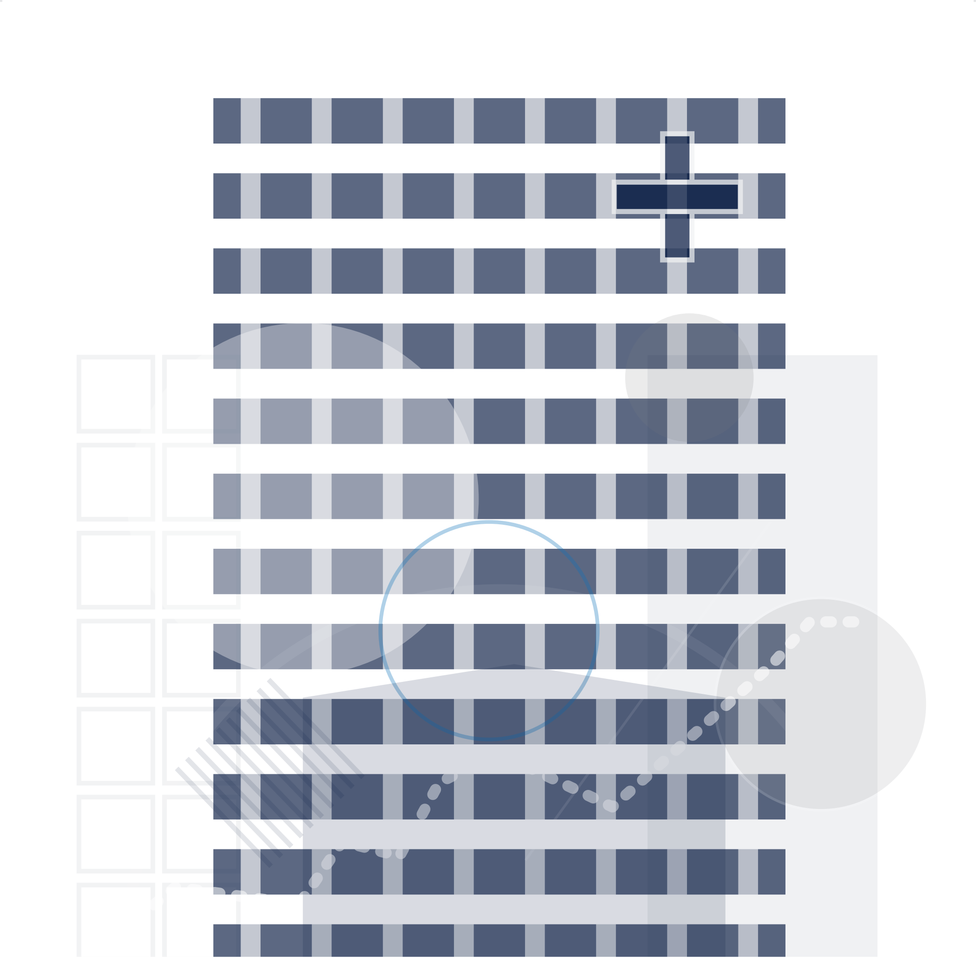
TOP 5 AMERICAN HEALTHCARE PROVIDER



CASE STUDY SUMMARY

Intelligent Buildings® Portfolio Cybersecurity Strategy

INTELLIGENT BUILDINGS™

Challenge

The company publicly committed to a full cybersecurity strategy and execution plan involving all aspect of the enterprise, information technology (IT), clinical technology (CT), and operational technology (OT). However, the OT cybersecurity was not owned by or assigned to any specific group in the organization and generally not part of traditional cybersecurity planning, even though many of the systems were connected to the corporate-wide area network. Traditionally, there has been no skill set or experience that spans the IT and OT in the industry or with the customer. Even though there were OT devices on the corporate network, often they were not appropriately segmented, nor were there device level and contractor level cyber policies developed.

Additionally, there was no OT vendor oversite, which was made even more evident during the international WannaCry ransomware crisis and resulting remediation. Hence, there was a real need to address buildings and facilities as a new pillar, as part of an overall cybersecurity plan, and to leverage outside expertise.

Solution

Intelligent Buildings® was asked to review the company's corporate cybersecurity plan, and to develop a roadmap for OT devices and contractors to comply with the strategy and standards for the broader enterprise network.

The plan also needed to be compatible with the company's approach of using the National Institute of Standards & Technology (NIST) cybersecurity framework. This required organizational alignment between multiple groups inside the company and various vendors and contractors. This was accomplished with a series of workshops, interviews, assessments, and documentation. One of the challenges to overcome was the extreme fragmentation in the entire real estate industry between owner, operator, property management, facility management contractors, and subcontractors.

