WARNERMEDIA-CYBERSECURITY

CASE STUDY

WarnerMedia pioneers end-to-end Smart Building cybersecurity at 30 Hudson Yards.

INTELLIGENT BUILDINGS™

Overview

WarnerMedia's new headquarters at 30 Hudson Yards was constructed over five (5) years as part of the Hudson Yards development project in New York City. As new construction began, WarnerMedia had oversight over the building design to meet its needs as a global media company. This included making the new headquarters a Smart Building that delivers tenant comfort, efficient building operation, and remote management. To provide these Smart Building capabilities, underlying operational technologies (OT) and software are networked together throughout the building. Like informational technology (IT) networks, OT networks can be compromised by cyberattacks. With the perspective that its headquarters is a high-profile target for cyberattacks, WarnerMedia evaluated OT cybersecurity risks the same way they would evaluate IT cybersecurity risks. However, WarnerMedia found that the OT systems available on the market did not comply with its existing IT Cybersecurity Policies. Determined to realize the benefits of a Smart Building while simultaneously decreasing cybersecurity risk, WarnerMedia engaged the services of Intelligent Buildings (IB). Leveraging over ten (10) years of experience in Smart Building cybersecurity, IB helped WarnerMedia achieve complete OT compliance with its IT Cybersecurity Policies.

EXECUTIVE SUMMARY

Building profile

- **Location:** 30 Hudson Yards
- **Office size:** 1.1 million square feet
- **Building type:** Commercial office
- **Owner:** WarnerMedia (formerly Time Warner)

Challenge

- Secure all operational technologies (OT) at WarnerMedia's new Smart Building headquarters to meet their enterprise informational technology (IT) cybersecurity policies

Solution

- Develop a strategy to achieve WarnerMedia's Enterprise Infrastructure Services (EIS) team cybersecurity policies in OT without impacting system behavior
- Work with building systems vendors to evaluate all building control devices' security capabilities and determine the security gaps between each device and the EIS cybersecurity policies
- Assist in implementing compensating procedural controls for devices unable to meet security standards and create control profiles for each device
- Develop an ongoing process and program for WarnerMedia to maintain OT cybersecurity compliance

Intelligent Buildings Services

- Actionable Strategic Consulting
- OT Cybersecurity Consulting
- OT Program Support

Benefits

- Realized Smart Building benefits while reducing risks of cyberattacks on WarnerMedia's networks
- Dramatically improved long-term OT system security

1.1M	90	20-25%
SQ FT	STORIES	ENERGY REDUCTION

WarnerMedia expands the scope of its enterprise cybersecurity to building infrastructure

Bringing a utility mindset to commercial cybersecurity at WarnerMedia's new headquarters

WarnerMedia began planning a new headquarters to consolidate seven (7) locations in New York City. In 2014, the company announced that it would purchase a 1.1 million-square-foot commercial condo at 30 Hudson Yards for its new headquarters[1]. As part of the Hudson Yards Project—one of the largest private real estate projects in the country—the new construction at 30 Hudson Yards presented a rare opportunity in Manhattan for WarnerMedia to tailor the development of its new headquarters to meet its needs as a global media company.

WarnerMedia and its media divisions—CNN, HBO, Turner, and Warner Bros.—relied on servers, applications, IT, and building infrastructure to deliver its media services. However, WarnerMedia assessed building infrastructure decisions more like a utility company than a standard commercial business. Building infrastructure that fails or is compromised by cyberattacks could cause a service outage. Like utility facilities, WarnerMedia considered its headquarters to be a high-profile target for both internal and external cyberattacks, leading the company to pursue sophisticated and secure OT for its headquarters.

WarnerMedia's bold initiative to completely secure its headquarters' OT

WarnerMedia identified several Smart Building capabilities to meet its business needs, including enabling efficient building operations, delivering a quality tenant experience, providing sophisticated backup sequences to support its mission-critical services if building technologies failed, and centralized remote access to view and manage building performance. While available Smart Building technologies could meet their performance requirements, they did not meet WarnerMedia's cybersecurity standards. Unlike IT cybersecurity, there remains limited market availability of OT systems that have strong cybersecurity capabilities[2]. With latent demand, market-wide OT security standards have not been established, presenting a monumental task for any existing or new building's OT cybersecurity to meet its IT policies. WarnerMedia broke with these market trends and engaged IB to create a cyber-secure Smart Building and bring all of their OT—including thousands of sensors—in line with their IT Cybersecurity Policies.

The underlying security challenges of OT

OT's and IT's contrasting network design pathways

OT and IT had nearly opposing priorities, as their networking structures developed in the '80s and '90s. OT required that all building systems interact within milliseconds to provide a quality occupant experience, such as turning the lights on quickly when occupancy is sensed. This led to networks that prioritized information availability over information confidentiality. In contrast, IT developed prioritizing information confidentiality over availability, such as safeguarding credit card data throughout a network. As a result, OT's incipient architecture left it inherently more vulnerable to security threats as its Use Cases expanded in the 2000s and 2010s[3].

