

# Guide to Cyber Protection for Buildings and Facilities

# Operational Technology for Buildings

Operational Technology (OT) for buildings refers to the hardware, software and network systems that manage, monitor, and control the physical devices and infrastructure within a building.

Systems include:

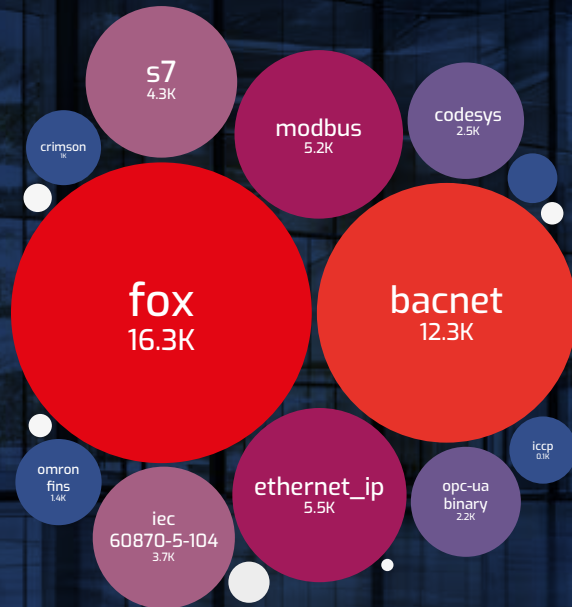
- Heating, Ventilation, and Air Conditioning (HVAC)
- Lighting
- Access Control
- Security Cameras and Alarms
- Elevators and Escalators
- Fire and Life Safety
- Environmental Monitoring

Unlike Information Technology (IT), which focuses on data processing and communication, OT is concerned with the direct control and automation of physical machines and processes.



# Building Technology Risks

Communication protocols commonly used in building control systems – Fox, BACnet, and Modbus - are the most publicly exposed in terms of the number of systems across all types of OT systems.<sup>1</sup>



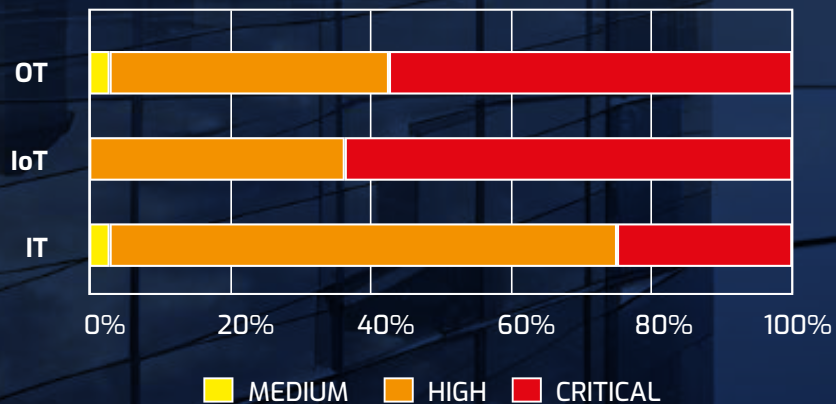
# Riskiest Connected OT Devices

- Uninterruptible Power Supply (UPS)
- Programmable Logic Controller (PLC)
- Engineering Workstation
- Building Automation
- Remote Terminal Unit (RTU)<sup>2</sup>

“Buildings typically contain several of the most riskiest connected devices”

