WHITE PAPER

BUILDING RESISTANCE

A LOOK AT OT, IT AND MITIGATING RISK

Part 2 | **Smart buildings: The evolution of operational technology hackers**

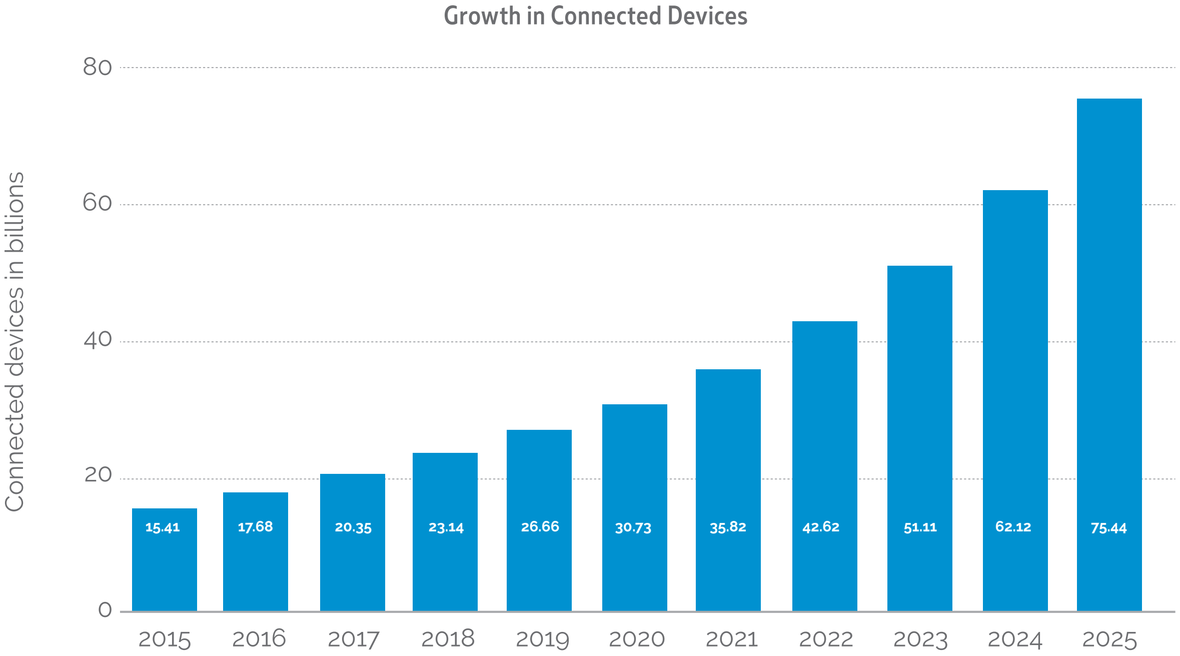
A New Threat Landscape

Cyberattacks on connected Internet of Things (IoT) devices are rapidly increasing. According to McKinsey Global Institute, an estimated 127 new devices connect to the internet every second,[1] bringing breed to a host of new access points for hackers to explore. And that number only stands to increase in the coming years as technology evolves and connectivity multiplies. "This year, there will be 26.66 billion devices connected, and 75.44 billion devices will be connected by 2025 (*Chart 1*).[2]"

Despite the inevitable increase in connection points and connectivity, there seems to be a disconnect with business leaders around what this new landscape will look like, with 98% of business leaders saying they're unclear on what IoT means.[3] With Gartner reporting that, "By 2023, the average CIO will be responsible for more than three times the endpoints they managed in 2018,[4]" it's more important than ever to start understanding the threat landscape that's on the brink of threatening many organizations.

This rise in IoT devices has greatly increased the attack surface for hackers, giving hackers a target-rich environment. With a much larger attack service, basic cybersecurity best practices are often not followed.

Chart 1

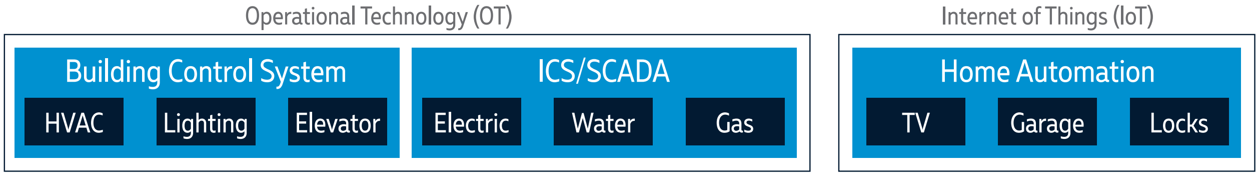


IoT vs. Operational Technology

Are IoT and operational technology the same thing?

