Summary of Outcomes of the 2019 Cybersecurity Roundtable

Eliot Crowe, Claire Curtin, Hannah Kramer, Jessica Granderson, Lawrence Berkeley National Laboratory
Cindy Zhu, U.S. Department of Energy
Hayden Reeve, Glenn Fink, Pacific Northwest National Laboratory

Prepared for:
Amy Jiron and Monica Neukomm, U.S. Department of Energy
October 2019

Cybersecurity Roundtable Organizers

Name	Organization
Eliot Crowe	Lawrence Berkeley National Laboratory (facilitator)
Hannah Kramer	Lawrence Berkeley National Laboratory
Claire Curtin	Lawrence Berkeley National Laboratory
Jessica Granderson	Lawrence Berkeley National Laboratory
Hayden Reeve	Pacific Northwest National Laboratory
Glenn Fink	Pacific Northwest National Laboratory
Cindy Zhu	U.S. Department of Energy
Monica Neukomm	U.S. Department of Energy

Building Industry Stakeholder Attendees

Name	Organization
David Bain	Telecommunications Industry Association
Sarah Bemporad	Realcomm
Howard Berger	Realcomm
Michael Chipley	PMC
Aaron Daly	Whole Foods Market
Kendall George	Carleton College
Susan Gerock	Washington REIT
Ken Kurz	Corporate Offices Properties Trust
Sabine Lam	Google
Martha Larson	Carleton College
Bayron Lopez Pineda	Kilroy Realty Corporation
Josh McKiddy	MGM Resorts
Charles Meyers	Wells Fargo
Neal Mohammed	Rudin Management
Chip Pierpont	General Services Administration
Julia Rotondo	PNNL
Francisco Ruiz	Oracle
Limor Schafman	Telecommunications Industry Association
Sandy Shadchehr	General Services Administration
Deborah Shands	SRI
Thomas Yeh	NYSERDA

Background

Photo: Thor Swift/Berkeley Lab

Cybersecurity concerns represent a significant barrier for many commercial building owners who are considering the addition of connected smart building technologies to improve their buildings' energy performance. The main goal of this full-day cybersecurity workshop, hosted and facilitated by Lawrence Berkeley National Laboratory (Berkeley Lab) was to gather insights into commercial building owners' and managers' current cybersecurity practices and concerns. Toward that goal, the Cybersecurity Roundtable, held on May 23, 2019, was structured to meet three key objectives pertaining to energy efficient smart building technologies:

- To understand the range of building cybersecurity risks and possible mitigation strategies
- To understand current cybersecurity management practices in the commercial sector
- To gain insights to inform publicly funded building technology research that takes account of cybersecurity risks and current practices/constraints within the commercial building sector

The event hosted representatives from 21 leading organizations that were identified as early adopters of smart building technologies from the commercial real estate, higher education, hospitality, grocery, utility, and government sectors, as well as representatives from industry associations. In addition to Berkeley Lab and the U.S. Department of Energy (DOE), the event was supported by Pacific Northwest National Laboratory (PNNL).

Cybersecurity Issues for Commercial Buildings

Operational Technology Versus Information Technology

Cybersecurity is a very broad topic, affecting a vast array of technologies; the focus of the Cybersecurity Roundtable was on Operational Technology (OT), as opposed to Information Technology (IT). More specifically, the Roundtable was concerned with connected energy efficient OT, such as energy management and information systems (EMIS), advanced connected controls, and "Internet of Things" (IoT)[1] devices. Typically, an IT group is responsible for overall cybersecurity in enterprise systems including, but not limited to, the business information networks. The IT group is also typically tasked with cybersecurity risk management. In contrast, OT groups are tasked with the well-being and function of individual building systems such as heating, ventilation and air conditioning (HVAC), lighting, and elevators. Table 1 summarizes the key differences between IT and OT systems.

[1] The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, that are provided with unique identifiers (UIDs) and can transfer data over a network without requiring human-to-human or human-to-computer interaction (Source: Wikipedia).

Table 1. Distinguishing characteristics of IT and OT systems

	INFORMATION TECHNOLOGY (IT)	OPERATIONAL TECHNOLOGY (OT)
Purpose	Process transactions, provide information	Control or monitor physical processes and equipment
Architecture	Enterprise-wide infrastructure and applications (generic)	Event-driven, real-time, embedded hardware and software (custom)
Interfaces	Graphical user interface (GUI), Web browser, terminal, and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices
Ownership	Chief Information Officer (CIO) and IT	Engineers, technicians, operators, and managers
Connectivity	Corporate network, Internet Protocol (IP)-based	Control networks, hard wired twisted pair, and IP-based
Role	Supports people	Controls machines

Source: Whole Building Design Guide, National Institute of Building Sciences

OT staff concentrate on maintaining the operational status of building systems for occupant comfort and convenience; thus, availability is most important to their mission, and cybersecurity is a relatively new concern. IT security staff, on the other hand, are more familiar with cybersecurity risks and mitigation strategies, but are often unfamiliar with OT systems and the ways in which they are becoming connected.

