by one of their JPL employees. A hacker gained access to it in April 2018 and stole about 500 megabytes of data from 23 files, two of which contained information related to a Mars mission. The hacker used an external user account and moved undetected within JPL's network for nearly 10 months.[6]

The point is, knowing which devices are connected to your building control network is crucial to protecting your organization. Inventories should be completed periodically so that no device goes undetected, leaving a vulnerability for hackers to exploit.

Best Practice: Inventory your control networks. This is easy to do by scanning the network and periodically walking the network.

Caution: Scanning these devices must be done correctly. Low-impact scanning must be done to ensure that devices will not lock up or be knocked offline. IT scanning tools are known to cause communication issues with controllers preventing them from functioning and causing interruption of service. Walking the network is done to inspect for rogue devices like the Raspberry PI visually. Both exercises must be completed regularly to discover changes that could introduce vulnerabilities.

After the inventory, all nonessential devices should be removed. Only devices necessary to the function of the system should be connected to the control network. This includes printers, cameras and wireless access points. It's also recommended that all the devices be maintained in an assessment management tool. Maintaining an up-to-date inventory of devices will help protect from vulnerabilities.

Example: A bad actor accessed an exposed printer in a company and remotely printed out the words "There is a bomb in the building." The building was evacuated, and the authorities were called to search for the bomb. None was found; however, the damage was done: brand damage to the owner of the building, loss of productivity and loss of tenants' confidence.

The Problem: When it comes to user IDs, a host of challenges can emerge given the widespread nature of functionality, access, volume and shared use. Some common scenarios that may surface within an organization include:

- Common user accounts for all who access the system, including facility and vendor employees
- Example: Facility employee user = engineer and vendor user = vendor
- A single unique user account used by multiple employees to access a system
- All users of the system have administration rights
- Facility users have unique user accounts; however, the vendor has a shared user used by all vendor employees

Best Practice: All users need to have unique accounts. Without unique user accounts, user control is nonexistent. If all users share an account and an event occurs, tracing user activity is impossible. In the IT world, when employees leave an organization, their usernames are removed from the system so that they no longer have access. Unlike IT, a lot of OT systems cannot be included in standard IT user management. This means that monitoring system users will require a more manual approach. New control-centric software is now available that can monitor users and their rights at the control system level. These should be incorporated if manual monitoring is not an option.

In addition to unique accounts, Least Privileges should be used. Least Privileges are used to control the level of access a user has. Not all users should have administrative-level access. With Least Privileges enabled, a user has access to enough rights to perform their job function, and only those users who will administer users should have administrative rights.

It's important to also audit vendor users. Policy should be established that limits vendor access—access that should be controlled by a facility administrator. Vendor users should be unique and only active when it is necessary for the vendor to perform their job. When not in use, the vendor user should be inactive.

Example: A customer had an employee that had full administrative rights for over 100 systems. The user was removed from Active Directory, which removed them from the business applications. However, it did not remove the employee from the control systems, which were connected to Active Directory. Once this was discovered, the user account was removed individually from each of the devices. This process took many hours. The problem wasn't just the time required to remove the access, but that removing his user communication to devices at over 100 sites resulted in the devices no longer communicating to the central server (there were multiple devices at each of the over 100 sites). Simply re-adding the user account would not work because they did not know his password and the end devices were dependent on this user's information being entered back in exactly as it was. It was not a situation where the employee could be contacted to retrieve that information. The manufacturer of the devices had to intervene, and the whole process took weeks to resolve.

PROTECT and DETECT

The Problem: The majority of control systems are not monitored for threats, vulnerabilities and configuration monitoring. Even systems that are monitored by IT stop at the PC or server that hosts the application. The downstream devices and underlying network are often not monitored.

Best Practice: IT solutions can monitor front ends / application servers. Monitoring your PC is a best practice recommendation; however, predefined testing with IT is required to ensure that the application can sustain the monitoring, which may also involve a vendor. This testing should be controlled as to not negatively impact the control system.

Network traffic should be monitored for anomalies such as unusual device-to-device traffic. While IT solutions can monitor network traffic, they do not necessarily "understand" control system traffic. For example, generators that suddenly start "talking" to air handling units could indicate someone has infiltrated the network.

But this is only part of the process. Devices are typically not capable of installing agents, so other means are necessary to monitor for configuration changes, versions, open ports and user activity. Until recently, this was only a mostly manual process available. New technologies have begun to emerge that can help advance these capabilities.