EXECUTIVE SUMMARY

CLIENT

- Help a Top 5 U.S. managed healthcare services provider develop standards for enterprise IT and OT networking in Clinical Facilities and Office Space

SOLUTION

- Develop full company Cybersecurity strategy and implementation
- Assess existing portfolio of buildings against developed company standards through software scanning of Enterprise IT and OT networks
- Reported on each building as a baseline with recommendations for mitigation where applicable

IB SERVICES

- Clinical Facilities and Office Space Building Cybersecurity & Contractor Risk (Inventory and?) Assessment

BENEFITS

- Establishment and implementation of a strong and cohesive OT cybersecurity strategy
- Baselining of over 300 buildings
- Actionable recommendations for Client

90 M
SQ FT

300+
SQ FT

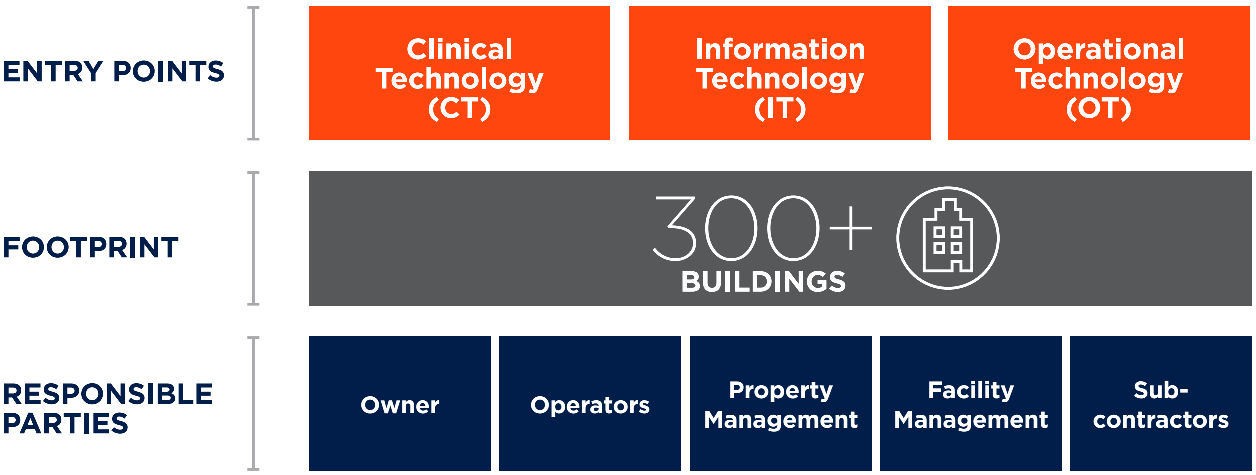
This coupled with the cultural gap between IT staff and facilities staff meant that many issues were lost in translation, resulting in cybersecurity gaps.

Contractors tend to control building systems, rather than the building owners. This often causes tremendous differences between the organization's policy and requirements and the realities in the systems. The resulting knowledge gap is manifested in the lack of basic inventory awareness of the actual devices, models, revisions, and the nature of their connectivity internally and externally.

IB conducted a comprehensive inventory and site audits of a representative set of buildings in multiple regions to determine inventory and configuration details, as well as the networking and external connectivity setup.

The networking and connectivity evaluation showed that traditional IT segmentation tools and methods were not sufficiently cataloguing the OT devices. IB then developed network profiles to correctly identify the OT devices and create appropriate network segmentation. The subsequent solution involved creating comprehensive OT cybersecurity FM playbooks. This is a combination of best practices, procurement guidelines and contractor policies and associated workflow.

The customer and the company then implemented new access management software and procedures, asset management software and procedures as well as developed new standards for controls profiles and device hardening guidelines for both manufactures and contractors. These standards will apply to existing and new solutions and documents end of life timelines.



ENTRY POINTS

Clinical Technology (CT)

Information Technology (IT)

Operational Technology (OT)

FOOTPRINT

300+ BUILDINGS

RESPONSIBLE PARTIES

Owner

Operators

Property Management

Facility Management

Sub-contractors

About Intelligent Buildings

Intelligent Buildings® is the only companyfocused on Smart Building advisory, assessment, and managed services at scale for new projects and existing portfolios. We help our customers manage risk, enhance occupant well-being, and continually improve performance by providing unmatched expertise, practical recommendations, and targeted services. Since 2004, we are the most trusted and experienced name in Smart Building services.

Assessment Services

- Building System Cybersecurity & Contractor Risk Assessment
- Building System Discovery & Capabilities Assessment

Smart Building advisory, assessment, and managed services at scale.

INTELLIGENT BUILDINGS™

Contact us today!
704.759.2700
Learn more at **intelligentbuildings.com**