Operational technology cyberthreats

Typically, financial or political desires motivate cyberattackers, and the most direct means of exerting their will is by targeting enterprise IT systems. They may wish to steal confidential customer financial information or deny the owners use of their systems, either for ransom or to influence the victim toward actions advantageous to the attacker. The impacts of financially motivated attacks are easiest to quantify, with research showing that hacks involving theft of personal information has resulted in losses of almost $1.5 billion in market value for the companies involved.[2]

While the IT community has long been aware of cybersecurity risks and has developed counter-measures and procedures, OT system management generally has lagged in addressing cybersecurity. Before OT networks were commonly networked with enterprise IT systems (and, by proxy, the Internet), their cybersecurity concerns were minimal. However, connection of OT systems to IT networks has become quite common, and these systems have become both vectors (i.e., an entry point enabling access to broader enterprise IT systems) and occasionally direct targets of cyberattack.

Because IT staff are often unfamiliar with the function and capabilities of OT systems, many have been unaware of the growing exposure from those systems becoming IP-enabled. However, recent incidents of OT-targeted cyberattacks are changing this perception. It is now common for building HVAC (and possibly lighting) system controls to be IP-enabled, and there is

[2] Orszag, Peter R. 2018. "How a Data Breach Affects the Bottom Line." *Bloomberg.* https://www.bloomberg.com/opinion/articles/2018-04-13/how-hacking-affects-a-company-s-market-valuation

proliferation of IoT devices emerging to support energy efficient building operations. Additionally, devices and systems like elevators that traditionally are not networked are increasingly becoming IoT devices because of the ease of use an Internet connection affords.

In 2016, the Mirai botnet appeared, compromising and employing millions of these consumer IoT devices to perpetrate denial-of-service attacks on web domains.[3] Beyond the headlines, cyberattacks on commercial building OT systems is increasing; building control systems are being attacked with ransomware and remote access control gained directly over building equipment.[4]

Data published by IntelligentBuildings shows that half of the buildings they assessed in 2018 had devices directly exposed to the Internet that could be accessed remotely, and 95 percent of the buildings had no disaster recovery plan or had not changed default configurations and ports.[5] This illustrates a lack of cybersecurity awareness and implementation of best practices by building operators.

Implications for adoption of energy efficient connected technologies

This lack of good cyber "hygiene" can slow the adoption of energy efficiency technologies. A survey by Bain and Company showed that concern over cybersecurity is the number one barrier to the adoption of IoT technologies by enterprise customers. Of the executives surveyed, 45 percent listed security as their number one concern, with 60 percent of respondents stating they were very concerned about the risks[6].

Photo: Thor Swift/Berkeley Lab

Furthermore, companies with more sophisticated cybersecurity practices actually had higher concerns about the risk of IoT devices. This suggests that raising awareness and education about cybersecurity best practices can help but is not the whole solution, as improvements in the cybersecurity of product offerings and service providers is also required. Based on the level of concern among building owners, cybersecurity continues to be an important issue of consideration and research for DOE's Building Technologies Office as it seeks to promote smarter, more energy efficient technology development for buildings.

[3] U.S. Department of Homeland Security. 2017. Alert (TA16-288A). Heightened DDoS Threat Posed by Mirai and Other Botnets. https://www.us-cert.gov/ncas/alerts/TA16-288A
[4] Gordy, Fred. The State of BAS Cybersecurity. 2019. AutomatedBuildings.com. http://automatedbuildings.com/news/apr19/articles/ib/190318022808ib.html
[5] Ibid.
[6] Ali, S., A. Bosche, and F. Ford. 2018. Cybersecurity Is the Key to Unlocking Demand in the Internet of Things. Bain & Company. https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things

Roundtable Format

The Roundtable workshop was structured to maximize collaborative group discussion (See Appendix A for the agenda). Brief introductory presentations by DOE and the National Laboratories were followed by a full day of whole-group discussion and focused breakout groups. The topic of cybersecurity is very broad and, by its definition, highly interconnected; to allow for a deeper dive and to help organize the Roundtable, the main topic was broken out into four sub-categories for breakout group discussions:

- Operations and IT collaboration
- Technology procurement - working with vendors and third-party service providers
- Corporate environment and workplace practices
- Cybersecurity risk assessment

Facilitation of the breakout groups was led by National Laboratory researchers and DOE Technology Managers. Attendees completed a brief pre-event survey to help organizers develop an agenda and discussion guides that took account of attendees' experiences and interests. The Roundtable also featured a cybersecurity role-playing game, as a way to spur further collaboration and discussion around cybersecurity defense strategies (see Appendix B).

Summary of Findings

Several high-level themes emerged from the cybersecurity roundtable, covering industry best practices and outstanding needs, including the following:

- Organizational structures need to account for cyber risks.
- Data collection and ownership needs to be clearly defined.
- Collaboration and contracting is key for leased properties.
- The smart building technology supply chain is complex, immature, and fragmented.
- The financial value of cybersecurity is difficult to quantify.
- Existing cybersecurity resources need to be tailored to the building industry.
- Training needs to evolve as buildings and cyberthreats become more sophisticated.
- There is a lack of testing standards and facilities.

