Improving O&M and IT Collaboration to Keep our Buildings Smart and Secure

PI: Laura Osburn, Construction Management, University of Washington

Co-PI: Dr. Carrie Dossick, Construction Management, University of Washington

Co-Investigators: Jessica Beyer, Jackson School for International Studies, University of Washington

Chuck Benson, Director of IoT Risk Mitigation Strategy at University of Washington

NSF Project URL: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1932769&HistoricalAwards=false

Challenges for IoT in the Built Environment

Internet of Things (IoT) devices are increasingly integrated into buildings. As these sensors are connected to the internet and networked to building technology (such as heating and lights), they introduce security vulnerabilities. Although technical solutions exist to counter security issues, implementation of these solutions are often impeded by the challenges that an organization's Information Technology (IT) staff and a building's Operations and Maintenance (O&M) staff have when they work closely together and share their knowledge about computer security and how buildings operate. These difficulties arise from different ways of working and different points of view about how technology works.

How Technological and Organizational differences in IT and OT systems Impact IoT

A foundational issue for cybersecurity in buildings is the integration between Information Technology and Operational Technology (OT), called *IT/OT convergence*. These two systems are embedded in the siloed institutional histories and work practices of the professional domains that have historically managed each type of technology. OT is predominantly within the domain of engineering and skilled trades, often governed by a building's O&M department. IT is a part of the computer science discipline and generally managed in an IT department.

The siloed evolution of these technologies has led to the following risks:

- Different work structures and cultures;
- A responsibility vacuum around IoT security; and
- A foundational misunderstanding between O&M and IT about how each system operates, complicating attempts to collaborate.

		OT	IoT Risks	IT
Technological	Purpose	Control/manage physical devices	Potential disruptions; data vulnerabilities	Manage information
	Connectivity	Often standalone applications	Connectivity creates risk that can disrupt OT and IT	Interconnected (applications)
	Architecture	Often closed, proprietary, task specific	Many can be reprogrammed by bad actors.	Frequently more open, standards-based
	Lifespan	Long (10-20 years)	May not be patched/upgraded; upgrades may be disruptive	Frequent, systematic patches and upgrades
	Discipline	Engineering, skilled trades	Different terminologies and siloed practices	Computer science
Organizational	Governance	O&M, engineers, technicians	Unclear responsibility when systems overlap	IT department
	Knowledge	Many workers only know older technology	O&M and IT may not understand each others' tech	Emphasis on keeping up with latest technology
	Practice	Interventions not required daily	Different expectations on how and when to intervene with tech	Needs daily human and automated support
	Culture	Maintaining/Managing physical processes	Conflicting/unclear obligations; difficulties aligning agendas	Maintaining and securing information

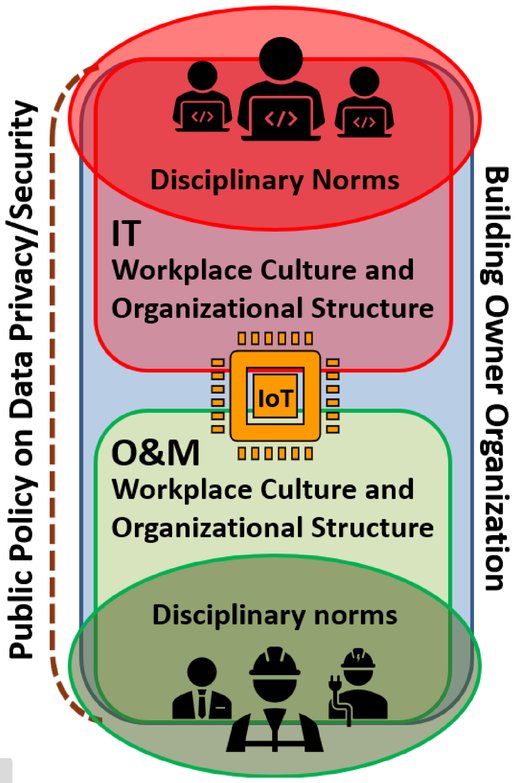
Solutions for Success

Stronger collaboration between O&M and IT may mitigate security challenges with IoT. However, this requires:

- Sharing expertise in meaningful ways;
- Coordinating IT and O&M work tasks; and
- Meeting organizational and policy requirements

We address this solution through studying:

1. How O&M and IT currently share their knowledge and skills and work together to improve IoT security; and
2. How public policies and an organization's own rules regarding privacy and security impact how IT and O&M collaborate.



Scientific Impacts for Cybersecurity Research

This study will have a high impact on cybersecurity theory and empirical research through:

- Providing much-needed empirical data on current collaborative O&M and IT cybersecurity practices;
- Building theory on how federal and state policies, organizational rules and procedures, and daily work practices impact cybersecurity collaborations;
- Identifying policies, procedures, and practices that help O&M and IT collaborate to improve IoT security;
- Learning how policies on data privacy and security affect cybersecurity practices and, in turn, how current practices affect he implementation of these policies.

Methodology

This project will collect data through observations, expert interviews, and document analysis in three phases:

1. Ethnographic research of three universities' IoT cybersecurity efforts between O&M and IT;
2. Interviews with IT and O&M IoT security experts in the U.S.; and
3. Regional case studies of higher education IoT security efforts in the Pacific Northwest.

Broader Impacts for the Industry

This study will inform cybersecurity policy and impact cybersecurity professionals in the building industry through:

- An industry report on successful O&M and IT collaboration strategies;
- Published white papers on policy findings and recommendations;
- Sharing our findings at public speaking events, in popular and academic publications, and through developing training for building professionals and students; and
- Improving the cybersecurity pipeline through prioritizing student researchers currently underrepresented in the cybersecurity field.

SaTC:CORE: Medium: Knowledge Work and Coordination to Improve O&M and IT Collaboration to Keep Our Buildings Smart AND Secure **Award ID#:1932769**