Appendix

Glossary

Automated Demand Reduction	Automated Demand Reduction systems are used to communicate signals from utilities to energy-using devices that cause them to turn off during high demand periods.
Automated Fault Detection	Also known as automated fault detection and diagnostics (AFDD). Software designed to identify the presence of a fault in equipment before it manifests into a physical breakdown of the system.
BACnet	Building Automation and Controls Network, a standard data communications protocol for building systems.
Battery Energy Storage Systems	Devices that can be charged with energy and stored for later use.
Building Energy Codes	Minimum energy efficiency requirements for new and renovated buildings to reduce energy use and emissions over the life of the building.
Building Management System (BMS)	Also known as a Building Automation System (BAS). A computer-based control system that can be used to monitor and manage the mechanical, electrical and electromechanical services in a facility.
CHP or CHPC	Acronym for combined heat and power (and cooling).
Controller	A piece of equipment that controls the operation of an electrical device.
Cybersecurity	Prevention of damage to, protection of, and restoration of digital informational and/or data systems from unauthorized access, use, disclosure, disruption, modification or destruction.

Cybersecurity Framework Core	A set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.
Cybersecurity Framework Elements	Identify, Protect, Detect, Respond, Recover
Cybersecurity Risk	Risk of financial loss, operational disruption or damage, resulting from failure of the digital technologies employed for informational and/or data systems via electronic means from the unauthorized access, use, disclosure, disruption, modification or destruction of the system.
Data Analytics	The collection, transformation, and organization of data in order to draw conclusions, make predictions, and drive informed decision making.
Data Logging	The process of collecting and storing data over a period of time in different systems or environments.
Daylight Harvesting	An energy-saving technique using sensor-based controls to automatically dim or adjust the brightness of electrically-produced light in response to the amount of incoming natural light into a building from the outdoors.
Demand Response	A utility strategy used to balance the demand on power grid by encouraging customers (usually via monetary incentives) to reduce electricity consumption during times of peak use, or to shift use to times when electricity is more plentiful or other demand is lower.
Demand Timing Mismatch	When the inventory of a product either surpasses or does not sufficiently meet the consumers' desire of a product. Excessive solar or wind power generation is an example, fairly common due to the variability of production inherent to these technologies.

Denial of Service (DOS) Attack	A malicious cyber attack that renders legitimate users unable to access an information system, device, or other network resource.
DER or DERS	An acronym that stands for Distributed Energy Resources, which refers to localized energy generation systems found at or near the energy loads they serve.
Diagnostics	The practices or techniques of diagnosing a problem.
Digital Lighting System	Lighting that is controlled by a digital control system connected via WiFi or digital low-voltage wiring, allowing centralized control and often capable of features like scheduling, dimming and/or color temperature adjustments.
Digital Networks	Physical networks that have switching and transmission components connected by servers.
Dimming (Controls)	Reducing the lighting output of the fixture or lamp.
Direct Digital Control (DDC)	Computer-based, automated control of a device or system of devices. DDC enables centralized control of a building's various mechanical and/or electrical systems, including HVAC, lighting, security, etc.
Distributed Power	Also known as distributed energy, or distributed energy resources (DER). Technologies which generate electricity at or near the site where it will be utilized. Examples of distributed power systems include solar photovoltaic panels and wind turbines.
Economizer Control	A mechanical system that uses outside air to help control indoor temperatures, which can achieve higher energy efficiency for a building by avoiding costly mechanical conditioning.
EEM	An acronym for energy efficiency measure.

Energy Information System (EIS)	Comprised of web-based software, data acquisition hardware, and communication systems that collect, analyze, and store building energy consumption data.
Energy Load	An electrical component or portion of a circuit that consumes (active) electric power, such as electrical appliances and lighting.
Energy Management System (EMS)	A system of software and hardware tools that monitor, analyze, and control building energy use and system performance. Also referred to as Energy Management Information System (EMIS).
Energy Storage	The capture and storage of energy for use at a later time.
Ethernet	A technology capable of connecting various computer systems within a local area to form a network for sharing information back and forth.
Fault Detection	The process of discovering the presence of a fault in any equipment, ideally before it manifests itself in the form of damage due to a failure.
Firewall	In the context of computer systems, a computer network security device that restricts data communication traffic to and from two connected networks, protecting against potential cyberattack threats.
Generation (Electricity)	A process of transforming other forms of energy to produce electricity. Some examples of common energy sources for electrical generation are fossil fuels, solar, wind, and nuclear.
Grid	An interconnected network of power transmission equipment for delivering power from producers to consumers.