Additional detail on each of these key themes is provided below.

Organizational structures need to account for cyber risks

Photo: Thor Swift/Berkeley Lab

Cybersecurity roles and responsibilities within an organization's structure vary greatly by company and its core mission, as described by Roundtable attendees. Large companies whose core business is IT typically have a mature organizational structure and processes for security embedded throughout the IT, legal, and HR departments. One Roundtable participant described a well-defined review process for any new technologies or equipment that the company considers, meaning all departments are aligned in process. For real estate landlords generally, offering a secure workplace to tenants is critical, so security is often prioritized at the leadership level. Some companies have IT departments co-located with their construction department. Others are incorporating dedicated IT security roles into their OT departments (or vice versa). In other cases, a Chief Information Security Officer (CISO) exists independent of IT and OT, with overarching responsibilities. In the higher education sphere, it is often the case that IT and OT staff report to different management streams, requiring more emphasis on accountability and communication in order to align interests when it comes to connected smart building technology adoption.

Historically, the natural departmental separation of the IT and OT groups, and the prior lack of connectivity of OT systems, has meant collaboration has not been the norm and established collaborative practices have not been developed. However, given growing OT connectivity and cybersecurity threats, collaboration has become a necessity. Principally, OT staff need to better understand security risks of remote management and vendor access to OT technologies, and IT staff need to understand the function and priorities of various OT platforms, which often include energy management. In distinguishing roles, IT can be responsible for securing the network, and OT can be held accountable to abide by the established security rules and best practices. When planning IP-enabled OT improvements it is recommended that IT staff be consulted at the earliest opportunity (and thought of as a kind of "insurance policy"), rather than as a final security check once new technology is installed.

Photo: Thor Swift/Berkeley Lab

For organizations looking to go beyond interdepartmental collaboration, it was also suggested that companies could create a new position in their operations departments, such as an "Operational Technology Manager." This person would be an OT specialist embedded in the IT

department but would work day to day with OT facilities staff. Another suggested new position would be "Director of IoT" within facilities. This person would communicate with IT teams when deploying networked OT solutions. It was clear that some organizational role must be established to help OT engineering teams understand and coordinate with IT. This role also would help IT staff understand building systems protocols and procedures, and enable greater support for deployment of energy efficient smart building technologies.

Data collection and ownership needs to be clearly defined

Using connected smart building technology to monitor and improve facility energy usage now results in the collection of a significant amount of data. Success in cybersecurity management also requires collection of data from building IT and OT infrastructures. However, data ownership remains a challenge in building cybersecurity. Some data may encompass overall buildings systems, some may be specific to landlord/tenant relationships, some may be owner/occupant personal data, and some may be buyer/vendor data. One organization may have origination rights to data being collected by another. For instance, monitoring the use of building-wide systems like lighting and HVAC may reveal activities or identities of building users, thereby raising privacy concerns.

To trace the origins of suspected cyberattacks, security personnel from the end-user organization (e.g., a building tenant) will need access to logging data from the Internet access points that may be owned by another organization (e.g., a third-party IoT service provider). These data may not even be collected by the building owner and/or they may have some sensitivity (e.g., tracking movement of people using data from a security card access system). Security data collection is a mainstay of traditional IT security, but collection of these data from common OT systems is both difficult to accomplish and often legally ambiguous when it comes to establishing data ownership and sharing strategies. Collected data must be secured and access to it must be provided to any tenant whose security relies on it. However, it is quite uncommon for data sharing agreements to be established contractually or even informally. The recommendation of one Roundtable breakout group was that organizations that have a stake in collected data or in its use should participate in multi-organization agreements on information storage and disposition.

Collaboration and contracting are key for leased properties

In leased properties, OT systems such as elevators, fire alarms, HVAC systems, and associated smart building technologies benefit all tenants, and thus are managed by the building owner. Building-wide IT infrastructure is also often used by many different organizations that occupy the same shared building or site. While it is possible for tenant IT networks and privately owned OT infrastructure to connect to building-wide systems, this creates a converged system with shared vulnerabilities and risks that cross multiple organizational boundaries. Relationships among tenants, owners, and the vendors that support them via patching[7] and maintenance also complicate matters.

[7] *Patching* is the practice of implementing scheduled or ad hoc changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, and improving functionality, usability, or performance.

Standard business processes do not always span organizations effectively, and this can result in delays and ambiguous assignment of responsibilities. Thus, it is often not possible to get all relevant groups to answer to a single management team. Because of the intertwined and often complex relationships between building owners, tenants, and users, the group recommended that a regularly occurring cybersecurity forum for key building stakeholders may be an effective collaboration mechanism. This working group could include OT and IT, along with operations staff who are responsible for planning, installation, and maintenance of buildings systems. The group recommended that the forum would meet once a month and discuss what approaches are working, and where gaps and challenges exist.

