2020 16th European Dependable Computing Conference (EDCC)

Smart Building Risk Assessment Case Study: Challenges, Deficiencies and Recommendations

A Practical Experience Report

John C. Mace*, Ricardo Melo Czekster*, Charles Morisset* and Carsten Maple†
*School of Computing, Newcastle University, Newcastle upon Tyne, UK
†Warwick Manufacturing Group, University of Warwick, Coventry, UK
Email: john.mace@ncl.ac.uk

***Abstract*—Inter-networked control systems make smart buildings increasingly efficient but can lead to severe operational disruptions and infrastructure damage. It is vital the security state of smart buildings is properly assessed so that thorough and cost effective risk management can be established. This paper uniquely reports on an actual risk assessment performed in 2018 on one of the world's most densely monitored, state-of-the-art, smart buildings. From our observations, we suggest that current practice may be inadequate due to a number of challenges and deficiencies, including the lack of a recognised smart building risk assessment methodology. As a result, the security posture of many smart buildings may not be as robust as their risk assessments suggest. Crucially, we highlight a number of key recommendations for a more comprehensive risk assessment process for smart buildings. As a whole, we believe this practical experience report will be of interest to a range of smart building stakeholders.**

***Index Terms*—Internet of Things, Cyber-Physical Systems, Security, Risk Management**

I. Introduction

Smart buildings have emerged from inter-networking intrinsic systems such as HVAC (Heating, Ventilation and Air Conditioning), lighting, water treatment and access control with other data networks [1]. Facilitated real-time data flow enables automated and centralised monitoring, control, response, and auditing functions. As a result, building systems interoperate harmoniously as a single system to offer a more time-responsive, safer and comfortable environment. This holistic approach also helps meet business and governmental demands to reduce operating and energy costs, improve occupant well-being and productivity, and increase environmental sustainability. However, their high reliance on IoT style technology means a large number of smart buildings face many real and potential security threats [2]–[7]. This is echoed by a 2019 survey by cyber security firm Kaspersky that found nearly 4 in 10 (37.8%) smart buildings had been affected by a malicious cyber attack [8].

The reason for deficient security of smart buildings is often multifaceted: inter-networked building systems can present large and complex attack surfaces, both physical (systems are located across all parts of a building) and cyber (connections to corporate networks and the Internet) in nature; building control networks are often designed, installed, and maintained by engineers who lack awareness of security; industry standard solutions are now favoured, resulting in a substantial growth of using open communication standards like BACnet [9] and KNX [10]; and computationally intensive security techniques such as encryption and authentication can be constrained due to the limited processing power of many smaller devices (e.g. sensors). Alarmingly, a 2017 survey by the Electrical Contractors' Association and Scottish electrical trade body SELECT found almost 4 in 10 clients (39%) don't take any steps to protect smart buildings from cyber threats [11].

Arguably no smart building can be 100% free from security risks, but it is vital that owners and managers are able to properly assess the security state of their buildings and provide reasonable and cost effective risk management. A risk assessment is a common method to identify vulnerable assets and the various risks that could affect those assets. We report on an actual risk assessment performed in 2018 on a real-world state-of-the-art smart building, hosting more than 1300 occupants on average. This provides an example of how smart building risk assessments are currently being conducted 'in-the-wild'. Based upon our practical experience of the assessment and our subsequent analysis of its process and outcomes, we believe current practice may be deficient due to a number of factors. As a result, the security stance of many smart buildings may not be as robust in reality as their risk assessment may suggest. The contributions of this practical experience report are as follows:

- We describe a recent risk assessment of a smart building;
- We highlight challenges and deficiencies that are potentially causing inadequate risk assessment processes;
- We outline recommendations for a more comprehensive risk assessment process for smart buildings.

The remainder of this practical experience report describes a real-world smart building risk assessment in Section II. Respectively, we describe challenges, deficiencies, and give high-level recommendations in Sections III, IV, and V with concluding remarks in Section VI.

This work was supported by UK EPSRC through 'NUSBIoT', a PRF project funded under grants EP/N02298X/1 and EP/N02334X/1 within the PETRAS IoT Research Hub.

978-1-7281-8936-9/20/$31.00 ©2020 IEEE
DOI 10.1109/EDCC51268.2020.00019

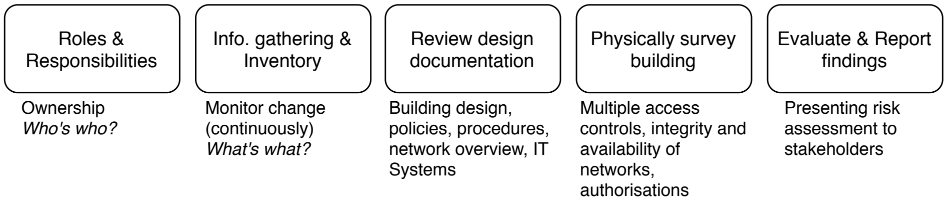
Roles & Responsibilities
Info. gathering & Inventory
Review design documentation
Physically survey building
Evaluate & Report findings
Ownership
Who's who?
Monitor change (continuously)
What's what?
Building design, policies, procedures, network overview, IT Systems
Multiple access controls, integrity and availability of networks, authorisations
Presenting risk assessment to stakeholders

Fig. 1. Smart building `SB1` risk assessment steps.

II. Risk Assessment of a Smart Building

In this section we introduce the smart building case study `SB1` followed by a description of its risk assessment.

A. Smart Building Case Study

Opening in 2017, smart building `SB1` is part of a university campus and designed for a variety of activities including teaching, laboratory research, events, and the testing of IoT technologies for urban sustainability. The building houses on average 1,200 students, 55 academic staff and 120 post-doctoral researchers as well as regular visitors from across academia, industry and government. Large parts of `SB1` are also accessible to the general public. Designed as a Building-as-a-Lab, `SB1` stands apart from most smart buildings by providing an operational test bed and demonstrator for understanding the relationship between buildings and their internal and external environments. The Building-as-a-Lab concept facilitates controlled experiments, with more than 20 plant rooms capable of differing configuration, and three building sections with their own circuits and supplies. In excess of 4 thousand digital sensors and over 15 thousand data networks are integrated into `SB1`'s open spaces and structure making it one of the most densely monitored buildings in the world. Indeed, the thousands of sensors make it possible to continuously collect and analyse data on a large scale (over 1 million data points on average per day) about how `SB1` is used, its performance and efficiency against defined standards, and how it interfaces with energy, water, Internet, and other national and international networks.

B. Risk Assessment of `SB1`

Chiefly motivated by `SB1`'s newness and uniqueness, coupled with academic literature, industry and press reports, a risk assessment was commissioned for `SB1` by its owner. The steps taken by the external assessor are shown in Figure 1 with more description below.

1) Identify Roles and Responsibilities: To carry out the risk assessment of `SB1`, the assessor needed to obtain and assess multiple building design documents and gain physical access to numerous building spaces. Many of the design documents and building spaces were considered to be of a sensitive nature, meaning the assessor needed the correct permissions in order to fully assess them. Although the risk assessment commissioner had ultimate authority to grant these permissions, in practice they had to be obtained from the personnel 'on the ground' who were responsible for multiple aspects of `SB1`'s design, operation, maintenance and security. In summary, the first step of the risk assessment was to define the key stakeholders, or a *who's who* considering several key questions: who has what role, authority and responsibility? Who holds the building design documentation? Who can provide physical access to building spaces? Who will have the answers to issues raised by the risk assessment?

Findings: We found increased interactions and good co-operation with each role was vital to ensure all those with the required authority were informed, involved and on-board with the impending risk assessment and its findings. A physical assessment of the building was to take place within a limited window over two days. Therefore, to prevent delays or restrict the assessment, it was important those with authority were prepared to give their time and permission to allow the assessor the required access to resources when needed. To facilitate this, it was necessary to make those in authority aware of potential risks in their domain of responsibility and understand why the assessment was important in order to gain their full co-operation.

2) Information Gathering and Inventory: The second step in the risk assessment of `SB1` was to define a *what's what* to ensure the right building elements (e.g. domains, spaces, infrastructure, systems, devices, networks, procedures) were to be assessed. This step utilised the who's who previously described to gather as much building related information from the listed stakeholders as possible. The documentation collected covered:

- *Architectural plans:* for all floors.
- *Networks and hardware:* Building Management System, IT network, normal and emergency electrical power, telephone communication, CCTV, water and waste management, gas; fire system, access control.
- *Procedures and policies:* maintenance and security management, incident response.

Findings: Studying this documentation enabled the assessor to construct a high-level inventory of all `SB1` elements that warranted assessment. Essentially, the inventory helped define the basic scope or logical boundaries of the risk assessment. This step was revisited several times as the risk assessment proceeded and new and unexpected elements were uncovered. The existing assessment boundaries also needed to be redefined. It was important that the right elements were to be assessed especially when constraints (e.g. time, money, personnel) meant it was not possible to assess everything. Also, the assessor did not want to waste time assessing elements that had no impact on SB1's security state, or were not impacted by security threats.

3) Review Design Documentation: The third step involved a more in-depth review of the information gathered in Step 2 to assess the security risks of SB1's design, policies and procedures in line with the current assessment scope. It was important to gain a detailed understanding of all building control networks in terms of interconnections and inter-dependencies, wireless links, protocols, and integration before analysing how they were isolated and whether they were isolated as much as possible. These aspects where explored to ensure the following:

a) Building networks: Virtual local area networks (VLANs) were implemented; firewalls were placed at every transition point into and out of the Building networks; business critical systems such as fire detection and control systems were air gapped as far as possible from IT networks; critical systems were only operated over wired networks (Note: wireless networks are susceptible to jamming from distance).

b) Remote access: Secure connections were used such as VPN; secure protocols and applications were used such as HTTPS, SSH, and SCP/SFTP whilst Telnet and FTP were avoided; remote access was restricted by using 2-factor authentication and access limited to required users only, e.g. system operators.

c) Building Management System (BMS): Full control of the BMS was limited to a small pool of trusted users; users with BMS access that leave the company or change roles have access revoked or modified immediately within the system; passwords are changed from default to secure passwords; duties of those monitoring the BMS are appropriately separated; regular maintenance and patching is recorded.

d) Data management: The location of data and how it flows between systems and stakeholders; data is stored relevant to the tasks to be accomplished; data controllers and data processors are identified; data protection regulation issues have been considered sufficiently.

The assessor looked at what building elements (e.g. systems, services and spaces) were critical and which were non-critical, especially to life safety, and prioritised them accordingly. Critical systems were defined as those essential to SB1 and the services it provides including electrical power, building control systems, cooling, water supplies, waste management, lighting and communications. Critical spaces included plant and server rooms, labs and some offices. Furthermore, from experience and expertise the assessor established which of these elements were high and low risk.

Findings: Access control cabling was deemed insecure as it was housed in a common data basket at ceiling level together with all other systems including CCTV. Cabling per floor was marshalled via the floors' plant rooms which gives access to anyone entering the room and produces multi-discipline single points of failure. Another potential single point of failure was the Uninterrupted Power Supply system providing battery back-up power to critical rooms and systems including the comms and server rooms. Regarding the fire system, if two or more fire detection points enter an alarm state then all electronic door locks will be opened to allow for evacuation; this could allow people to access areas to which they are unauthorised. The BMS design raised concern in a number of areas, chiefly: the KNX network structure was found linked to nearly all field control devices in a completely open way. All KNX systems were also linked together across all floors which means accessing the KNX network allows easy access to all devices connected to it. KNX/BACnet gateway devices were found to be over excessive in terms of functionality and did not provide the specific security requirements obtainable with more suitable devices. The building control network was found to have numerous connection points for various systems to plug into (e.g. BMS, KNX, CCTV), both within and next to every control panel and throughout SB1 as a whole. Direct cable connections would be more suitable to avoid unauthorised devices being plugged into the network.

4) Physically Survey Building: The assessor attended SB1 to physically survey the building and investigate areas of concern that had arisen as a result of reviewing the various design drawings. It was important to ensure SB1's physical security prevents unauthorised access to its building control devices, networks, and information. Without sufficient physical security controls, attackers could potentially circumvent all other security controls. It was particularly important to assess the interactions between cyber and physical elements to identify any vulnerabilities in systems and analyse the potential impact of worst case scenarios. Most locations within SB1 were visited to ensure:

a) Building control networks: High integrity and availability was evident; all entry points were enumerated; each network entry and exit point was secured; communication cable runs were protected with conduit or rugged cable chases (i.e. dug into walls); that no devices are connected to the Internet without prior knowledge; security was based on password controlled access to workstations and the presumption only authorised devices will be permitted access to building control networks (Note: Connection of unauthorised devices to unprotected network points can allow normal security measures to be bypassed. As well as each system being a potential access point to other systems it is also a means to gain entry to other IT networks).

b) Access control: Multiple access control layers are in place at building, room and cabinet level; mission critical devices are in access controlled areas or locked/tamper-proof cabinets (Note: It is essential to prevent unauthorised access to networked devices: routers, firewalls, switches. Central control panels support several systems, arrays of manual user switches or fascia, allowing users to override automated control processes. An attack here could have disruptive effect and take hours to find. Controllers and networks can be accessed from control panels).

c) Authorisation: Authorisation requirements are established for individual areas and devices such as routers, servers, embedded controllers and workstations; a DMZ has been created for public access by placing a server within the zone with the required information mirrored onto it; tamper alarms are prevalent especially in public areas.

d) Third parties: Third parties who manage building security are vetted (Note: a weak link is through remote management or via engineers with infected laptops); laptops are checked for malicious software before work takes place; a permit-to-work system is in place; system elements are ring fenced to stop access to other critical systems.

Findings: Despite elevator, lab and research space access being largely controlled by RFID card points it was possible to access the majority of building floors via various sets of stairs. A large portion of critical system cabling was laid in common baskets and left open for anyone to potentially interfere with it via a ladder. Access to all plant rooms was gained via a single key obtained without question from the building reception. Once inside, many of the control panels were found to be secured with standard panel locks which can be opened using an engineers' key available from any hardware store. Similarly secured control panels related to the fire system network, including smoke ventilation, were found in a corridor access space which anyone can access. No leak detection system was found in the comms room to help prevent equipment being damaged by condensation leaking from the water-based cooling units. The building control and IT networks were found to be separated by VLAN configurations within managed network switches. This still left numerous unprotected and non-defensive pieces of automation equipment connected to the same physical network. In essence the entire network system was totally dependent on the VLAN configuration for security.

5) Evaluate and Report Findings: Arguably, the most important part of `SB1`'s risk assessment was for its findings to be evaluated and appropriately documented. The final report was the only document the assessment commissioner and other stakeholders saw, so it was essential that it accurately captured all findings and reflected all the time and effort put into the risk assessment. The report included: an overview of the report and `SB1`; a review of the `SB1`'s design including its BIoT and communication networks; findings/conclusions on `SB1`'s accessibility, building control network, communications, sensitive spaces (e.g. labs, server and plant rooms), policies and procedures; further recommendations; and a final report summary. The readers of the report were both technical (e.g. BMS administrators, building control network technicians, IT, security) and non-technical (e.g. operations management, occupants), therefore findings were clearly communicated, allowing all stakeholders to understand the nature of the assessment, how the findings were identified, and resulting recommendations. Furthermore, the report was expected to encourage key stakeholders to buy into the assessment process enough to support action plans and continuous improvements to current risk management.

General Findings, Recommendations, and Outcomes: `SB1` was considered quite benign in its operations and its current level of security regarded as being quite low. However, a change in the use of part of the building for something far more serious or sensitive and it would be found lacking and in need of a further review. In general, it does not really matter if a building is secure or not if no assets in the building (e.g. data, research, property, servers) have any real value. However, such assets may interact with building elements being controlled by an attacker and be negatively impacted. Once an asset of value is located within a building then an exercise must be conducted to ascertain the asset's worth, and where that worth lies, and then gauge whether the security posture of any building elements which could interact with the asset are up to the job of protecting it. A physical asset of value requires physical security elements to prevent its theft and all systems that support its protection should be reviewed. Sensitive information or software with an intellectual value (IP), while requiring physical security, also requires IT security elements to prevent it being modified or copied.

a) Building control network protection: The extent to which the building control network converges with other facility systems needs to be fully understood together with generic mitigation strategies that can be established to protect these systems. Protection includes: situational threat driven security risk management; understanding system architecture and its critical points; integration or closer working relationship between previously segmented departments; a degree of network isolation and greater awareness.

b) Strengthen access management: The ease with which people can generally access the building should be reviewed and re-thought. Different locks and keys for each plant room are required. Many building control network connected devices should cater to physical security requirements, such as using anti-tamper detection, monitored supervised connectivity or even battery backup. Access to both plant room and control equipment panels should be electronically monitored by an independently networked system. The fire, smoke and life services panels must be secure, made tamper proof, and tamper monitored. A permit-to-work system should be put in place and tightly managed for all critical areas.

c) Protect plant: The fire alarm design should be reviewed and modified so that it is fit for purpose. The Uninterrupted Power Supply infrastructure design should also be reviewed and an N+1 segregation employed. Leak detection systems should be added to critical rooms with cooling.

d) Monitor research projects: When operating a Building-as-a-Lab such as `SB1` and adapting its systems for learning or research projects it is imperative that continuous monitoring of these projects is performed to ensure no additional measures become required to maintain overall security. Additionally, on completion of such a project there needs to be an agreed procedure in place so that any temporary software, hardware or systems are removed and `SB1`'s systems are returned to their original state of operation. At this time a security review of the building should again be performed as an adaptation to it has been performed.

Risk assessment outcomes: The report was distributed to all relevant stakeholders for their consideration and action. We are unable to report on the details of this due to confidentiality reasons. We have brought the attention of the report to the university Ethics Committee who review and approve research projects. We are currently working with the committee to include a process to review and monitor projects related to SB1 to ensure they will and are carried out in an ethical manner in accordance with university policies and legal regulations.

III. Risk Assessment Challenges

We now report on the key challenges we witnessed during the risk assessment of SB1.

Challenge 1: No single complete inventory of SB1's systems existed and it was not clear which stakeholders held the documentation needed to construct this before conducting the risk assessment. As much as possible, building related information was collected from stakeholders. However, differing priorities meant this process took several weeks with some documentation not arriving until after the assessment had begun. Furthermore, constraints (e.g. time, money, personnel) meant it was not possible to assess everything.

Challenge 2: The identification of roles and responsibilities for those authorised to provide all documentation and physical access required for the risk assessment of SB1. We found responsibilities laid across multiple departments and roles, not only in the building, but across the entire university. For instance: separate technical roles within the Estates department were responsible for SB1's BMS, maintenance, and security; different roles in the IT department were responsible for the IT networks, computing equipment, and communications; whilst different non-technical roles oversaw general building operations and university operations/management within SB1. Furthermore, third party organisations operating within SB1 have their own private lab and office spaces, whilst much of the design documentation was in the hands of the architects and building contractors. In essence, each role we identified generally worked with different social structures and priorities, and focused only on their areas of practice, resulting in silos of responsibility and knowledge.

Challenge 3: We found a lack of assessment awareness from personnel operating in the building which led to us being denied access to some locations in SB1. On the other hand, we did gain access to two locations by maintenance engineers (who we had never met and vice versa) which we were later told should not have entered without formal approval. This led to the conclusion that key stakeholders had not been informed of the physical assessment dates or had not filtered the information to their staff on the ground. Furthermore, it led to a feeling of uncertainty regrading what areas we could and could not enter, and we were ourselves doing something suspicious.

IV. Risk Assessment Deficiencies

This section highlights potential deficiencies in smart building risk assessment based upon our experience and material from industry blogs on current practice. In general, risk assessment is a common tool to study vulnerabilities, threats, likelihood, loss or impact, and the theoretical effectiveness of security measures [12]. Risk assessment guidance exists in the form of high-level risk management standards, e.g. ISO/IEC 27005 Information Security Risk Management [13] and NIST SP 800-30 Risk Management Guide for IT Systems [14]. Some domain specific risk assessment methodologies are starting to emerge for smart infrastructure including cyber-physical systems (e.g. [15]), critical infrastructure (e.g. [16]), industrial control systems (e.g. [17]) and SCADA systems (e.g. [18]), IoT (e.g. [19]), smart grid (e.g. [20]), and smart homes (e.g. [21]).

Deficiency 1: For smart buildings there is a lack of a clear standardised risk assessment methodology leaving assessors with little guidance on how to assess specific physical and cyber risks. As a results, the steps shown in Figure 1 taken to assess SB1 were of the assessor's own design, derived from their deep-rooted knowledge and experience of smart building BMS consultancy, design, and installation.

Deficiency 2: Smart building risk assessments may be conducted by building experts who are not necessarily cyber security experts as was the case with the assessment of SB1. Yet these risk assessors must operate and provide risk guidance in a domain where the cyber security threat landscape is complex, dynamic and high risk if not addressed adequately.

Deficiency 3: Smart building risk assessments may not be technical in nature and lack an in-depth assessment of the cyber risk. Such understanding is critical as building control networks are often designed, installed, and maintained by engineers experienced in installation and facilities management but lack awareness of security. Many building control networks are largely unsecured and can be accessed with minimal effort to intercept, disrupt and exploit data flow for monitoring or changing a smart building's environment. Furthermore, construction and installation differences between buildings mean building control networks can have varying, sometimes unknown, levels of access. As a result, many smart buildings may be exposed to multiple cyber threats which may be launched locally or remotely. Detailed information can be gained about many building control network devices exposed to the Internet, through the use of IoT search engines such as Shodan [22] and Censys [23].

Deficiency 4: There is a vast array of smart buildings in operation coming with different functions and architectural elements. It may be the case that a risk assessment process conducted in one smart building may not be suitable in another. Future analysis is planned with smart buildings being constructed both on and off the university campus to understand whether the assessment of SB1 is fully representative for all smart buildings including those in university, industry, commercial and residential sectors.

Deficiency 5: There may be no clear risk assessment commissioning process between the smart building owner (the customer) and the risk assessor. Discrepancies may arise between what the customer wants from the assessment (their requirements) versus what was delivered. It may be the case that the customer themselves do not know or understand what they want. Full customer buy-in becomes an issue here when certain elements of the customer's organisation are not included or not accepting of the assessment findings. This can result in little or no action to address identified risks.

Deficiency 6: It may be the case that a smart building risk assessment is not a pure risk assessment at all. The assessment report of SB1 contained no data or quantification of risk one would expect in a risk assessment. As a result, the whole process could be described as a vulnerability survey rather than a risk assessment.

V. Risk Assessment Recommendations

Following our experience and observations, we now present some high level recommendations we believe would lead to more effective and comprehensive smart building risk assessments.

- The creation of **domain specific guidelines** which are detailed enough to adequately assess both physical and cyber security risks in depth yet can be applied to a range of different smart buildings.
- Establish a recognised smart building risk assessment process which includes a stronger **focus on technical elements** including network separation and firewalls, Internet connectivity scenarios, endpoint security, penetration testing, control network user access, patching, anti-virus protection, database and server security.
- Establish a comprehensive guide to smart building security and risk which provides **support for quantifying risk** and recommending appropriate and effective defence measures
- The development of risk assessors with **cross-cutting expertise** in smart building technology, operations, physical and cyber security.
- Establish **data and systems ownership** within a smart building to prevent security responsibility gaps. By nature, a smart building is a cross-cutting operation by estates, IT, network, admin, or even physical security departments.
- Develop a process to **establish customer requirements** and total buy-in of a smart building risk assessment. In doing so, the correct results will be gathered and used to develop and harden appropriate and specific security requirements and specifications. An action plan outlining risks and controls can be developed with full endorsement from all those responsible for building operations and security.

VI. Conclusion

Assessing security risk in smart buildings can facilitate better decision making in response to the level of exposure a building is facing, and inform managers to devise more cost effective action plans for mitigating possible attacks or other security incidents. In this practical experience report we have uniquely described a recently witnessed risk assessment of a state-of-the-art smart building. On reflection, we believe current smart building risk assessment practice may be inadequate. We highlight the challenges we faced with the risk assessment and describe potential assessment deficiencies. High-level recommendations geared toward a more comprehensive risk assessment process are also given. As future work we plan to start co-designing such a process with smart building technology and security industry partners.

References

[1] A. Buckman, M. Mayfield, and S. BM Beck, "What is a smart building?," *Smart and Sustainable Built Environment*, vol. 3, no. 2, pp. 92–109, 2014.

[2] "New report outlines IoT security vulnerabilities." https://www.cpomagazine.com/cyber-security/new-report-outlines-iot-security-vulnerabilities/.

[3] "Sabotaging common IoT devices in smart buildings by exploiting unencrypted protocols." https://www.forescout.com/company/blog/sabotaging-smart-building-iot-devices-using-unencrypted-protocols/.

[4] "Cyber attacks could 'shut down a building with one click' research shows." https://memoori.com/cyber-attacks-could-shut-down-a-building-with-one-click-research-shows/.

[5] "IBM's X-Force team hacks into smart building." https://www.csoonline.com/article/3031649/ibms-x-force-team-hacks-into-smart-building.html.

[6] "Lock out: The Austrian hotel that was hacked four times." http://www.bbc.co.uk/news/business-42352326.

[7] "Hacker takes control of hundreds of rooms in hi-tech 5-star Shenzhen hotel." https://www.scmp.com/news/china/article/1561458/hacker-takes-control-hundreds-rooms-hi-tech-shenzhen-hotel.

[8] "Nearly four in ten smart buildings targeted by malicious attacks in h1 2019." https://usa.kaspersky.com/about/press-releases/2019_smart-buildings-threat-landscape.

[9] "ISO 16484-5:2017(en) Building automation and control systems (BACS) — part 5: Data communication protocol." https://www.iso.org/obp/ui/#iso:std:iso:16484:-5:ed-6:v1:en.

[10] "ISO 22510:2019(en) Open data communication in building automation, controls and building management — home and building electronic systems — KNXnet/IP communication." https://www.iso.org/obp/ui/#iso:std:iso:22510:ed-1:v1:en.

[11] "ECA/CIBSE/SELECT Survey finds clients 'unprepared' for smart buildings revolution." https://www.risk-uk.com/ecacibseselect-survey-finds-clients-unprepared-smart-buildings-revolution/. Accessed: 11-12-2019.

[12] L. T. Ostrom and C. A. Wilhelmsen, *Risk assessment: tools, techniques, and their applications*. John Wiley & Sons, 2019.

[13] "ISO/IEC 27005:2018 Information technology - security techniques - information security risk management." https://www.iso.org/standard/75281.html.

[14] "SP 800-30 Rev. 1 Guide for conducting risk assessments." https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[15] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Computers & Security*, vol. 68, pp. 81–97, 2017.

[16] G. Giannopoulos, B. Dorneanu, and O. Jonkeren, "Risk assessment methodology for critical infrastructure protection," *JRC–Scientific and Policy Report*, 2013.

[17] A. Hristova, R. Schlegel, and S. Obermeier, "Security assessment methodology for industrial control system products," in *The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent*, CYBER, pp. 264–269, 2014.

[18] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Computers & Security*, vol. 56, pp. 1 – 27, 2016.

[19] J. R. C. Nurse, S. Creese, and D. D. Roure, "Security risk assessment in Internet of Things systems," *IT Professional*, vol. 19, no. 5, pp. 20–26, 2017.

[20] V. Lamba, N. Simkova, and B. Rossi, "Recommendations for smart grid security risk management," *Cyber-Physical Systems*, vol. 5, pp. 1–27, 04 2019.

[21] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, 2018.

[22] "Shodan." https://www.shodan.io/.

[23] "Censys." https://censys.io/.