Grid-Interactive Efficient Buildings (GEB)	Buildings that can provide the load flexibility that the modern electrical grid requires for reliable operation. Key characteristics for GEB are that they are efficient, connected, smart, and flexible.
Grid Flexibility	The ability for the electrical grid to adapt and adjust to varying supplies of energy from both constant and fluctuating sources of generation while meeting consumption needs at any given time.
Grid Responsiveness	How quickly the grid can adjust to the supply and demands of the grid.
Human-Machine Interface (HMI)	The hardware or software interface that an operator uses to interact with a controller. Sometimes referred to as a dashboard.
HVAC	Acronym for heating, ventilation and air conditioning.
Integrated Building Systems	The integration of various different systems in a building, such as mechanical, lighting, life safety, and security, by utilizing software to allow seamless communication regardless of differences in formats or protocols between the systems.
Internet of Things (IoT)	A network of physical devices embedded with sensors, software, and other technologies and interconnected with each other via the internet, which allows for data exchange.
ISO	An acronym for independent system operator, an independent organization that handles grid operations and energy market facilitation.
Lighting Control System	A central computing system that facilitates communication between various inputs (e.g. sensors) and output controls (e.g. switches, dimmers) to control lighting conditions within a building.

Load	Any component of a system that consumes energy.
Load Shedding	A strategy enacted when demand strains the capacity of a power distribution system that involves interrupting electrical delivery in part of the system in order to prevent an outage of the whole system.
Load Shifting	Load shifting is an electrical load management practice which shifts load demands from peak hours to off-peak hours.
Machine-in-the-middle attack (MiTM)	Also known as "man-in-the-middle" or "on-path" attacks. A form of cyber attack in which the attacker intercepts and modifies data to pose as one or more legitimate entities in a communication.
Malware	Software, firmware, or hardware that is secretly inserted into a system for a harmful purpose.
Microgrid	A group of interconnected loads and distributed energy resources that acts as a single controllable entity, which is able to connect or disconnect from the grid (grid-connected or island mode, respectively).
Modern Energy Grid	An interconnected network for electricity delivery from producers to consumers, enhanced with computer processing technology. This enables two-way communication between control systems to facilitate increased reliability and resiliency in accommodating fluctuating supply and demand.
Motion Sensing	Utilizing input from a motion sensor or sensors to control equipment, commonly lighting.
Occupancy Control	A sensor-based system used to detect the presence of a person to control lights, temperature and other equipment.

Optimal Start Controls (HVAC)	Also known as optimum start/stop control, this control strategy uses an algorithm to calculate the timing needed to bring a space to the desired temperature. The system delays the start-up of space conditioning equipment and initiates shut down as soon as possible to meet the desired temperature during occupied hours while reducing energy consumption of HVAC equipment.
Photocell	A sensor that changes its resistance when light shines on it.
Photovoltaic (PV)	A technology that produces electrical current with exposure to light.
Plug and Process Loads (PPL)	Building energy loads that are not related to lighting, HVAC, and/or cooking activities.
Plug Load	The energy used by devices powered by plugging into an electrical receptacle using A/C power.
Plug Load Control	Plug load control is the ability to use energy saving efforts to automatically discontinue power to designated plug loads when a space is not in use.
Power (electric)	The transfer of energy within a circuit.
Ransomware	A type of malware designed to render files and systems unusable until the victim pays the attacker a ransom.
Remote Accessibility	The ability for users to access control of a device or network remotely from any location.
Renewable Energy Resources	Sources of energy production, such as wind and solar, that are naturally replenished and do not run out.
Sensor	A device that detects or measures a condition (e.g. temperature or light) and communicates information about the condition to a controller.

Smart Building	A classification of buildings that are equipped with technology-based systems, typically integrated with each other, to deliver a building environment that is safe, efficient, comfortable, high-performing, and sustainable.
Smart Meter	Meters equipped with the ability to measure, record, archive, and report energy or water consumption using established digital communication protocols over wired or wireless media.
Smart Plug (Smart Outlet)	An electrical receptacle that is individually addressed within a network and can be integrated with the smart building's energy management or lighting systems to control the flow of electricity to connected devices and equipment.
Software	A set of instructions, data or programs used to operate computers and execute specific tasks.
Spyware	Software that is installed in a system without the legitimate user's knowledge, for the malicious purpose of gathering information that can then be used to exploit valuable assets.
Task Lighting	Provides increased light for a specific task in a room that already has minimum ambient light for the space.
Thermal Comfort	The condition of the mind that expresses satisfaction of the environment, which is assessed by subjective evaluation.
Thermal Sensing	The process of utilizing sensors to track temperature changes in an environment.
Thermostat	A device that automatically regulates the temperature of a conditioned space by using thermal sensing control HVAC equipment.
Trojan horse	Software that appears to have a legitimate function but also secretly has a malicious function or functions.

