TEKsystems Own change | INTELLIGENT BUILDINGS™

WHITE PAPER

BUILDING RESISTANCE

A LOOK AT OT, IT AND MITIGATING RISK

Part 3 | **Smart buildings: Risks and reality**

A New Threat Landscape Takes Shape

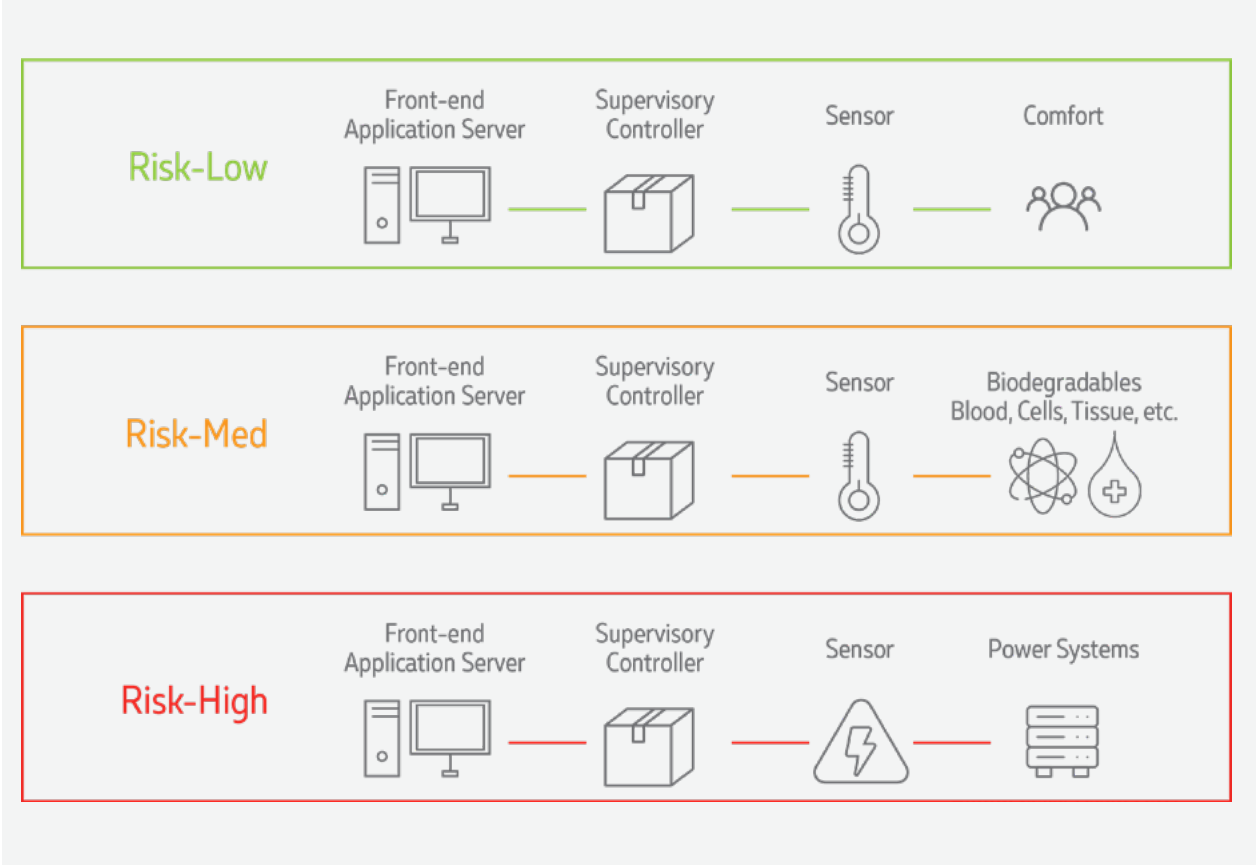
The field of cybersecurity for building control systems is a relatively new space. Statistics and findings have only recently become available as a heightened sense of attention has been applied to this emerging threat landscape as organizations seek to better understand it. What is apparent is that there are varying degrees of awareness around what cyber and operational risks are currently present within these critical systems and some of the real-world examples of how threats have taken shape within them.

