

THE IMPORTANCE OF NETWORK SECURITY IN BUILDING MANAGEMENT SYSTEMS

Protecting smart buildings in an increasingly connected world

White Paper — October 2026

BMSI
Create. Connect. Control.

+44 (0) 1753 738000 sales@bmsi.co.uk www.bmsi.co.uk

EXECUTIVE SUMMARY

Modern buildings have become highly connected digital environments. Building Management Systems (BMS), once isolated operational platforms, now integrate with corporate networks, cloud services, mobile applications, Internet of Things (IoT) devices, and third-party service providers. This connectivity has transformed how facilities are managed, delivering greater operational efficiency, enhanced occupant comfort, and improved energy performance.

However, increased connectivity has also introduced significant cybersecurity risks. Research conducted by Claroty found that three out of four organisations operate Building Management Systems with cybersecurity vulnerabilities, while more than half have internet-connected systems containing known exploited vulnerabilities associated with ransomware activity. The study analysed more than 467,000 BMS assets across 500 organisations. [**facilitiesdive.com**]

Recent real-world incidents demonstrate the consequences of inadequate cybersecurity controls. In October 2026, attackers compromised refrigeration management systems manufactured by Danfoss, forcing refrigeration units into defrost mode and causing tens of millions of dollars in food losses across hundreds of European supermarkets. [**facilitiesdive.com**]

As buildings become more intelligent and interconnected, network security must be viewed as a fundamental component of operational resilience, business continuity, and risk management.

INTRODUCTION

The built environment is undergoing a profound digital transformation. Smart buildings increasingly rely on interconnected technologies to automate and optimise critical services such as heating, ventilation, air conditioning, lighting, physical security, energy management, refrigeration, and environmental monitoring.

Historically, these systems existed independently from corporate technology environments. Today, they form part of broader digital ecosystems that support organisational objectives and occupant experience.

While this evolution has delivered substantial benefits, it has also blurred the traditional boundaries between Information Technology (IT) and Operational Technology (OT). As a result, cyber threats that once primarily targeted enterprise networks can now directly affect building operations and physical infrastructure.

For building owners, facilities managers, and operational leaders, cybersecurity is no longer solely an IT issue. It is a business-critical responsibility.

UNDERSTANDING BUILDING MANAGEMENT SYSTEMS

A Building Management System serves as the central intelligence platform for a facility, providing monitoring, automation, and control of building services.

Typical functions include:

Lighting Management

- Occupancy-based lighting control
- Automated scheduling
- Energy efficiency programmes

Energy Management

- Power monitoring
- Sustainability reporting
- Utility optimisation

Physical Security

- Access control systems
- CCTV integration
- Visitor management

Environmental Control

- Heating, Ventilation and Air Conditioning (HVAC)
- Indoor air quality management
- Temperature optimisation

Critical Operational Environments

- Refrigeration systems
- Data centre cooling
- Laboratory control environments
- Clean room operations

Building Management Systems commonly utilise industrial communication protocols such as BACnet, Modbus, KNX, LonWorks, and OPC. Many of these protocols were developed decades ago, prioritising reliability and interoperability rather than cybersecurity.

WHY NETWORK SECURITY MATTERS

Protecting Occupant Safety

Building systems support critical aspects of occupant wellbeing and safety. Cyber incidents affecting HVAC, access control, environmental monitoring, or life-safety systems may disrupt operations and create safety concerns, particularly within healthcare, pharmaceutical, educational, and industrial facilities.

Ensuring Business Continuity

Modern organisations depend heavily on automated building infrastructure. A cyberattack that disrupts operational systems may result in:

- Facility shutdowns
- Lost productivity
- Service interruption
- Tenant dissatisfaction
- Supply chain disruption

Reducing Financial Risk

The costs associated with a cyber incident frequently extend beyond technical recovery. Potential impacts include:

- Business interruption
- Product spoilage
- Emergency remediation
- Regulatory investigations
- Reputational damage
- Insurance claims

Supporting Compliance

Organisations are increasingly expected to demonstrate robust cybersecurity governance through frameworks and standards such as:

- ISO 27001
- IEC 62443
- NIST Cybersecurity Framework
- Cyber Essentials Plus
- UK NIS Regulations

THE CURRENT THREAT LANDSCAPE

A Growing Exposure Problem

Cybersecurity researchers are increasingly identifying significant vulnerabilities across Building Management Systems worldwide.