Variable Energy Source	An energy source that is not consistently available; for example solar (not available when the sun is down) or wind (not available when the wind doesn't blow).
Window Shading System	A system utilizing shading devices on windows that minimize solar radiation coming into a building when it is not desired, but can allow solar gain when it is desired.
Zero Energy Building	A building equipped with smart technologies to achieve high energy efficiency and renewable energy to offset energy used from the grid, resulting in net-zero energy use from the grid. Also known as a net-zero energy building.

Cybersecurity Resources for Smart Building Technologies

Sections:

Introduction

According to a recent report by the US Department of Energy Pacific Northwest National Laboratory:[1]

- Around half of all US commercial buildings have devices exposed to the internet.
- 95 percent of sites do NOT have a disaster recovery plan.
- It is likely that nearly 40% of BMS (Building Management System) servers in US buildings have been targeted by malware, phishing scams or ransomware.

"According to a 2019 report from Kaspersky, 37% of the computer systems used to control smart buildings were subject to some form of malicious attack in the first half of 2019. In most cases, computers that control BAS were compromised."[2]

Potential areas of risk:[2]

- Poorly protected IoT devices, such as IP security cameras, especially when integrated into legacy systems
- Insecure passwords (including passwords shared among multiple people, passwords posted near the equipment, not changing passwords from the default upon installation, etc.)
- Software vulnerabilities and errors.
- Non-encrypted communication.
- No authentication for connected devices
- Outdated software (attackers often target vulnerabilities that have been fixed or patched in later versions)
- Lack of (or improperly configured) security features such as firewalls, network security monitoring, and/or access controls (internal and remote, including poor port security).
- Integrating older or legacy systems with poor security protocols into the wider network
- Poor management control of vendor access, third party maintenance, and other third parties that access the BAS.

- Connectivity to wider organizational systems such as financial, procurement, maintenance, asset management, and other corporate systems.
- Connectivity to the wider internet (including secure websites and web/email messaging).
- Rapid changes in technology. For example, the increasing use of 5G technology in the smart building market comes with new risks linked to larger and faster data flows and how building automation networks are structured for security.
- Human vulnerabilities and errors:[3]
    - Working remotely using a computer on an unsecured network
    - Clicking on a link containing malware
    - Using insecure passwords

Notes on IoT Devices[3]

(From article *The Cybersecurity Threats Facing Smart Buildings* by Chester Avey, published on Facility Manager Advisor website)

"For smart buildings to function effectively they rely on a multitude of IoT devices to communicate with each other. However, all it takes is one compromised IoT device for hackers to get in, and it could take months before any malware they have used is detected. Fifty-seven percent of IoT devices are vulnerable to medium- or high-severity attacks, making them low-hanging fruit for attackers.

IoT devices are common appliances that you might even find around your home but that are connected to the internet. Examples of IoT devices include doorbell cameras, smart meters, fitness trackers, smart speakers, and connected cars. An unprotected device is like leaving the backdoor open or a key under the mat."

How To Plan Cybersecurity for Smart Buildings

The following is an excerpt from an article by Laura Osburn and Chuck Benson, published on FacilitiesNet.com, addressing procurement and operations aspects of smart building technology:[4]

"***Procurement:***

- Articulate, document, and propagate owner cybersecurity criteria for IoT devices and systems in the built environment. Establish governance, roles, and responsibilities with IoT as well as criteria to assess vendor risk.
- Require cyber liability coverage from the IoT systems provider. Establish who will be responsible when a system or device is compromised by a malicious group.
- Require a device software update plan (i.e., 'patch plan') and establish who will perform it and pay for it.
- Integrate cybersecurity reviews and IT Subject Matter Experts earlier in the procurement process.

Operations:

- Establish governance of IoT systems for networks, devices, and data. Strongly consider collaborative forms of IoT systems governance between IT and facilities that includes systems and network expectations and performance.

- Clarify roles and responsibilities of IT and facilities professionals working together on specific tasks. Know who is responsible for specific systems and equipment and know how to contact that person. Responsible-Accountable-Consult-Inform (RACI) charts are one example of a tool used to establish roles and responsibilities and to set expectations across multiple organizations.
- Establish and maintain relationships between IT and facilities departments and personnel through cross-departmental planning meetings, interorganizational liaisons, and informal activities such as brown bag lunches. This builds trust and begins to blend and integrate organizational cultures.
- Consider developing Operational Technology (OT) teams that blend traditional facilities and IT professions and approaches. “

Cybersecurity Standards

The following are excerpts from an article by Richard Miller, published by BuildingsIOT.com:[5]

“IoT Cybersecurity Standards for Smart Buildings:

The IT security standards series ISO 27000 and IEC 62443 are the two most common international cybersecurity standards series used for IT and OT networks in smart buildings. Stakeholders in smart building environments need to ensure that the equipment and processes used for building automation and control meet these standards to avoid security breaches.