The Reality of Risks

Control systems are designed to perform a wide variety of objectives that vary in complexity and risk surface. These objectives include simple operations—like controlling the heating and cooling of office spaces—where the associated risks are low. However, heating and cooling more critical environments—like operatory suites—increases the risk surface (*Figure 1*).

Identifying risks within these control systems and devices is often overlooked, and as a result, the reality of risks may not be identified until after an event occurs. For example, an inexpensive communication converter used by a data center fails and the device didn't have a risk assessment completed prior to the failure. Without a documented response for the event, a vendor may spend more than three days trying to bring the device back online. Neither the data center nor the vendor had a replacement device on deck to use in the event of a malfunction, leaving them without functionality in the interim. Additionally, the communication converter was over 11 years old and well past its end-of-life manufacturer support.

Figure 1



Had a risk assessment been performed, the data center would have been positioned to mitigate these risk points and prepare for such an event, thus limiting the impact should a failure ever occur.

To truly start to identify risks, you must first understand a device's strengths, limitations and overall objective. In the previous example, the communication converter was designed to convert serial (two-wire) communication to IP (network) communication. If a risk assessment had been performed prior to the failure, the data center would have understood the following information about the device:

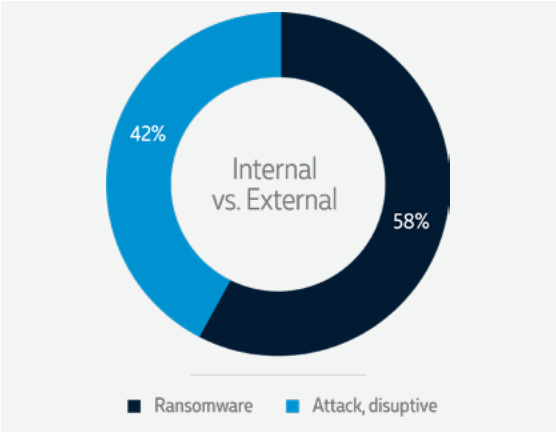
- **Objective:** monitoring the cooling of the data center server floor
- **Function:** communication from the field equipment to the application server
- **Life cycle:** support had run out—it was past end-of-life status for manufacturer support
- **Vendor support:** did the organization have personnel that could support this device
- **Recovery:** the steps required to recover the device or replace it, if needed

Based on the minimal cost of the communication converter, it would have been advantageous for the data center to have a backup device on hand or require the vendor to maintain a backup. After the risk assessment, the data center may have also determined (because of the criticality of the malfunction) to have personnel trained to replace and recover the system, should a malfunction ever occur.

Attacks Risk vs. Operational Risk

Attacks from outside hackers are usually what come to mind when considering control system threats. The risks associated with this type of attack should always be a part of a robust cybersecurity strategy. However, attacks can also come within. Disgruntled employees—both internally at the organization and system vendors—can pose potential threats. To create a well-rounded cybersecurity strategy, operational risks must be reviewed and planned for to round out a fully instituted risk program (*Chart 1*).

Chart 1



Attack risk

External attacks are starting to occur more frequently. The primary source of these attacks is ransomware delivered via phishing emails. Incidentally, this form of attack on a control system's front end is almost 100% avoidable if machines are used only for their intended purposes.

In all of the incidents we have investigated, ransomware was deployed because an employee staff member checked their email on the front-end / application server. Historically, facility staff has treated the front-end / application server as a workstation and used it much like a personal machine. This would be akin to someone in your organization using a SharePoint server or email server to browse Facebook. The front-end / application server needs to be treated for what it is: an application server and not a personal machine. Users should only access applications from a workstation (*Chart 2*).