IoT and operational technology (OT) are not the same thing but are related. IoT can be found in homes and personal devices, while OT is found in buildings and controls—things like commercial HVAC, lighting, elevators, access control, cameras, water treatment and power monitoring. This type of OT is commonly referred to as building automation or building management systems (BMS). Critical infrastructure (e.g., oil and gas, power grid, water control) is also considered OT but is known to vendors as industrial control systems (ICS) / supervisory control and data acquisition (SCADA).

Image 1



Hackers

What is a hacker?

Merriam-Webster defines hacker as "a person who illegally gains access to and sometimes tampers with information in a computer system."

Stuart Coulson, director of hosting and cloud computing specialist, puts it this way: "But contrary to popular belief, not all are motivated by the prospect of obtaining credit card details or personal data that they can sell for cash. Not all that fall into the hacker category are cybercriminals. Not all are human.[5]" Other experts, such as Eric Chabrow, GovInfoSecurity, agree and further simplified Coulson's list of hacker categories. Below is Chabrow's list of real-world, cybersecurity-defined hacker levels. The higher the number, the greater the threat they pose.

Image 2

1. **Script Kiddies:** Use existing computer programs designed to hack. They are not true programmers.
2. **Hacking Group:** Informal groups of hackers whose goal is disruption and publicity.
3. **Hacktivists:** This group's goal is also disruption and publicity; however, their motivations can range from social change to political agenda. This group is cause oriented.
4. **Black Hat Professionals:** This hacker type is usually an expert programmer. They do not seek publicity and usually do not seek to destroy. They figure out ways to penetrate challenging targets and have been known to cost businesses and governments sizeable amounts of money.
5. **Organized Criminal Gangs:** Organized crime hackers who follow a code of conduct to avoid detection. Attacks from this group tend to be long-term, targeted attacks against banks, law firms and big business in general for financial gain or reputation damage.
6. **Nation-States:** Backed by a national government to infiltrate other national governments, although they're now also targeting businesses. This is the most sophisticated and organized of all the groups.
7. **Automated Tool:** Other names are bot, botnet and zombie. It is software designed to perform a malicious task. Usually there are a large number of bots used to perform attacks.

Social engineering is often a central strategy used to access target networks.[6] By finding the weakest, most vulnerable entry point—unfortunately often an individual employee—they're able to infiltrate and organization despite the best laid IT security protocols, firewalls or infrastructure.

What is a hacker's motivation to attack OT systems?

To understand why a hacker attacks OT systems, we must first understand the ground-zero motivation. People's innate curiosity is to understand how and why devices operate. To hackers, these devices are like puzzles to be solved and led to the earliest hacking episodes. In addition to curiosity, hackers are motived by gain.

With the digital revolution taking place in today's society, owning and accessing data is paramount. Sensitive data such as financial information, health information or other personal information can be sold at a high price, thus making "hacking" a growing field. As such, the risk profile for a typical company in 2019 has increased and protecting data has elevated to a core corporate concern.

Other motivations include:

- Ego
- Making a statement (hacktivist)
- Disgruntled employee
- Corporate espionage
- Country vs. country

Hackers with these motivations either hack anonymously, gain notoriety or cause damage (brand or physical). Hacking of this nature is typically aimed at IT systems.

Since the introduction of IoT and OT devices, the attack surface has grown exponentially. Hackers now have many more points of entry and vulnerabilities to exploit. Hacking used to be easier, as these networks were not monitored, had little to no security and, in some cases, bridged to the corporate network.

Signs that devices are being manipulated become more prominent as hackers are able to gain access to control systems and subsequent devices. This malicious infiltration can lead to a host of problems for an organization, including brand damage, corporate espionage and lost data. Today, the damage created by hacking also includes life safety and property/equipment damage. The opportunity to attack life safety and property/equipment is especially attractive to nation-states and other organized criminals.

Preparedness and Entry Points

The "arms race"–IT vs. hackers and the "third world" OT security

IT has been playing defense in an arms race with hackers for years. IT defense tends to be reactive rather than proactive in its response to hacking and cyberthreats. Hackers continually change their methods and attack vectors, making it hard for IT to get ahead of the attacks. Hackers have a wealth of tools at their disposal—and what they don't have they can either build, buy or steal to get around IT defenses.

