ARMIS®

WHITE PAPER

Securing Building Management Systems (BMS) in Financial Services

Introduction

As financial services companies continue to adopt cutting-edge technology to streamline operations, enhance customer experiences, and optimize resources, their reliance on smart building systems grows in parallel. Building Management Systems (BMS), often referred to as Building Automation Systems (BAS), have become vital components for managing HVAC systems, lighting, physical security, and other building functions. These systems offer efficiency, cost savings, and greater control. However, as their connectivity to the internet and internal networks increases, so do their vulnerabilities, exposing financial services companies to a growing array of cyber threats. Securing BMS is no longer just an operational necessity—it is a matter of protecting critical infrastructure, data, and organizational reputation.

This white paper explores the challenges of securing BMS in financial services, highlights real-world examples of cyber threats, and offers actionable strategies to strengthen cyber defenses.

What is a Building Management System?

A Building Management System (BMS) is a centralized system designed to control, monitor, and optimize building operations to boost efficiency, reduce costs, and improve comfort and security for occupants. Key components of BMS include:

HVAC Systems:
Ensuring optimal indoor temperature and air quality.

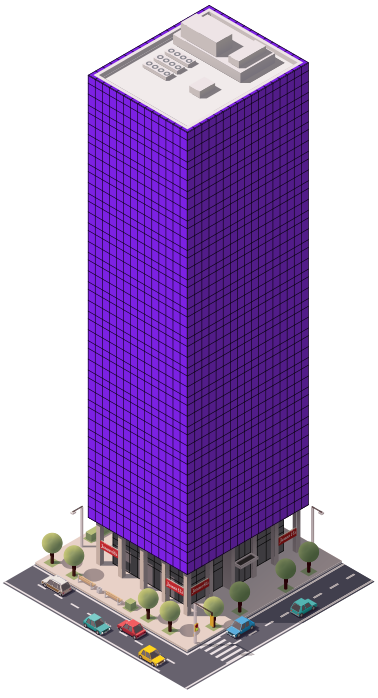
Lighting Controls:
Managing interior and exterior illumination schedules.

Fire & Life Safety Features:
Operating smoke detectors, emergency alarms, and fire response systems.

Data Center:
Centralized monitoring and control, power infrastructure management, prompt alarms and notification, environmental monitoring, date-driven insights.

Physical Security Systems:
Administering access controls, surveillance, and alarms.

Elevators & Critical Systems:
Managing elevator operations and infrastructure reliability.



While BMS offers enormous benefits, its functionality increasingly intertwines with IoT devices and cloud-based platforms, introducing new vulnerabilities. These entry points are known to be targeted by cybercriminals.

- Energy Efficiency and Cost Management
- Physical Security and Access Control
- Smart Workspace Management
- Environmental Monitoring and Compliance
- Disaster Recovery and Business Continuity
- Cybersecurity Integration
- Operational Efficiency
- Employee and Visitor Experience
- Data Integration and Analytics
- Remote Monitoring and Control

Use Cases for Building Management Systems (BMS) in Financial Services Organizations

Financial services companies in major cities around the globe are increasingly adopting BMS to optimize their modern offices, attract top talent, and stay competitive in a rapidly evolving and innovative market. These systems enhance energy efficiency, monitor critical infrastructure, and improve experiences for employees and customers.

Energy Efficiency and Cost Management

- Monitoring and controlling HVAC, lighting, and power systems to reduce energy consumption and operational costs. Keep datacenters at proscribed temperature and humidity.
- Integration with IoT sensors for real-time energy usage data and dynamic adjustments.

Physical Security and Access Control

- Managing access to restricted areas using integrated keycard systems, biometric readers, or facial recognition.
- Real-time monitoring of building entrances and exits via cameras and alarm systems.

Smart Workspace Management

- Automated control of lighting and climate based on occupancy data to enhance employee comfort and reduce wastage.
- Dynamic space allocation based on real-time occupancy data.

Environmental Monitoring and Compliance

- Monitoring indoor air quality to meet health and safety standards.
- Ensuring compliance with green building certifications like LEED or WELL.

Disaster Recovery and Business Continuity

- Automated shutdowns or diversion of systems in case of fire, flood, or other emergencies to minimize damage and protect critical infrastructure.
- Integration with backup power systems for seamless operations during outages.

Cybersecurity Integration

- Protection against cyber-physical threats by securing connected building systems.
- Detection and response to unauthorized attempts to access restricted areas.

