Cybersecurity as an Organizational Problem: Integrating Cybersecurity Expertise into the Project Life-Cycle

Abstract

Technologies such as the Internet of Things (IoT) connect buildings and infrastructure to networks, cloud computing, and the Internet, which creates new vulnerabilities to cyberattacks. Cybersecurity emerged in the domain of computer sciences. To that end, many think of cybersecurity as a technical rather than an organizational field. The research project we present here makes the argument that cybersecurity is an organizational problem. The siloed organizational practices of operations and information technology teams create cybersecurity risks. In this research, we identify and analyze cybersecurity risks in three categories: Design and construction of new or renovated buildings and infrastructure, vendor procurement practices, and the management of IoT operations and future operations planning. We found that in current practices, the integration of cybersecurity expertise into the project life-cycle is fraught in that it requires new processes, practices, and policies as well as an understanding and management of disciplinary differences.

Introduction

The owner organizations are increasingly implementing Internet of Things (IoT) devices and systems in new construction and building renovations (Tang et al., 2019). These devices are nodes connected to either private networks, such as those dedicated to managing buildings, or public networks like the Internet. Each device collects data, such as temperature data, occupancy data, and/or energy-use data, that provide operations professionals with information about building performance, energy management, and operations and maintenance (O&M) (Tang et al., 2019). For those working and living in the built environment, IoT devices and systems can provide environmental, social, and economic benefits, such as improved energy- and water-use efficiency, increased occupant health and safety, and optimized management and operations (Borhani et al., 2020). However, IoT devices and systems also come with a number of cybersecurity risks for owner organizations. IoT devices are considered high risk, particularly access controls and Heating Ventilation and Air Conditioning (HVAC) (Forescout 2020). A 2021 Honeywell survey found that 33% of education facilities from the U.S., Germany, and China had experienced security breaches in their operational systems during a twelve-month period. This was higher than the number of breaches occurring in data centers (Honeywell 2021). As IoT becomes more ubiqouitous, there is a need to understand and update owner organizations processes, practices, and policies as it relates to IoT and cybersecurity.

Points of departure

There are five foundational issues that make IoT devices and data vulnerable to cyber threats such as ransomware. First, a lack of international or national cybersecurity requirement standards, in conjunction with the internationalization of device components in supply chains, leads to poorly made devices with out-of-the-box cybersecurity issues (Boddy and Pompon, 2019; Lee and Beyer, 2017; Benson, 2018). Second, the large quantity and type of devices used in the built environment exponentially expands the number of opportunities for attackers to exploit technical vulnerabilities of IoT device systems. The quantity also increases opportunities for misconfiguration of devices during their deployment and implementation (Hardin et al., 2015). Third, the policy landscape lacks clear cybersecurity standards for IoT vendors (Lee and Beyer 2017). Cybersecurity policymakers are also generally not aware of the risks that building-owner organizations face, including the complexity of building-industry practices and building-industry-compliance needs. Fourth, there are still many unknowns surrounding the future of data-privacy policy with IoT devices, including a lack of guidance on how to apply international data-policy laws, such as the European Union's General Data Protection Regulation (GDPR), to IoT devices. This is an emerging area that could create complications for building owners in the future. Taken together, the issues related to cybersecurity are dynamic and complex, which results in individuals who specialize in cybersecurity.

As we introduce IoT into the operations of buildings and infrastructure, there is a need to integrate cybersecurity experts into design, construction, and operations teams. However, this integration is often overlooked (Benson 2017). The complexities related to the building life-cycle, including the number and types of stakeholders involved alongside the professional and organizational silos between Information Technology (IT) and operations professionals, have led to a lack of IoT oversight, poor device installation, and a shortage of centralized management and understanding of an often-unknown number of IoT devices in the built environment (Benson 2017). This research focuses on the organizational and cultural issues related to the integration of cybersecurity expertise into the project life cycle, which is not yet well studied, particularly empirically. The research questions we ask here are how can an organization manage cyber vulnerability issues raised by the introduction of IoT devices and systems through the integration of cybersecurity and IT expertise into the project life cycle?

Findings

The findings are organized into three categories of work: design and construction, vendor procurement, and operations. The integration of IT experts in general and cybersecurity expertise in particular is a shared theme across all three categories. The introduction of IoT into building operations brings with it the need for information technology expertise. These professionals come with different disciplinary cultures than typical design, construction, and operations staff.

In the design and construction phase, we found that operations, IT, and cybersecurity personnel were not typically consulted early enough in the process, thereby missing opportunities to

include those disciplinary perspectives and expertise in design decision-making. This led to reworking designs that were incompatible with operational requirements or fitting new IoT systems into existing networks in haphazard ways.