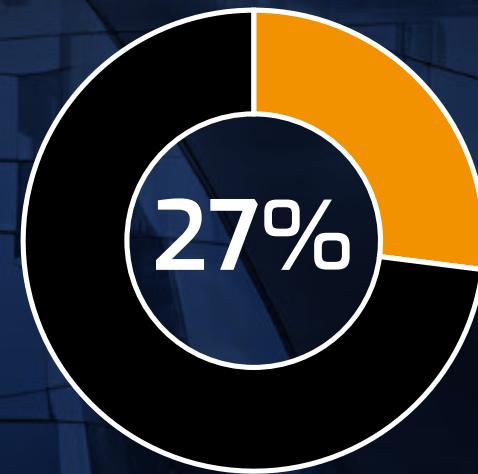
## Vulnerability Severity Category

OT and IoT devices each account for >50% of critical vulnerabilities<sup>3</sup>



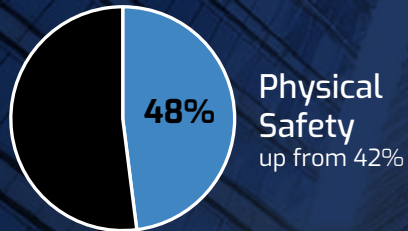
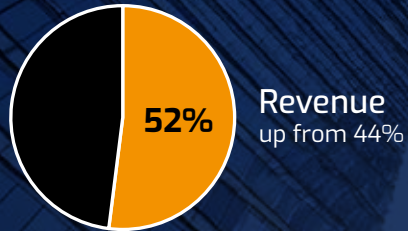
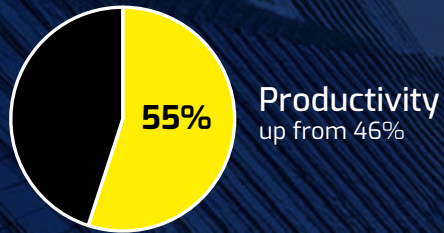
## Prevalence of Building Cyberattacks

More than 1 in 4 facilities experienced a cybersecurity breach in the past 12 months<sup>4</sup>



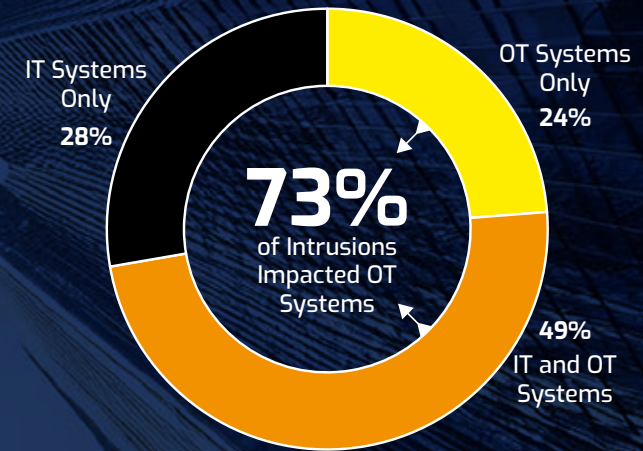
# The Impact of Intrusions

Operational outages made the following impacts<sup>5</sup>:



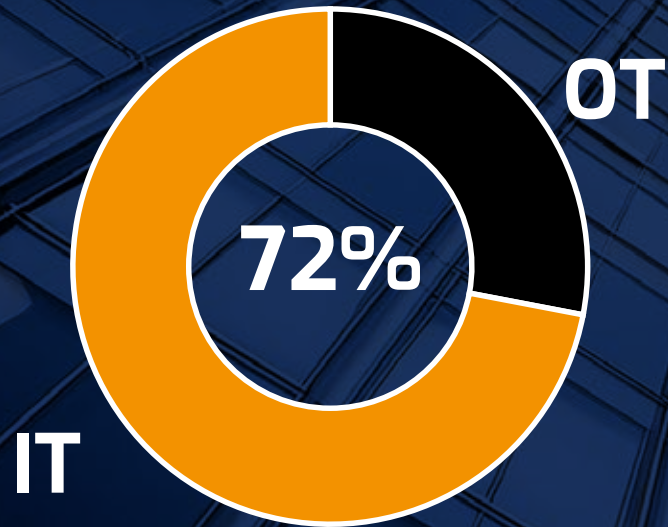
# Intrusion Prevalence on OT Systems

The majority of intrusions impact OT systems<sup>5</sup>



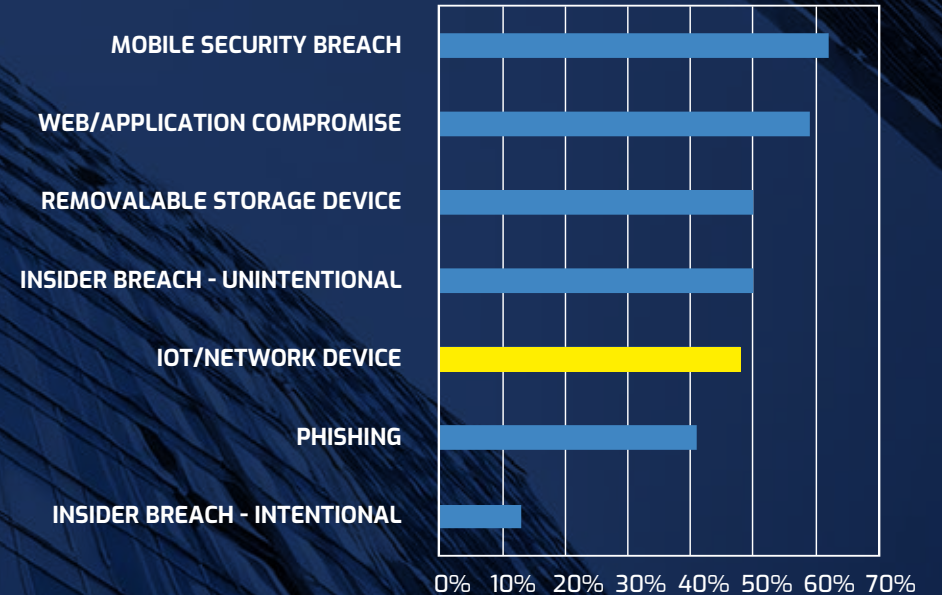
# OT Attack Origination

The majority of OT attacks started with IT systems<sup>6</sup>








# Most Prevalent OT Intrusion Techniques

Nearly 50% of OT intrusions involved an IoT/network device<sup>7</sup>

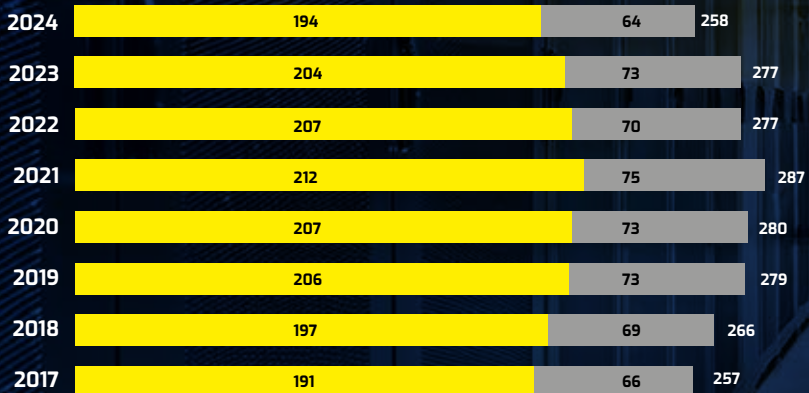


# Building Cyber Incidents and Related Impact<sup>8</sup>

 LOCATION	 BUILDING TYPE	 INCIDENT	 IMPACT	 COST
Los Angeles, CA	High-Rise Office	Printed bomb threat to a printer on a public-facing network	The building was evacuated for 2 days.	<b>\$300K</b>
New York, NY	Fortune 500 Global HQ, 90+ stories	60% of 1000+ building systems were knocked offline by an untested IT vulnerability detection tool	Contractors had to manually restart, restore, and re-verify systems. 15 days to complete, and 2000 hours from IT.	<b>\$1.25M</b>
Southeast US	Healthcare Facilities	An IT update knocked offline an outdated BMS computer.	All surgeries (1600) in 50+ buildings were cancelled for 2 days due to the inability to monitor airflow in operating rooms.	<b>\$8M</b>
Canada	Class A Office Building	Phishing attack deploy ransomware and a virus on a BMS computer maintained by a BMS contractor that had no usage controls. The system back-ups were also hosted on the attacked computer.	The BMS was shut down and central plant equipment was damaged. 92 days of emergency labor, 1000 hours by facility managers.	<b>\$325K</b>
Germany	Office Building	Through an unsecured UDP port in the network, 75% of BAS devices were taken over by hackers and locked down making them inoperable.	Outside security experts were engaged to unlock the devices and facility staff had to manually turn on breakers to power the lights for several weeks.	<b>\$\$\$</b>