However, IT has had years to prepare and budget for cybersecurity. If IT experiences a cyberattack, they can buy new or update existing tools to bolster their defenses. IT now expects and reacts promptly to change—budgets allow for hardware to be replaced every three to five years and software to be upgraded and updated often.

OT, on the other hand, performs upgrades only out of pure necessity. Because OT operates on a delicate balance of what is necessary to maintain a functioning control system, updates and patches are often viewed as having the potential to disrupt and create additional work. Unlike IT, OT has not prepared for cyberattacks and as such, often doesn't have insight into proper security.

Image 3

IT
ready to go

Hacker
all the tools

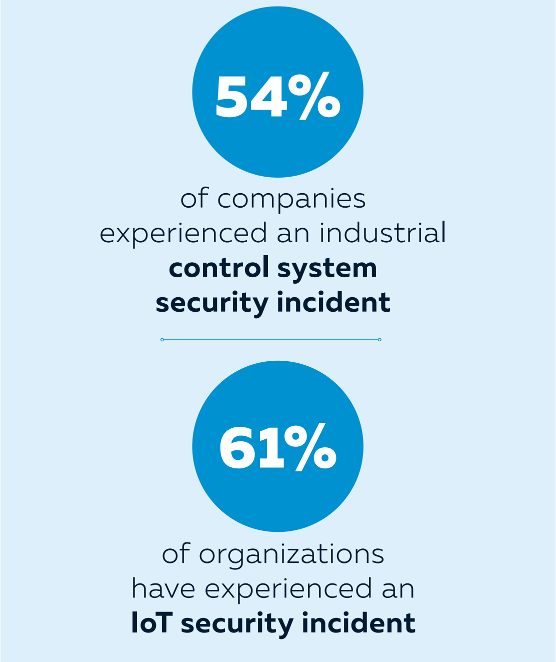
OT
no idea

Looking for the weakest point

Hackers now understand that control systems can often be the weakest point of a company's security. This attack vector is becoming more and more appealing.

Cybercriminals are looking for easy targets, like systems that are not using strong passwords, intrusion detection or detailed activity logs. A hacker can access an OT network for up to a year without being detected. According to CSO Online, "It takes organizations an average of 191 days to identify data breaches.[7]" If a hacker finds an OT network that is bridged to the corporate network, they can quickly enter the network, access the data and leave before they are detected. The hacker can also observe the network for reactions to their probing, if any, leaving them at a great advantage for future attacks. These entries are possible because the OT network is not being scanned.

Image 4



54%

of companies experienced an industrial **control system security incident**

61%

of organizations have experienced an **IoT security incident**

What have they done?

Ransomware is the number one attack vector (*Chart 2*) of OT system front ends. This is because employees will use the OT system front end to access email, surf the web and check social media. In the majority of cases, backups did not exist or were stored on the infected machine. This year, the number of ransomware attacks has increased to 400% from 2016 (*Chart 3*).

Other attacks, while less numerous, had the most potential to cause equipment damage and life safety issues. Many different types of buildings have been attacked, such as central plants and air handling units that controlled critical environments. In one instance, an attacker hacked a parking garage printer and printed a bomb threat, causing a building-wide evacuation. These attacks can cause lasting damage. For example, a recently attacked central plant required 92 days to fully recover. These are just some examples of attacks; the full extent of OT hacks is unknown due to lack of reporting.

