TEKsystems Own change | INTELLIGENT BUILDINGS™

WHITE PAPER

# BUILDING RESISTANCE

*A LOOK AT OT, IT AND MITIGATING RISK*

Part 4 | **Smart buildings: What to consider when building an operational technology incident response plan**

## Assessing and Responding to Cyber-Risk

Incident response and disaster recovery for IT are not directly transferrable to operational technology (OT) / control systems. Some IT lessons learned and best practices can be used as starting points and frameworks for OT, but control systems and the underlying devices that support OT system requirements can introduce unique challenges to IT systems. Responding to a cyberevent in the control system space requires new and different strategies from those typically put in place within the IT space.

## What is an Incident Response Plan (IRP)?

According to Cisco, "an incident response plan is a set of instructions to help IT staff detect, respond to and recover from network security incidents. These types of plans address issues like cybercrime, data loss and service outages that threaten daily work.[1]" This is also true for an OT environment with a few edits. For OT, this statement would read: an incident response plan is a set of instructions to help OT (facility) staff detect, respond to and recover from control system and network security incidents. These types of plans address issues like equipment failure, physical damage, life safety as well as cybercrime, data loss and service outages that threaten daily work.

Webroot shows a six-step approach (*Figure 1*) of how to build an incident response plan, defined as "a detailed document that helps organizations respond to and recover from potential—and, in some cases, inevitable—security incidents.[2]" These steps are the basic outline for formulating an effective response plan to position an organization to quickly address breaches with the least amount of damage.

*Figure 1*


## Types of Incidents

A hacker may try to gain access to IT assets (e.g., databases) by using the control system as a pivot point to the corporate network. A control system attack adds a layer of complexity to defending the parameter of the company because the motivation may not always be clear. Some motivations are listed below:

- **Diversion from the actual intended target**—Disruption of operations could be a diversion to get attention focused away from the attacker's intended target.
- **Backdoor access into the corporate network**—Hackers have realized that systems could be nonsecurely connected to the corporate network. In this instance, they would want to remain invisible.
- **Disruption of service**—Attacking equipment with no other goal other than disruption.
- **Life safety**—An attack designed to either directly cause physical harm or cause chaos that could potentially cause physical harm.
- **Brand damage (defacing media)**—Attacks that infiltrate digital signage and display pornographic or other inappropriate or offending material.
- **Equipment damage**—Similar to disruption of service but with the expressed purpose of destroying equipment.
- **Ransom**—Financial gain through ransomware.

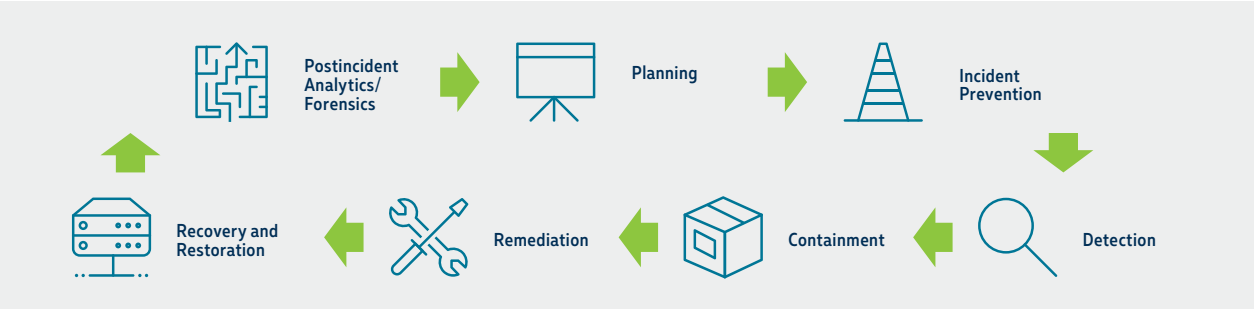
Motivations are varied, and they affect not only equipment/devices but can impact comfort and even safety. Therefore, the handling of an incident requires sometimes different or additional steps depending on the nature of the incident.