Photo: Thor Swift/Berkeley Lab

In some cases, the group believed that legal instruments would be needed to delineate and enforce cybersecurity roles and responsibilities. For example, patching and maintenance of building-wide OT systems could be stipulated in lease contracts to protect building tenants/occupants from cyberattack. Roundtable breakout group participants believed that building owners should be responsible to implement minimum cybersecurity safety requirements for the good of all tenants. Existing infrastructure may not be ready to provide secure data transport to the stakeholders who need it. Thus, it is recommended that whatever entity owns the network infrastructure should provide data collection, provenance, and security for the users of that infrastructure regardless of their role (e.g., building owners, tenants, vendors).

The smart building technology supply chain is complex, immature, and fragmented

The adoption and delivery of cybersecurity best practices for smart building technologies is hampered by many of the same supply chain challenges that are generally present for emerging technologies in the buildings industry. For example, the value and need for cybersecurity is often not well understood by vendors and third-party service providers. A typical example cited by Roundtable attendees concerned patching and regular software and firmware updates. In IT circles, these are staple requirements, and vendors that do not supply free security updates and patches would be considered borderline negligent. But patching and free updates are much less common in OT practice. OT vendors do not generally support ongoing patch management and often make subscribers pay for the patching labor (rather than pushing out patches for end-user installations as part of an existing license). Further, patching older OT systems can have unexpected consequences; one Roundtable attendee cited an extreme example where an older system was patched and subsequently became inoperable. OT staff are motivated to open trusted remote access to OT infrastructures to their vendors for the purpose of maintenance and patching, but this can be problematic from an IT security standpoint. Standardized patch management for OT will require dialogue among OT and IT organizations and technology vendors.

In addition, the delivery process for smart building solutions typically has different parties specifying, designing, installing, and then maintaining the system. This can result in unclear roles and responsibilities when it comes to ensuring technology is installed and maintained correctly. Engagement with the smart building technologies supply chain (and key stakeholders) is highly complex but can be divided into three main phases: definition, delivery, and operations.

- **Definition phase:** In this step building owners (often working through their facilities teams and consulting engineers) seek to understand the respective value and cost of various levels of cybersecurity and effectively specify requirements. This often requires input from other functions (IT, legal, purchasing) to ensure that contract language is appropriate and IT policies are met.
- **Delivery phase:** Integrators need the capability to procure and deliver sufficiently secure systems and to ensure that features are not "value-engineered" out. Commissioning providers need to be able to verify that systems are installed and commissioned appropriately and meet cybersecurity requirements (cybersecurity is not in the typical skillset for a commissioning provider). For example, if default passwords and ports are not reconfigured, and if data recovery strategies are not created and tested, even the best designed cybersecurity protocols will not meet objectives.
- **Operations phase:** Operation of the newly installed technology is handed over to facility operators and service providers who are responsible for the final phase—ongoing management and maintenance of the system. These operators need sufficient training to maintain the system consistent with cybersecurity best practices (e.g., implementing patches, maintaining inventory, user credential management, detecting anomalous behavior) and having recovery plans in place that are regularly tested and reevaluated. To enable this, original equipment manufacturers (and tenant IoT technology providers) need to provide solutions that are secure and patchable, and have appropriate end-of-life management. Roundtable attendees emphasized that cybersecurity is an ongoing process; it is not simply a case of procuring "secure" technology and then forgetting about it.

Some attendees have developed cybersecurity specifications for new construction projects. This leverages the knowledge that assessing and mitigating risks at the design stage is far more efficient than having to address cyber issues in existing buildings with a complex mix of legacy equipment. For commercial real estate, assessing risk at the time of acquisition is a recommended best practice, and given that real estate transactions have a tight timeline and high concentration of resources, the addition of a cybersecurity risk assessment could be a relatively small incremental cost. Conducting a cybersecurity risk assessment for the first time in an existing building can be a daunting task, however, even with useful industry guidance documents. One fundamental challenge cited by roundtable attendees is to develop an accurate inventory of IP-enabled devices, without which it is hard to conduct a comprehensive risk assessment. Once initiated, risk assessments should be repeated regularly; one attendee recommended quarterly, though frequency will vary based on an organization's risk tolerance

Photo: Thor Swift/Berkeley Lab

profile and breadth of smart building technologies being implemented or explored.

A wide range of smart building technologies is available, including cloud-based analytics, IP-enabled building automation systems, light fixtures with embedded controls, occupant-centered mobile apps, and more. In many cases new technologies are offered by companies that have existed for only a few years; and even established OT system providers may be relatively new to the topic of cybersecurity. This lack of market maturity adds to perceived risk for an owner.

