CABA™

Intelligent Buildings and Cybersecurity

LANDMARK RESEARCH REPORT

EXECUTIVE SUMMARY

CABA AND THE FOLLOWING CABA MEMBERS FUNDED THIS RESEARCH:

RUBY FUNDER

WATERFALL® Stronger Than Firewalls

EMERALD FUNDER

AcuityBrands · BOSCH · CF Cadillac Fairview · Honeywell · Hydro Québec · Ingersoll Rand Inspiring Progress™ · intel · John Hancock Real Estate · Johnson Controls · Manulife Real Estate · PHILIPS · ROGERS™ · Schneider Electric · SIEMENS

DIAMOND FUNDER

BODVOC LTD. · CSA Group · ISA Security Compliance Institute · TRIDIUM · United Technologies

CABA Intelligent Buildings and Cybersecurity: 2015/2016 Landmark Research

This report was prepared for CABA by Compass Intelligence, LLC.

About Compass Intelligence

Compass Intelligence is one of the leading market analytics and consulting firms specializing in metrics-driven market intelligence and consulting focused on the mobile, Internet of Things/M2M, green technology, and emerging technology markets. Compass Intelligence provides a number of key services including strategic advisory, market sizing/modeling, competitive benchmarking, executive-level consulting, and turn-key survey services. Providing quality services over 10 years, many of the top technology vendors rely on Compass Intelligence's expertise and insights to make better and more informed planning, strategy, and development decisions. Visit us at www.compassintelligence.com to learn more.

About CABA

The Continental Automated Buildings Association (CABA) is an international not-for-profit industry association, founded in 1988, dedicated to the advancement of connected home and building technologies. The organization is supported by an international membership of over 330 organizations involved in the design, manufacture, installation and retailing of products relating to home automation and building automation. Public organizations, including utilities and government are also members. CABA's mandate includes providing its members with networking and market research opportunities. CABA also encourages the development of industry standards and protocols, and leads cross-industry initiatives.

TABLE OF CONTENTS

Executive Summary 5
- Introduction 5
- Funders 5
- Role of the Steering Committee 6
- Report Structure and Layout 6
- Report Methodology 7
- Background 7
- Key Recommendations and Study Highlights 10
- Case Study: Research Park Campus Case Study - Waterfall Security Solutions 12
  - Project Overview 12
  - Waterfall Security Solutions 12
  - Original network 13
  - Waterfall Solution 14
  - Impact on Operations 14
  - Predictive Maintenance Cloud Provider 15
  - Key Achievements 15

Main Report 16
- Intelligent Building Overview 16
- Building Management Systems Adoption 19
- Degree of Integration among Building Systems 21
- Review of Cybersecurity Threats in Intelligent Buildings 23
  - Intelligent Building Ecosystem 23
- Intelligent Buildings and Cybersecurity: An Overview 25
- Survey Data Analysis 27
  - Survey Respondent Profile 28
- Case for Cybersecurity in Intelligent Buildings 29
- Cybersecurity Areas of Concern 32
- Level of Preparedness against Cybersecurity 33
- Types and Sources of Cybersecurity Threats 37
- Cybersecurity Budgets and Spending 42
- Willingness to Pay and Buying Influences 45
- Cybersecurity Purchase Influencers 48

Final Findings & Recommendations 51
- Overall Observations 51
- Building Owners, Administrators, or Managers 52
- IT Managers 53
- Intelligent Building Products & Services Vendors (BMS/BAS) 53
- Glossary of Terms 55
- References 57
- Appendix 58
  - Intelligent Building Entry Points 58
  - End-user Insight on the Ecosystem 59
  - Inhibitors to Industry Growth 60
  - Additional Case Studies 61