Converging OT and IT networks reveal formidable security gaps

Traditionally, IT and OT operated independently of each other. However, as IT infrastructure became ubiquitous and demand for more sophisticated OT grew, OT networking systems drew on IT to deliver new features[4]. New OT capabilities, like remote access and the proliferation of data from the network-connected Building Internet of Things (BIoT) devices, required IT networks to support building standards and other OT components. The two (2) networks continue to evolve to perform similar tasks, setting OT and IT on a path toward convergence[5].

OT technologies developed these new capabilities in phases, layering new technologies on top of the original network design, which led to an OT architecture without a standard pathway for system-wide software management. For example, a security patch for a company's servers may take only a few hours to install, but installing a similar security patch throughout an OT system may take several weeks due to bottlenecks that require coordination between the facilities and IT teams, integrators, and vendors.

These cybersecurity gaps between IT and OT are rippling across industries, as demonstrated by the top BIoT security concerns listed in a 2018 survey of organizations representing utility, government, technology, finance, education, and other sectors[6]:

1. Difficulty or lack of patching BIoT devices and systems, leaving them vulnerable
2. Accidental exposures resulting from user or vendor error and system complexity
3. Difficulty controlling, locating, tracking, preventing, and managing BIoT connectivity to critical infrastructure and other mission-critical systems
4. Failure to incorporate good security practices into the BIoT design, build, and operation and maintenance lifecycle models for systems
5. BIoT used as infection vectors to spread in the enterprise
6. Management of vendor access and system behavior

Policy initiatives addressing the rising OT security risks

Both government and industry initiatives are working to develop BIoT and overall Internet of Things (IoT) security standards, though there remains no consensus on BIoT cybersecurity best practices. The National Institute of Standards and Technology (NIST) developed an initial framework in 2014 outlining methodologies to mitigate the risk of IoT cyberattacks and is working toward BIoT and building control systems cybersecurity standards[7].

Additionally, the Industrial Control Systems Computer Emergency Response Teams (ICS-CERT) centralizes known OT vulnerabilities identified by governments, system owners, operators, and vendors, and then releases multiple control system security advisories per year[8]. These ICS-CERT advisories and the corresponding vendor patches can address known vulnerabilities in a system, but only if facility managers have visibility into all of the OT elements in a building and their current configurations. However, like BIoT cybersecurity as a whole, there is also no industry-wide standard to achieve network visibility.

WarnerMedia implements end-to-end OT cybersecurity to achieve a secure Smart Building

Bringing the OT cybersecurity at 30 Hudson Yards in line with IT standards

IB began its work by defining WarnerMedia's OT cybersecurity objectives through collaboration with WarnerMedia's Enterprise Infrastructure Services (EIS), which maintains the company's Cybersecurity Policies. EIS provided fifty (50 Cybersecurity Policy documents that IB reviewed to determine application strategies for building technologies that did not impact the functionality of the system and culminated in a defined OT Cybersecurity Policy for WarnerMedia.

IB then reviewed the security capabilities of every BIoT device and identified any required security functions that a device could not perform. If a device was unable to meet a component of the Cybersecurity Policy when installed, the IB team worked with vendors to create compensating controls to meet the requirement. A compensating control is an alternative method to reduce the risk that a BIoT device poses to the network (e.g., by implementing physical isolation, network segregation, or continuous monitoring). Because most BIoT devices have different security controls, every compensating control needs to be designed for a specific device. The IB cybersecurity team leveraged their experience with BIoT devices and implementing building integrations to create compensating controls for every cybersecurity gap in thousands of BIoT devices at 30 Hudson Yards.

Figure 1. IT Data Priorities

CIA

- **Confidentiality**
  RBAC dictates that this information is on a "need to know" basis.
- **Integrity**
  The integrity of the data is also a priority and must be protected through confidentiality.
- **Availability**
  Data is on a need to know basis and should only be granted after the user proves the need to know.

Figure 2. OT Data Priorities

AIC

- **Availability**
  The majority of communication is Machine-to-Machine (M2M) and happens in milliseconds. Without high availability, sequences of operations can be impacted and the system will not function as designed.
- **Integrity**
  The data passing between machines must be correct in order for the system to function as designed. Additionally, the human operator needs to know the correct responses of the system to diagnose and operate the system.
- **Confidentiality**
  Historically, confidentiality has had little to no consideration. Confidentiality must always be viewed through the operational risk lens.

