BUILDING INNOVATION
Conference

Enhancing Cyber Safety for National Critical Infrastructure

A Call to Action for a Cyber Safety Engineering Standard of Care

Lucian Niemeyer, F. SAME
CEO, BuildingCyberSecurity.org

BUILDING INNOVATION
Conference

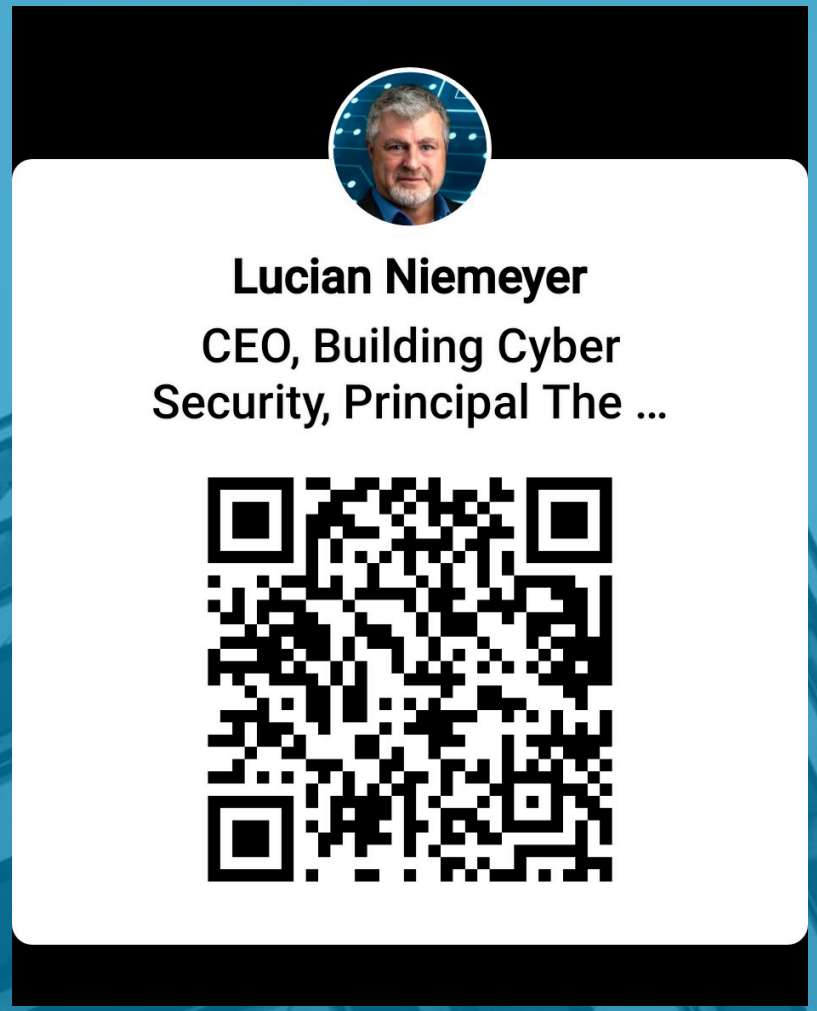
Former Asst Secretary of Defense (Installations, Energy, Environment)

Former White House Office of Management and Budget

Former staff of U.S. Senate Armed Services Committee

National Expert on Cybersecurity and Energy Issues

Fellow in the Society of American Military Engineers: Member of the National Academy of Construction and Association for the Improvement of American Infrastructure



Enhancing Cyber Safety for National Critical Infrastructure

Learning Objectives: AIA 1.0 HSW ICC 0.1

- Discuss essential cyber safety concepts
- Establishing frameworks for a standard of care for cyber safety in buildings and infrastructure
- Apply cyber safety practices to mitigate risk to life, safety, and health
- Foster productive collaboration with IT and cybersecurity experts to protect buildings and infrastructure against threats

2025 Cyber Threat Headlines

Jan 13 - Outgoing FBI director calls China and its cyber program the ‘defining threat of our generation’

Typhoon Series - China’s cyber program has already infiltrated critical American infrastructure and is poised to “wreak havoc” at a whim. Beijing has targeted water treatment plants, the electrical grid, natural gas pipelines, telecommunications and other systems. China has already pre-positioned malware to “lie in wait on those networks,” where it can “inflict real-world harm at a time and place of their choosing,” – CBS 60 Minutes interview

Feb 14 - Russian hacking group targets critical infrastructure in the US, the UK, and Canada

Seashell Blizzard - Active since 2021 - Obtaining access to targets including energy, oil and gas, telecommunications, shipping, arms manufacturing, in addition to international governments. Since early 2024, the subgroup has expanded its range of access to include targets in the U.S and UK – Microsoft Report