FIGURES

Figure ES 1: Standalone vs. Converged Building Systems 8
Figure ES 2: Protection Requirements 10
Figure 1: Primary Touchpoints for Intelligent Building Market (2015, North America) 17
Figure 2: Commercial Building Market Size in the U.S. and Canada 18
Figure 3: Building Management System (BMS) Primary Levels 19
Figure 4: BMS Penetration by Commercial Building Size (U.S. and Canada) 20
Figure 5: BMS Penetration by Building Type (U.S. and Canada) 21
Figure 6: Integration of Security Systems (2014) 22
Figure 7: IT/Horizontal Convergence 22
Figure 8: Cost Savings Drive Building Owners' Interest in Making Changes to Infrastructure 23
Figure 9: Intelligent Building and Smart City Connection 24
Figure 10: The Cybersecurity Ecosystem, 2016 25
Figure 11: Selected Access Points for Cyber-Attacks 27
Figure 12: Survey Respondent Profile 28
Figure 13: Survey, Breakout by Size of Business 29
Figure 14: The Change in Severity of Building/Facility Security Incidents over the Last 12 Months 30
Figure 15: Importance of Cybersecurity 30
Figure 16: Truths of Those in the Market 31
Figure 17: Building Elements Perceived to Be at High Risk 32
Figure 18: Top Areas of Concern for Securing and Protecting Buildings and Offices 33
Figure 19: The Availability of Resources and Skills to Tackle Cybersecurity 34
Figure 20: Readiness Level by Group 35
Figure 21: What Is Being Done to Reduce Risk? 36
Figure 22: Modern Cybersecurity Threats 37
Figure 23: Profile of Cyber Attackers and Types of Attacks Carried Out (2015, North America) 40
Figure 24: Perceived Sources of Cyber Threats 41
Figure 25: Most Spend between 5-20% of an IT Budget on Cybersecurity 42
Figure 26: Changes in Security Budget from 2014 to 2015: Survey Results 43
Figure 27: Percentage Increase in Cybersecurity Budget 43
Figure 28: Global Cybersecurity Expenditures, 2015-2022 44
Figure 29: Willingness to Pay for Cybersecurity 45
Figure 30: Pros and Cons of Wireless vs. Wired Networks 46
Figure 31: Top Barriers to Adoption 46
Figure 32: Awareness of Standards 47
Figure 33: Level of Buying Influence by Group 48
Figure 34: Top Areas for Advice Regarding Security 49
Figure 35: Who Is Trustworthy and Reliable? 50
Figure 36: Snapshot of an Intelligent Building 58
Figure 37: Ecosystem Map for the Intelligent Building and Cybersecurity Market (2015), North America 59
Figure 38: Market Constraints for Intelligent Building and Cybersecurity Market (2015, North America) 60
Figure 39: Key Pillars to Success for Intelligent Building and Cybersecurity Market (2015), North America 60

EXECUTIVE SUMMARY

INTRODUCTION

This study has been has been authored by Compass Intelligence, a metrics-driven market research and consulting firm, for the Continental Automated Buildings Association (CABA). CABA is a leader in initiating and developing cross-industry collaboration research. The report was created under the direction of the CABA Research Program.

This study analyzes potential cybersecurity risks that are faced by owners and managers of intelligent buildings. Given the increased degree of building automation and the use of converged information technology (IT) and building systems or operational technology (OT) networks, the risk of cyber-attacks launched against building structures has risen tremendously. This study specifically focuses on the extent to which cyber-attacks can arise from and are targeted at integrated building control systems. This study also lists steps that can be taken to limit the likelihood of such incidents and their impact. In addition, the study leverages end-user research that involves IT managers, in order to further elaborate the extent to which the real estate industry and IT professionals understand the concept of cybersecurity within the built environment. The study only focuses on the North American (U.S. and Canada) commercial intelligent building market, and residential structures are excluded from the discussion. Lastly, the study provides recommendations to building owners and facility managers and highlights potential hardware and software-based security solutions, which are specifically designed to identify and prevent cybersecurity threats in intelligent buildings.

FUNDERS

Funders of this research include the following organizations: Acuity Brands, Inc., Bodvoc Ltd., Cadillac Fairview Corporation, CSA Group, Honeywell International, Inc., Hydro-Québec, Ingersoll Rand, Intel, ISA Security Compliance Institute, Johnson Controls, Manulife/John Hancock, Philips, Robert Bosch LLC, Rogers Communications, Inc., Schneider Electric, Siemens Industry, Inc., Tridium, Inc., United Technologies Corporation, and Waterfall Security Solutions Ltd.

RUBY FUNDER

WATERFALL® Stronger Than Firewalls

EMERALD FUNDER

AcuityBrands. BOSCH CF Cadillac Fairview Honeywell

Hydro Québec IR Ingersoll Rand Inspiring Progress™ intel John Hancock Real Estate

Johnson Controls Manulife Real Estate PHILIPS ROGERS™

Schneider Electric SIEMENS

DIAMOND FUNDER

BODVOC LTD. CSA Group ISA Security Compliance Institute TRIDIUM United Technologies

ROLE OF THE STEERING COMMITTEE

The Steering Committee represents a cross section of solution providers in the intelligent buildings marketplace. Representatives from each company joined Compass Intelligence and CABA on regular teleconference calls to ensure the research scope met the project objectives. The Steering Committee played a vital role in outlining the research product, in terms of defining the required content and collaborating on the research approach, including the development of the survey, requested input, report structure, and final output. Only Ruby and Emerald funders served on the Steering Committee, which included: Acuity Brands, Inc., Cadillac Fairview Corporation, Honeywell International, Inc., Hydro-Québec, Ingersoll Rand, Intel, Johnson Controls, Manulife/John Hancock, Philips, Robert Bosch LLC, Rogers Communications, Inc., Schneider Electric, Siemens Industry, Inc., and Waterfall Security Solutions Ltd.