Operational Efficiency

- Predictive maintenance for critical infrastructure (e.g., HVAC systems, elevators) to prevent downtime.
- Automated fault detection and diagnostics to optimize system performance.

Employee and Visitor Experience

- Personalized settings for employees (e.g., desk preferences, lighting).
- Visitor management systems that streamline check-ins and access permissions.

Data Integration and Analytics

- Centralized dashboards for real-time monitoring and historical analysis.
- Insights to optimize operational costs and enhance sustainability initiatives.

Remote Monitoring and Control

- Cloud-enabled BMS for remote access to manage multiple facilities across geographic locations.
- Mobile apps for facility managers to respond to issues anytime, anywhere.

The integration of BMS with financial services companies operational networks amplifies the risk of cyberattacks. A successful breach could compromise not only the physical infrastructure but also sensitive data and daily operations. For organizations that store vast amounts of customer data and handle high-value financial transactions, even minor disruptions can have severe financial and reputational repercussions. For example, a weakly secured HVAC system may serve as a gateway for attackers to infiltrate critical IT systems. This was demonstrated in past incidents where cyberattacks leveraged third-party vendor systems tied to building operations. Such breaches highlight the need for financial institutions to treat BMS as an extension of their IT infrastructure, ensuring that security measures are equally robust and regularly updated.

Regulatory bodies are also starting to impose stricter guidelines on securing operational technologies, including BMS, in sectors like financial services. Non-compliance with these regulations could result in fines, legal action, or reputational damage. Addressing the risks associated with BMS is therefore not just an optional enhancement but an absolute necessity for ensuring business continuity, regulatory compliance, and stakeholder trust.

Regulations and Frameworks:

> Examples of financial services cybersecurity frameworks addressing BMS include PCI-DSS, the SEC's expanded disclosure requirements and those from the FDIC, NCUS, FFIEC, and NYDFS and DORA.

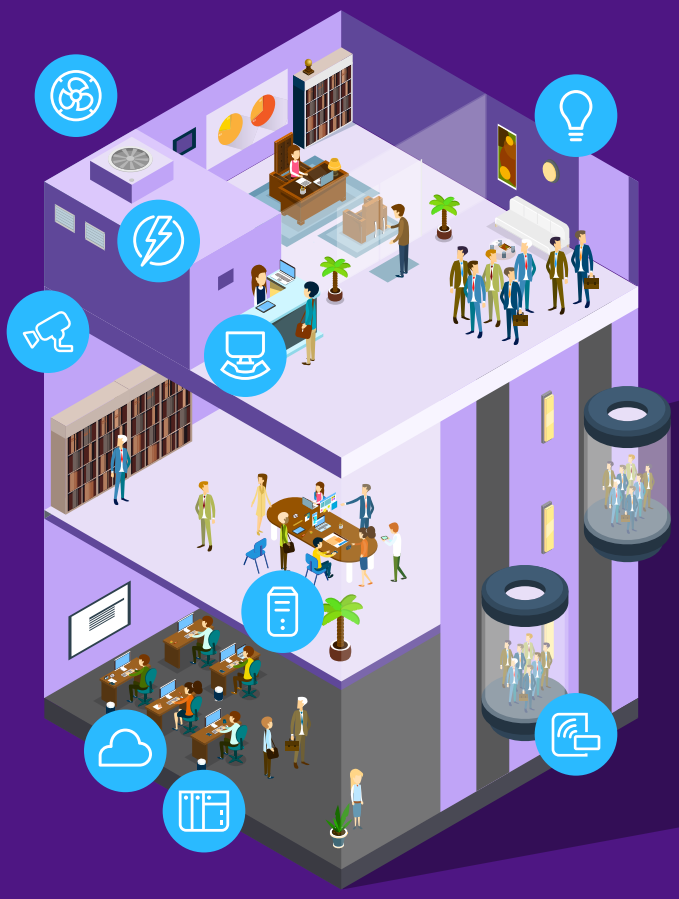
> The FFIEC provides guidance to help financial institutions integrate Building Management System (BMS) security into their overall risk management framework. As BMS becomes increasingly connected through IoT devices, adherence to FFIEC guidelines is crucial to mitigate vulnerabilities and ensure robust protection against cyber threats targeting physical infrastructure.

Modern Cybersecurity Challenges Facing BMS

Challenges At-a-glance

When it comes to improving operational efficiencies, reducing energy consumption, and extending the life of critical, costly equipment, building management systems (BMSs) are indispensable. But attacks on unprotected critical systems can also pose risks to everything from peoples' safety and comfort to production runs.