Chart 2

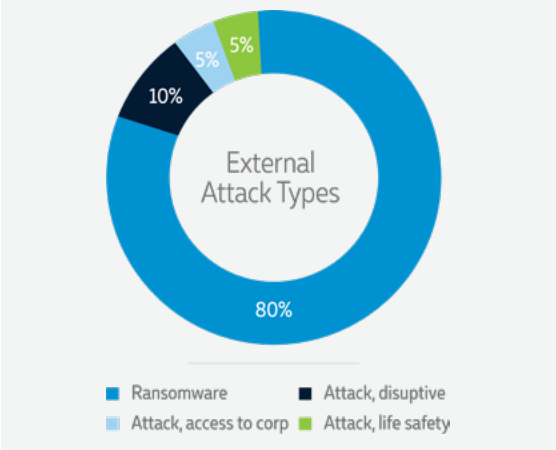


Chart 3

Response to Facility-Specific Phishing Campaigns

	Yes	No	Description
% Phished	58%	42%	Percentage of users who clicked on the link in the body of the email and were redirected to the training video
% Replied	10%	90%	Percentage of users who replied to the phishing sender's email address
% Avoided	25%	75%	Percentage of users who took action
% Trained	5%	95%	Percentage of users who were phished that completed the training video

As part of a risk assessment process, facility-specific phishing campaigns (FPC) are used. An FPC is not like typical IT-type phishing campaigns. FPCs are designed to appeal to facility staff to test their awareness. To date, these types of tests have shown that facility staff are generally not ready for this type of attack (*Chart 3*).

Ransomware can be easily overcome if a system is being backed up to any location other than the front-end / application server. In almost 90% of the attacks we've observed through our work/observations, the systems had no viable backups in place. Those that did back up their system:

- 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

A disruptive attack can cause service interruption or sometimes even physical threats. For example, a bad actor accesses an exposed company printer and prints out a document saying, "There is a bomb in the building." In such an event, the building would be evacuated and authorities called to search for a bomb. Despite no bomb being found, the damage has already been done: brand damage to the owner of the building, loss of productivity and loss of confidence of the tenants. In this case, if a risk assessment of the control system network had been performed, it could have identified the exposed printer. As with most control systems, an accurate inventory helps identify devices that are not supposed to be connected to the network.

Operational risk

Control systems for operational technology (OT) devices are not like IT, and operational risk can often slip under a company's radar. A control system requires high availability and accessibility between devices. These devices work in concert to run finely tuned sequences of operations to deliver their services in the most efficient and effective way. A lot of these devices are not as robust as IT assets, which means they can't withstand IT scanning and monitoring tools. These tools can knock these devices offline, and manual intervention may be required to restore communications.

In Figure 2, supervisory controller (SC) A requires a value from SCs B and C in order to perform the critical function of maintaining a constant temperature in a blood storage unit. It may also control airflow in operatory suites. An IT scan locks up SCs A, B and C (*Figure 3*) and communication is lost from the front-end / application server. SC A needs the values from SCs B and C to maintain temperature or airflow. As a result, facility staff can't monitor the system because communication to the SCs is lost. Because the SCs will also not be able to receive high-temperature alarms from the blood monitoring, blood may be lost due to high temperatures and low-flow alarms from the operatory suites—which causes positive air pressure and may create unsanitary conditions.