Financial value of cybersecurity is difficult to quantify

Roundtable attendees agreed that cybersecurity is a priority issue for organizations, since damage to reputation and brand if a breach occurs can have a material impact. However, the economics behind valuing cybersecurity when making purchasing decisions on smart building technologies are still difficult to quantify. Some attendees expressed that addressing cybersecurity depends on how much risk the company is willing to "buy down." For example, large technology companies are attractive cyberattack targets and have a very high reputation risk at stake, so there is no room for compromise or half-measures when implementing cybersecurity strategies. Similarly, a publicly traded real estate investment trust (REIT) is beholden to investor reporting and risk assessments, wherein regularly reporting on cybersecurity measures is required. However, for many organizations it is much harder to justify high expenditures on human resources and technology to address cybersecurity risks that have no dollar value.

Attendees reported that a risk assessment framework (examples provided in Appendix C) could allow organizations to budget cybersecurity measures accordingly. To help stakeholders better understand cost factors, it could be useful for an industry organization or researcher to collect cost data (and associated human resource costs) from leading organizations that have already implemented cybersecurity measures for smart building OT technologies, as a benchmarking exercise. In the future, established cybersecurity best practices should already be fully integrated into tested and certified connected technologies, reducing the additional time and money spent by individual organizations assessing and mitigating risks. This could be modeled on processes that have matured in the IT cybersecurity industries, as well as other industries that contain risk management elements; for example, fire safety and automobile safety.

Existing resources need to be tailored to the building industry

Attendees cited many existing industry resources that can support an organization's cybersecurity risk management needs, including the following:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Unified Facility Criteria
- Cyber Security Evaluation Tool (CSET®)
- TR60 Information and Communications Technology (ICT) Lifecycle Management

Even with established cybersecurity guidance it can still be challenging for a building owner to adapt the guidance to building-specific OT situations that suit their unique considerations. There is a need to understand how and when to select and integrate these various tools. Different

market segments are at differing maturity levels when it comes to standardizing approaches and requirements, and also in setting appropriate thresholds for risk tolerance.

Mapping and adapting these and other existing resources and best practices to the building domain and ensuring they are granular, meet a range of risk profiles, and are actionable would be of great value. Such resources could be graduated, allowing stakeholders to find the right entry level based on their current needs (e.g., risk profile) and maturity (e.g., education and implementation) level.

Example building domain cybersecurity resources could include the following (in approximate order of required effort):

- Education on basic cybersecurity challenges, vulnerabilities, and threats, and associated best practices applicable to building control systems
- Resources such as a buyers' guide to allow operators to prequalify smart building technology providers from a cybersecurity perspective (that is, how to be an informed buyer)
- Development of draft technical specifications that can be used when developing requests for proposals (RFPs) for energy efficient connected technologies
- Tools and resources to perform cybersecurity self-assessments and develop action plans
- Certifications specific to smart building cybersecurity

No single organization needs to be responsible for developing these resources. A key first step is to identify all relevant organizations in this space, and their respective roles, and determine how they can partner on development of these resources going forward. An impactful first deliverable would be to compile and disseminate a list of existing key resources (including communities of practice like RealComm, ASHRAE, and The Real Estate Information Sharing and Analysis Center [RE-ISAC]). To this end, Appendix C includes a list of resources identified at the Roundtable. Further work is warranted to more broadly identify existing resources and identify gaps in more detail.

Training needs to evolve as buildings and cyberthreats become more sophisticated

Cybersecurity training and certification for IT/OT staff with a focus on smart building technology is highly recommended to balance the need for facilities' availability with the equally important needs for data confidentiality and IT system integrity. Workforce training and education around cyber hygiene is critical, as human error and lack of awareness is often the weakest link in cybersecurity protection. Education around cybersecurity is a common interest among staff members, especially those with building operational roles. Most Roundtable attendees agreed that organizations have a responsibility to provide education and training for their employees as building systems become more connected, and cybersecurity should be a key component of that training. Attendees noted that security best practices are evolving quickly, and without regular training this evolution can leave employees behind and at risk for exposure. For example, multifactor authentication[8] has swiftly moved from an optional security strategy to a basic requirement.

[8] Multifactor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism, e.g., a correct password and answering a security question.

Photo: Thor Swift/Berkeley Lab

One suggested approach to increase training was to make government training currently in use by the U.S. Department of Defense (DoD), Federal Energy Management Program (FEMP), General Services Administration (GSA), and others available to private industry. Several Roundtable participants stated they would value access to established government programs for buildings under its purview. Of specific interest was training on how to implement IT networks that include OT management capabilities but isolate them from core enterprise systems.

Participants also recommended that cybersecurity training be tailored where possible for OT staff, recognizing that some staff are less familiar and comfortable with concepts around connectivity of physical objects, processes, and systems. Conversely, those with an expectation that "everything is connected these days," may not be fully aware of the cybersecurity ramifications of IP-enabled OT systems. Creating a standard certification for OT cybersecurity and devising a training regimen to support it would help ensure organizational cybersecurity readiness for connected OT.