- Most BMSs lack built-in security controls and can't host security agents;
- Software patches are often difficult or impossible;
- New smart devices create new attack vectors;
- Ransomware targeting physical infrastructure is on the rise, given all the security blind spots attackers can exploit in a BMS.



In addition to servers and computers, attackers are increasingly focused on unprotected critical systems in buildings.

01 Expanded Attack Surface

Modern BMS are interconnected via IoT sensors, software platforms, and external integrations, resulting in a web of potential access points. Breaches via a single weak link, such as an unprotected device, threaten the entire organization.

02 Outdated Systems & Protocols

Legacy systems continue to run without modern updates or secure protocols. Commonly used systems like Bacnet or Modbus often lack built-in encryption, leaving sensitive data streams vulnerable to interception.

03 Inadequate Network Segmentation

BMS networks are often connected to broader IT infrastructures without sufficient segmentation. A cybercriminal who compromises one BMS component may gain access to unrelated systems, such as financial transaction networks or customer databases.

04 Weak Authentication

Default passwords, improperly configured controls, and the absence of multifactor authentication make BMS systems easy targets and compliance risks.

05 Complexity and Oversight

Many organizations struggle to maintain visibility into the plethora of connected BMS devices distributed across locations. This results in blind spots that hackers can exploit.

Real-World Impacts of BMS Cyberattacks

> **Hotel Lock System Sabotage:** A luxury hotel in Austria suffered a ransomware attack that locked guests out of their rooms. Hackers disabled the hotel's key card system, demanding payment to restore access. The hotel was forced to pay to avoid further disruption to guest services.

> **Smart Elevator Hijack:** An office building in Singapore experienced a cyberattack on its smart elevator system. Hackers manipulated the controls, causing operational delays and safety concerns. The building management had to spend thousands on system restoration and security upgrades.

> **Warehouse Robotics Breach:** A distribution center in the UK faced a cyberattack targeting its robotic systems used for inventory management. The attack disrupted operations for days, delaying shipments and resulting in significant financial losses and reputational damage.

> **Smart Thermostat Attack:** In the United States, a cyberattack targeted the smart thermostat system of a corporate office building. Hackers gained control of the temperature settings, causing extreme discomfort for employees and disrupting daily operations. The company had to implement costly security measures to prevent future breaches.

These additional incidents further highlight the dire consequences of inadequate BMS security and the critical need for preventative measures.

How BMS Security Leads to Operational Resilience

Building Management Systems (BMS) play a critical role in ensuring operational resilience by providing smart, automated solutions that improve efficiency, enhance security, and reduce costs. By integrating advanced technologies like IoT and cloud platforms, BMS creates a seamless, unified approach to managing building operations. Let's explore how BMS can directly impact energy management and security, along with the benefits and new advances driving innovation.

Practical Example

> **Energy Management:** BMS optimizes energy usage by automatically adjusting lighting and HVAC systems based on occupancy and external conditions. For instance, lights can dim in unoccupied rooms, while HVAC systems reduce energy consumption during off-peak hours.

> **Security:** BMS integrates access control and surveillance systems for real-time monitoring and automated alerts, such as notifying staff if unauthorized access is detected.

Benefits

> **Improved Efficiency:** Automated control minimizes manual intervention and optimizes system performance.

> **Cost Savings:** Energy-efficient operations lower utility bills significantly.

> **Enhanced Comfort:** Automated adjustments ensure a comfortable environment for occupants.

New Advances

> **Smart Buildings:** IoT integration enables advanced data analytics and predictive maintenance for proactive management.

> **Cloud Connections:** Remote monitoring via cloud platforms offers greater flexibility and oversight.

> **Singular Control Systems:** Unified interfaces simplify building management and improve response times in critical situations.

With BMS, organizations can achieve high levels of operational resilience, blending efficiency, security, and innovation to meet modern building demands.

Solutions to Protect Building Management Systems

Securing BMS requires a comprehensive approach that builds upon and complements existing IT and operational technology (OT) frameworks while addressing BMS-specific concerns.

01 Gain Full Situational Awareness

Seamless identification and tracking of managed and unmanaged BMS devices, including HVAC and mechanical controllers, SCADA servers, and PLCs.

The first step in securing BMS is understanding what devices and systems are connected to your infrastructure. Implement real-time monitoring tools to gain full visibility into all connected systems. This allows you to identify vulnerabilities, suspicious behaviors, and potential threats before they escalate.