Figure 2

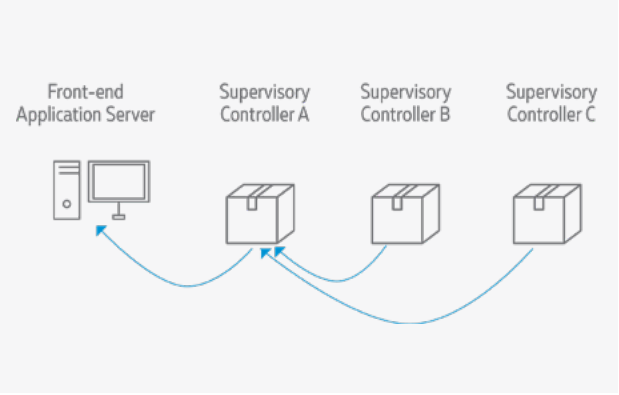
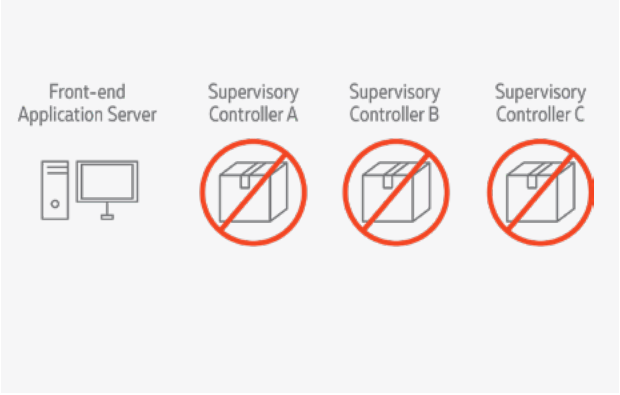


Figure 3



In one case, a client's IT department updated Java on several control system front-end / application servers. The update crashed the application and it couldn't be restarted because the Java version was not compatible with the application. As a result, surgeries had to be canceled, which caused a ripple effect on the schedules and a lot of unhappy patients. IT had to uninstall the Java update and the control system vendor had to reinstall the application. Vendor intervention was required to get the systems fully functional, but the damage due to the failure was already done.

IT is becoming more involved in the process of security building control systems, but policy and education must occur for both IT and OT. Patching a control system front-end / application server must be tested either internally or by the servicing vendor before installing. When a patch installation is scheduled, trained facility staff and/or the service vendor needs to be on site to ensure the system is fully functional post-install.

Vulnerability scans by IT should also be tested in a nonproduction environment because scans have been known to knock controllers offline. IT and vendors can work with facility staff to develop a scan profile that can function on the control network without causing issues. It's also recommended that when scans are performed with a modified-for-control system scan profile, facility staff be notified of the date and time of the scan so they can monitor the system for disruption to system device communication.

Human behavior and error can also create operational risk. Human behavior—such as misusing the front-end / application to check personal email—opens the system to vulnerabilities. Shared user accounts, simple passwords and passwords taped to monitors are other examples of behaviors that increase operational risk. Implementing and enforcing user policies significantly decreases this risk (*Chart 4*). However, introducing and integrating these policies takes time and effort. Introducing a new policy must occur in stages, tackling the riskiest behaviors first. Implementing the policies and training in stages increases the likelihood that employees will adopt and maintain them. Onboarding existing facility staff through policy workshops is recommended.