# Time to Resolve and Impact of Data Breaches

Data breach identification and containment takes over 250 days on average<sup>9</sup>

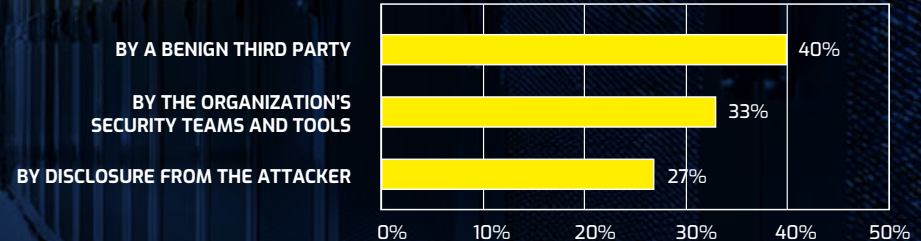


■ MTTI : Mean Time to Identify (Days)  
■ MTTC : Mean Time to Contain (Days)

# \$4.88M

Average total cost of a data breach  
Up 10% over 2023

## How was the breach identified?<sup>9</sup>





# What is Zero Trust OT Security?

**Zero Trust** - a security framework requiring all users/devices to be authenticated, authorized, and continuously validated before being granted or keeping access to applications/data/devices

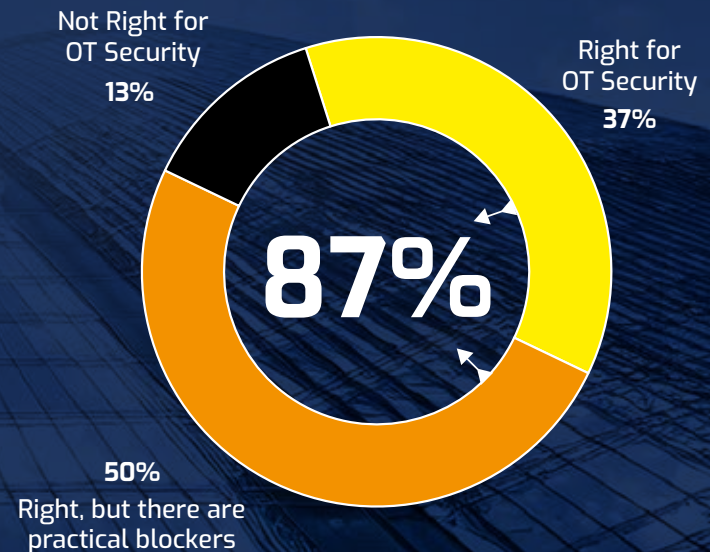


**Zero Trust is PRO-ACTIVE security method that protects against both external and internal threats**

The NIST Zero Trust framework can be applied to numerous applications, including securing building automation and OT network devices.

# Zero Trust Relevance for OT Security

Nearly 90% of respondents felt Zero Trust was right for OT Security<sup>10</sup>



# Best Practices for Building Cybersecurity

## BUILDING MANAGEMENT SYSTEMS | BUILDING AUTOMATION SYSTEMS | IOT DEVICES | SMART BUILDINGS



### 1. NETWORK SEGMENTATION:

Keep the IT and building management system network separate.



### 2. AUTHENTICATION:

Implement robust identity verification mechanisms for users, devices, and data. Multi-factor authentication and strict access controls based on roles for users. Mutual authentication for devices are integral to the Zero Trust approach.



### 3. CONTINUOUS MONITORING:

Deploy real-time monitoring systems to detect anomalies and potential security incidents. Automated alerts and responses ensure that any deviation from normal behavior is addressed promptly.



### 4. ENCRYPTION:

Secure data in transit and at rest through the use of strong encryption protocols. This safeguards sensitive information exchanged between devices and systems within the smart building ecosystem.