There is a lack of testing standards and facilities

Today, few specifications and resources exist to test and evaluate the cybersecurity attributes of connected energy efficiency technologies. Roundtable participants stated that they typically have to test and assess the cyber capabilities of new technologies as part of existing technology implementation projects. Given the budget and schedule pressures of commercial real estate projects, this can greatly limit the risk tolerance of operators to adopt new energy efficient connected technology. If a technology does not initially meet a project's cybersecurity requirements this can result in significant delays; one attendee shared an example of this type of challenge, where the inclusion of a tenant comfort app delayed a building's occupancy by multiple months. This has significant negative financial implications and can hinder the future adoption of smart technologies.

Lack of OT cybersecurity testing standards and facilities presents a challenge that is similar in nature to that faced in the adoption of many advanced energy efficiency technologies: there is a need to demonstrate that new technologies work before risk-averse building owners will adopt them. For energy efficiency solutions, this challenge has been addressed by the independent evaluation of technology in laboratory settings and field demonstrations by trusted independent parties in collaboration with key stakeholders. During the roundtable discussion GSA detailed how it has a dedicated cybersecurity testing and evaluation program for devices. Once devices have passed these tests they are then approved for procurement by federal operators.
Industry would greatly benefit from a capability to collectively test the claims of smart building technologies (including cybersecurity capabilities) prior to their selection and specification in actual buildings. Roundtable participants noted the National Laboratories' experimental facilities

(for example, FLEXLAB®, and the Energy Systems Integration Facility [ESIF]) and discussed whether these could be extended to help define the requirements for cybersecurity assessment capability. Once fully defined, testing could be undertaken by traditional third-party testing entities.

One Roundtable attendee noted their use of Device Automated Qualification[9] (DAQ), an online coding-based resource that has recently been created as a framework to test and operate IoT devices in an enterprise IoT environment. DAQ is designed to help owners and vendors test cybersecurity of IoT devices, and also to develop and manage secure networks on which diverse IoT devices can run.

Conclusions

The Cybersecurity Roundtable resulted in a day of vibrant discussion on a topic that is key to spurring greater adoption of energy efficient smart building technologies like EMIS, advanced controls, and IoT devices. Attendees shared insights and examples to illustrate the range of building cybersecurity risks and possible mitigation strategies, and described a range of commercial sector cybersecurity management practices. With IP-enabled building controls becoming mainstream it is impossible to completely avoid cybersecurity risks for OT. All organizations need to develop cybersecurity strategies, even if they are not exploring newer cutting-edge IoT technologies and EMIS. (On the contrary, connecting older legacy systems has a unique set of challenges and risks to be managed).

Developing and implementing a successful OT cybersecurity strategy often requires the creation of new organizational roles and interdisciplinary collaboration models to ensure effective partnering between IT and OT groups as well as other key participants (such as legal and purchasing). Organizations also need to be cognizant of data collection, ownership, and protection considerations for OT technologies, particularly as they relate to privacy and cybersecurity monitoring. (This challenge is compounded in building environments where multiple legal entities may generate, own, or require OT data, such as tenant/landlord relationships.)

The ability of the building industry to deliver and maintain secure OT technology throughout its lifecycle is mixed, at best. Practitioners often do not know how to develop, specify, procure, install, commission, and maintain OT technology with sufficient cybersecurity features and processes in place. This is compounded by the inability of many organizations to determine how best to value investments in cybersecurity for OT systems, and where investments will show the best return in terms of risk management.

There is a wide array of useful resources and best practice examples for addressing cybersecurity risks in adjacent industries (e.g., IT and industrial control) that can help address the challenges above, but they need some work to be tailored to buildings, and to be accessible to more organizations in order to see best practice adoption become the norm. These resources, paired with robust training and certification, would provide a strong foundation for buildings' cybersecurity, taking account of the fact that cybersecurity is a continuous risk management process with human inputs, as opposed to a technological end state.

[9] GitHub. DAQ (Device Automated Qualification) framework for IoT devices. https://github.com/faucetsdn/daq

In the absence of clear standards and practices around building OT cybersecurity, the Roundtable demonstrated the strong desire of the building community to network and share best practices. Many organizations (such as the Real Estate Cyber Consortium, ASHRAE, and others) are working to educate and inform practitioners about cybersecurity issues and best practices. This knowledge sharing is important to address the needs raised above. Extending this work to more formal training courses and certifications would be very beneficial. However, these organizations rely on volunteers to drive key initiatives and develop resources, often limiting the rate of deployment. Seeking ways to support the acceleration and dissemination of this work would be extremely beneficial. In the meantime, organizations are forging ahead with varied approaches to address cybersecurity risks that can serve as best practice examples.