Chart 2

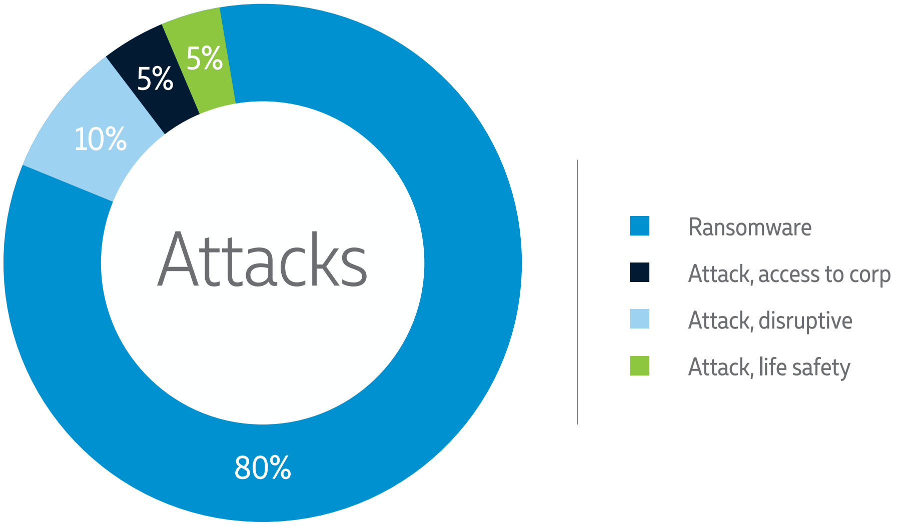
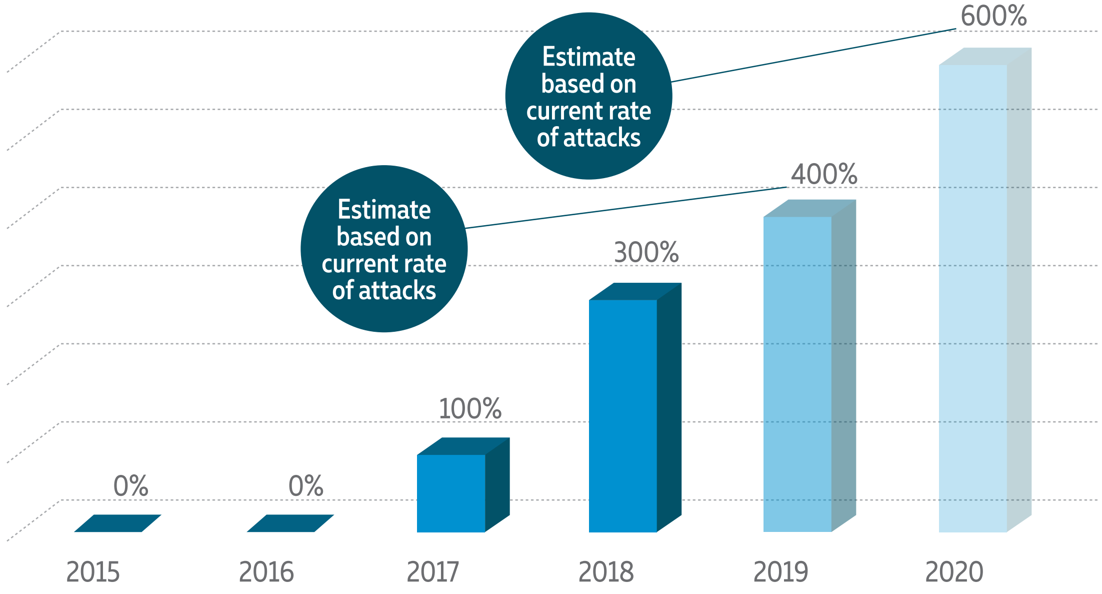