Example: A customer's IT group began vulnerability scans on thousands of devices. As a result, over 60% of the devices were knocked offline. A hard restart at the device level was required to get the devices back online. Several systems were impacted, which required integrators to restart each device. IT tried backing down the scan, but there were still many affected devices, which required the integrators to return to perform more hard restarts. The entire event resulted in a full week of lost time, money and productivity.

RESPOND

The Problem: At many facilities, there are no documented response plans focused on facility systems. There is often little understanding of the potential impact a cyberevent may have on facility systems, which is why many facilities do not plan for these issues. Ignoring these threats can have potentially devastating effects on a facility.

Best Practice: IT departments typically have a response plan that is documented and practiced so that in the case of an event, each team member knows their role and the steps they must perform. If an organization has an IT department and documented response plans, then facility staff should work with IT to develop response guidelines. This could potentially help the facility with the learning curve of developing their OT response plans. If IT does not exist or this not an option, there are other organizations that can aid in this development process.

At a minimum, facilities should have documented processes in place to minimize the impact of an attack on equipment or devices during and after an event. Team member roles should be defined and assigned, and members should maintain documentation of process as systems evolve and grow.

Example: Recently, an inexpensive communication converter being used by a facility failed. There was no documented response for the event, and the vendor spent more than three days trying to bring the device back online. Neither the facility nor the vendor had a replacement device on hand. The device was over 11 years old and past end-of-life manufacturer support. This event could have been mitigated in less than a couple of hours had there been a documented response plan.

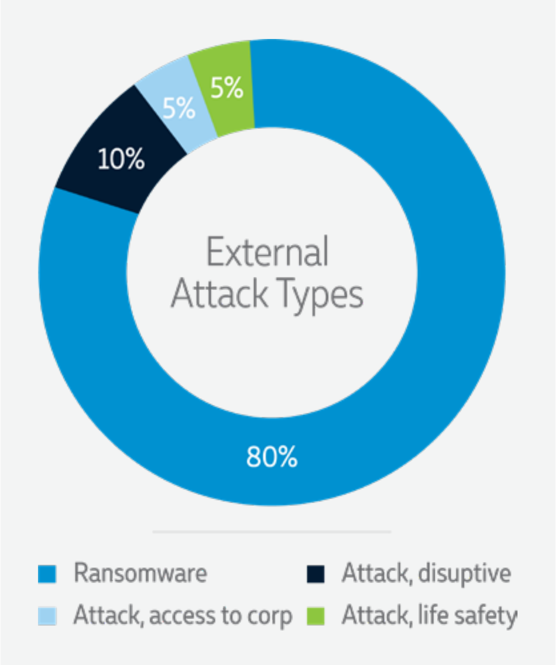
RECOVER

The Problem: There are many aspects to a good recovery plan. Many areas of control systems should be addressed in a robust recovery plan, but the reality is that the majority of facility staff do not have a formal or informal recovery plan.

Best Practice: There are several options for how best to address recovery issues.

Currently, the primary vector of attack for most control systems is ransomware (*Figure 3*). A sound backup strategy is a necessity for recovery plans. To date, almost 90% of ransomware victims we've observed had no viable system backups in place. Those that did back up their system:

Figure 3



- Backed up to the same machine that got ransomed (making the backup inaccessible)
- Relied on an extremely old backup that needed updating to be effective
- Relied on a vendor to control the backup, and the user had to wait until the vendor could dispatch a tech to the site to restore the system

Setting Your Organization Up for Success

Following the NIST Cybersecurity Framework has proven to help organizations shore up their control system cybersecurity. However, this is only part of the process; it will require time and effort. It is doable if you "crawl–walk–run." Take the time to choose the steps that can be added in with the least disruption.

Bo Rotoloni, principal research engineer at Georgia Tech Research Institute, said in a cybersecurity panel that "this is a problem for which there is no solution." Bad actors are always looking for vulnerabilities and paths to access information. Right now, the path through a control system is by far the easiest.