02 Integrate IT and OT Tools & Workflows

Operational technology, such as BMS, often exists in silos, separate from IT systems that govern network security. Bridging these divides allows organizations to extend IT expertise and tools to safeguard physical systems. Integration optimizes incident response and threat detection by creating shared workflows.

03 Enforce Network Segmentation

Use network segmentation practices to isolate critical BMS components from non-critical or public-facing systems. Design your BMS networks to minimize lateral movement between systems, drastically reducing an attacker's ability to spread within your environment.

> **Implement Microsegmentation**
>
> Microsegmentation takes network security to the next level by breaking down broader segments into smaller, more controlled zones. Each of these microsegments is governed by specific security policies, ensuring that only authorized communications are allowed between systems. By applying microsegmentation, organizations can minimize the risk of lateral movement by attackers, even if they successfully breach one segment. Additionally, this approach provides enhanced visibility into traffic flows and enables real-time monitoring of potential threats, making it a critical layer of defense for protecting BMS.

04 Deploy Strong Authentication Protocols

Implement robust password policies and enable multifactor authentication (MFA) across all BMS systems. Eliminate the use of default credentials and regularly audit access controls.

Ensure Secure Remote Access

Secure remote access is essential for maintaining the integrity of Building Management Systems. Use Virtual Private Networks (VPNs) or encrypted communication channels to safeguard remote connections. Additionally, restrict remote access to authorized users and enforce strict access controls to minimize vulnerabilities and risk.

05 Vulnerability and Security Findings Management

Early Warning Intelligence

Time is critical in responding to cyber threats. Utilize early warning systems that provide operational efficiencies with a proactive approach to achieve a preemptive cybersecurity strategy by following the vulnerabilities that threat actors are exploiting in the wild or are about to weaponize. Automated threat detection tools with guided playbooks can help reduce mean-time-to-detect (MTTD), mean-time-to-respond (MTTR) and prevent attacks in the formulation stage.

Remediation Management

Alerts and monitoring are of little use without clear steps for resolution. Find risk, deduplicate alarms, prioritize response, identify the owner, and operationalize the remediation lifecycle. Cut time spent on identifying owners and assigning tickets by 90%, with custom ticketing rules.

Cybersecurity as a Competitive Advantage

Financial institutions don't just protect their assets when they secure their BMS — they safeguard their reputation and operational efficiency. By implementing enhanced BMS security measures, banks and other financial organizations can:

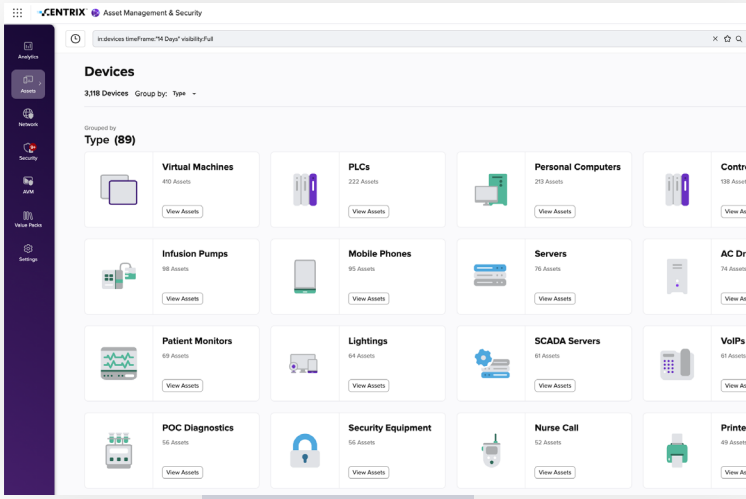
- Build trust with stakeholders and customers.
- Reduce downtime caused by cybersecurity incidents.
- Ensure compliance with evolving regulations regarding cybersecurity and data integrity.

Strong foundations in BMS security also position organizations to leverage emerging technologies with confidence, empowering them to stay competitive in an era of escalating technological complexity.