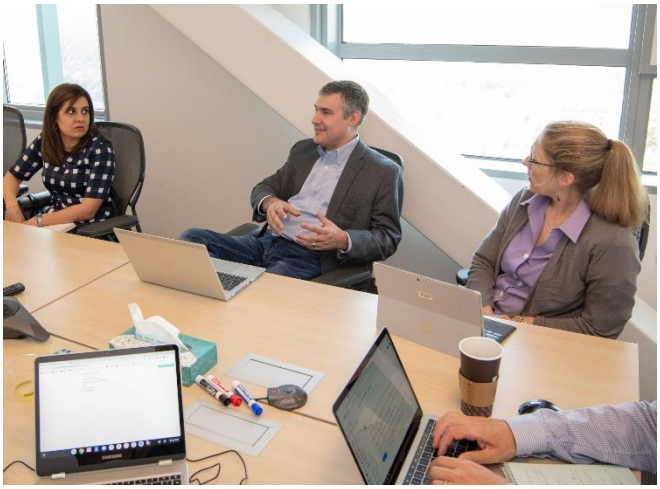

Photo: Thor Swift/Berkeley Lab

The NIST cybersecurity risk management framework identifies five classes of activity when addressing cybersecurity threats: (1) Identification, (2) Protection, (3) Detection, (4) Response, and (5) Recovery. It was notable that the majority of the Roundtable discussions centered on efforts to identify cyberthreats and protect against them, representing the first two NIST framework elements. The remaining three hardly surfaced at all in discussions. This emphasis serves to highlight the progress being made in the first two categories while also indicating the need to engage in more dialogue on the remaining three.

The U.S. DOE's technology development efforts are affected directly and indirectly by cybersecurity issues. For example, if DOE supports new connected technology development it should have cybersecurity considerations built into its full lifecycle. Indirectly, industry concerns about cybersecurity risks act as a barrier to all connected technologies. Suggestions for how DOE might address these types of barriers include the following:

- Development of standard cybersecurity policies and technical guidance for any DOE-funded technology development
- Publication of cybersecurity best practice case study examples of owners implementing smart building technologies, and gathering data for cost benchmarking purposes
- Collaboration with key industry groups to define specific standards and guidance needs, and to adapt existing guidance for connected OT applications
- Provision of cybersecurity training and guidance to labs offering market engagement campaigns that involve connected technologies
- Collaboration with GSA, DoD, and other public agencies to determine the applicability/ adaptability of training programs for broader market use
- Explore the possibility of using existing National Laboratory facilities as cybersecurity test beds

- Continuing market engagement with public agencies and beyond, particularly to better understand considerations and needs around cyberattack detection, response, and recovery
- Continue partnerships with industry leaders and key industry groups to understand evolving cybersecurity needs and barriers related to the adoption of smart, energy efficient technology

Based on the success of the Cybersecurity Roundtable, DOE may consider convening additional workshops and/or virtual working groups to address some of the topics raised above, or perhaps with a different target participant group, such as technology vendors.

Appendix A: Cybersecurity Roundtable Agenda

Date & Location: May 23, 2019 – Lawrence Berkeley National Laboratory
8:30 Continental Breakfast
9:00 Safety presentation
9:05 Session 1

- **Labs/DOE Introduction presentation (20 minutes):**
    - Historical and current DOE thinking relating to cybersecurity. Summarize objectives and expected outcomes for the Roundtable
    - Brief presentations by Labs to summarize the types of work they're doing, and how that work intersects with the cyber topic
    - Summarize key findings from pre-event survey
    - Cyber overview, to breakdown the components of what we mean when we say 'cybersecurity for operational technology'

- **Attendee introductions (~35 minutes)**
    - Name and organization, and one thing their company is doing to address cyber-risks related to operational technologies

What's going on: Whole Group discussion (~35 minutes)

- Facilitated discussion exploring the current level of "normal practice" and experience around cyber.

10:30-10:50 MORNING BREAK

10:50 Session 2: Breakout groups

- Breakout groups will explore the gaps and challenges faced within each of the breakout group categories, e.g. lack of priority / buy-in, lack of resources, training needs, unaware of practical guidance, etc.
- Note-taking using the 5 NIST risk management framework elements

11:50-1:00 LUNCH & CYBER-SIMULATION GAME (See Appendix B)
Attendees divided into 4 groups for cyber-sim game

1:00 Cyber-sim game report out

1:15 Session 3: Breakout Groups Report-Out & Discuss

- Group representative will report out findings followed by feedback/questions from all attendees.
    - Optional:
        - Identify the top 3-5 insights within that breakout category.
        - Distinguish in quadrants based on cheap/expensive and short-term/long-term

2:45 - 3:05 AFTERNOON BREAK

3:05 - 4:15 Session 4: All-Group discussion, wrap-up, and next steps (Eliot facilitate, Hannah take notes)

- Organizers report out their key takeaways from the day's discussions, with respect to DOE/labs R&D
- Facilitated discussion
    - Key takeaways and priority next steps for attendees
    - Most valuable insights they've taken from the day

Appendix B: Cybergame

Introduction to the Cybergame

As a lunchtime activity, the participants played a cybergame where teams of attackers and defenders role-played a fictitious scenario (Table B-1). During the game each attacker and defender team independently determined how best to allocate their resources to various strategies to achieve their goals. These were documented and at the end of a round were evaluated by a judge to determine which attacks would defeat the proposed defenses and whether they would be sufficient to achieve the stated objectives.