Research by Claroty found:

3/4

Three out of four organisations operate Building Management Systems with cybersecurity vulnerabilities.
[facilitiesdive.com]

2%

Approximately 2% of business-critical assets were operating at the highest level of risk exposure.
[facilitiesdive.com]

>50%

More than half of organisations had internet-connected systems with known exploited vulnerabilities.
[facilitiesdive.com]

X

Many systems were no longer fully supported by vendors, leaving vulnerabilities potentially unpatched.
[facilitiesdive.com]

These findings suggest that cyber exposure within building systems is not exceptional but widespread throughout commercial real estate, hospitality, retail, healthcare, education, and industrial sectors.

LEGACY INFRASTRUCTURE CHALLENGES

Many Building Management Systems remain operational for ten to twenty years or more.

While this provides long-term value from physical infrastructure investments, it can create challenges including:

- Unsupported operating systems
- End-of-life controllers
- Unpatched software
- Insecure communications protocols
- Lack of encryption

Legacy technology remains one of the most significant contributors to operational cybersecurity risk. [**facilitiesdive.com**]



BMSI Create. Connect. Control.
+44 (0) 1753 738000
sales@bmsi.co.uk
www.bmsi.co.uk

CASE STUDY 1

IBM X-Force demonstrates how a Building Management System (BMS) can be compromised

One of the clearest demonstrations of BMS vulnerability came from a security assessment conducted by IBM X-Force, later analysed by Smart Buildings Academy. [**blog.smart...cademy.com**]

Rather than relying on advanced or highly sophisticated techniques, researchers used a series of common and preventable weaknesses to gain access to a Building Management System.

The Attack Sequence

Researchers reportedly:

1. Discovered an internet-facing remote access router.
2. Exploited vulnerabilities to obtain credentials.
3. Conducted network reconnaissance to identify BMS assets.
4. Found password reuse across systems.
5. Reverse engineered software components containing authentication information.
6. Successfully gained access to the Building Management System.

Lessons Learned

This incident highlighted several recurring industry challenges which still exist today:

- Weak password management – familiar words, use of 0000 or 1234, or as we see on many sites, the credentials for the BMS being written on the BMS headend / in the control panel / notice board.
- Credential reuse
- Insufficient patch management
- Poor remote access security
- Lack of collaboration between IT and facilities teams

The assessment demonstrated that attackers often exploit a combination of small weaknesses rather than a single major vulnerability.

[**blog.smart...cademy.com**]

CASE STUDY 2

The Danfoss Refrigeration Controller Attack

In October 2026, a large-scale operational technology attack illustrated the real-world business consequences of insecure building systems.

Hackers compromised refrigeration control systems manufactured by Danfoss, impacting supermarket operations across France, Germany, Belgium, Poland, Spain, and Portugal. The attack forced refrigeration systems into defrost mode, leading to the spoilage of refrigerated products and losses estimated in the tens of millions of dollars.

According to reports, affected systems included legacy AK-SM800 and AK-SC355 refrigeration controllers that no longer received security updates.