REPORT STRUCTURE AND LAYOUT

This research engagement entails a final written report, which includes an executive summary and the main report. The executive summary highlights the key findings in the research, and provides high-level recommendations. The main report houses multiple sections, which set the stage for both the cybersecurity market and the intelligent building market. It also delves into key sections to further explore the most relevant and actionable intelligence gathered during this research engagement. The report includes a number of key elements, including direct results from a recent survey, market forecasts,

feedback from key stakeholders that are based on interviews and briefings, directional analysis gathered from key stakeholders and vendors operating in the building and technology market, depictions/figures/graphs/visuals, and third-party resources for further exploration. The final section of the report includes a list of recommendations and key findings, based upon the overall research and the survey.

REPORT METHODOLOGY

Compass Intelligence took a phased approach to conduct this research. The research elements comprised both primary and secondary research. Secondary research included a thorough review of internal and external research sources, including cybersecurity studies conducted by Compass Intelligence and other IT and building systems vendors. In addition, a detailed review of industry case studies and government cybersecurity reports was conducted, in order to identify threat sources and analyze the extent to which such sources posed a risk to building control systems.

In phase 1, Compass conducted research interviews (both phone and face-to-face) and had discussions with key stakeholders. These interviews directly examined security breaches, including those of real estate investment trusts (REITs), and privately-held buildings. IT decision-makers and corporate building owners and managers were interviewed. Compass Intelligence also conducted interviews with companies that influence the purchase of intelligent building solutions, including systems integrators, consultants, engineers, contractors, and other decision-makers.

This phase also included a Web-based survey with stakeholders and decision-makers in the intelligent building and IT market. Compass Intelligence completed a 15-20 minute survey with approximately 500 end-users and influencers. Below is a summary of the survey methodology. The online survey research was conducted over the course of one week, using opt-in email lists from a well-regarded Internet research panel vendor and the Compass Intelligence Thought Leaders' Panel. The survey involved 939 people who started the survey: 543 of these qualified for the survey, and a total of 502 completed it in its entirety.

For Phase 2, Compass Intelligence interviewed 30 key market participants and had various discussions with the CABA Steering Committee. In addition, Compass Intelligence conducted interviews with 15 traditional security and IT firms.

The report also contains a case study from the Ruby Funder, Waterfall Security Solutions Ltd.

BACKGROUND

In the past few years, a growing interest has occurred among commercial and residential real estate owners and operators to improve the operational efficiency of commercial and residential buildings. Several factors are responsible for the rising interest in enhancing efficiency and safety of building operations, while also maintaining a conducive in-building environment for internal (tenants) and external (visitors) users. These factors include needs to curb energy costs (e.g., green buildings and corporate sustainability), reduce building maintenance expenditures, protect buildings against both man-made and natural disasters, and improve environmental sustainability through the reduction of carbon footprints, as well as resource conservation.

In order to accomplish these objectives, building owners are increasingly seeking and implementing a variety of technologies, which range from remote building monitoring systems to advanced energy management software. These technologies ensure the efficient and effective operation of commercial and residential structures - specifically multi-tenant and multi-dwelling units. In addition, state-of-the art communications networks are also being installed to improve the commercial attractiveness of buildings.

Furthermore, the utilization of related Internet of Things (IoT) solutions, such as automation and smart-meters, are also on the rise. Building owners and operators are aiming to boost the performance of both their legacy and newly built commercial structures. Last but not least, in the wake of rising

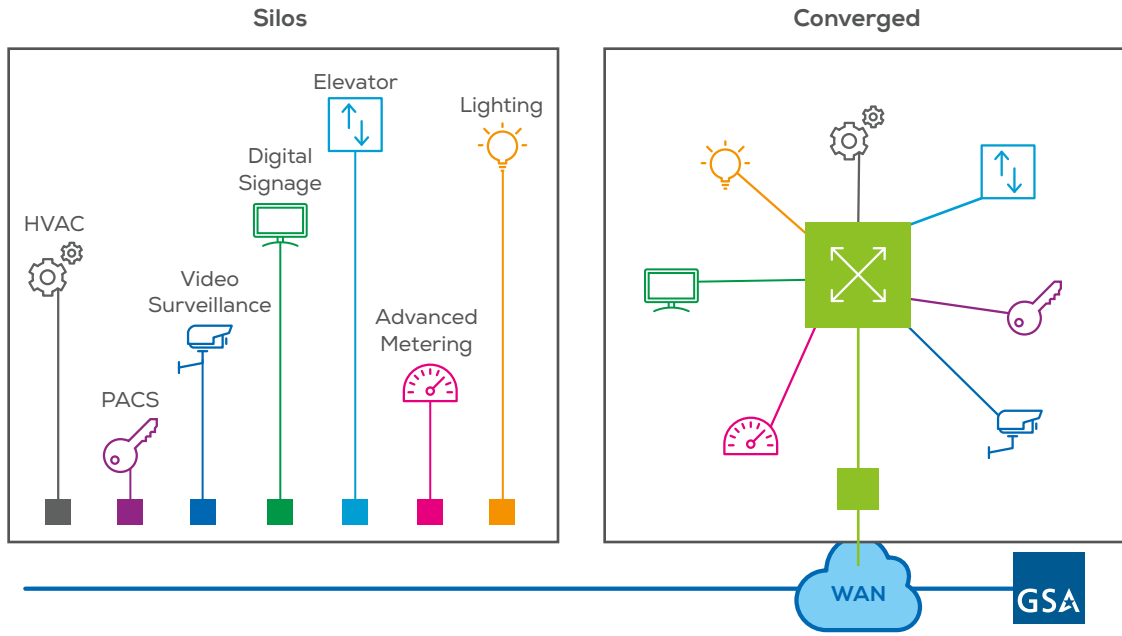
global terrorism, commercial building owners are also being tasked with implementing physical security systems, which proactively identify and alert building occupants of any active incidents within the environment.

The plethora of technologies that are being implemented within the commercial building segment has brought the concept of an intelligent building (or smart building) to life. An Intelligent Building is a commercial real estate structure that "employs technology and processes to reduce its environmental impact, protect occupant health and safety, improve employee productivity, and become more operationally efficient for its owners."[1]

Essentially, an intelligent building is comprised of a building management system (BMS) or building automation system (BAS), also referred to as building control systems (BCS) or industrial control systems (ICS). These systems are effectively integrated with information technology (IT) systems to enable or support a variety of building management functions. BMS/BAS/BCS are also often referred to as building operational technology (OT). The economic value proposition of an intelligent building resides in its ability to allow building owners and facility managers to accomplish a variety of economic and operational objectives. These objectives can include, but are not limited to, cost reduction and greater environmental responsibility.

Figure ES1 highlights the growing trend toward integrated or converged IT networks and building technologies.

Figure ES 1: Standalone vs. Converged Building Systems



Source: GSA, https://www.wbdg.org/resources/cybersecurity.php 2015

Some of the key drivers impacting greater integration between building control systems and IT include:

- Increasing availability and implementation of advanced building management systems, which are capable of leveraging infrastructures that are based on Internet Protocol (IP). Examples include:
  - **Schneider Electric's SmartStruxure** integrated solution, which helps building owners and facility operators effectively monitor and manage their energy usage.
  - **Johnson Controls' Metasys Building Automation System** not only connects a variety of in-building systems, such as lighting and security. It also provides information on

a single platform to simplify building management functions.
    - **Siemens Building Technologies' APOGEE** building automation system enables integration of disparate building systems thereby helping facility owners and managers accomplish their operational efficiency objectives.
- A greater focus on reducing building energy costs is leading to the implementation of advanced building systems, which integrate with electrical systems to constantly gather and report data - over a variety of platforms and to a number of stakeholders.
- The rising adoption of various IoT-related technologies are designed to improve building safety, operational efficiency, and environmental sustainability. Examples include smart meters, parking sensors, and HVAC automation.
- The need to future-proof buildings, while also improving the commercial attractiveness through implementation of state-of-the art communications and IT solutions. Focus on securing endpoints, connectivity, applications/data, and implementing threat management solutions.

However, while offering significant operational benefits, the ongoing movement toward integrated building systems and IT networks is also creating a "spill-over" effect. As a result, integration is exposing building owners and facility managers to the risk of cybersecurity breaches—incidents that are all too prevalent within the IT sector. These cybersecurity threats against building systems include hacking and denial of service (DoS). They can adversely impact the overall operational viability of a commercial structure, render an intelligent building unsafe for its occupants, and expose building owners to significant liability risk. Moreover, a cybersecurity breach launched through BMS/BAS can also compromise the integrity and security of corporate networks that are operating within the building. This study specifically analyzes the potential cybersecurity threats that exist within the intelligent building segment. The study also offers insights from a survey of IT managers and also offers potential recommendations for all stakeholders.

The well-documented security breach at Target offers a rather intimidating example of a cybersecurity breach, in which hackers used login credentials from the retailer's heating, ventilation, and air-conditioning (HVAC) provider to gain access to point-of-sale (POS) registers. The hackers then proceeded to steal customer credit card data and routed it to various international locations. The data connection between Target and its HVAC vendor, Fazio Mechanical Services, was strictly being used for "electronic billing, contract submission, and project management."[2] The Target incident reveals that even when a third-party vendor of a building system does not perform remote building monitoring and management functions, the mere connection to the building portal for basic business transactions can render the building susceptible to a full-blown cybersecurity attack.

The severity of a targeted cyber-attack launched against critical infrastructure can be visualized from the impact of the BlackEnergy malware that shut down power systems supporting as many as 80,000 customers in Ukraine.[3] While there is no evidence as of yet that the attack utilized BAS/BMS, it nonetheless aimed to wipe-out supervisory control access and data acquisition (SCADA) servers hence causing delay in power restoration. The hackers then proceeded to launch a denial of service (DoS) attack that prevented the utility company from receiving customer reports of the outage.

A 2014 study by the Government Accountability Office (GAO) in the United States found that the number of cybersecurity breaches involving building control systems experienced an increase of 74 percent - from 140 incidents in 2011 to 243 incidents in 2014.[4] Similarly, in February 2016, the Hollywood Presbyterian Medical Center in Los Angeles suffered what is deemed as an emerging yet critical pattern in cyber-attacks. The crypto-ransomware cyber-attack shut down critical hospital information systems thereby causing significant operational disruption. Such ransomware attacks are increasingly being aimed at large institutions and may eventually target BMS/BAS in larger structures such as mass transit facilities, convention centers, hospitality, healthcare, government plazas, and others in order to shutdown critical building functions such as elevators, HVAC, or entry/access points.

KEY RECOMMENDATIONS AND STUDY HIGHLIGHTS

BMS/BAS and other integrated building control systems can be breached through a variety of IT devices and systems. Conversely, cybersecurity attacks may also originate through integrated BMS/BAS and expand to other IT networks and devices. Figure ES2 lists the primary protection requirements based on the results of this study.

Figure ES 2: Protection Requirements

Full Assessment
- Processes, Systems, Tech

Stakeholder Roles
- Priorities, Escalation
- Responsibilities

ID Types & Risk
- Network, Security, Spam, DoS

Coordination Across
- Stakeholders

ID & Evaluate Threats
- Sources of Vulnerability
- Inside and External

Structured Audits
- Accountability and Review
- Adaptation

Source: Compass Intelligence, 2015

From the perspective of a building owner or facility manager, protecting building systems against cybersecurity breaches requires the following:

- The **detailed assessment** of the processes, systems, and technologies involved in integrated building and IT systems.
- The **accurate identification and understanding of the types of cyber-attacks**, such as viruses and denial of service (DoS) and malware (including ransomware) - which can be targeted at intelligent buildings.
- The **identification and evaluation of threat sources.** These sources comprise both insiders and external entities, such as disgruntled employees or business partners, hackers, competitors, and rogue states (that may proactively sponsor and condone such activities). Moreover, cybersecurity breaches can occur through the intrusion of the building vendors' internal and external Web portals and applications.
- A thorough **understanding of the roles, responsibilities, and capabilities of various stakeholders** (such as building owners, tenants, building/industrial control system vendors, IT personnel, and third-party security vendors). When developing cybersecurity strategies, analysis is vital prior to instituting changes to systems, people, and processes.
- The **effective and continuous coordination** of all stakeholders, including building systems vendors, IT personnel, and systems integrators.
- **Routine audits** of BMS/BAS hardware, software, and processes to identify any cybersecurity vulnerabilities.

In addition, the National Institute of Standards and Technology (NIST) in 2014 provided a rather comprehensive framework[5] for implementing effective cybersecurity solutions to guard critical infrastructure (including buildings) from cyber-attacks. Research conducted by Gartner Group shows that 30 percent of the organizations are using the Framework. Examples include: Bank of America, U.S. Bank, Apple, Walgreens, Pacific Gas & Electric and several others.

The NIST Framework comprises the following components:

A. **Framework Core** which includes a set of cybersecurity activities that are deemed common across various infrastructure sectors:
   - *Identify* - Develop an organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
   - *Protect* - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
   - *Detect* - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
   - *Respond* - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
   - *Recover* - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

B. **Profiles** which help organizations assess, align, and prioritize their cybersecurity efforts, while also providing a mechanism to measure their progress toward a targeted cybersecurity state.

C. **Tiers** which categorize organizations based on their approach and procedures for managing cybersecurity.

From a building owner/facility manager's perspective, planning for preventive measures against cyber-attacks may also require the consideration of purchasing adequate cyber insurance in order to limit the negative financial consequences stemming from such incidents. The growing threat of ransomware attacks, such as Cryptowall, further underscores the importance of obtaining cyber insurance in order to mitigate post-attack financial losses. Compass Intelligence lays out a number of additional key recommendations and steps to consider for stakeholders in the intelligent building and building systems industries. As a result of discussions with stakeholders and extensive research that includes survey analysis, it is imperative that the industry coordinate and work together to educate, develop a structured approach, and introduce solutions to prevent attacks in a manner that is proactive rather than reactive. The latter may be expensive, pose stricter insurance requirements, and introduce risks to building tenants and corporations.

Recommendations are provided for IT managers, building administrators, owners, managers, and companies that provide solutions, equipment, and products to intelligent building end-users. A highlight of some of the key recommendations are provided below:

- Building owners and operators need to accurately understand both intra- and inter-system integration, including understanding the differences among industries and building types.
- Building owners and operators need to understand and identify the preparedness level that is needed to protect against the risk of BMS/BAS-related cybersecurity.
- Strong collaboration and coordination is required among all building stakeholders, including building control systems' vendors and cybersecurity vendors.
- Stringent policies and procedures to guard both IT and OT against cybersecurity threats must be implemented. Cybersecurity is not just a technology issue; it is also a "people" issue.
  - A comprehensive cybersecurity plan is critical and must include all threats, including employees, tenants, and even ex-employees.
- Vendors of BMS/BAS-related security solutions must continue to educate building owners and facility managers about cybersecurity issues.
- As the industry moves to IP and cloud-enabled building management and automation solutions, the need to protect and secure both IT and OT networks is increasing. Security starts with the building systems companies and products, and it ends with the customer. Again, focus on securing endpoints, connectivity, applications/data, and implementing threat management solutions.

- Reducing vulnerabilities and risk may involve the investment and implementation of:
  - Securing and hardening wireless and IP networks
  - Stricter authentication and access management
  - Further security protocols to restrict access
  - Security software and ongoing updates and maintenance
  - Separation of the IT and OT networks
  - Other planned measures to harden the building system's infrastructure and networks

CASE STUDY: RESEARCH PARK CAMPUS CASE STUDY – WATERFALL SECURITY SOLUTIONS

Project Overview

A private investment firm owns and operates a small west-coast research park: 15 buildings, 750,000 square feet of office space, 100-130 tenants and 600-900 occupants. The facility is managed by a state-of-the-art building management system (BMS) that integrates utility meter reading, HVAC, physical security badging controls, lighting, elevator controls and emergency fire suppression air flow controls into a single, Web-based user interface. The BMS user interface can be accessed via touchscreens in tenant facilities, from the Internet, via Web browsers, and cell phones.

A successful spear phishing attack prompted a review of cybersecurity protections. A stolen administrator password for the Web-based management system enabled the theft of additional account names and passwords. These credentials were subsequently used to break into the investment firm's remote access system. A forensic investigation revealed that the intruders had, over the course of six weeks, logged into a number of computers, including several of the building automation servers.

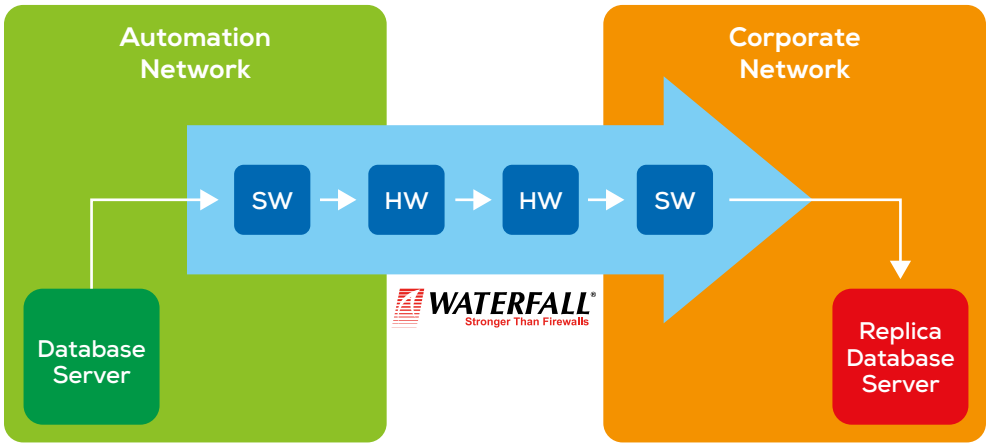
A more sophisticated attack that damaged firmware on individual controllers could have shut down the HVAC systems and forced all tenants to evacuate until the equipment could be replaced. Direct and indirect damages from such an event would be significant, both in direct costs, and in damage to reputation. In many cases, these events are covered by insurers only if the facility can demonstrate that "reasonable and prudent" cybersecurity measures were in place.

The risk analysis also concluded that, given the need to connect building automation systems to corporate systems and the Internet, no IT security mechanisms could assure defeating this class of attacker with a high degree of confidence. Specific improvements, such as two-factor authentication, can improve security, but as long as a system is connected to the Internet through a firewall, that system is at risk. A wider search for security solutions found industrial control system security standards for now routinely recommended Unidirectional Security Gateways to address network-based cyber-sabotage threats, even for Internet-connected systems.

Waterfall Security Solutions

As Waterfall Security Solutions is the market leader for Unidirectional Security Gateways, the investment firm asked Waterfall to look at their system and recommend a solution. Waterfall recommended deploying the Waterfall FLIP.