### 5. SYSTEM UPDATES:

Maintain up-to-date software and hardware to ensure that building systems are running on the latest, most secure versions.



### 6. INCIDENT RESPONSE PLANNING:

Develop comprehensive incident response plans tailored to the unique challenges of building management systems. These plans should outline clear procedures for addressing security incidents, minimizing the potential impact on building operations.



### 7. USER EDUCATION AND AWARENESS:

Foster a culture of cybersecurity awareness among building occupants and personnel. Educate users about potential risks, the importance of adhering to security protocols, and their role in maintaining a secure Smart Building environment.



### 8. CONTRACTOR PERFORMANCE:

Require system integrators and contractors to implement your cybersecurity procedures when accessing your building management system for monitoring, modifications or additions.



### 9. REGULAR SECURITY AUDITS AND ASSESSMENTS:

Conduct regular security audits and assessments to identify vulnerabilities and areas for improvement. Regular testing ensures that security measures remain effective against evolving cyber threats.



# Cybersecurity for Existing Building Controls



**Retrofit Security for Existing Devices**  
No need to replace or upgrade existing devices



**Zero Trust Authentication**  
Communication blocked from all un-authenticated devices



**Installs with Existing Technicians**  
No expensive cyber/IT resources needed



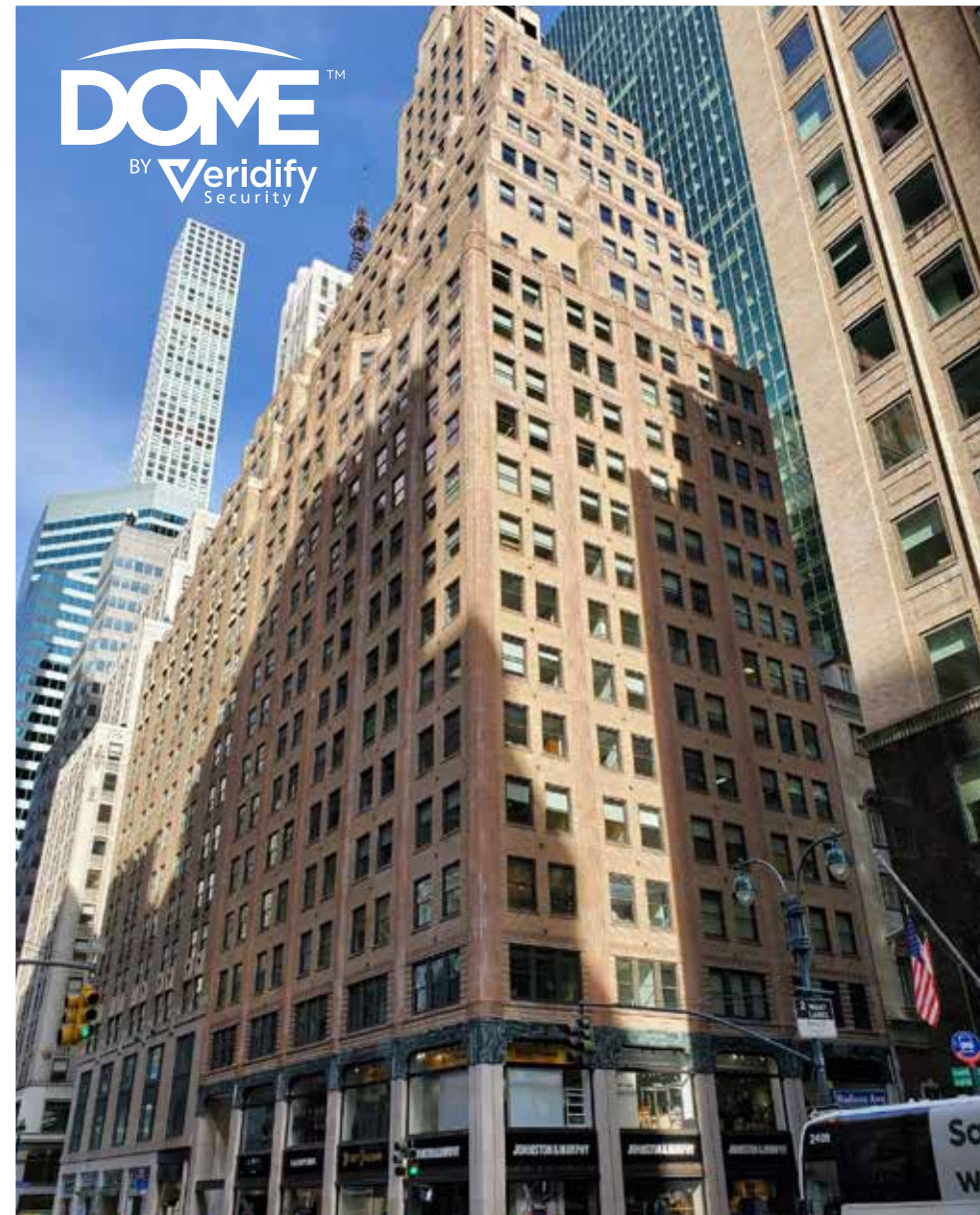
**Protect IP and non-IP Devices**  
No changes in the architecture or operation of the network, no new IP addresses needed