[**facilitiesdive.com**]

Key Takeaways

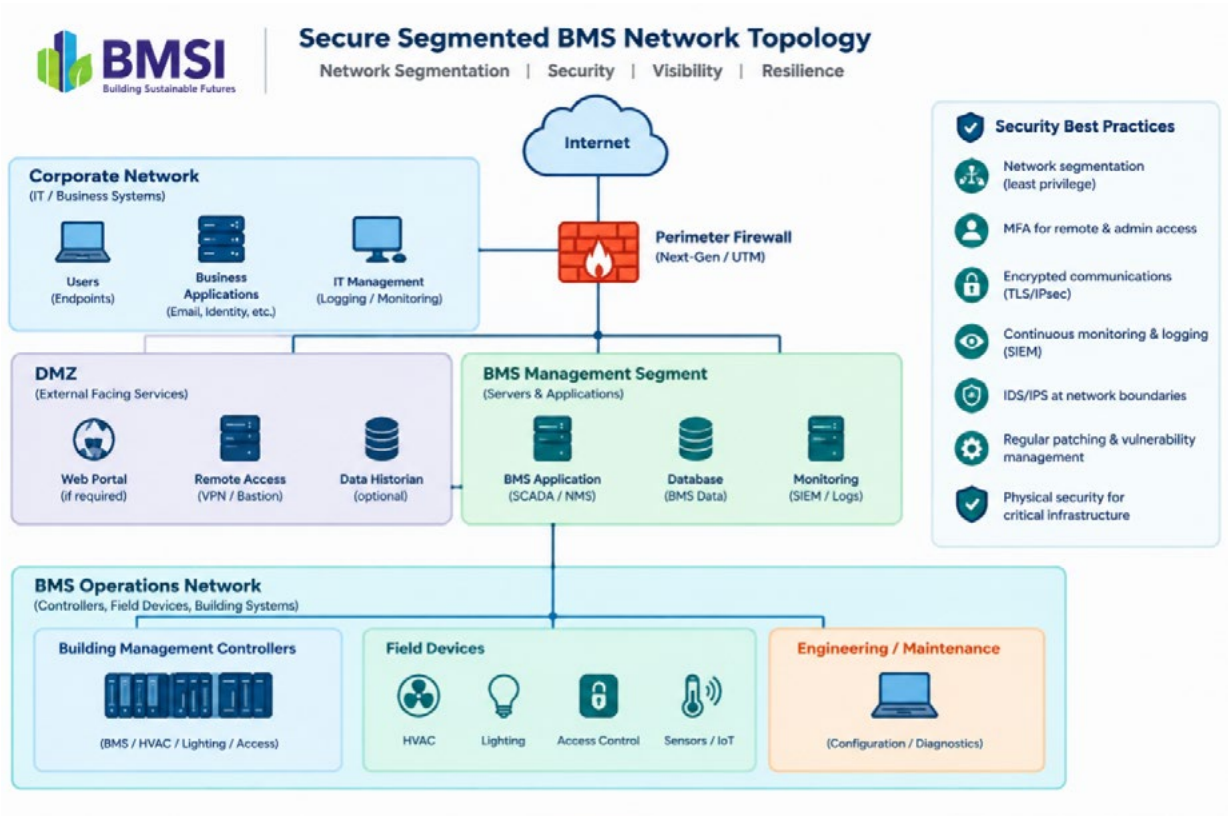
- **Legacy Systems Increase Risk**
  Unsupported systems create long-term exposure because security vulnerabilities may never be corrected.
- **Operational Technology Is a Target**
  Building systems are no longer overlooked by attackers. Operational technology can provide a direct path to disruption and financial leverage. [facilitiesdive.com]
- **Cyber Incidents Cause Physical Consequences**
  Unlike traditional IT breaches, attacks on operational systems can directly impact physical processes, products, and facilities. [facilitiesdive.com]
- **Lack of MSI knowledge**
  Individual elements of plant are becoming smarter with embedded remote technology, such as pumps, motors and inverters. Businesses over time lose sight of individual components that reside within their estate that might be equipped with 4G, Bluetooth, wireless or WiFi connectivity. Allowing vulnerabilities to the overall BMS network to occur.