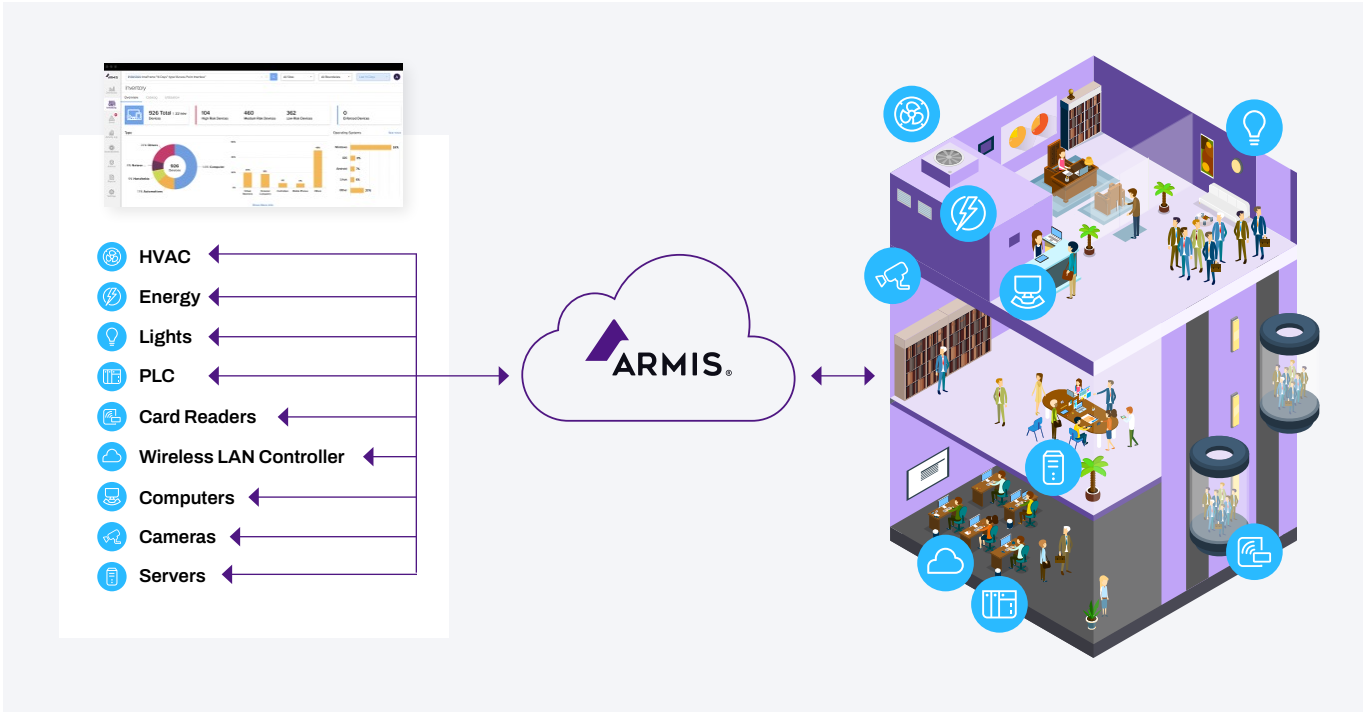
Introducing Armis Centrix™

Whether connected assets are located onsite or in distributed locations, the Armis Centrix™ platform's holistic approach makes it easy to inventory and quickly understand all of them. Get visibility of financial services BMS assets, including thermostats, sensors, elevator controllers, and fire and safety systems. And keep a close eye on every other connected asset, including smart devices like TVs, IP cameras, and printers with comprehensive asset details.

- Device manufacturer, model, firmware version, and serial number
- Location/site, username, IP address, MAC address
- Operating system (OS) and installed applications
- Known vulnerabilities associated with each OS/application
- Changes in device state and state anomalies
- Activities and connections made over time
- Device risk scores based on static and dynamic analysis



Inventory screen example of a typical office building. The Armis platform gives you a high-level view of every asset type, along with the ability to quickly and easily drill down into the specifics of every device that is sharing data on your networks, including HVAC and mechanical controllers, lighting systems, PLCs, security cameras, and more.



The Armis platform provides a central management console for every cyber asset and building across the enterprise.

Mitigate Security Risks

Protects your business from disruption by relying on the world's largest crowdsourced, device knowledgebase to detect threats with a high degree of accuracy.

Monitors devices communicating in the airspace via peer-to-peer protocols, which are invisible to traditional security products.

Enables you to automatically disconnect or quarantine devices operating outside of "known good" baselines.

Manage BMS with Confidence

Complete network visibility with automatic discovery and deep situational awareness of every BMS asset.

Continuous network monitoring and detection of anomalous, suspicious, or malicious behavior, and unauthorized actions.

Real-time detection of device misconfigurations, unscheduled changes, and device malfunction.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial