CYBERSECURITY IN SMART BUILDINGS
INACTION IS NOT AN OPTION ANYMORE

FROST & SULLIVAN

A Frost & Sullivan Collaborative Industry Perspective

9835-19
September 2015

Contents

Executive Overview

Background: Cybersecurity Vulnerabilities in Smart Buildings

Today's smart buildings are increasingly enabled by Internet of Things (IoT) and made functional by the ongoing convergence of operational technology (OT) systems and information technology (IT) systems in buildings. A host of new elements such as the cloud, remote access, data sharing and analytics, and connected and shared networks has fundamentally changed how built environments are being used and operated. Additionally, these elements have thrown open an otherwise closed-loop building architecture into one that necessitates the open access and control of many operators and service providers.

The role of these entities is, to a large extent, crucial in reaping the benefits of a converged and connected space. However, buildings are exposed to a new threat that has been downplayed and undervalued for a long time. After witnessing a recent slew of security breaches, stakeholders of the smart buildings industry are recognizing the potential damaging impact cyber threats pose for the industry and its related businesses.

Smart buildings are ushering in a host of technology paradigm shifts. While fundamentally changing how built environments operate, these shifts expose buildings and all associated with them to susceptibilities and risks of cyber threats.

Strategic Messages for the Industry

Through dedicated research and dialogue with industry participants, Frost & Sullivan concludes the following:

- Investigating the issue of cyber threats in smart buildings is timely and pertinent.
- While avoidance may not be an option, the ability to minimize the impact of cyber threats needs exploring.
- Thought leaders and technology experts must collaborate to address various aspects of cybersecurity.
- Evaluating the efficacy of technology solutions pioneered by leading companies at an industry level is important.

- A well-rounded strategic initiative is necessary to deal with this disruptive trend.
- Cyber threats demand the utmost recognition and intervention of administrators and regulators to implement industry-wide changes.

Pervasiveness of technology, ubiquitous connectivity, and an increasingly evolving machine-to-machine (M2M) environment will continue to impact and influence how smart buildings are operated, which will raise the need for protection against cyber risks quite significantly. A delayed head start not only poses huge challenges in dealing with this complex issue but undermines the value and adequacy of initiatives that could potentially be used to ward off adversarial impacts. Irrespective of such shortfalls, however, inaction is no longer an option for the smart buildings industry.

Defining Smart Buildings and Cybersecurity

Listed below are some key definitions of various terminologies used in this paper:

- Frost & Sullivan defines a smart building as one that uses both technology and processes to create an environment that is safe, healthy, and comfortable and enables productivity and well-being for its occupants. A smart building is characterized by active IT-aided intelligence, smart sensors and controls for seamless operation, real-time dissemination of operational information for predictive analytics, and diagnostics to facilitate better management, maintenance, and optimization over time.
- Cybersecurity in the context of a smart building is defined as the quantum of technologies, processes, and practices designed to protect from unauthorized access all building systems and networks, including front-end physical and IT systems within the building, accessories and field-level devices, data and application platforms, and data aggregation systems such as all localized and remote systems that help in operating and maintaining a smart building. This definition has been adopted following the work of the National Institute of Standards and Technologies (NIST) in the area of development of the cybersecurity framework[1] for critical infrastructure.

[1] In February 2013, Executive Order 13636, Improving Critical Infrastructure Cybersecurity was issued, which requires the National Institute of Standards and Technology to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). http://www.nist.gov/cyberframework/index.cfm

- In the context of this research, the smart building market[2] is defined as the total value of smart sensors, systems, hardware, controls, and software sold into the smart building market by various products and solution manufacturers.
- Although the issue of cybersecurity in smart buildings is discussed in the global context in this paper, specific references made in certain regards such as policy and standards primarily pertain to the North American context.

Takeaways

The aim of this discussion paper is to provide a preliminary assessment of the issue of cybersecurity as it pertains to smart buildings. As advancements in connectivity, new technology, and service deployments powered by IoT and Big Data continue to make their way into the smart buildings' landscape, cybersecurity concerns will intensify further. When the Stuxnet virus was discovered in 2010, the implications were immediately clear: industrial control systems (ICS) were no longer secure from hacking; protection through obscurity vanished. Through targeted research and evaluation of the concerns cited by various stakeholders of the smart buildings industry, the systems of a smart building can undoubtedly become low-hanging fruit for motivated cyber attackers. The question is not how but when. The solution lies in recognizing the scope and magnitude of cyber crimes that can impact smart buildings, understanding ICS vulnerabilities, evaluating cost of damage, devising mitigation methods, and pursuing an ongoing robust cybersecurity plan for smart buildings.

[2] The Smart Building Systems Market in North America, ND78, Frost & Sullivan, 2014

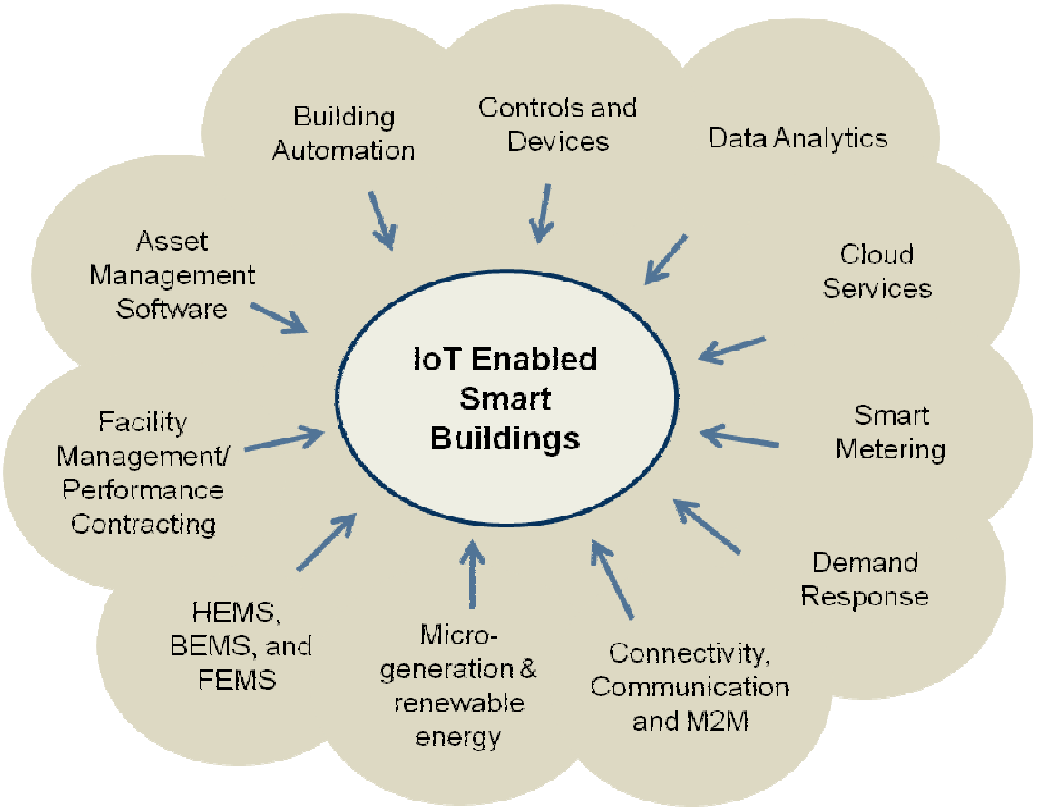
Cyber Risks in Smart Buildings

Technology Progression

The building automation system (BAS) or a building operating system (BOS) has moved considerably from the physical realm to one with IT enabling all aspects of its functioning. Furthermore, there is now a new generation of connected and intelligent buildings powered by IoT. The continued entry of many technology vendors and service providers (ranging from billion-dollar IT conglomerates, established building technology companies, consultants, and a vast number of enabling technology and service providers) marks a completely transformational phase in the smart buildings' trajectory.

Exhibit 1 provides a snapshot of the developing service provider landscape of the smart buildings industry.

Exhibit 1: Smart Buildings Industry Service Provider Landscape, Global, 2014



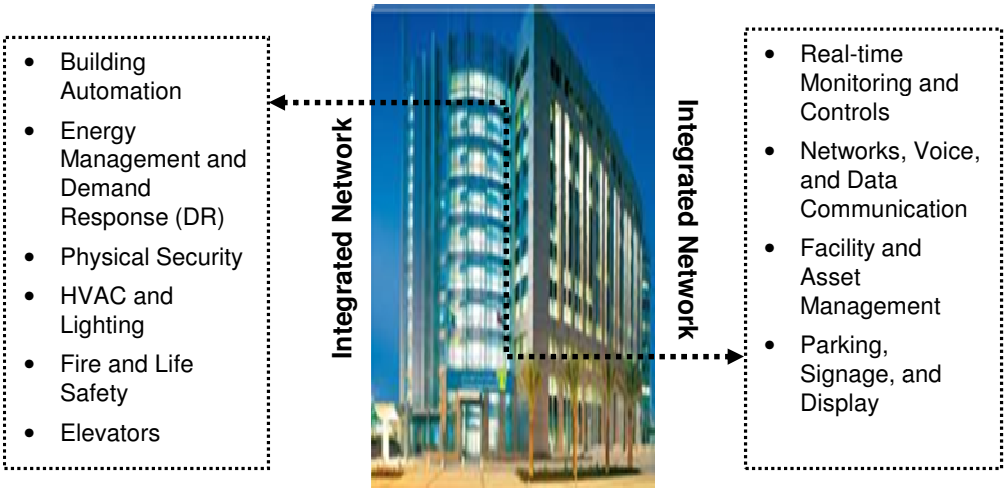
Source: Frost & Sullivan

The Integrated Building Network

The integrated network of a smart building is where the true benefits of a smart and converged infrastructure are realized by building owners and operators; however, this is also the point where extreme exposure to security vulnerabilities are manifest, as shown in exhibit 2. From a traditionally static and proprietary environment of standalone systems, the smart buildings industry has gradually moved towards a dynamic environment characterized by open systems and protocols governing their operational aspects.

Exhibit 2 shows the security vulnerabilities of a smart building's integrated network.

Exhibit 2: Security Vulnerabilities of a Smart Building's Integrated Network



The integration portion of a smart building's software is subject to extreme vulnerabilities, in which the BAS is connected to virtually any other aspect of the building, and from which a skilled hacker could access nearly any system in a corporate network.

Source: Frost & Sullivan

Protection through obscurity that standalone systems have enjoyed is no longer an available option for the present intelligent and interconnected systems running on open protocols and with virtually every other physical system within the building under their supervisory control. For instance, a network-enabled BAS that can control practically every physical system from heating, ventilation, and air conditioning (HVAC); lighting; physical security; and access control to energy management and data aggregation systems has the potential to trigger wide-scale security compromises for all such systems. Attackers infiltrating the BAS can potentially infiltrate the enterprise.

However, the scale of damages can inflate significantly when such open systems are overlayed with IoT, which essentially impies connecting all building systems and services such as monitoring, disgnostics, and analytics with an overlay of an Internet Protocol (IP) network that eliminates all human intervention. With IoT, the value of devices and data is closely interlinked, with each becoming meaningless without the other. With that comes the importance of aggregation of such data for providing granular inputs of a building's performance hosted in a virtual and highly risk-prone frontier: the cloud.

IoT and Cyber Risks

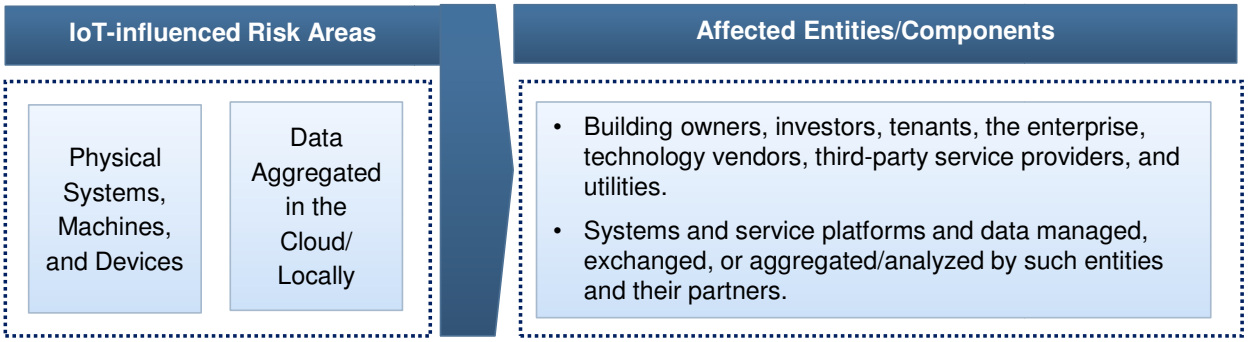
Activities centering on IoT are delivering increasingly unique advantages and novel challenges. The advantages include real-time access, vast data generation and analytics, and interconnectivity of systems and devices. These advantages by themselves, however, offer little value unless the crucial decision to share the data and networks is simultaneously taken, thus permitting access to multiple service providers to tap into a smart building's various systems and devices.

This access implies potential security breaches that could render a smart building, its occupants, and service providers powerless over an adversary's damaging actions to corrupt networks, misuse critical information, and cause significant operational and financial loss.

With IoT, 2 broad buckets of elements are at risk in the event of a cyber breach (machine and data), as depicted in exhibit 2.4. Firstly, by definition, the elimination of human intervention in the realm of IoT implies an M2M environment within the building that encompasses all physical systems that can interconnect and intercommunicate through an IP network that is at stake in the event of a cyber breach. Secondly, the inseparable relationship of device and data brought together through aggregation in the cloud or locally can be compromised in the event of a cyber breach. These 2 broad buckets of machine and data and their intrinsic interlinks may result in cumulative damages that could potentially permeate into all layers of the enterprise, building and facility portfolio, users, operators, and service providers and their respective businesses and associated infrastructure. Interestingly, the smart buildings industry and its stakeholders have not evaluated, either wholly or partially, the extent of such damages in their complete manifestation.

Exhibit 3 depicts the IoT-influenced cyber risk areas in a smart building.

Exhibit 3: IoT-influenced Cyber Risk Areas in a Smart Building



Source: Frost & Sullivan

Cyber breach incidents, the critical assets they affect, and the response mechanisms to which they can be resorted are varied and complex for smart buildings, as illustrated in exhibit 2.5.

Exhibit 4 illustrates the impact of cyber threats to BAS/BOS infrastructure.

Exhibit 4 Impact of Cyber Threats to BAS/BOS Infrastructure

BAS/BOS Infrastructure and Cybersecurity Threats

Cybersecurity Breach Incidents	Impact Areas	Cyber Defense Components	Preventative Aspects
• Systems failure • Nuisance tactics to life-threatening damage • Infection by viruses or malicious software • Theft or fraud by staff or attacks by unauthorized outsiders • Unintentional damage caused by authorized third-party service providers because of cybersecurity compromises affecting their own infrastructure	• Users • Remote access by operators/third parties • Physical access to connected devices, networks, and apps • Integration platforms • Communication gateways • Wireless access • Bring-your-own-device (BYOD) access	• Identity validation • Endpoint device security • Network security • Data security • Multi-layered security • Dynamic cybersecurity hub	• Access to a fire system (allowing the trigger of a false alarm to evacuate the building) • Access to a security system (allowing unauthorized access) • Access to communication networks • Access to utility-installed devices • Hijacking the BAS for blackmail (ransomware) to damage property or to destroy or steal sensitive data

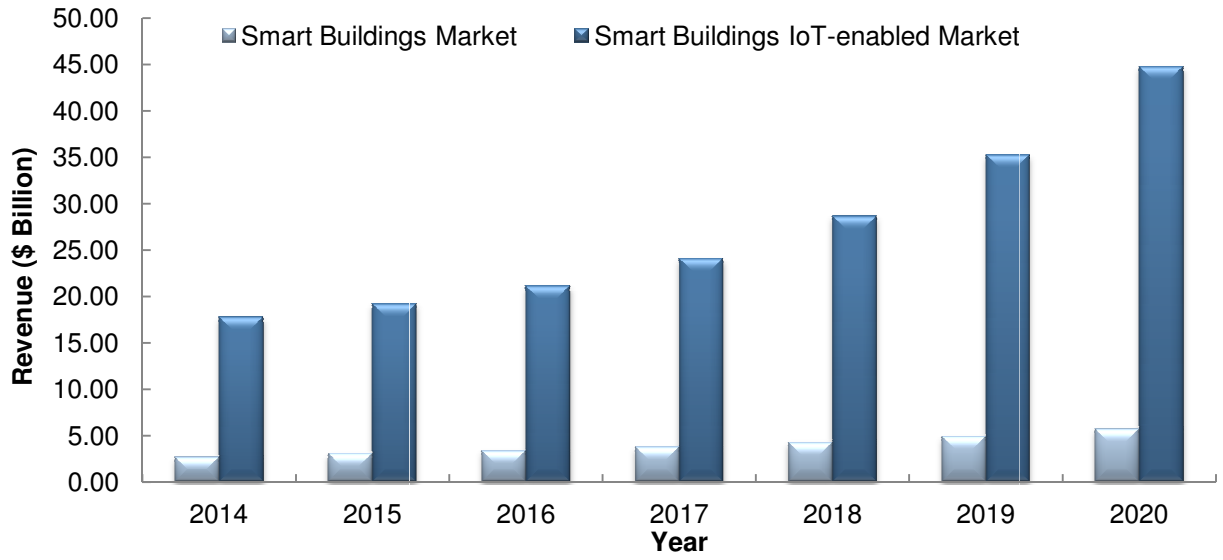
Source: Frost & Sullivan

Smart Buildings Market Dynamics and Risk Evaluation, Global, 2014

As the smart building industry redefines itself with the proliferation of IoT, looking at the market value riding on this technology evolution is important. The total North American smart buildings market, comprising the total value of smart sensors, systems, hardware, controls, and software sold into this market by various products and solution manufacturers, is estimated at $2.7 billion in 2014[3] and projected to grow at a compound annual growth rate (CAGR) of 13.4% between 2014 and 2020. The revenue potential for IoT in the smart buildings market can be evaluated by considering the additional value of components such as further requirements in connectivity for new and existing building systems as well as corresponding demand for network hardware, data services, and platforms that will be driven by IoT. When these components are considered, the potential opportunity size of the smart buildings IoT-enabled market for North America is estimated at $17.8 billion[4] in 2014 and projected to grow at a CAGR of 16.6% between 2014 and 2020.

Exhibit 5 shows the market potential for smart buildings with IoT in North America from 2014 to 2020.

Exhibit 5: Smart Building Market: Opportunity with IoT, North America, 2014–2020



Note: All figures are rounded. The base year is 2014. Source: Frost & Sullivan

[3] The Smart Building Systems Market in North America, ND78, Frost & Sullivan, 2014

[4] Based on Frost & Sullivan's estimated value of services and solutions deployed for IoT in smart buildings

IoT has the potential to trigger market growth significantly for smart building products and solutions over the next 5-year period. More devices, sensors, and controls will continue to vie for inclusion within the expanding realm of smart buildings and become intrinsically linked with IoT-enabled hardware, networking components, and data service elements. Simultaneously, however, their native security-enabled features and their ability to protect the BAS/BOS-controlled infrastructure of a smart building will be rigorously put to the test.

Risk Exposure versus Market Prospects

Various organizations and independent entities have separately evaluated security threats to the BAS. In one such exercise undertaken in January 2015, California-based Whitescope LLC,[5] which is involved in the assessment of threats to industrial control systems (ICS), discovered a significant number of IP addresses pointing to a device or system that supports a BAS deployment. A sizeable number of these exposed IP addresses could be reached and were considered live on the Internet. Further, nearly 50% of the devices accessible through the Internet offered one or more interfaces that were accessible without any authentication. These exposures did not require a username. Additionally, they provided enough identifying information to associate the device with a specific industry or organization. Often such vulnerabilities results from the involvement of third parties such as contractors and installers. As Billy Rios of Whitescope stated, ""In most cases when customers try to retrofit or make improvements to their buildings through third party devices and systems, there are often other entities such contractors and engineering firms involved who install and enumerate these systems within their own IP space. Therefore when the building owner/customer tries to scan the Internet to locate such IPs discovery is impossible simply because such IPs do not reside within their own IP domain. Furthermore, there may be liability issues associated with such blanket Internet scans for certain customer types as it may infringe upon competing customers' IP space and confidential data."

Attackers infiltrating such systems could potentially gain access to a building's other physical control systems through the BAS (such as HVAC, lighting, and access control), IoT-related data management systems, and even financial and enterprise resource planning systems (ERP). Disruptions from such access could range in severity, starting with nuisance tactics to large-scale physical security breaches, including endangering occupants. These evaluations have prompted several organizations to question if IoT is being pursued without paying enough heed to BAS security in smart buildings.

[5] Reference produced in consultation with Whitescope LLC, www.whitescope.io

Exhibit 6 sums up the exposure, threats,[6] and impact of such security risks.[7]

Exhibit 6: IoT influence and BAS Risk Exposure

BAS Risk Exposure	Mode of Threat	Cost Impacts

• Creating unplanned or unauthorized pathways
• Allowing unauthorized access to systems or data loss
• Revealing occupants' personal data to adversaries
• Causing physical damage (e.g., fire or flooding)
• Disrupting temperature set points: building overheating or overcooling causing equipment and material damage and possibly human fatalities
• Damaging vertical transport functions such as lifts and escalators, thus hampering evacuation possibilities
	• Direct manual interference by insiders and outsiders
	• Generic deployment of malware or hacking, specifically, infiltration, exfiltration, and aggregation
	  ○ Phishing
	  ○ External attacks
	  ○ Denial-of-service (DoS)
	  ○ Keystroke logging
	  ○ Botnet system
		• System repairs and retrofit costs
		• Personnel redeployment cost to implement manual checks in place of automated systems
		• Cost of record/data/IP loss
		• Construction/ redevelopment/ decommissioning costs
		• Legal and other investigation costs
		• Mitigation costs
		• Cost of reputation loss

Source: Frost & Sullivan

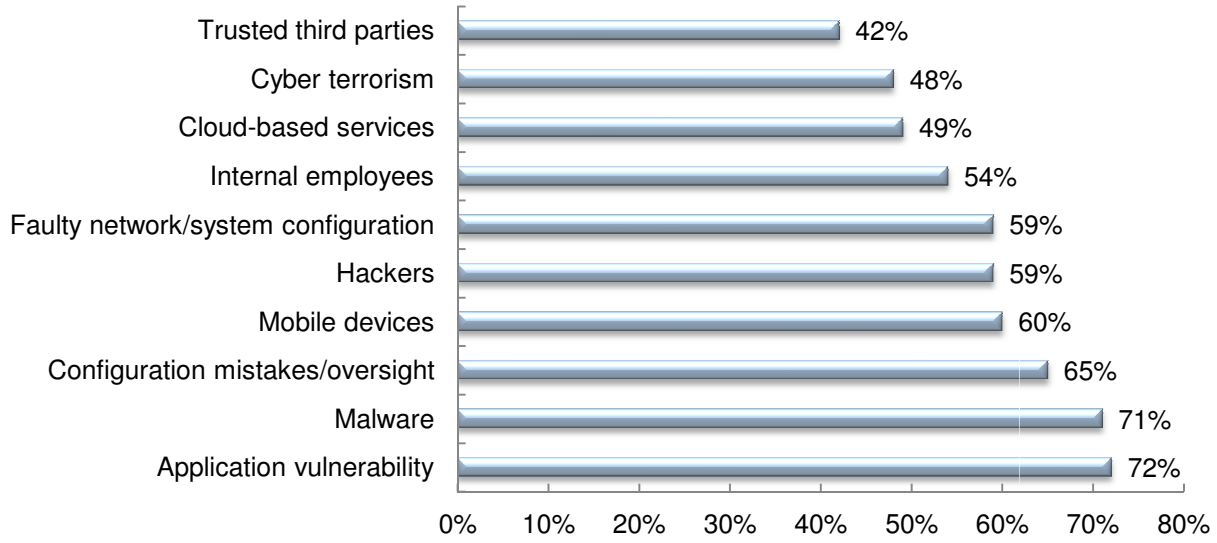
Apart from the cost of addressing physical damage, the cost of data recovery will add tremendously to overall recovery costs after a cyber breach incident. The 2015 Cost of Data Breach Study conducted by the Ponemon Institute estimates the average cost of a total data breach for organizations at $3.79 million, which represents a 23% increase in the total cost of a data breach since 2013.[8]

Among the identified key root causes of a data breach, the study found the per capita cost of data breaches caused by malicious attacks was significantly higher than that of other causes such as human errors or system glitches. This finding interestingly correlates with Frost & Sullvian's findings on top security concerns of IT and operational staff depicted in exhibit 2.8. This 2015 end-user research among IT and operational staff[9] depicts major upward trending of key issues. Application vulnerabilities and malware topped the list of concerns as they can cause a significant financial impact on an organization when dealing with post-event casualities. However, human errors and configuration mistakes could lead to similar financial damages. While the focus of these researches may not represent a direct correlation of such breaches with physical building systems, envisioning the potential of that occurance in the over-expanding IoT realm is not difficult.

[6] White Paper developed by Frost & Sullivan and the Continental Automated Buildings Association: "Cybersecurity in Smart Buildings: Preventing Vulnerability While Increasing Connectivity," www.frost.com; www.caba.org/research
[7] Developed from Frost & Sullivan's industry reviews and references such as "Intelligent Buildings: Understanding and managing the security risks," a paper developed by The Institution of Engineering and Technology, United Kingdom.; www.theiet.org/sectors
[8] 2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2015
[9] The 2015 (ISC)2 Global Information Security Workforce Study, Frost & Sullivan, n=13,000+

Exhibit 7 illustrates the North Amesrican key security issues identified by IT and operational staff in 2014.

Exhibit 7: Key Security Issues Identified by IT and Operational Staff, North America, 2014



Application vulnerabilities and malware top the list of high concerns.
Configuration mistakes/oversights and faulty network/system configuration appear among the top 6 concerns.
This finding mirrors the weak link of exploitive behaviors of today's cyber attackers.

Note: All figures are rounded. The base year is 2014. Source: Frost & Sullivan

As advancements in connectivity, new technology, and service deployments powered by IoT and Big Data continue to make their way into the smart buildings landscape, these concerns will intensify further. When the Stuxnet virus was discovered in 2010, the high cyber risk profile of ICS was immediately brought to light. With revelations such as the one from Whitescope LLC cited earlier and the concerns expressed by various stakeholders of the smart buildings industry, a smart building and its associated systems are easy targets for cyber criminals. Beyond understanding ICS vulnerabilities and the cost of damage, it is important to analyze the scope and magnitude of cyber crimes that can impact smart buildings, mitigation methods, and an ongoing robust cybersecurity plan that can be considered for smart buildings.

Cyber Risk Management for Smart Buildings

Dealing with cyber risks and threats demands a sophisticated and robust approach for smart buildings, which essentially consists of a systematic review and analysis of aspects such as the following:

- ICS vulnerabilities
- Cost of damage
- Scope and magnitude of cyber crimes
- Technology initiatives and mitigation methods
- A cybersecurity management strategy

The preceding section looked at the first 2 issues. This section reviews the scope of cyber crimes that relate to smart buildings before considering other aspects such as technology development for mitigation and plans for cyebrsecurity management.

Scope and Magnitude of Cyber Crimes in Smart Buildings

Cyber crime encompasses a broad range of activities; however, cybersecurity professionals tend to group criminal activity into categories based on capabilities and impact. Frost & Sullivan has categorized these under the following 4 groups:[10]

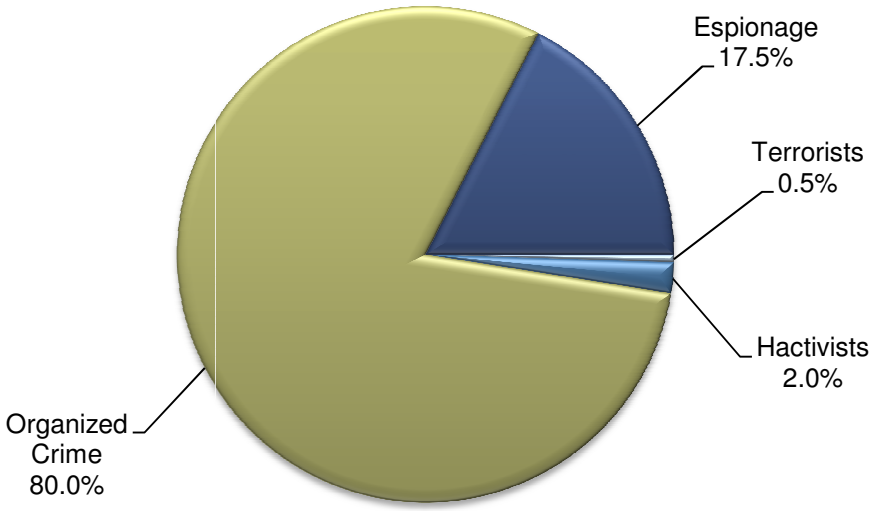
- Terrorist organizations (e.g., ISIS and Al-Qaeda) are considerd low-to-moderate in impact and directed mostly for propaganda and recruitment; however, they could potentially launch high-impact attacks in the future.
- Hacktivists (e.g., politically motivated groups such as Anonymous and LulzSec) depict a steep upward trend since 2011 and are prone to high and low fluctuations as technology changes and as the business, economic, and socio-political landscape changes over time.
- Organized crime (e.g., profit-seeking criminals and criminal organizations) is considered a medium/high threat in terms of capabilities and impact and is primarily focused on data theft and not directed at destroying the host system so as to maintain a lifeline to illicit revenues.

[10] Cybersecurity: A Global Economic Security Crisis, 9856, Frost & Sullivan

- Espionage (e.g., corporate and government) is considered a high-skilled and high-impact growing threat involving computer and physical network attacks to obtain, destroy, and render critical information unavailable.

Exhibit 8 shows the global concentration of cyber crimes by perpetrator type in 2014.

Exhibit 8: Cyber Crimes by Perpetrator Type, Global, 2014



Note: All figures are rounded. The base year is 2014. Source: Frost & Sullivan

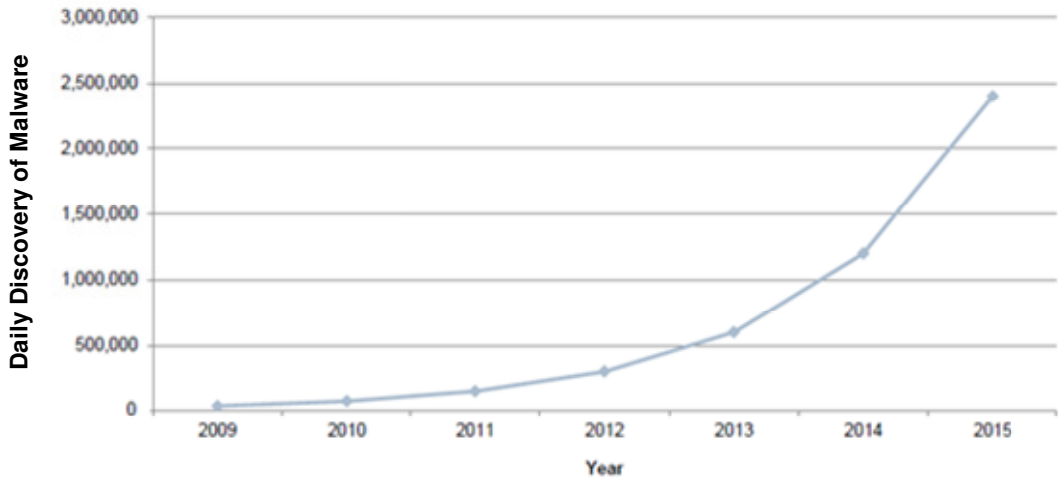
Among the 4 categories discussed above, the 2 considered most applicable to smart buildings, with the ability to inflict substantial damage, are espionage and organized crime.

However, the potential of hactivism impacting a smart building cannot be ruled out. Similarly, depending upon the nature and strategic importance of the building, terrorist-devised cyber threats could be a strong possibility as well.

Exhibit 9 shows the historical and future growth projections of malware.[11] The vast proliferation of malware has facilitated a much broader probing of the Internet, leading some cyber crime operators to realize there is an immense number of interesting targets that might have been ignored 5 years ago.

Exhibit 9 shows the global historical and future growth projections of malware from 2009 to 2015.

Exhibit 9: Historical and Future Growth Projections of Malware, Global, 2009–2015



Over a million cases of malware are believed to be active as of 2014.

Both quantity and quality of malware have drastically increased.

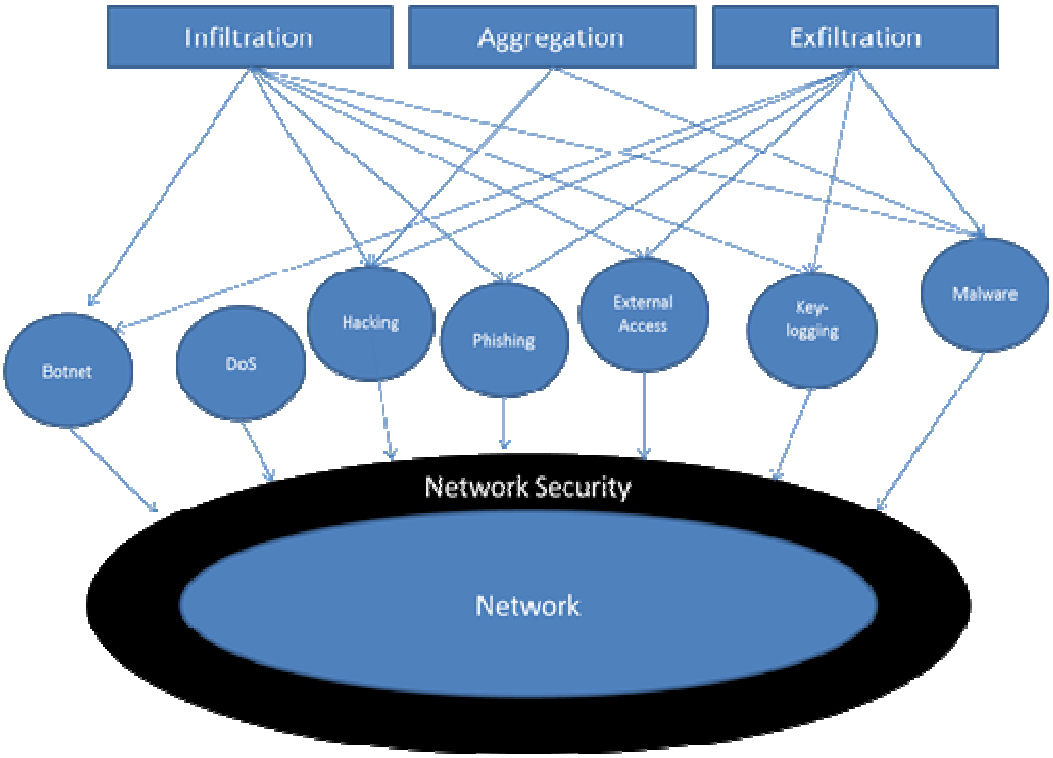
Buildings and ICS pose a lucrative target for illicit revenue generation, nuisance attacks, and irreparable financial loses for adversaries aiming at malware infiltration.

Note: All figures are rounded. The base year is 2014. Source: Frost & Sullivan

[11] Cybersecurity: A Global Economic Security Crisis, 9856, Frost & Sullivan

Exhibit 10 depicts the global potential attack scenarios[12] that could impact smart buildings.

Exhibit 10: Potential Attack Scenarios for Smart Buildings



Source: Frost & Sullivan

[12] White Paper developed by Frost & Sullivan and the Continental Automated Buildings Association, "Cybersecurity in Smart Buildings: Preventing Vulnerability While Increasing Connectivity," www.frost.com; www.caba.org/research

Buildings as a Component of Critical Infrastructure

The inclusion of buildings and ICS under the definition of critical infrastructure[13] and the initiatives of NIST[14] to include buildings within the cybersecurity framework state in no small measure that the built environment and ICS are crtical assets that require due attention and protection as vulnerable targets from cyber threats.

The cybersecurity framework is proposed to include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. Additionally, voluntary consensus standards and industry best practices are proposed within this framework. The Federal Information Security Management Act (FISMA)[15] has mandated stringent cybersecurity standards and requirement govering IT systems since the act was passed in 2002. However, the same level of protection for building systems is only now being push for, and despite the late start, it is a step in the right direction.

Cyber Physical Systems and the Critical Infrastructure Cybersecurity Framework

Ongoing convergence of OT and IT systems in buildings has led to a review of the definition of physical systems within a smart building. In this regard, the National Science Foundation and NIST have attempted to classify the hybrid IT and OT systems as cyber physical systems (CPS). “CPS are defined as integrated, hybrid networks of cyber and engineered physical elements; co-designed and co-engineered to create adaptive and predictive systems, and respond in real time to enhance performance.” CPS is essentially coined to represent the transition and evolution in systems from industrial revolution/physical systems to the Internet revolution/cyber systems and, at present, evolving into industrial Internet revolution/cyber physical systems.[16]

[13] Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the president issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. It directed NIST to work with stakeholders to develop a voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure.

[14] National Institute of Building Sciences: Whole Building Design Guide. NIST to lead the development of a framework to reduce cyber risks to critical infrastructure, "Cybersecurity Framework"). https://www.wbdg.org/resources/cybersecurity.php

[15] Department of Homeland Security: FISMA, http://www.dhs.gov/federal-information-security-management-act-fisma

[16] NIST; NIBS/WBDG

In the case of buildings and structures, CPS encompasses all components of smart ICS, from BAS, HVAC, and lighting to the overlay of networked infrastructure that enables such systems. While this may be another extension of terminology of the smart buildings industry, its recognition and classification as part of NIST's initiatives in defining the critical infrastructure cybersecurity framework is vitally important and achieves a few critical milestones for smart buildings:

- It formalizes the need and urgency of evaluating cybersecurity risks for ICS/CPS in buildings.
- It aids the development and recommendation of tools and procedures for such evaluations, including mitigation processes.
- It encourages the ongoing development of standards, guidelines, and best practices from which the industry can learn.

Cybersecurity Measures Adopted for Smart Buildings

Cybersecurity solutions currently being offered to the smart buildings industry combines IT and physical security options, in addition to technology deployment approaches that attempt at annomaly detection and reduce vulnerabilities for IT and OT staff. In reviewing such technology options, it is important to begin by looking at a building's critical vulnerability areas that gain top consideration. Exhibit 10 provides a snapshot of the technology initiatives presently witnessed in the smart buildings industry. This partial snapshot is by no means exhaustive or representative of activities across the industry.

Exhibit 10 provides a snapshot of the technology initiatives presently witnessed in the smart buildings industry.

Exhibit 10: Technology Initiatives Addressing Cybersecurity in Smart Buildings

Cybersecurity Component	Description	Highlight of Activities
Critical Vulnerability Areas	• BAS tops the list, but shared networks, data management, and third-party services are equally impacted. • Open protocols and interoperability platforms have little cyber defense mechanisms.	**Identifying system vulnerabilities:** • Users • Remote access by operators/third parties • Physical access to connected devices, networks, and apps • Integration platforms • Communication gateways • Wireless access • BYOD access **Building cyber defense layers:** • Identity validation: username/passwords and PIN/biometrics • Endpoint device security: mobile device security and remote-user validation • Network security: firewall and anti-virus/malware • Data security: data encryption and data recovery
Technology Initiative	• The trend is towards isolated secure system development. • Technology companies supplying BAS controllers, software, and sensors are engaged, to an extent, in developing secure systems. • Secure BAS controllers that imbed firewalls and provide encryption are an example.	• Control solutions from Johnson Controls, Schneider Electric, Honeywell, Ultra Electronics 3eTI, and Lynxspring that imbed cybersecurity elements • Built to provide pre-emptive threat protection across a building network and for remote access to devices and systems in these networks • Designed for managing and monitoring all account access and activities • Generally supports leading open building automation protocols such as BACnet, local operating network (LonWorks), MODBUS, wireless, and TCP/IP networks
Alliance-led Initiative	• Alliance-led initiatives are being pursued in an ad-hoc manner to develop cybersecurity standards and technology development protocols.	**Focus of smart buildings:** • NIST cybersecurity framework • ASHRAE standards • InsideIQ Building Automation Alliance Cybersecurity Committee **Others from adjunct industries that offer best practices:** • Cybersecurity research alliance: Intel, AMD, Lockheed, Honeywell, and RSA/EMC • Cyberthreat alliance: Fortinet, McAfee, Palo Alto Networks, and Symantec

Source: Frost & Sullivan

Cyber Risk Mitigation

The smart buildings industry is currently adopting mitigation methods that are varied and somewhat specific and/or proprietary to every organization. Upon closer inspection, however, several best practices and commonalities in techniques have emerged from these approaches, which range from simple best practices to more rounded strategies based on life-cycle principles discussed below.

Best Practices for Adoption

Industry experts agree that simple best practices can be applied for protection from cyber attacks. These best practices include the following steps as examples:

- Restricting BAS access to virtual private network (VPN) connections only
- Using a Web server-based human machine interface (HMI) because it relies on IT technologies to secure access and restricts ports that need to be opened on a firewall
- Segregating the BAS network from the IT backbone using virtual local area network (VLAN) IT technologies to restrict internal attacks/breakdowns
- Maintaining password etiquette
- Keeping BAS software and firmware up to date and installing patches on a timely basis
- Encrypting the data at rest to protect further an organization and backing up to a separate system for access during a data breach
- Conducting security audits to validate security measures to help avoid complacency
- Educating database users, owners, and operators on the need for and methodology of cybersecurity

According to Professor David Fisk[17] in his paper on cyber security, building automation and the intelligent building, "All cybersecurity defenses are potentially breachable; therefore, one has to plan for the worst." For protection, Fisk advocates the development of a back-up plan that involves identifying a building's minimal level of functionality and then adding hardwired, back-up equipment with hands-on controls to provide basic service. He asserts that such a strategy may be enough of a deterrent to ward off potential aggressors before an attack is even launched.

[17] David Fisk, professor of Systems Engineering at Imperial College London, in his article "Cyber security, building automation, and the intelligent building," which appeared in the July 2012 issue of Intelligent Building International: http://www.tandfonline.com/loi/tibi20

Addressing the Dilema of Convergence

With so many network vulnerabilities, there is a need to scrutinize the benefits of IT-OT convergence. One approach put forward by technology and service providers emphasizes network segregation to reduce anomalies and vulnerabilities. Keeping the OT and IT elements of the building in their respective separate networks will help reduce vulnerabilities of one network inflicting danger on and bringing down the other. Several leading and emerging smart building technology solution providers such as Optigo Networks, Switch Automation, Lynxspring, and Schneider Electric see this approach as a logical start. Mark Duszynski, Vice President Business Development-Federal, for Johnson Controls, Inc's Building Efficiency Business states, "The fundamental differences in how IT and OT technologies have developed lead to the 2 professions being alien to each other's domains. However, IT and OT networks, overlaid with IoT, is an imminent risk area. Therefore, these 2 functions have a lot at stake when it comes to effective management of a building's cyber threats. I believe the issue of cybersecurity could act as a conduit to bring these traditionally divided camps together to address the common vulnerabilities, share responsibilities and accountability."[18] At the end of the day, it comes down to what makes organizations comfortable and how they view risk and employ a defense-in-depth cyber strategy. Marc Petock, Vice President-Marketing at Lynxspring states, "I believe there is no right or wrong answer/way, as long as organizations realize building systems and OT are subject to the same cyber threats and risks as IT and they are addressing both from a cyber security perspective."[19]

Addressing Data Security

The scale of damages in a cyber attack can inflate significantly when open systems and converged networks are overlaid with IoT. A key attribute is the inseparable relationship of device and data brought together through aggregation in the cloud or locally that can be compromised in the event of a cyber breach. One approach is to aggregate and encrypt data locally at the building level and not push it out to the cloud. Analytics and diagnostics can still be carried out on this aggregated data locally through interfaces and applications installed by third-party service providers for the building's operations and IT staff. Switch Automation is one company adopting this approach, with its energy management platform Switch Smart Hub.[20] CEO Deb Noller of Switch Automation states, "Security in buildings and in IoT is becoming increasingly more important to our clients, and our industry needs to adopt an IT approach to securing devices and buildings. There is an established best practice for enterprise security. Buildings should be no more difficult or different."

[18] Interview with Mark Duszynski, Vice President Business Development-Federal, for Johnson Controls, Inc's Building Efficiency Business
[19] Interview with Marc Petock, Vice president, Marketing, Lynxspring, Inc.
[20] https://www.switchautomation.com/

When it comes to data aggregation and analytics, an area impacted the most is building energy management systems (BEMS) data. The method of data treatment by BEMS service providers vary; however, most are resorting to providing their energy dashboards as an application to the building management staff, pushing energy and operation data to the cloud for further analytics and diagnostics, and offering predictive optimization inputs for the building. For ensuring data security, it is important to insist on best practices in terms of the following:

- Transport data through encrypted channels with secure sockets layer (SSL)
- Segregate energy data from other sensitive data collected such as those related to critical operations and financial data
- Store such segregated data in separate servers and anonymize it
- Collect only what is necessary for analytics and optimization

Secure System Development—Life-cycle Processes

One key challenge for smart building technology and service providers is to ensure cybersecurity processes and best practices are adopted across the entire spectrum of the value chain. Today's smart building technologies have a slew of embedded components that enable various aspects of their functionality to offer value-adds to the customer. While product suppliers may implement cybersecurity best practices and features into their solutions, component manufacturers may not comply with the same level of stringent practices.

For cybersecurity to be implemented at an industry-wide level, all stakeholders must incorporate such processes and procedures across the value chain. As a resolution to this challenge, some leading smart buildings technology vendors are adopting a life-cycle approach to secure system development. As Mark Duszynski of Johnson Controls[21] pointed out, "We incorporate cybersecurity measures broadly across our product development lifecycle processes. Given Johnson Controls wide portfolio of products and services, and the depth of our engagement with customers, we have to take a very comprehensive approach to cybersecurity. It starts right from conceptual planning and product selection to development and final deployment. We educate our customers about the cyber threats to embedded control networks and advise them on procuring and configuring the most secure building automation systems possible."

[21] http://www.johnsoncontrols.com

Michael Pyle, Vice President of Cybersecurity, Partner Business, at Schneider Electric[22] states, "We strongly emphasizes the three principles of 'secure by design,' 'secure by default' and 'secure by deployment' in ensuring security principles are followed stringently throughout the various stages of product conception, development and deployment. Thereafter, continuing on the same emphasis through stages of commissioning and ongoing operations helps us ensure that an end-to-end life cycle approach towards cybersecurity is adopted by the company as well as the partners we work with."

Some key features of the company's cybersecurity policy and approach include the following:

- Carefully vetting all third-party products and solutions before integration
- Providing thorough code analysis to be satisfied with a partner's security features and product resilience before opening a specific application program interface to interact with a Schneider Electric product/interface
- Training internal teams, installers, and partners in secure architecture for product deployment
- Undertaking threat modeling of solutions and performing static code analysis
- Maintaining proper documentation of secure product deployment in the field
- Securing data transport, segregation, anonymization and compliance with geographic regulations

For a cybersecurity strategy to be implemented successfully, the life-cycle approach to cybersecurity should essentially apply to the entire process, starting from conceptual planning, construction, operation, commissioning, and decommissioning of a smart building. Furthermore, cybersecurity requirements across the various stages of a smart building's life cycle need to be evaluated in conjunction with the resilience requirements that are fundamentally linked with each stage.[23]

[22] http://www2.schneider-electric.com/sites/corporate/en/products-services/cybersecurity-solutions/cybersecurity-solutions.page

[23] "Resilience and Cyber Security of Technology in the Built Environment," The Institution of Engineering and Technology, published in 2013, www.iet.org and Frost & Sullivan Industry Insights

Exhibit 11 depits the cybersecurity rquirements across the smart building's life cycle.

Exhibit 11: Cybersecurity Requirements across the Smart Building's Life Cycle

Life Cycle	Cybersecurity Planning Requirements
Specification and Design	• Location and site review, utility lines, and alternate route planning in case of inaccessibility during breakdown/failure • Nature of occupancy • Regulatory aspects • System availability requirements and functional criticality • IT-OT convergence needs • Network requirements, including wireless • Change management requirements • Interconnections and ICS standards • IP and commercial data protection • Adequate planning for physical security, network infrastructure, and device selection
Construction	• Managing the supply chain • Monitoring design integrity • Maintaining physical security • Implementing systems security
Installation and Operation	• Properly configuring the security features of each system component • Threat detecting and mitigating; device hardening • Configuring firewalls and user accounts • Preventing unauthorized access or actions • Addressing insider threats • Addressing change management in a secure manner • System monitoring, account management, patch management, and firewall maintenance
Decommissioning	• Taking appropriate steps for maintaining the security of any personally identifiable asset/data • Evaluating insider risk • Securing removal of ICS, security systems, and other crucial equipment

Source: Frost & Sullivan

Despite supporting strong cases for convergence over the years, ICS and corporate IT systems are fundamentally different and governed by different operating practices. Not recognizing these differences can significantly heighten cybersecurity risks. Compared to corporate IT systems, ICS systems are generally built for longer life, built to provide continous operation as opposed to frequent rebooting done on corporate IT systems, have rare instances of patching, often have multiple users and user accounts, and can be difficult to deploy security options. Understanding these differences and planning around them can help build cyber risk resilience for smart buildings at the design and operation stages.

Objectives of an Effective Cybersecurity Strategy for Smart Buildings

The incidences and impact of cyber threats will only advance in severity and sophistication; therefore, any counter initiatives undertaken by the smart buildings industry participants will have to incorporate predictive capabilities to combat such organized and orchestrated adversarial tactics. Given these fundamental complexities, obtaining a consensus to adopt cybersecurity measures from the entire spectrum of participants representing the smart building industry value chain is imperative. Making cybersecurity response a mainstream component of the industry by all stakeholders involved is equally daunting.

Exhibit 12 depicts the core objectives that should oversee the development of a cybersecurity strategy specific to smart buildings.

Exhibit 12: Objectives for an Effective Cybersecurity Strategy for Smart Buildings

Objective	Description	Outcome
Establish Magnitude and Response	• Current and potential magnitude of cyber threats • Implications on infrastructure, assets, and occupants • Interdependency in risk sharing and common damages • Adequacy of standards and regulations • Training and education efforts	Develop objective reviews and critical analyses
Design Optimal Value Proposition	• Standards for risk mitigation and technologies • Responsibility delegation among stakeholders • Cost of business, compliance criteria, and penalties • Rationale for cyber risk prevention	Determine best plan of action
Highlight Pioneering Efforts	• Industry best practices: success stories from which to learn • Technology showcase of noteworthy innovators • Alternate value propositions: out-of-the-box innovators • Organize thought leadership and collective stewardship	Recognize best-in-class Initiatives
Chart Implementation Plan	• Roadmap for the smart building's cybersecurity • Harmonization of stakeholder initiatives • Charting milestones: compliance, education, standards, and enforcement • Lobbying for implementation and change	Drive effective debates and offer a platform for change

Source: Frost & Sullivan

In practice, elements and outcomes may be highly interlinked rather than orchestrated in a stepwise manner as depicted in the preceding exhibit. Additionally, gaining stakeholder buy-in to implement these could pose significant challenges. However, cyber risks and the imminent disruption they will inflict on buildings are real. Any action (total or partial) is critical as opposed to procrastination. The smart buildings industry has in certain respects a head start over other industry sectors, where it has been too late for industry participants to drum up action to combat cyber crimes. Given this status, industry participants must take due advantage of this situation and respond in a timely manner.

Cyber Risks and Stakeholder Review

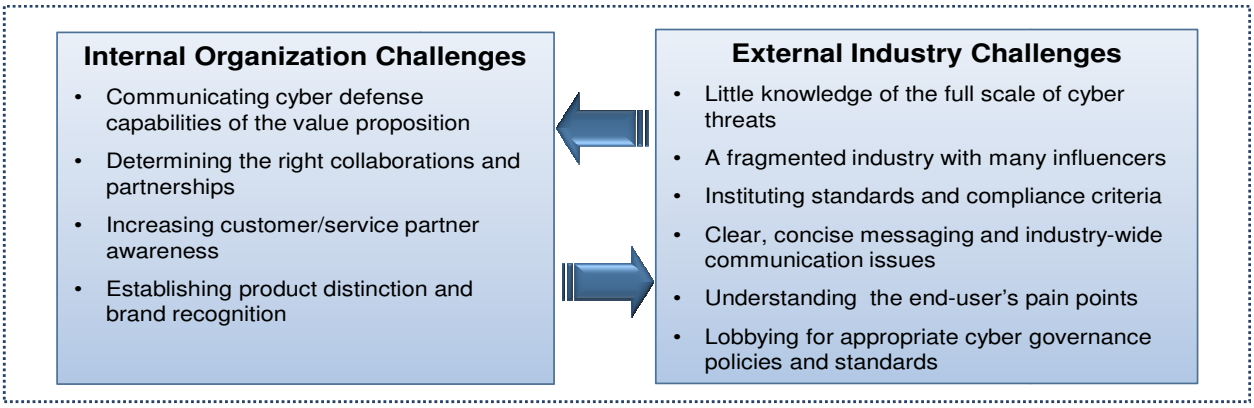
The pervasiveness of technology in smart buildings means the impact and incidences of cyber threats are no longer limited to traditional targets. The expanded ecosystem of all suppliers and service providers will likely share in the burden of dealing with post-event casualties. Mitigating such interdependent vulnerabilities and risks is a key challenge for industry stakeholders.

Critical Challenges for Stakeholders

Cybersecurity preparedness in smart buildings is scant at best, despite buildings being in the forefront of IT and OT convergence. In dealing with this issue, industry stakeholders face some critical internal and external challenges that could further impede the pace of response and strategy development, as discussed in Exhibit 13.

Exhibit 13 depicts the internal and external challenges to inustry participants.

Exhibit 13: Internal and External Challenges to Industry Participants



Source: Frost & Sullivan

New technology adoption requires the consensus of various stakeholders involved in this industry. Effective industry-wide consensus building depends on how participants deal with these critical internal and external industry challenges.

Recognizing and learning from best practices and success stories are ways to address the internal challenges. While successful participants may not willingly share strategic initiatives for fear of losing their competitive edge, companies are willingly publicizing several approaches for concisely stating their stand on cybersecurity and gaining partner and customer confidence, as discussed in the previous section. These examples could offer valuable insights for organizations that are beginning to create internal initiatives, training, and educational efforts to build their organization's cybersecurity strategy.

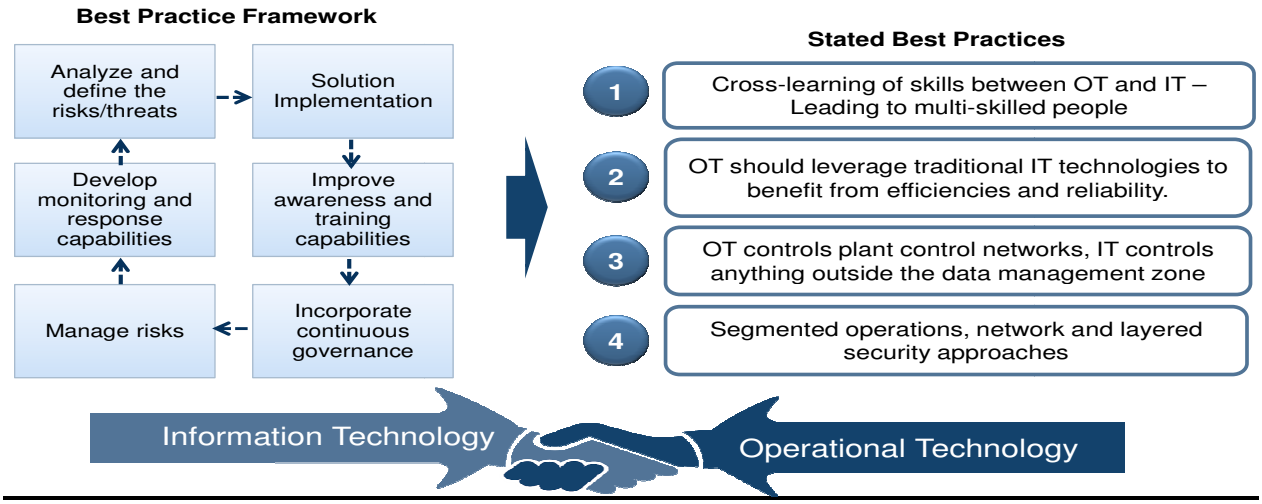
On the other hand, external challenges could take longer to address, given they are dependent on exogenous variables such as policy, compliance, standard development, and partner initiatives as well as value chain behavior and the varying degree of seriousness with which value chain partners view cybersecurity.

Interdependency in Risk and Responsibility Sharing

Cybersecurity is a common issue for all stakeholders involved within the smart buildings industry. Various stakeholders are expected to share jointly the risks and responsibilities of addressing this issue, including common responsibility and risk evaluation during the partner engagement processes as well as following secure design, development, and deployment processes that are discussed in the previous sections. However, when it comes to sharing risks and responsibility in dealing with cybersecurity within a smart building, the area that stands out is the one encompassing the stakeholders in charge of operational and IT technology within the building. IT and OT convergence is a critical risk areas and professionals from both functions have a lot at stake in a cyber creach.

Exhibit 14 depicts best practices that emerged from a recent customer analysis pertaining to managing vulnerabilities with IT and OT convergence in critical national infrastructure.[24]

Exhibit 14: Managing Vulnerabilities with IT and OT Convergence, Global, 2014



Source: Frost & Sullivan

The traditional challenges that kept these 2 functions siloed continue to persist. Lack of knowledge and understanding of each other's domains have resulted in a less smart or sub-optimally managed building. However, that scenario is forgiving compared to the eventuality these buildings face if silos are allowed to continue undeterred. As a consequence, allocation of accountability in a cyber breach incident could be extremely challenging. However, beyond accountability, the critical issue would be the total inability to devise a predictive countermeasure in building resilience towards cyber attacks.

The basic differences in IT and OT technology evolution processes have kept the two domains separate from one another to begin with. Therefore, professionals of each domain must review and understand the key characteristics govering the technology and operational aspects applicable to each. For instance, IT professionals need to appreciate that a building automation controller cannot be easily turned off and on, that there is a consequence to occupants if a controller is turned off, and that there are sometimes lengthy sequences for turning them off and on.

Further, IT professionals need to understand the BAS is not designed to be modified easily. Critical questions include what operating system IP-connected components have and how they can be upgraded or patched and at what frequency. The answers will help IT professionals gain a better understanding of the BAS and help them manage a smart building's IT and ICS infrastructure when planning for cybersecurity.[25]

[24] State of Cybersecurity Preparedness, Analyst Briefing on Insights from Voice of the Customer Analysis Across Critical Infrastructure Markets, Frost & Sullivan, February 2015

[25] White Paper by Frost & Sullivan and CABA: Cybersecurity in Smart Buildings: Preventing Vulnerability While Increasing Connectivity www.caba.org/research

Industry Consensus Development on Core Issues

To create an effective countermeasure to deal with cyber threats, certain areas require ongoing consensus building and efforts. These areas pertain to standards development and certification of products and solutions as cybersecure, management of effective changes with regard to new technology integration and innovation, and continued upgrades to existing policies and standards to encompass such innovations.

Exhibit 15 provides a snapshot of industry core issues and the activity details

Exhibit 15: Industry Core Issues and Activity Details

Core Issues	Activity Details
Redefining Systems	• Physical systems need to be redefined into cyber physical systems (CPS) with a hybrid IT-OT framework. • Chief information and security officers (CISO) could emerge as key technical personnel.
Standards and Platforms	• Existing network security platforms such as Plan X (DARPA[26]) offer customization. • Ultimately, not-for-profit bodies such as Underwriters Laboratories (UL) certification could serve as a basic model for driving IoT and CPS product security.
Cyber Governance and Policy	• So far, governments' moves on cybersecurity have been termed grossly inadequate. Reactions to the most recent bill on the Protecting Cyber Networks Act[27] was presented in the White House in April 2015: ". . .security professionals and privacy advocates warn that the measure would place sensitive consumer information at risk and would not even protect networks."—USNews.com. ". . .written more as surveillance bill rather than a cybersecurity bill."—Center for Democracy and Technology. "It only authorizes the sharing of cyber threat indicators and defensive measures – technical information like malware signatures and malicious code,"—Permanent Select Committee on Intelligence, the United States House of Representatives. "We do not need new legal authorities to share information that helps us protect systems from future attacks,"—joint response from technology companies, including Twitter and Cisco. "Encryption is one of our most important cybersecurity tools, and we can't allow the short-sighted worries of some law enforcement officials to undermine the longer term goal of creating a truly secure Internet, which in itself will help prevent countless crimes," —Commented by the New America Foundation's Open Technology Institute think tank.

Source: Frost & Sullivan

[26] http://www.darpa.mil/program/plan-x
[27] https://www.congress.gov/bill/114th-congress/house-bill/1560/text

Redefining Systems and Operators

Redefining physical systems into cyber physical systems with a hybrid IT-OT framework, as proposed by NIST, is an important step towards recognizing the transition and evolution in smart building systems influenced by IoT. While redefining the physical systems formalizes the need and urgency of evaluating cybersecurity risks for ICS/CPS in buildings, it also necessiates redefining roles, responsibilities, and qualifications of personnel in charge of such systems. As the terminology gains mainstream focus, professionals with hybrid qualifications positioned as system experts for smart buildings are expected to emerge, essentially CISOs as key technical personnel within the smart buildings industry. Consequently, new training and certification requirements will be created that will be instrumental in hiring and meeting ongoing technical expertise development needs of such personnel. This area will require persistent attention from the smart buildings industry, particularly as it relates to developing training tools and ensuring they are compliant with ongoing technology innovation and the industry's security requirements.

Standards, Certifications, and Platforms

At present, there are no distinct smart building or ICS-related internationally approved standards that encompass cybersecurity, which poses particular challenges for organizations that operate globally and have to consider compliance across the geographies in which they carry out business. Some companies are using options such as ISA99[28] standards to incorporate better security into product development.

In the area of certifications, not-for-profit bodies such as UL certification could ultimately serve as a basic model for driving IoT and CPS product security. In a recent media interview, Maarten Bron, Director of Innovations at UL, states there is a possibility for UL to work closely with the White House in developing standards for IoT.[29] This effort underpins the need for the government and private sectors to come closer to fight cyber crime. Having a not-for-profit consortium devise certification for product safety and security does lend a distinct credibility. Meanwhile, cybersecurity is definitely on UL's radar, given the consortium is in the process of finalizing a test and certification program of its own IoT products that have been influenced by customers' needs and concerns for cybersecurity.

[28] The ISA99 standards development committee brings together global industrial cybersecurity experts to develop ISA standards on industrial automation and control systems security. This original and ongoing ISA99 work is being utilized by the International Electro-technical Commission in producing the multi-standard IEC 62443 serieshttps://www.isa.org/

[29] Stated in a July 2015 interview to Information Week: Dark Reading, included in the Endpoint segment: http://www.darkreading.com/endpoint/underwriters-laboratories-to-launch-cyber-security-certification-program/d/d-id/1321202

In the smart buildings industry, various suppliers are currently offering integration platforms that focus on cybersecurity. For instance, specific participants such as Lynxspring (Cyberpro®), Siemens Industry, Schneider Electric, and Johnson Controls have introduced such systems and platforms that offer customers a focused solution to mitigate cyber risks.

Developed by the Defense Advanced Research Projects Agency (DARPA) over the last 3 years, Plan X (a network security platform) was unveiled in early 2015. The platform's purpose is to enable Department of Defense (DoD) cyber missions in real time. DARPA anticipates versions of the program to be made available publicly for both businesses and consumers, and parts of it are already available to open source projects. Although Plan X is in its nascent stages, it is hailed as a promising solution for the future of information security, cyber defense, and the Internet by making cybersecurity more accessible, which could potentially offer a base for developing a cybersecurity platform specific to smart buildings.

Cyber Governance and Policy

When it comes to cybersecurity, dedicated policies and legislations are needed to create better safeguards within the legal system; however, most legislations created so far in this regard have met with vehement public opposition and critical review. These legislations are considered more as surveillance bills rather than ways to provide legal recourse to victims and the industry in the event of cyber breaches. The Protection of Cyber Networks Act is the most recent legislation presented in the White House in April 2015. The act was passed amid strong criticism from privacy organizations and is expected to increase private sector spying, including sharing information more readily with the government as opposed to protecting information. However, supporters feel this legislation has been amended to address those concerns, with more provisions than the preceding Cybersecurity Information Sharing Act (CISA) bill that passed the House in 2014. Supporters argue that this bill has stricter provisions that would regulate how the government can use that information.

Given the early stages of rulemaking, proponents of the smart buildings industry need to lobby for the right legislations to obtain specific safeguards incorporated into them for the industry's benefit. Otherwise, the industry may have to contend with generic legislations that might not provide adequate legal recourse in safeguarding against cyber threats and in taking action against adversaries.

Concluding Remarks

Smart buildings are creating new standards in technology, comforts, efficiency, and operational gains for owners, users, operators, service providers, and the community at large. The influence of IoT in smart buildings has drastically changed both services and value delivery models; however, IoT has exposed buildings to unprecedented vulnerabilities of cyber space. While still in the early stages, cybersecurity concerns have the potential to derail an otherwise fast-growing smart buildings industry and its associated markets, primarily because of significant operational and financial loses that all stakeholders will have to sustain in the event of a cyber breach.

The following are key conclusions of this paper:

- The smart buildings industry has the ability to prevent, or at least minimize, the damaging impact of cyber threats if it acts in a timely manner.
- The industry should consider creating and implementing a robust cybersecurity strategy, factoring in anticipated technology changes.
- Development of a dedicated cybersecurity workforce, particularly the emergence of CISOs, is expected to be a widely sought after trend to service the smart buildings industry effectively.
- Availability of products focused on cybersecurity is a key unmet need because ICS systems were not designed with cybersecurity in mind.
- As more ICS equipment becomes networked, the silos of IT and OT must work in collaboration to maintain uptime, integration, security, and real-time visibility.
- In the future, more secure systems, devices, and advanced authentication techniques are expected to enter the smart buildings industry. The ability to segment the network into risk or trust zones is important.
- Cyber threats demand the utmost recognition and intervention of administrators and regulators to implement industry-wide changes.

Evolving technology, advances in connectivity, and an M2M environment will continue to shape the trajectory of smart buildings, thus raising the need for protection against cyber threats. David Fisk[30] rightly states in his paper, “If intelligent buildings are the future, then so too are cyber threats to building services.” The question is not how but when a cyber attack will strike smart buildings. It would be in the interests of all stakeholders if an appropriate response strategy is put in place without delay, such that cyber threats do not exert a destabilizing impact on the smart buildings industry.

[30] David Fisk, professor of Systems Engineering at Imperial College London, in his article “Cyber Security, Building Automation, and the Intelligent Building” which appeared in the July 2012 issue of Intelligent Buildings International; http://www.tandfonline.com/loi/tibi20

Author and Key Contributors

Author:

Konkana Khaund

Principal Consultant

Energy & Environment

Frost & Sullivan

Konkana.khaund@frost.com

www.frost.com

Special Thanks to Key Contributors and Industry Experts:

Michael Pyle

Vice President of Cybersecurity, Partner Business

Schneider Electric

www.schneider-electric.com

Mark M. Duszynski

VP Business Development, Federal

Building Efficiency

Johnson Controls, Inc.

www.johnsoncontrols.com

Deb Noller

CEO

Switch Automation, Inc.

www.switchautomation.com

Marc Petock

Vice President Marketing

Lynxspring, Inc.

www.lynxspring.com

Legal Disclaimer

Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan is not responsible for incorrect information supplied to us by manufacturers or users.

Our research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering, subscribing, or downloading, that Frost & Sullivan research services are for customers' internal use and not for general publication or disclosure to third parties.

No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan

331 E. Evelyn Ave., Suite 100

Mountain View, CA 94041

© 2015 Frost & Sullivan. All rights reserved. This document contains highly confidential information and is the sole property of Frost & Sullivan. No part of it may be circulated, quoted, copied or otherwise reproduced without the written approval of Frost & Sullivan.

The Frost & Sullivan Story

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation, and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best-practice models to drive the generation, evaluation, and implementation of powerful growth strategies. Frost & Sullivan leverages over 50 years of experience in partnering with Global 1,000 companies, emerging businesses, and the investment community from more than 40 offices on six continents.

Frost & Sullivan helps our clients “Accelerate Growth” by:

- Delivering the broadest industry and market coverage of any research and consulting firm globally, 10 industries, 35 sectors, and 300 markets—ensuring our clients not only understand their industry challenges and opportunity but growth opportunities in aligned industries and an understanding of competitive pressures from previously unknown sources,
- Providing a 360 degree perspective—integrating 7 critical research perspectives to significantly enhance the accuracy of our clients’ decision making and lowering the risk of implementing growth strategies with poor return,
- Leveraging our extensive contacts within chemicals and materials value chain, including manufacturers, distributors, end users, and other industry experts,
- Ensuring our clients maintain a perspective of opportunities and threats globally through our 1,800 analysts in our 40 offices—making sure our clients receive global coverage and perspective based on regional expertise,
- Researching and documenting best practices globally—ensuring our clients leverage proven best-practice answers to tough business challenges for successful growth, and
- Partnering with our clients team, in addition to delivering our best practices research and experience, to ensure success.

SILICON VALLEY
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

SAN ANTONIO
7550 West Interstate 10,
Suite 400,
San Antonio, Texas
78229-5616
Tel 210.348.1000
Fax 210.348.1003

LONDON
4 Grosvenor Gardens
London SW1W 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

FROST & SULLIVAN

Frost & Sullivan, the Growth Consulting Company, partners with clients to accelerate their growth. The company's Growth Partnership Services, Growth Consulting and Career Best Practices empower clients to create a growth-focused culture that generates, evaluates and implements effective growth strategies. Frost & Sullivan employs more than 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from more than 40 offices on six continents. For more informationabout Frost & Sullivan's Growth Partnerships.