Securing the OT networks through segmentation and segregation was the next step of the process. This isolates the OT networks from other networks—such as the Internet—by creating restrictive gateways to OT domains that minimize the methods and level of access to OT networks. Securely implementing OT networks becomes complex at the enterprise level, because every implementation is unique to the building. For example, at 30 Hudson Yards, the OT and IT networks needed to share the infrastructure. After the IB cybersecurity team determined the OT network architecture required to meet WarnerMedia's cybersecurity goals, EIS isolated the OT networks on the shared infrastructure by developing a series of virtual local area networks (VLANs) for each OT system.

Maintaining OT cybersecurity compliance

Lastly, WarnerMedia needed a process for maintaining OT cybersecurity compliance as regular software updates are released or patches for newly identified vulnerabilities became available. This began with providing facility managers the existing security features of every BIoT device. As they reviewed BIoT devices and implemented any compensating controls, the IB cybersecurity team created and refined control profiles for every device. The control profiles include rules for how the device could securely interact with IT networks by security function, such as whether the device is capable of strong passwords. If the device is capable of the security function, the control profile lists the associated process for the device. If it is not capable, the compensating control is listed. The control profile also includes guidance for manufacturer default credentials, settings for auto lockout, and known vulnerabilities at the time of installation. In addition to the control profiles, IB ensured complete visibility throughout the building control systems and BIoT devices with standard naming and tagging to enable facility managers to query devices easily.

> “Control Profile identifies the hardware/software characteristics that can be used to identify security and operational risks.

Maintaining OT security requires the facilities management and IT teams to work together to align cybersecurity needs across the systems. Both teams' BIoT cybersecurity work will be coordinated by updating the device control profiles with any changes. The EIS team will continue to work with BIoT vendors to update devices and systems to meet the cybersecurity requirements The facilities team will monitor and evaluate ICS-CERT security advisories, as well as manufacturer security advisories and updates, for any impact on WarnerMedia's OT using the device control profiles. If a security vulnerability is identified, WarnerMedia worked with IB to establish patch management protocols with device vendors to test and perform the security patches. The facilities management team will manage the end-of-life plans for OT devices by monitoring when a vendor announces the end of their support for a specific device, or if a device has no capable pathway to meet WarnerMedia's cybersecurity policies.

Meeting OT cybersecurity concerns head on to demonstrate the potential of large-scale, cyber-secure Smart Buildings

By taking OT cybersecurity risks seriously, WarnerMedia committed to bringing their BIoT devices in line with their IT cybersecurity policies. While the industry struggles with its concerns about BIoT cybersecurity risks, WarnerMedia worked with IB to overcome these concerns by implementing patch management protocols, creating control profiles detailing how to securely use devices, providing complete visibility into their building control systems and BIoT devices, and delivering end-to-end OT cybersecurity in line with their IT policies. This allowed WarnerMedia to confidently implement sophisticated Smart Building capabilities that provide business value, which may not have been viable otherwise.

References

1. Bagli, C.V. (2014, January 16) Time Warner is planning a move to Hudson Yards. *New York Times*. Retrieved from https://www.nytimes.com/2014/01/17/nyregion/time-warner-announces-a-move-from-columbus-circle-to-hudson-yards.html
2. Weiss, J. (2016) *Cybersecurity in Operational Technology.* Putman Media, Retrieved from https://www. researchgate.net/profile/Ljubomir_Jacic2/post/What_is_information_security/attachment/59d62ed979197b807798d097/AS%3A355807511236611%401461842529717/download/Cybersecurity_in_ Operational_Technology.pdf
3. Cihola, P., Lennie, A., Sadigova, P., & Such, J. (2019). *The Security of Smart Buildings: a Systematic Literature Review*. Retrieved from https://arxiv.org/abs/1901.05837
4. Gartner. (2011) IT and operation technology: convergence, alignment, and integration. Retrieved from https://www.gartner.com/doc/1548729/it-operational-technology-convergence-alignment
5. Olawuyi, J.O. & Friday, M. (2012) Technological convergence. *Science Journal of Physics,* Article ID sjp- 221, 5p. doi:10.7237/sjp/221.
6. Filkins, B. (2018) *The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns*. Retrieved from https://www.sans.org/reading-room/whitepapers/ICS/2018-industrial-iot-security-survey-shaping-iiot-security-concerns-38505
7. Barrett, M. P. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.* Retrieved from https://doi.org/10.6028/NIST.CSWP.04162018 6. About Us. (2019) ICS-CERT. Retrieved from https://ics-cert.us-cert.gov/about-us
8. National Institute of Standards and Technology. (2018) *Considerations for Managing IoT Cybersecurity and Privacy Risks Workshop Summary*. Retrieved from https://www.nist.gov/sites/ default/files/documents/2018/08/10/considerations_for_managing_iot_cybersecurity_and_privacy_risks_workshop_summary.pdf

119-2021