**End-to-End Data Encryption**  
End-to-end encryption makes communications secure



**Transparent Operation, No Network Changes**  
No changes in the architecture or operation of the network, no new IP addresses needed



## Case Study – Commercial Office Building

### SITUATION

A 32-story office building in downtown Manhattan experienced a costly cyber-attack on their HVAC network which uses BACnet/IP and BACnet MS/TP. The repairs required multiple days for system recovery, prompting the building owners to find a way to better secure their building.

### SOLUTION

The office building installed DOME – a device-level cybersecurity solution developed with our partners Intel and AWS. The solution included DOME's Interface Appliance management software, and four DOME Sentry devices – a low-cost security gateway – in front of key BACnet/IP points on the buildings' network.

### RESULT

DOME created a secure tunnel over the existing BACnet/IP network, authenticated all end points (Zero Trust) and encrypts all traffic to protect sensitive data. By using the DOME Sentry, no additional hardware or upgrades to the building's existing systems were necessary and the implementation was completed while the building was fully occupied.

# References

- 1) ShadowServer, May 2024  
(<https://www.shadowserver.org/>)
- 2) Forescout Research, July 2023  
(<https://www.forescout.com/blog/riskiest-connected-devices-it-iot-ot-iomt/>, <https://www.forescout.com/research-labs/riskiest-devices/>)
- 3) Forescout Research, July 2023  
(<https://www.forescout.com/blog/riskiest-connected-devices-it-iot-ot-iomt/>)
- 4) Protecting Operation Technology In Facilities from Cyber Threats, Honeywell, 2021  
(<https://buildings.honeywell.com/us/en/lp/protecting-operational-technology-in-facilities-from-cyber-threats>)
- 5) 2024 State of Operational Technology and Cybersecurity Report, Fortinet  
<https://www.fortinet.com/resources/reports/state-of-ot-cybersecurity>, <https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf>
- 6) The State of OT Security 2024, ABI Research, Palo Alto Networks  
(<https://www.paloaltonetworks.com/resources/research/state-of-ot-security-report>)
- 7) 2024 State of Operational Technology and Cybersecurity Report, Fortinet  
(<https://www.fortinet.com/resources/reports/state-of-ot-cybersecurity>)
- 8) Intelligent Buildings, Dark Reading  
(<https://www.darkreading.com/cyberattacks-data-breaches/lights-out-cyberattacks-shut-down-building-automation-systems>)
- 9) Cost of a Data Breach Report 2023, 2024 IBM  
(<https://www.ibm.com/reports/data-breach>)
- 10) The State of OT Security 2024, ABI Research, Palo Alto Networks  
(<https://www.paloaltonetworks.com/resources/research/state-of-ot-security-report>)



**Veridify**  
Security

---

[www.veridify.com](http://www.veridify.com)

