Cybersecurity

Barrier Description: Cybersecurity refers to risks associated with digital technologies for building energy efficiency relying on internet connections and computer networks. All digitally connected devices are at risk for attacks, from building management systems to smart appliances.

Phase 1: *Planning and design of cybersecurity frameworks*		**Phase 2:** *Pilot-scale implementation of cybersecurity frameworks and "security by design"*		**Phase 3:** *Continued maintenance of cybersecurity frameworks for wide-scale deployment*	
Challenges	**Practices**	**Challenges**	**Practices**	**Challenges**	**Practices**
A single set of technical security standards may not be implementable by all digitally connected devices and tools: Security standards should be adequately flexible and allow for various technical implementations [1].	**Create and use protection profiles** [1].	**Smart meter functions might accidentally result in energy supply disruptions that affect operations within buildings:** Unintended consequences and malfunctions should be avoided [1].	**Set a minimum service level/set of functionalities that must be met by business operators and ensure their security framework allows this level to always be met** [2].	**Security incidents, implementation problems, needs for updates, and/or data leaks may occur:** Cybersecurity planning and implementation should be a continuous, iterative process [1].	**Implement continuous improvement for threat and leak monitoring** [2]. **Require secure software updates** [1]. **Certify software updates before implementing** [1]. **Certify hotfixes after implementing** [1]. **Encourage manufacturers to show ability to update software without replacing hardware** [1].
Security standards may be decentralized and vary between manufacturers: Security standards should instead be centralized and uniform [1].	**Create a rigorous federal certification process that includes annual surveillance audits and recertifications** [1].	**Connected devices and networks can serve as access points for attackers:** Safeguards should be enacted to prevent connected devices and networks from being access points to other devices and systems in the building [3].	**Practice secure design** [1]. Separate internal and external connection networks [1] [2]. **Monitor external communication logs** [2]. For external connection providers, **assign responsibility to report incidents and conduct risk assessments** [2]. **Use certified smart meter gateways** (SMGWs) as the communication platform [1]. **Encrypt communication channels** [1].	**Consumers are concerned about third-party theft of their data:** Consumers should be able to have confidence that their data is protected from unauthorized third parties [1].	**Use electronic identifiers and allow only known participants/devices to access data** [1]. **Use public key infrastructure for data sharing to enable mutual authentication** [1]. **Encrypt communication channels** [1]. **Secure communication paths cryptographically** [1].

Key Objectives

- Secure operation and data transmission. Vulnerabilities, according to the United States Department of Homeland Security, are physical features or operational attributes that render an entity open to exploitation or susceptible to a given hazard. Connected devices and networks, which can be infiltration points, should be secured and data transmission should occur in a manner that mitigates risk of a cyberattack on a building or building system occurs.
- Incorporate security into all digitalization tool lifecycle phases. Technical and regulatory decisions can be impactful across sectors and shape market design. To reduce unintended consequences and unaddressed security concerns, cybersecurity awareness should begin with policy planning and the design of digitalization tools, consider future technology developments and needs, and continue through all remaining phases of the policy and tool life cycles.

Description of Phases

Phase 1: *Planning and design of cybersecurity frameworks*

Design of cybersecurity protocols are challenging due to the variable nature of devices and technologies which make it difficult to implement universal standards. Developing approaches to cybersecurity design, including protection profiles and a rigorous certification process are key to building effective cybersecurity frameworks.

Phase 2: *Pilot-scale implementation of cybersecurity frameworks and "security by design"*

Smart meters and connected devices can be points of vulnerability for cybersecurity attacks. Coupling policy with technological development (cybersecurity by design) can lower risk associated with these points of vulnerability.

Phase 3: *Continued maintenance of cybersecurity frameworks for wide-scale deployment*

At the large-scale level, there must be a variety of initiatives to monitor security breaches and appropriately respond to them. Cybersecurity frameworks must be dynamically updated to respond to threats in real time, requiring innovations in both technology and policy.

Examples cited in the report and other sources:

[1] Germany: Act on Digitalisation for the Energy Transition (Report section C.4)
[2] Japan: Next-Generation Smart Meter Study Group Summary (Report section C.5)
[3] Cybersecurity barrier (Report section 4.2)