

Delivering Effective Cybersecurity for Facilities Management

The Convergence of
Physical & Cybersecurity

Delivering Effective Cybersecurity for Facilities Management



The Convergence of Physical & Cybersecurity

A group of property and facilities management organizations needed to move from fragmented, ad-hoc security practices to a structured cybersecurity program that could satisfy regulators, investors, and enterprise clients. Using our proven process delivery model; Test-4-Fit, Plan-4-Impact, Prep-4-Success, and rapid Time-to-Value, Simple Security replaced underperforming, big-ticket vendors, and helped the organizations build measurable, program-driven cybersecurity capabilities.

At-a-Glance Summary (Executive Snapshot)

Industry

Property Management /
Facilities Management

Environment

Cloud-native, SaaS and
mobile / remote endpoints

Primary Stakeholders

Enterprise clients,
regulators, investors

Primary Challenge:

Technology and cybersecurity had been implemented in an ad-hoc manner over time, leaving the organizations with inconsistent security practices, dissatisfied vendor relationships, and increasing regulatory pressure.

Solution Delivered:

Simple Security applied our structured cybersecurity delivery process to evaluate existing vendors, implement effective change management, and transform reactive security practices into a coordinated security program.

Key Outcomes:

- ✓ Vendor selection driven by measurable value
- ✓ Programmatic cybersecurity strategy implemented
- ✓ Improved stakeholder confidence
- ✓ Board-level security metrics and reporting
- ✓ Rapid time-to-value within 30 days



Customer Context (The Before State)

These organizations operate in property and facilities management, supporting well-known hospitality brands and commercial office environments.

Their core expertise and historical focus was the management of physical assets; buildings, facilities, and operational infrastructure.

While one organization had pivoted during the pandemic to become fully remote and cloud-native, the other had retained an office presence for their workforce. However, both organizations had transitioned all back-office and server infrastructure to third-party SAAS providers.

These SAAS implementations were undertaken without a unified cybersecurity strategy, shifting and expanding the risk surface, resulting in inconsistent technology governance.

The Challenge (The Real Problem)

The organizations faced growing scrutiny from regulators, investors, and enterprise customers following highly visible exposure events.

Cloud-native or cloud-first transformation initiatives, rely heavily on third-party SaaS platforms for identity management, productivity, and operational systems.

Despite modern infrastructure, cybersecurity maturity remained low because tools and services had been implemented reactively in silos, rather than strategically consolidating in a unified manner.

Additionally, existing service providers had failed to deliver the level of engagement and strategic support required, resulting in visibility and coverage gaps.

Why Change (The Trigger)

Regulatory oversight and investor expectations increased after brand and reputationally impacting events highlighted blind spots in the organizations' cybersecurity controls, and a lack of governance.

This pressure created urgency to establish a structured cybersecurity program capable of demonstrating measurable progress to boards, regulators, and enterprise customers.



The Simple Security® Approach

Simple Security introduced its proven delivery framework designed to move organizations from reactive, project-based security practices, to building a structured cybersecurity program.

The engagement began with the first step in our proven process, Test-4-Fit. During this foundational stage, Simple Security evaluated the organizations' existing vendor ecosystem, security tools, and operational practices to determine where capability gaps and vendor underperformance existed.

This evaluation allowed each organization to make informed decisions around technology coverage, effectiveness, and suitability; replacing ineffective providers, tuning controls, and introducing a unified security strategy.



Implementation

The program continued through the next stages of the Simple Security delivery model.

Plan-4-Impact focused on establishing a clear security strategy aligned with business priorities and regulatory expectations.

Prep-4-Success ensured stakeholder buy-in through structured change management, detailed documentation, and regular communication with leadership teams.

This collaborative approach allowed Simple Security to transition the organizations away from fragmented security projects toward a coordinated and strategically-aligned cybersecurity program.

Results

The engagement delivered measurable improvements in security maturity, operational trust, and governance.

Key Outcomes:

- ✓ Underperforming vendors replaced through structured evaluation
- ✓ Security transformed from ad-hoc projects to a formal program
- ✓ Board-level metrics and reporting introduced
- ✓ Improved alignment with regulatory and investor expectations
- ✓ Rapid time-to-value delivered within 30 days

Why It Matters

For organizations whose primary focus is managing physical assets and operations, cybersecurity often evolves reactively.

By introducing a structured delivery framework, Simple Security helped these organizations transform cybersecurity into a strategic capability that supports long-term business growth.

Who This Is For

- Property and facilities management companies
- Organizations operating primarily in these environments
- Businesses needing board-level security reporting
- Companies dissatisfied with existing cybersecurity vendors
- Organizations seeking a structured cybersecurity program rather than isolated projects

“For the first time, we felt like cybersecurity was being delivered as a program rather than a disjointed collection of ineffective tools and short-term projects. Simple Security restored confidence across our leadership team.”



Transforming Security, Simplified



If your organization is struggling with fragmented security tools, inconsistent vendor performance, or regulatory pressure, Simple Security can help. Our proven delivery framework helps organizations move from reactive security practices to a measurable cybersecurity program aligned with business objectives.

Book a conversation to learn how we simplify cybersecurity.





Protecting what matters
shouldn't be complicated.