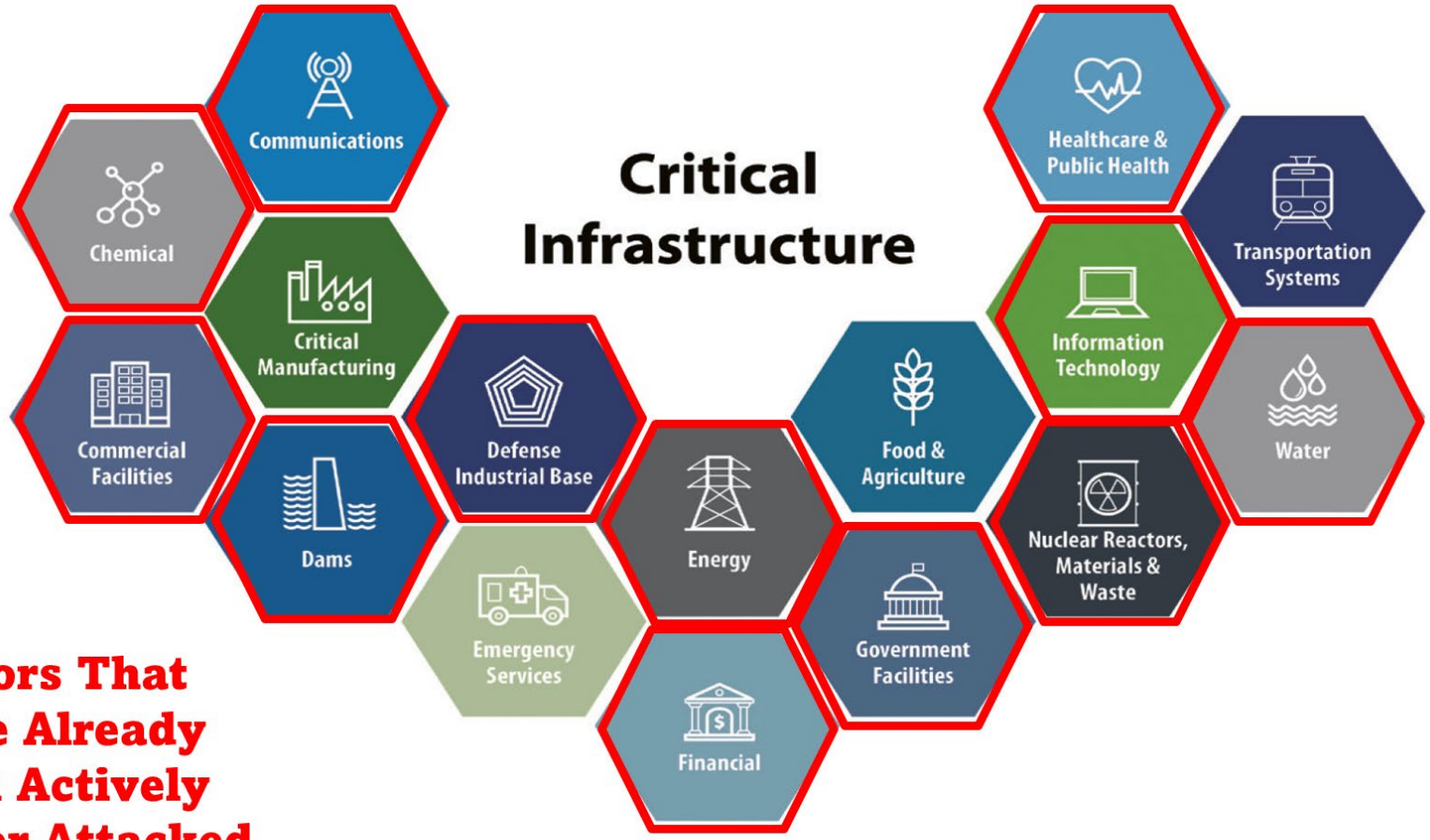
What the Experts Said in Congressional Testimony

“China’s hackers are positioning on American infrastructure in preparation to **wreak havoc and cause real-world harm to American citizens and communities**, if or when China decides the time has come to strike.. Let’s be clear: **Cyber threats to our critical infrastructure represent real world threats to our physical safety**.”