## Foundational Structure of an OT IRP

The U.S. Department of Homeland Security (DHS) recognizes that industrial control systems (ICS) have requirements not outlined in IT IRP guidelines. In 2009, the DHS released "Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability" planning guide.[3] ICS is akin to building control systems (BCS); although while ICS is usually associated with industrial automation, BCS is not as structured as ICS and uses different types of controllers. Additionally, BCS influences human environments more directly. But even with these differences, the similarities are enough that using the DHS ICS incident response planning guide is a great starting point.

The DHS ICS IRP (*Figure 2*)[3] shows the overall process differently than the Webroot six-step approach. They put an emphasis on cyclical steps and position it as a revolving and evolving process. As new events occur, the steps in the process must be reviewed to ensure that it keeps pace with emerging threats, with refinements being made after an event to improve future outcomes.

*Figure 2*




The key to a successful incident response is planning the steps necessary to respond, contain and recover from an event.

In order to prevent an incident, particularly in a control system environment, threat monitoring should be a part of the control system infrastructure. These systems provide far fewer detection capabilities, compared to typically IT. So, while IT solutions will provide some benefit, solutions designed specifically for the OT environment should be used.

"Detecting an incident early will help limit or even prevent possible damage to the control system and reduce the downstream efforts to contain, eradicate, recover, and restore the affected systems."

Documenting the steps necessary to contain an event for OT may require review on a system by system basis. What may work for one system may not fully work for another. Additionally, each unique incident will require tailored preventative steps to contain the situation depending on the origin of the incident (e.g., internal employee, external attacker).

Containing the event can prevent not only equipment damage but also life safety issues. When outlining containment steps, care must be given so that the act of containment does not introduce further issues in addition to the attack itself. You'll want to address the source of the initial problem while thinking through what other remediation steps may be required prior to getting a system fully back online (e.g., restricting/limiting access, removing equipment and malware).

"The control system environment introduces additional complexities related to recovery and restoration that would not be found in typical IT systems." Postrecovery there also steps such as recommissioning of the system to verify that full sequences of operations have been restored.

Postincident analysis and forensics consist of three subject areas: lessons learned; reoccurrence prevention or remediating weaknesses; and forensics.

*Source: U.S. DHS*

## Crawl, Walk, Run–Get Started

A good way to approach cybersecurity is using the "crawl–walk–run" strategy. Most organizations are in the crawling stage as far as cybersecurity control systems are concerned. With that as the baseline, creating an IRP will be successful if you build it in steps.

The first step is creating a control system incident response team (CSIRT). This team will work together to build out the IRP and be responsible for implementation and follow-through during and after an event. The second step is creating the policies and procedures that will govern the IRP.

### Team assembly and roles

An effective CSIRT will comprise a wide range of roles and perspectives to ensure incident response is met with a holistic approach to timely action, thorough analysis and future prevention, mitigation and organizational safeguarding. A CSIRT may be composed of a combination of specialists dedicated to this effort or part-time staff with other day-to-day responsibilities. CSIRT refers to the internal response team directly supporting the security of the building control systems.

The responsibilities of a CSIRT will vary (*Figure 3*). Responsibilities may also be shared among different departments that have not traditionally provided support to the BCS security team. The CSIRT's responsibilities may include:

- Acting as an expert resource on cybersecurity threats and vulnerabilities
- Serving as a clearinghouse for incident prevention, information and analysis
- Developing organizational policies and procedures related to incident response
- Understanding safeguards on the control systems
- Identifying operational impacts to the organization in the event of an incident
- Creating and testing an incident response plan
- Acting as a single point of contact for all internally reported incidents or suspected incidents
- Responding to incidents if one occurs
- Reporting to key stakeholders and external agencies after incidents, such as law enforcement
- Gathering forensic information to support analysis and any legal actions
- Implementing safeguards to prevent a recurrence of an incident
- Remediating the control systems after an incident

Although every organization will not be able to staff each position directly, each role should be identified and assigned, even if it's part time, with staff having multiple roles or with personnel from a control system integrator. Facility operations engineers have unique knowledge and experience and should always be a key member of the CSIRT.