Outcomes from the Cybergame

This game was intended to be just for fun, but the solutions provided by the participants showed some issues that they were seriously concerned with. Many practitioners use similar "tabletop" exercises to bring new thinking to their cyber posture as well as to evaluate their response and recovery plans.

One major recurring theme was the danger of deception. The attacker teams proposed elaborate systems of ruses within ruses to misdirect the defenders' efforts at identifying or stopping the attack. The deceptions listed included phishing and spear-phishing attacks, hired groups of humans doing demonstrations, fake facilities, sensor deception, and malware attacks.

Of course, the attacks chosen were influenced by the scenario. For instance, most attacks involved harming and deceiving cyber-physical infrastructures, and none really included data loss prevention. This makes sense since the fictitious defender was a manufacturing concern without much public exposure or personal data storage. However, the fear of social engineering attacks and deceptions certainly would extend to protecting personal data assets.

Table B-1: Cybergame scenario

Defender
Your team, the administrators of KavaCorp's IT and OT networks, have received information that pro-caffeine activists intend to disrupt your product launch of bedtime decaffeinated coffee products. You are responsible for the IT (including the web presence) of the corporation and IT and OT infrastructures for over a dozen coffee processing and packaging plants across the Pacific Northwest. You must keep your product delivery on schedule for your customers and not allow attackers to tamper with your product's caffeine levels or quality. You have the support of law enforcement; however, they are not known for quick or sophisticated responses, so act accordingly. **Goal**: Ensure that there is less than 6 hours of downtime across the entire system and that the product is not tampered with. **Secondary Goal:** Be able to identify your attacker to the degree that law enforcement can find them when they get around to it. Identification without prevention is only a partial success. **Anti-goals**: Don't kill anyone. **Resources:** Team of 30 personnel, 1M USD, 1 month preparation time **Assumptions:** KavaCorp is a large manufacturer and wholesale industry specializing in its own brand name coffees. It does not have any retail outlets, but its factory operations span a multi-state region in the Pacific Northwest and its corporate offices are in Washington state.
Attacker
KavaCorp, the nation's leading provider of delicious caffeinated drinks is abandoning its consumers and reducing the caffeine in its products! Your team, the Anti-Decaffeination Directive (ADD), must stop the launch of KavaCorp's new line of bedtime coffees and deliver a message of your own – safe mental stimulation for all! Also, you wish to ensure that your group's message is broadcast more loudly than the product announcement, so defacing KavaCorp's website is a good place to start. **Goal**: Disrupt KavaCorp's decaffeination plant operations and its corporate office buildings. Extra points if you can force KavaCorp's plants to *increase* caffeine levels in its products! **Secondary Goal:** Make a public statement declaring the criticality of caffeine to modern society and claiming responsibility; a public statement without disrupting KavaCorp's business operations is only a partial success. **Anti-goals**: No harm done, or possibly done, to any human or animal. **Resources:** Team of 30 personnel, 1M USD, 1-month preparation time **Assumptions:** KavaCorp is a large manufacturer and wholesale industry specializing in its own brand name coffees. It does not have any retail outlets, but its factory operations span a multi-state region in the Pacific Northwest and its corporate offices are in Washington state.

Appendix C: Summary of Cybersecurity Resources

A number of cybersecurity resources were identified during the planning of this event and during discussion at the Roundtable. They are provided here to aid the reader. This is in no way to be considered a complete or comprehensive resource list:

Federal Resources

1. NIST, Security and Privacy Controls for Information Systems and Organizations, SP 800-53-r5: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft
2. NIST, Guide to Industrial Control Systems (ICS) Security, SP 800-82-r2: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
3. NIST, Cybersecurity Framework Manufacturing Profile, NISTIR.8183: https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile
4. DHS-NCCIC, ICS-Cert Website: https://ics-cert.us-cert.gov/
5. DHS, Cyber Security Evaluation Tool (CSET®): https://cset.inl.gov/SitePages/Home.aspx
6. DOD-ESTCP, Cybersecurity Facility Related Control System: https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity
7. DOD-Unified Facilities Criteria (UFC), Cybersecurity Of Facility-Related Control Systems, UFC-4-010-06: https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06
8. DOD-Unified Facilities Guide Specifications (UFGS), Cybersecurity of Facility Related Control Systems, UFGS 25 05 11: https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11
9. DOD, Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DOD Installations: http://www.wbdg.org/files/pdfs/ics_handbook.pdf

Industry Best Practices and Guidance

1. The Real Estate Cyber Consortium (RECC), Best Practices Documents: http://re-cc.com/
2. Google, Application Security Requirements for IoT Devices: https://partner-security.withgoogle.com/docs/iot_requirements
3. Microsoft, Seven Properties of Highly Secure Devices: https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf

Industry Organizations:

1. The Real Estate Cyber Consortium (RECC): http://re-cc.com/
2. The Real Estate Information Sharing and Analysis Center Group (RE-ISAC): https://www.reisac.org/