Disclaimer

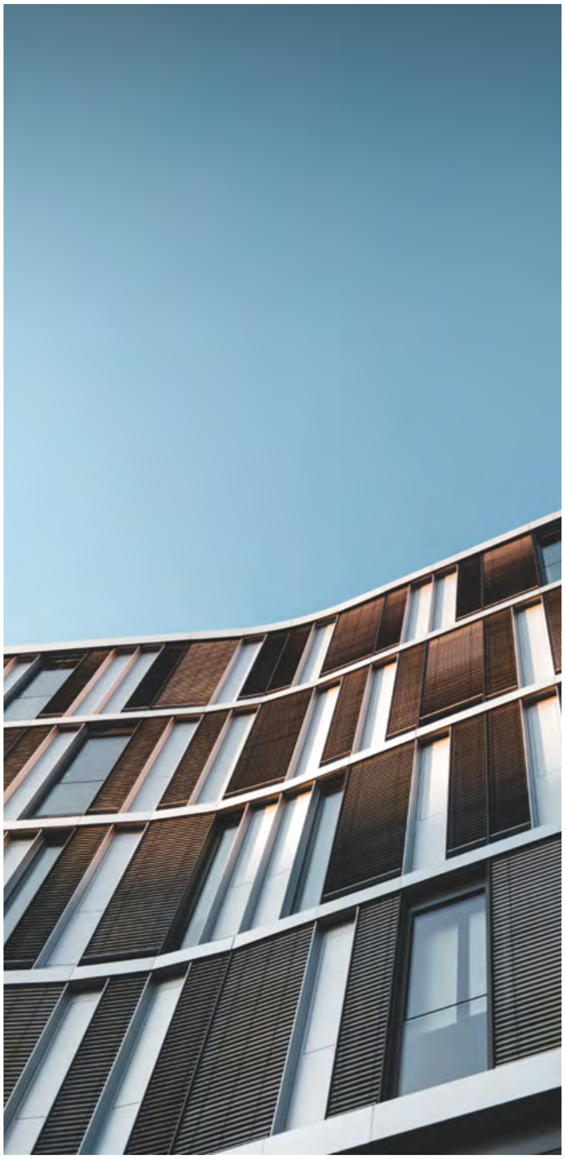
This paper is not advocating a particular standard for installation. Each organization should review its needs and abilities to determine the best path to cybersecurity resilience. The intent of the paper is to inform the reader about the NIST Cybersecurity Framework. No claim is made that the information included in this paper is sufficient enough to base a fully vetted cybersecurity program on.

Additional Information

- Framework for Improving Critical Infrastructure Cybersecurity
- Framework Core
- Components of Cybersecurity Frameworks
- Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev. 4), NIST
- Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013), ISO
- COBIT 5, ISACA
- CIS ControlsTM, Center for Internet Security
- Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program (ISA 62443-2-1:2009), The International Society of Automation
- Security for Industrial Automation and Control Systems – Part 3-3: System Security Requirements And Security Levels (ISA 62443-3-3:2013), The International Society of Automation

Sources

1. NIST
2. Five Most Common Security Frameworks Explained, Origin
3. What is the NIST Cybersecurity Framework?, Digital Guardian
4. Five Functions, NIST
5. Raspberry Pi
6. Business Insider



About the Authors

Fred Gordy

Director of Cybersecurity, Intelligent Buildings

Fred Gordy is a smart building industry expert and thought leader with 20 years of experience in secure control system development and implementation for Fortune 500 companies. His control systems knowledge gives him insight on challenges of interlacing traditional IT environments with control systems for cohesive and security OT platforms. He has authored and participated in over 30 articles on building control cybersecurity with industry magazines as well as *The Wall Street Journal*, CNBC and healthcare publications. In the last decade, he has led control system cybersecurity workshops and has been a passionate speaker and teacher on the subject of building-control cybersecurity.

David Englebrick

Practice Manager, TEKsystems

With over 28 years in the telecommunications field, David Englebrick brings extensive experience in telecom design, operations, and research and development. His focus has been serving clients in the higher education and government markets.

TEKsystems
Own change

We're partners in transformation. We help clients activate ideas and solutions to take advantage of a new world of opportunity. We are a team of 80,000 strong, working with over 6,000 clients, including 80% of the Fortune 500, across North America, Europe and Asia. As an industry leader in Full-Stack Technology Services, Talent Services and real-world application, we work with progressive leaders to drive change. That's the power of true partnership. TEKsystems is an Allegis Group company.

INTELLIGENT BUILDINGS™

IntelligentBuildings® is an nationally recognized Smart Building consulting and managed services company who leads the industry in operational technology cybersecurity and vendor risk management solutions. We help customers leverage solutions that enhance experience, increase productivity, lower costs and reduce risks for new building projects, existing portfolios and smart community development.