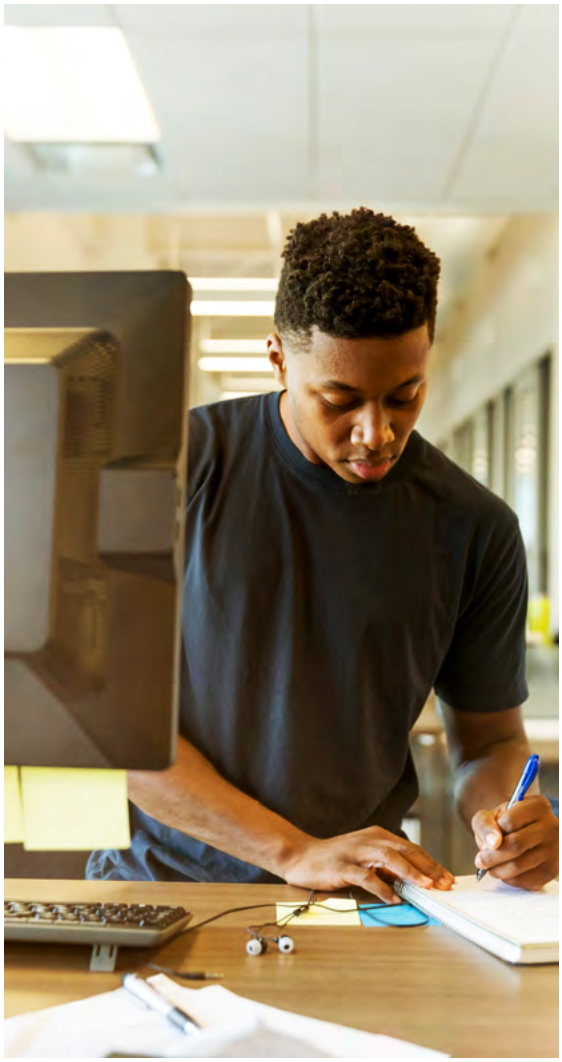


*Figure 3*

**Possible CSIRT Team Members**

| ROLE | RESPONSIBILITY |
|---|---|
| **CSIRT Team Manager** | Sees that the team is organized and accomplishes its objectives |
| **Facility Operations Engineer** | Serves as the subject matter expert on building control system architecture and understands the system components and products being produced or supported by the control system(s) |
| **Network Administrator** | Provides a key role if the incident involves a cyberattack originating from the computer network |
| **Security Experts** | Provides cybersecurity expertise but may include physical security and law enforcement |
| **Legal Experts** | Provides expertise across legal several areas including:<br>• Ensuring compliance with all national, international, federal, and state laws and regulations<br>• Explaining what evidence is admissible when taking action<br>• Specifying how evidence can be collected<br>• Knowledge of third-party maintenance liability exposure<br>• Helping the team understand what pitfalls (e.g., privacy rights violations) should be avoided<br>(Also critical in preparing the IRP, enabling state and status reporting, and conducting forensics and data collection) |
| **Public Relations Specialist** | Plays a critical role if the incident causes noticeable disruption to service or impacts the owner to fulfill contractual obligations; ensures the appropriate information and messaging is sent to the public via the news media |
| **Human Resources Specialist** | Supports CSIRT activity if the incident is being attempted or carried out by someone inside the organization; typically handles legal issues, policies and procedures, and punitive actions |
| **Vendor Support Engineers** | Provides technical support to the asset owner, given the specific and essential knowledge held as a member of the vendor's technical staff |

While the primary focus of the CSIRT is to handle cyber-related incidents, the response team can also be involved in noncyber events, such as control system outages, catastrophic equipment failure or natural disasters.