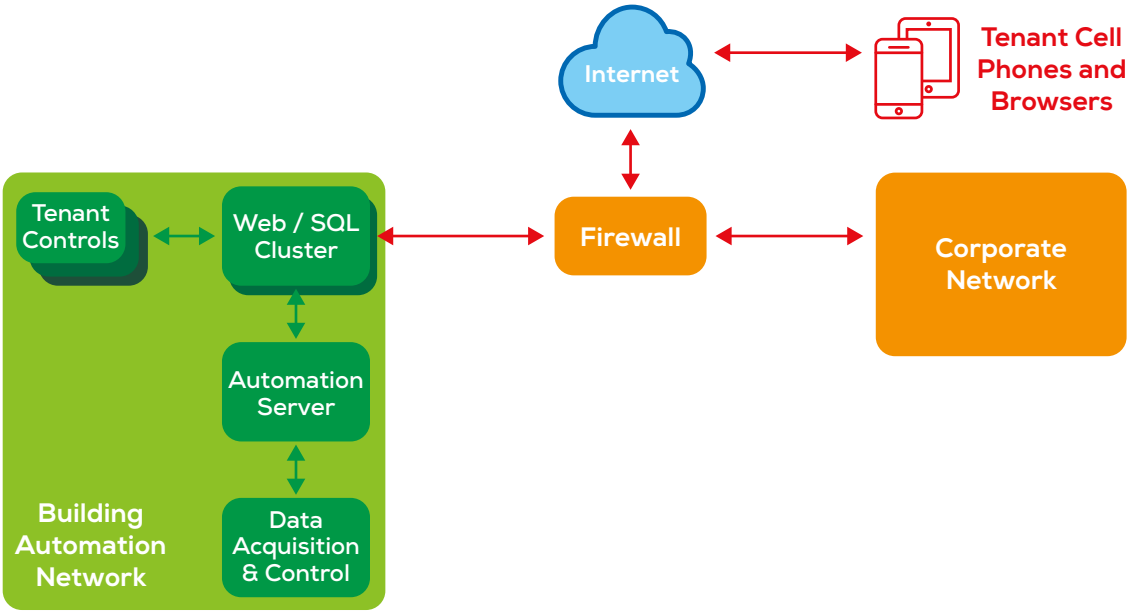
The Waterfall FLIP is a variation on Waterfall's pioneering Unidirectional Security Gateway product. Unidirectional Security Gateways replicate control system servers across unidirectional hardware connections. The hardware is able to send information from a control system network to an external network, such as a corporate network or the Internet, but is physically unable to send any information or any attack, back into the control system network.



The FLIP contains all of the unidirectional communications hardware of a Unidirectional Security Gateway, with additional switching logic. The FLIP can only send information in one direction at a time, and can reverse direction on a schedule. Like Unidirectional Security Gateways, the FLIP replicates servers, and never forwards packets. The controller that determines the FLIP's orientation is blind to traffic passing through the FLIP, and so cannot be compromised without physical contact with the FLIP hardware.

Original network

The original network architecture for the research park's building automation solution is shown below:

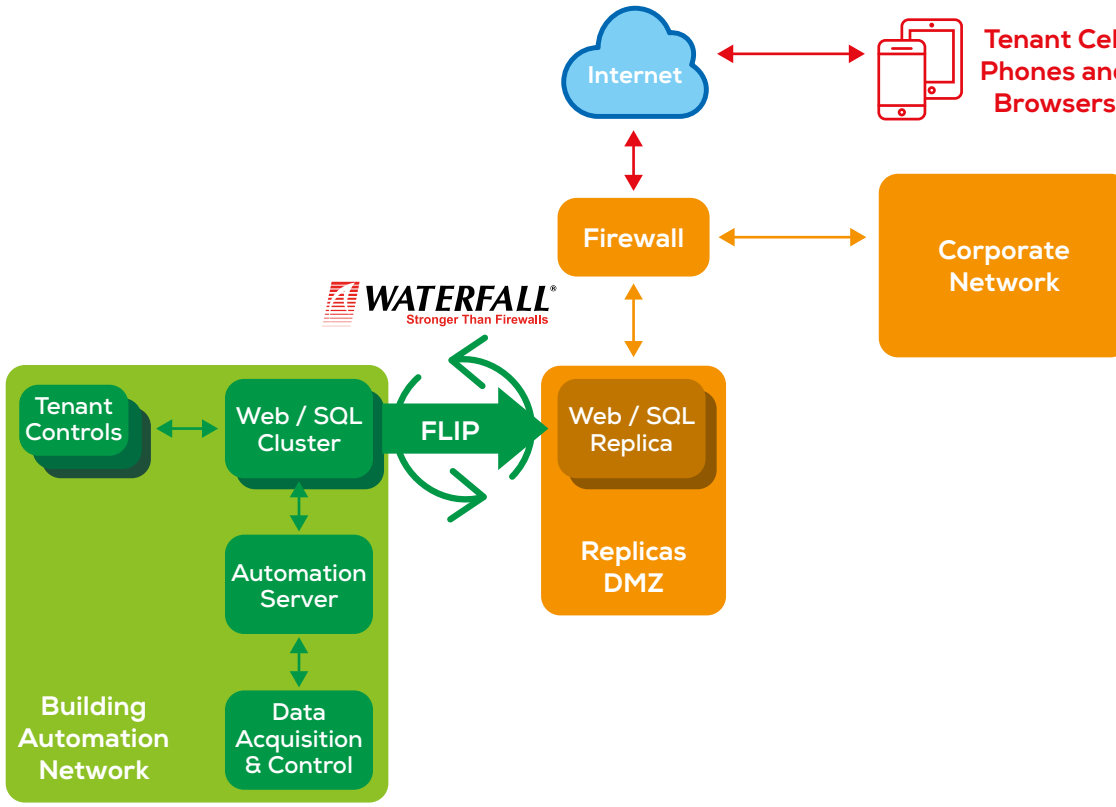


An Automation Data Server aggregates data from all of the site's building automation systems, carries out site-wide optimizations, and animates control system screens in the site operations center. A structured query language (SQL) server cluster hosts the SQL Server database and building-automation Web server functions. The database contains both historical data and current real-time data, updated every minute. Control requests are routed from touchscreen, tenant-control Web clients to the building automation system via the Web server and the SQL Server database. A firewall separates the building automation network from the branch of the investment firm's corporate network at the research park

campus. Web requests from tenant browsers and cell phones accessing the Internet are routed through the firewall directly to the building automation Web server.

Waterfall Solution

The Waterfall Solution is illustrated below.



A “demilitarized zone” (DMZ) network was added to host a replica of the SQL Server / Web server cluster. The Waterfall FLIP is deployed at the interface between the automation network and the new DMZ, and the DMZ communicates with the corporate network and the Internet through the existing firewall. The FLIP is configured to request all data from the live SQL Server cluster, and populate the replica cluster in real time.

The FLIP reverses orientation once per day at 4 AM for five minutes. The FLIP software in the DMZ queries a weather forecasting Web site hourly and stores the latest weather forecast for the research park campus as an XML file. Every day at 4 AM, while the FLIP's orientation is reversed, the folder containing the forecast is replicated to the automation network. In the automation network, the FLIP software forwards the weather forecast to the building automation system so that the system can plan a schedule for air conditioning that is likely to minimize peak energy usage, while still meeting tenant cooling commitments.

Impact on Operations

With the FLIP in place, there is no longer any possibility of a remote control attack from the corporate network or the Internet interfering with building automation systems. This means however, that remote control of tenant suites from the Internet is no longer possible. Tenants can still control their environment from the touchscreen control consoles in their units, and can see energy usage, cooling statistics and other information from the replica Web server on their cell phones, but can no longer control their suites from their cell phones. This is seen as an acceptable trade-off, because any network design that

permits tenants to control building automation systems from their cell phones also permits hacktivists and other attackers to sabotage the entire building automation system from their cell phones.

With the Waterfall FLIP in place, security updates can be installed on the live automation equipment at whatever schedule is deemed appropriate by the operations team. The automation system's Web/SQL cluster is no longer exposed to high-risk Internet connections, and no longer requires updates as strictly as did the Internet-exposed server. Security updates on the replica Web/SQL cluster are applied automatically. If any problem arises during application of an update, the replica Web/SQL cluster most likely does not restart. A broken replica cluster means that reporting functions to tenants are impaired, but all building control functions and emergency functions still operate normally. The control functions are implemented on the primary Web/SQL cluster, not the replica. If the replica cluster malfunctions, or is attacked, the replica can be erased and restored from backups to a last known-good state as time permits.

Predictive Maintenance Cloud Provider

A subsequent upgrade of the automation system to use a cloud provider for predictive maintenance went smoothly. The predictive maintenance system produces a maintenance schedule for HVAC and other equipment using information about equipment usage. Usage history for all equipment at the campus is available in the live Web/SQL cluster, and is therefore available in the replica Web/SQL cluster as well. To enable predictive maintenance, the replica's ASHRAE Web services for predictive maintenance were enabled, and a virtual private network (VPN) was established from the DMZ network to the cloud provider's systems on the open Internet.

The VPN connection permits the cloud provider to query the replica Web/SQL cluster for all of the data needed to provide predictive maintenance schedules and other benefits to operations teams at the site. No change was needed to the live Web/SQL cluster or any other part of the campus building automation system in order to deploy the connection to the cloud provider. No new security threats were introduced by the connection to the cloud provider.

Key Achievements

- Eliminated the risk of a remote-control cyber-sabotage attack impairing HVAC systems, physical security systems, or emergency fire response systems.
- Increased flexibility to schedule security updates on weekends or holidays reduced the likelihood of tenants seeing any impairment of service due to a failed security update.
- With remote sabotage of building automation systems no longer possible, there is a reduced need to monitoring firewall access logs and other security logs for Internet-exposed systems.

Deployment of the Waterfall FLIP dramatically reduced cyber-risks, security operations costs, and security-update maintenance complexity for the research campus, with no reduction in tenant/customer satisfaction.

CABA™

Intelligent Buildings and Cybersecurity

LANDMARK RESEARCH REPORT

CABA 2016
888,798.CABA (2222)
613.686.1814 (x226)

Connect to what's next™

www.caba.org