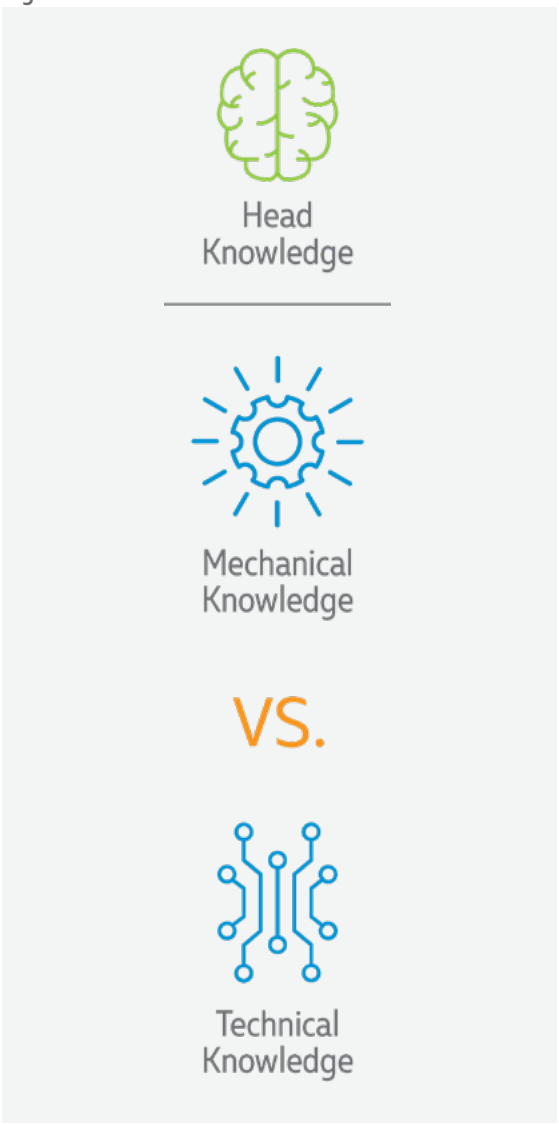
Chart 4

***Chart 4** – Most facility users are not trained in cyber-awareness. Even the trained user can fall prey to an attack. The cybersecurity landscape is always changing, so reoccurring training is recommended.*

Know What You Know and What You Don't Know

One type of risk that may be surprising is knowledge (*Figure 4*). Knowledge becomes an operational risk when it is isolated to one or a few employees. Many facility groups fail to consider that failing to properly document system knowledge poses a significant risk to a company's operational efficiency.

Figure 4



Head knowledge

Too many organizations have an employee that maintains the bulk of the knowledge for a system. If anything happens to the system, that employee is the one who takes care of the issue. But what happens when that employee is not available to fix an issue? Perhaps they are off site or worse, left the company entirely. When that happens, a department is often left in a bind and can't function at all until someone is located who knows how to fix the issue, which costs time and money.

To minimize the risks, critical knowledge must be documented and maintained so that others can react to issues during an event. The documentation should be configured in a step-by-step format to allow others to systematically return the system to an operational state—and if possible, not damage any forensic data. These states should be tested and reviewed to ensure the appropriate staff is trained to handle possible situations.

Mechanical vs. technical knowledge

Mechanical—Traditionally, building systems were mostly mechanically based. The knowledge needed to run these systems didn't require computer knowledge, but this has since changed for facility staff. Staff is trained to use computers but could potentially still run a building without a computer.

Technical—Facility staff now includes a generation that grew up with the internet and home computers. Buildings now include smart, app-controlled T-Stats, lighting control and locks with more connectivity points being developed every day. For this generation, navigating complex control systems, fault detection and diagnostics (FDD), analytics, and unified user interfaces (UUI) comes more naturally and intuitively. Some of these employees can even reload operating systems and reinstall applications.

The risks

As the workforce ages and mechanically based staff retire, evidence is surfacing that less tenured staff may not be ready to assume control of building systems without a computer interface. This points back to head knowledge and documenting the systems. However, there are times that even this documentation can't replace a full understanding of the mechanics, troubleshooting and diagnosis needed for these systems. Planning for this transitional period through internal training and/or vendor support must be initiated to position an organization for success.

Adapting to Change

Minimizing operational risks requires expanding knowledge across IT, OT and facility management staff.

IT/Facility Staff—IT's role is to secure the parameter. These employees are very skilled at doing so; however, IT can be an unintentional hindrance if they're not educated on how to handle all needed devices. A working group of an IT representative, facility representative and various system vendors may be needed and can succeed if all parties respect each other's strengths and create solutions that mitigate risks and strengthen the overall security posture of the building control systems.

Behavior—Facility staff must begin to view the building systems as a target for hackers. Companies must recognize the risks involved and take the appropriate precautions to mitigate risks, such as implementing and enforcing user policies. Quickly adhering to a cyberaware culture will minimize the number of sites that fall prey to hackers.

Knowledge—Sometimes being the primary knowledge keeper of a subject translates to job security. However, isolating this knowledge can also lead to large-scale issues if a system goes down and no one is on site to fix it. This process could lead to major negative impacts on an organization through brand damage, loss of productivity, loss of data and even life safety issues. Head knowledge must be documented knowledge, followed up with processes and dissemination to the appropriate user groups. The wealth of knowledge that both sides possess will only help the overall resilience of your organization.

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.