ISO 27000

The ISO 27000 series includes 60 sub-standards for information security management systems. The series provides specific cybersecurity guidelines for smart building equipment including:

- Digital controllers and automation components such as sensors
- Building energy management systems
- Distributed components of smart grid environments such as energy grids
- Remote maintenance platforms for building systems

IEC 62443

The IEC 62443 standards focus especially on security risks to OT networks, including those in smart buildings. The series outlines specific technical requirements for building automation systems with which service providers should comply and provides guidance for manufacturers of automation components.”

Cybersecurity Best Practices[5]

"Best cybersecurity practices in smart buildings include:

- ***Use Zero Trust approach:*** All internal and external users, devices, and applications must be verified before access is granted.
- ***Inventory control networks:*** Periodically scanning the building's control networks helps identify unknown devices that may pose a risk.
- ***Create unique user accounts:*** Unique user accounts are essential for tracking user activities.
- ***Implement least privilege access*****:** User access should be controlled according to the principle of least privilege, which states that users should only be given the level of access necessary to do their jobs.
- ***Monitor network traffic:*** Along with monitoring frontend/application servers, network traffic should be monitored to detect any unusual device-to-device traffic.
- ***Document response plan:*** A well-documented and practiced response plan that clearly defines the roles and responsibilities of stakeholders can minimize the impact of a cyberattack.
- **Develop a recovery plan:** A majority of cyberattack victims do not have viable system backups in place. Developing a sound strategy for data backup can help you recover critical building data in the event of a security breach. "

Other Cybersecurity Resources

Cybersecurity & Infrastructure Security Agency
https://www.cisa.gov/

National Institute of Standards and Technology (NIST)
Computer Security Resource Center
https://csrc.nist.gov/

Challenges and Opportunities to Secure Buildings from Cyber Threats
Reeve, H., Gourisetti, S. N. G., McKenzie, P., Hagerman, J., Nicholls, A., Mylrea, M., Ehrlich, P., Fink, G., Vrabie, D., Glantz, C., & Underhill , R. (2020, March). *Challenges and Opportunities to Secure buildings from Cyber Threats – Pacific Northwest National Laboratory*. U.S. Dept. of Energy Building Technologies Office.
https://www.energy.gov/eere/buildings/articles/challenges-and-opportunities-secure-buildings-cyber-threats

Cybersecurity: How Safe is Your Building?
Nguyen, A., Yan, Q., Aliento, W., & Aski, P. (2023, March 1). *Cybersecurity: How Safe Is Your Building?*. Cundall. https://cdn.cundall.com/uploads/documents/Cyber-Security-How-safe-is-your-building-web.pdf?v=1677667266

Citations

1. Reeve, H., Gourisetti, S. N. G., McKenzie, P., Hagerman, J., Nicholls, A., Mylrea, M., Ehrlich, P., Fink, G., Vrabie, D., Glantz, C., & Underhill , R. (2020, March). *Challenges and Opportunities to Secure buildings from Cyber Threats – Pacific Northwest National Laboratory*. U.S. Dept. of Energy Building Technologies Office. https://www.energy.gov/eere/buildings/articles/challenges-and-opportunities-secure-buildings-cyber-threats
2. Beh, C. R. P. (2022, November 23). *Smart and intelligent buildings: Cybersecurity considerations*. Marsh. https://www.marsh.com/uk/services/risk-consulting/insights/smart-intelligent-buildings-cyber-security-considerations.html
3. Avey, C. (2022, December 6). *The Cybersecurity Threats Facing Smart Buildings*. Facilities Management Advisor. https://facilitiesmanagementadvisor.blr.com/building-controls/the-cybersecurity-threats-facing-smart-buildings/
4. Osburn, L., & Benson, C. (2023, May 2). *How to Plan Cybersecurity for Smart Buildings*. Facilitiesnet. https://www.facilitiesnet.com/security/article/How-to-Plan-Cybersecurity-for-Smart-Buildings--19850
5. Miller, R. (2022, June 21). *Why Smart Building IOT Cybersecurity Standards Are Important*. Buildings IoT Blog. https://www.buildingsiot.com/blog/why-smart-building-iot-cybersecurity-standards-are-important-bd