In both the design of new buildings and the retrofit of existing structures, owner organizations interacted with vendors who develop and manage IoT systems. The new paradigm of software as a service led to new business models that required ongoing interaction with the vendor long after the initial point of sale and installation. We found that often cybersecurity professionals were not consulted during procurement, and that the owner organizations lacked clear cybersecurity criteria or procurement policies. Consequently, questions emerged regarding data governance and a need to clarify roles and responsibilities for ongoing IoT management and security.

In the operational phase, we observed persistent silos between operations and IT teams. These silos created unclear network governance of IoT systems, challenges in coordination and scheduling between IT and operations personnel, and misunderstandings and cultural differences that led to misaligned assumptions and impede collaboration.

Overall, the integration of cybersecurity expertise into the project life cycle is fraught with the need for new processes, practices, and policies. Teams need to develop ways of working across disciplinary differences, create a shared understanding of cybersecurity risks, and develop standards for design, construction, and vendor engagement.

Implications and Conclusions

The results of this study suggest an urgent need for integration and collaboration between design, construction, operations, and IT disciplines as it relate to the selection, implementation, and maintenance of IoT systems. The siloed practices and disciplinary divisions lead to cybersecurity risks and ineffective management of new construction and retrofit projects. To accomplish the needed integration, we must understand the disciplinary differences that create tensions, miscommunication, and misunderstandings; then building owners can create effective design, construction, and operational teams. The results of this research include strategies and recommendations for creating processes, practices, and procedures that support an effective cybersecurity culture. These include consulting cybersecurity and operations professionals at specific points of IoT decision-making such as establishing procurement vetting committees and creating IoT network governance that includes IoT and operations professionals working collaboratively.

Acknowledgments

This research is funded by the National Science Foundation (NSF #1932769, “SaTC: CORE: Medium: Knowledge Work and Coordination to Improve O&M and IT Collaboration to Keep Our Buildings Smart AND Secure.”) I want to also thank the 2019 - 2022 research team and the

authors of the technical report “IoT Cybersecurity in the Built Environment 2022: Laura Osburn, Madison Snider, Jessica Beyer, and Chuck Benson (http://cyber.be.uw.edu).

References

Benson, Chuck (2017), “Bathtubs, Manageability, & IoT,” Long Tail Risk: Internet of Things Systems Risk Management (blog),
October 19, http://longtailrisk.com/2017/10/19/bathtubs-manageability-iot/;

Benson, Chuck, Hearing: Before the U.S.–China Economic and Security Review Commission, 115th Congress (March 8, 2018) (Statement by Chuck Benson, Assistant Director for IT in Facilities Services, University of Washington),
https://www.uscc.gov/sites/default/files/transcripts/Hearing%20Transcript%20-%20March%208%2C%202018.pdf [uscc.gov].

Boddy, Sara and Raymond Pompon, (2019) “The Hunt for IoT: The Opportunity and Impact of Hacked IoT,” July 15,
https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot-the-opportunity-and-impact-of-hacked-iot;

Borhani, Ali, Julie Jupp, and Carrie Sturts Dossick, (2020) “Working Paper: IB INDEX: Towards a Standard for Building Intelligence Evaluation” (working paper, Engineering Project Organizations Virtual Conference, Oct 21–23.

Forescout Research Labs, (2020) “The Enterprise of Things Security Report: The State of IoT Cybersecurity in 2020,” Forescout,
https://www.forescout.com/the-enterprise-of-things-security-report-state-of-iot-security-in-2020/.

Hardin, Dave, Eric Stephan, Weimin Wang, Charles Corbin, and Steven Widergren, (2015) “Buildings Interoperability Landscape,” December, https://energy.gov/sites/prod/files/2016/01/f28/BuildingLandscapeReport.pdf.

Honeywell, “Protecting Operational Technology in Facilities from Cyber Threats: Constraints and Realities,” Georgia: Honeywell International, 2021.
https://buildings.honeywell.com/us/en/lp/protecting-operational-technology-in-facilities-from-cyber-threats.

Lee, Stacia and Jessica Beyer, (2017) “Internet of Things Device Security and Supply Chain Management” (policy paper), Wilson Center, October, 2017,
https://www.wilsoncenter.org/publication/internet-things-device-security-and-Supply-chain-management;

Tang, Shu, Dennis Shelden, Charles Eastman, Pardis Pishdad-Bozorgi, and Xinghua Gao, (2019) “A Review of Building Information Modeling (BIM) and the Internet of Things (IoT)

Devices Integration: Present Status and Future Trends," Automation in Construction 101 (May): 127–39, https://doi.org/10.1016/j.autcon.2019.01.020.