Chart 3

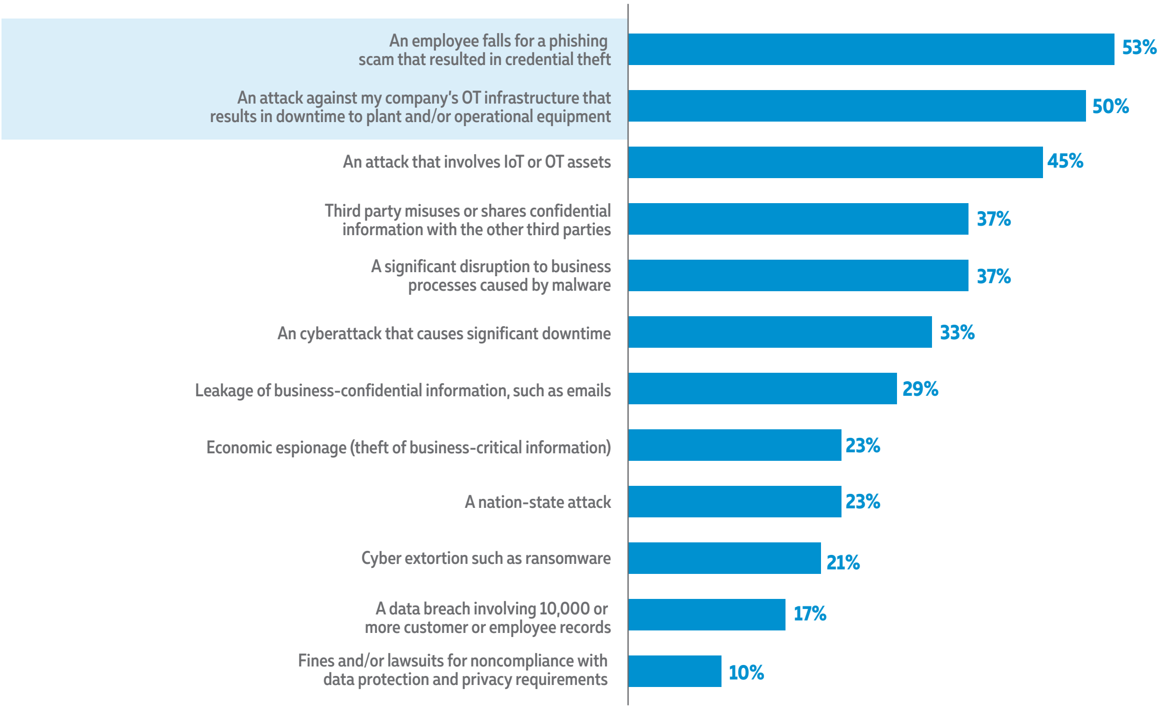
Annual Rate of Ransomwear Attacks on BAS Front Ends



According to an April 2019 posting from *SecurityWeek*, "A majority of organizations that have operational technology (OT) infrastructure experienced at least one damaging cyberattack in the past two years, according to a survey conducted by Ponemon Institute and Tenable[8]." Half of the respondents reported that the OT hacks they suffered resulted in downtime of the plant and/or operational equipment.

Chart 4

Cyberevents Experienced in the Past 24 Months

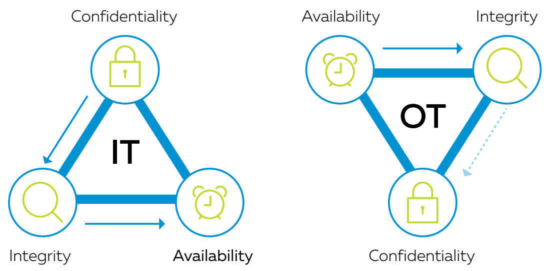


Conclusion

Hackers are opportunists. The end always justifies the means. In other words, their primary focus is accessing, stealing and/or disrupting information and systems. OT, in most cases, offers a pathway of least resistance to a hacker's end goal. Hackers can easily attack OT systems due to years of building openness (e.g., cross-platform interaction for manufacturers, ease of system serviceability and the reduced cost of ownership). Simply put, OT systems are designed to be available.

Image 4 shows both the IT triad and the OT triad. The IT triad places priority on "confidentiality," followed by "integrity" and lastly "availability." Conversely, the OT triad's first priority is "availability" closely followed by "integrity." "Confidentiality" is usually not even considered in most cases. With "availability" comes opportunity for the hacker.

Image 4



Due to the nature and function of OT systems, it needs to stay highly available to the other devices and to the staff that supports these systems. However, a layer of protection around the systems must be incorporated. Availability needs to be controlled. The system inside this protective bubble can remain open, but external access has to be restricted and monitored to curtail the ever-growing threat that hackers are posing to these systems. Doing this requires the following basic best practices:

- Start with an IT/OT assessment to identify connected devices, giving you a baseline of all connected devices in the network
- Remove all unrestricted public-facing access to components of the OT system
- Control vendor access through policy and enforcement
- Establish unique users and role-based access control
- Incorporate threat monitoring designed and implemented specifically for OT systems
- Remove both vendor and manufacturer default credentials
- Develop policies and procedures

Although not a complete list, these steps can take an organization off the hacker's radar as the organization continues to improve its overall OT cyber posture.

Sources

1. 127 New IoT Devices Connect to the Internet Every Second, McKinsey Global Institute
2. Internet of Things–Number of Connected Devices Worldwide 2015-2025, Statista 2019
3. Aruba Networks
4. Gartner
5. The Seven Levels of Cyber Security Hacking Explained
6. The 7 Levels of Hackers
7. Top Cybersecurity Facts, Figures and Statistics for 2018
8. Most OT Organizations Hit by Damaging Cyberattacks: Survey

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.