Common Vulnerabilities in Building Management Systems

The most frequently observed security weaknesses include:

- **Default Credentials**
  Factory-supplied passwords that remain unchanged after installation.
- **Password Security**
  The same, or weak credentials used across multiple systems and environments. Often written down close to or on BMS equipment [blog.smart...cademy.com]
- **Unpatched Infrastructure**
  Devices and software running without current security updates. [facilitiesdive.com], [facilitiesdive.com]
- **Poor Network Segmentation**
  Building systems connected directly to corporate networks.
- **Excessive User Privileges**
  Users granted more access than necessary to perform their role.
- **Limited Asset Visibility**
  Organisations lacking a complete inventory of connected devices and associated risks.

BEST PRACTICES FOR SECURING BUILDING MANAGEMENT SYSTEMS



1. Network Segmentation

Separate Building Management Systems from corporate IT infrastructure. Benefits include:

- Reduced attack surface
- Improved monitoring
- Contained security incidents
- Restricted lateral movement

2. Secure Remote Access

All remote access should require:

- VPN connectivity
- Multi-factor authentication (MFA)
- Session auditing
- Access approvals
- Time-based controls

3. Strengthen Identity Management

Implement:

- Unique user accounts
- Strong password policies
- Least-privilege access
- Periodic access reviews

BEST PRACTICES FOR SECURING BUILDING MANAGEMENT SYSTEMS

4. Establish Patch Management Processes

Develop formal procedures for:

- Firmware updates
- Software updates
- Vulnerability assessments
- Security testing

5. Improve Asset Visibility

Maintain a constantly updated inventory of:

- Servers
- Controllers
- Sensors
- Gateways
- Network devices
- Third-party connections

Visibility is the foundation of any cybersecurity programme.

[**facilitiesdive.com**]

6. Monitor Continuously

Monitor for:

- Unusual network traffic
- Suspicious login activity
- Configuration changes
- Operational anomalies
- Security alerts

7. Manage Third-Party Risk

Assess service providers based on:

- Security controls
- Access practices
- Incident response capability
- Compliance certifications
- Patch management procedures

8. Lifecycle Upgrades

The recent targeting of BMS systems has highlighted organisations that have kept equipment beyond the lifecycle and support of the manufacturer. BMS equipment can be extraordinarily reliable, often exceeding its support life by many years. This means security patching and updates are no longer supplied as part of a maintenance visit.

- Identify controllers that are beyond their lifecycle
- Replace controllers that are no longer supported by the manufacturer
- If a full replacement cannot take place, identify controllers that are most critical and adopt a phased approach to replacement.

STRATEGIC ROADMAP

Immediate Actions (0-3 Months)

- Conduct a BMS security assessment / audit
- Identify internet-facing systems
- Remove default credentials
- Enable MFA
- Review remote access arrangements
- Identify controllers that are no longer supported by the manufacturer
- Medium-Term Actions (3-12 Months)
- Implement network segmentation
- Establish vulnerability management processes
- Deploy monitoring solutions
- Develop incident response plans
- Indentify priority controllers for lifecycle replacement

Long-Term Actions (12+ Months)

- Adopt Zero Trust principles
- Conduct penetration testing
- Integrate OT risks into enterprise risk management
- Establish continuous improvement programmes

Conclusion

The convergence of smart buildings, operational technology, and enterprise networking has fundamentally changed the cybersecurity landscape for modern facilities.

Research from Claroty demonstrates that Building Management System vulnerabilities are widespread across industries. The IBM X-Force assessment showed how easily attackers can exploit common weaknesses in poorly secured building automation environments. The 2026 Danfoss incident then provided a stark illustration of the operational and financial consequences that can occur when those vulnerabilities are exploited.

The message for building owners and operators is clear: cybersecurity is no longer optional. It is a fundamental component of safe, resilient, and efficient building operations.

Organisations that invest in network segmentation, secure remote access, vulnerability management, continuous monitoring, and collaboration between facilities and IT teams will be best positioned to protect their assets, occupants, and operations in an increasingly connected world.

[**facilitiesdive.com**] [**blog.smart...cademy.com**] [**facilitiesdive.com**]

BMSI
Create. Connect. Control.

+44 (0) 1753 738000 sales@bmsi.co.uk www.bmsi.co.uk