## Policies and procedures

While having policies and procedures is critical in most business functions, it's extremely important in incident response because decisions are being made under pressure of production stoppage, high financial cost and in situations where those with authority may not be readily available. IIt's also crucial when developing these foundational procedures and supporting policies that team members are not under pressure, making sure these policies are thoroughly thought through, informed and vetted..

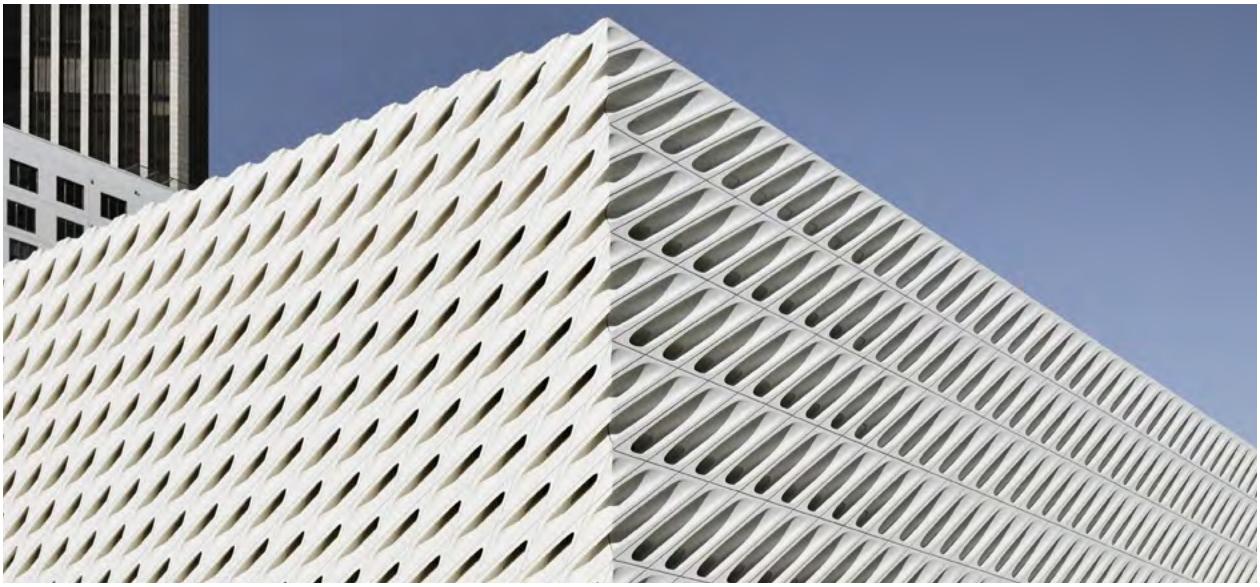
Clearly written, detailed operating procedures should be developed to implement the incident response policy. The procedures found in an IRP are similar to those found in noncyber emergencies and should be tested before an event occurs.

The initial incident response policy should direct the establishment of the CSIRT and lay the foundation for the IRP. The IRP should define the authority of the CSIRT and will be the backbone of the procedures and actions defined in the plan.

## Building the IRP

The cyber IRP establishes and documents the procedures and actions that implement the incident response policy for the BCS. It defines security incidents, outlines the steps that should be taken to respond to the incident and mitigates damage to the organization. The following key sections should be considered when creating the plan:

- **Overview, goals and objectives**—These sections define what will be accomplished. Here, the organization can provide direction and guidance for overall business objectives in comparison to the response options to the incident.
- **Incident description**—In the control system environment, clear definitions of what a security incident is must be identified and communicated. This is particularly important when considering whether equipment failure or unexpected software behavior is caused by a cybersecurity incident, due to mechanical failure because of wear, environmental conditions or other nonsecurity-related factors. Differentiating between cyber-based incidents and those caused by other sources is critical.
- **Incident detection**—This is also called "discovery" and includes ways to identify and report an incident. Detecting most incidents will require automated analysis tools, system behavior patterns and an awareness of what to look for among operators, supervisors and other staff.
- **Incident notification**—Once an abnormal event is identified, it needs to be prioritized to determine the cause and whether this is a minor system event or if it requires immediate escalation.
- **Incident analysis**—Procedures in the plan should address how to evaluate and analyze a reported incident. The incident might be reported by internal or external sources and could happen at any time.
- **Response actions**—This section is essential to the plan because it defines the procedures to follow for each type of detected incident. An incident never occurs at a convenient time—there will be increased stress and pressure on staff, little time for testing options, and every action will be watched and measured by upper management, stakeholders and perhaps even by the public.
- **Communications**—While elements of communications can be included in the response actions, the topic is unique enough that it could be addressed in a separate section in the IRP.
- **Forensics**—Cyberforensics focuses on collecting, examining and analyzing data related to an incident, along with protecting incriminating evidence for use in legal action against a suspected offender. This data can be found in available logs (e.g., networks, servers, workstations), physical components (e.g., hard drives, bitmap images of the affected real-time operating system), emails, voicemail, texts and telephone records. While the information gathering can be useful in understanding the incident and preventing further actions, the approach has nuances related to data integrity and protection that go well beyond just learning about an incident.



## A Foundation for Success

Once the team is assembled, the policies and procedures are created and the IRP is built, we recommend conducting drills to ensure that all members of the team, and potentially affected personnel, understand their roles and responsibilities. During an event is not a time to discover how the process works or doesn't work. Even the best response plans can't anticipate all the obstacles brought about by a real incident, nor can they anticipate how people will react to unforeseen situations. The people who were expected to be available and fill certain roles will often be inaccessible, or new people may have replaced previously trained workers. Unanticipated events may also occur where decisions need to be made with little or no time for analysis.

There are many ways to build an effective IRP capability within a company and specifically for OT used in providing control, comfort, safety and convenience in today's smart buildings. The steps outlined throughout lay the foundation for analyzing and understanding the BCS environment and preventative actions responses and management needed should an incident occur.

Three key areas to keep in mind as you assess, plan and start to develop an IRP:

1. Learn from the experiences of previous incidents, both internal and external, to the organization.
2. Prepare for incidents by formulating an effective response plan with well-thought-out policies and procedures.
3. Assess the vulnerabilities within the control system(s) and then implement protective measures to safeguard those systems.

In the event of a real cyberincident, additional reactive actions should be discussed. They include ways to detect an incident, contain its effects, remove the threat from the control system(s) and restore the system(s) to normal operations.

Many times, the only thing preventing an incident from becoming a disaster is a robust IRP. Developing a strong and diverse CSIRT will ensure that the IRP has a broad scope and is inclusive of the largest number of possible threats. Practicing an IRP on a regular basis and learning from the events will make it efficient and effective, and better position you to protect your organization at large as the threat landscape continues to evolve.

## Disclaimer

*This paper is intended to give the reader a general overview of what an IRP may involve, rather than providing a step-by-step guidebook. The information included may not be sufficient enough to build a fully vetted IRP. It's recommended that the organization consult subject matter experts to construct a formal IRP.*

## Additional Information and Resources (for ICS)

- H.R.1158 - DHS Cyber Incident Response Teams Act of 2019
- Developing an Industrial Control Systems Cybersecurity Incident Response Capability, U.S. DHS
- Updating Antivirus in an Industrial Control System, U.S. DHS
- Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies, U.S. DHS
  - Abstract
  - Full Report
- Creating Cyber Forensics Plans for Control Systems, U.S. DHS
  - Abstract
  - Full Report
- Developing an Industrial Control Systems Cybersecurity Incident Response Plan, U.S. DHS
  - Abstract
  - Full Report
- Patch Management for Control Systems, U.S. DHS
  - Abstract
  - Full Report
- Remote Access for Industrial Control Systems, U.S. DHS
  - Abstract
  - Full Report

## Sources


1. Cisco
2. 6 Steps to Implement an Incident Response Plan, Webroot
3. Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability, U.S. DHS

## 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.