"Imagine not one pipeline, but many pipelines disrupted and telecommunications going down so people can't use their cell phone. People start getting sick from polluted water. Trains get derailed. Air traffic and port control systems are malfunctioning,“

“We are no longer discussing hypotheticals – China’s action, “**is the cyberspace equivalent of placing bombs on American bridges, water treatment facilities, and power plants.**.There is no intelligence gathering rationale. **The sole purpose is to be ready to destroy American infrastructure,** which will inevitably result in mass American casualties.”

Bad Actor Targets



Sectors That Have Already been Actively Cyber Attacked

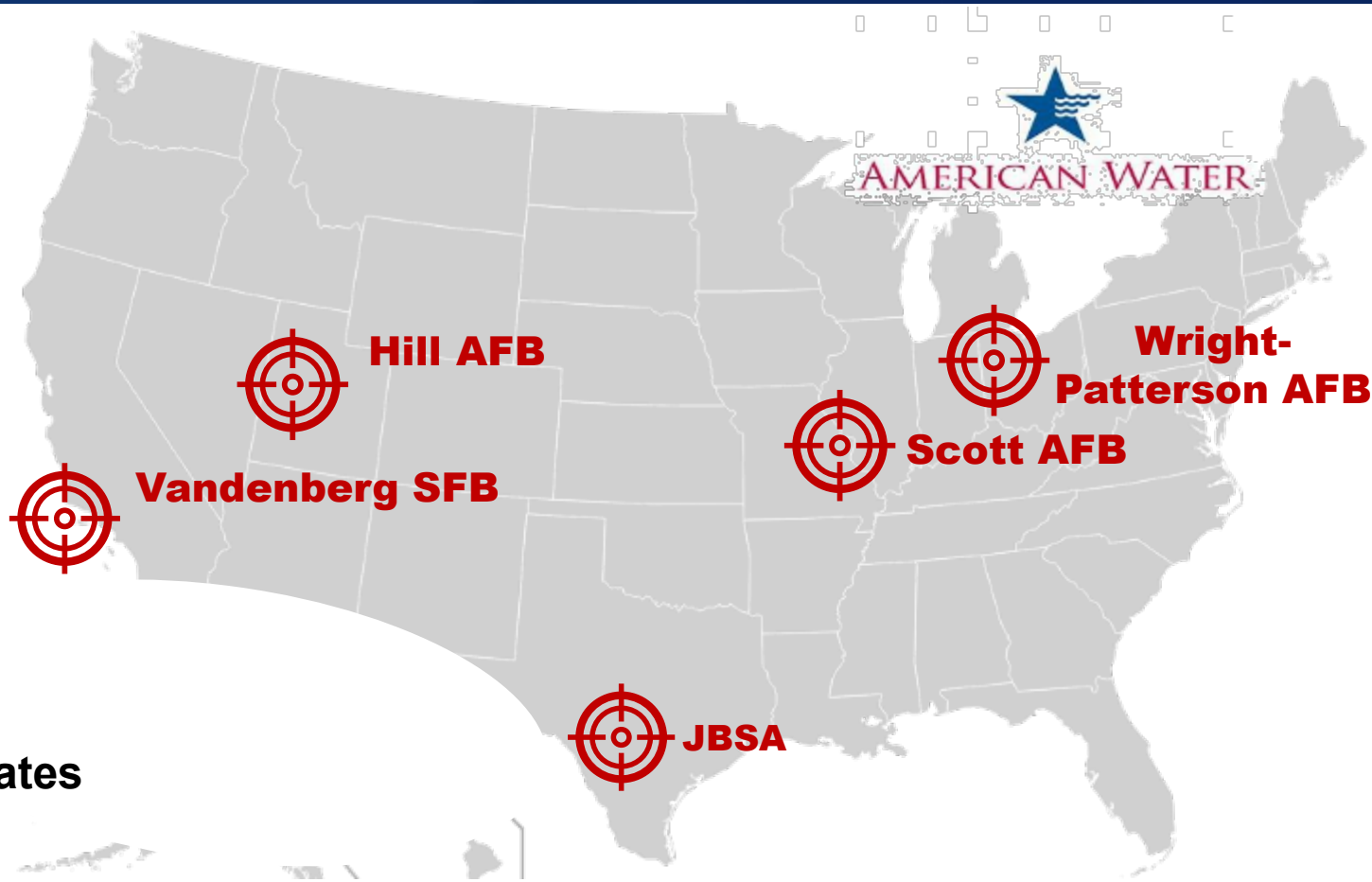
© US Cybersecurity & Infrastructure Security Agency (CISA)

2024

In the News: American Water Cybersecurity Attack (Oct '24)

BLUF: 07 Oct '24 -largest water and wastewater utility company in US, American Water (AW), announced that it was victim of a cyberattack

- **Cyberattack against AW billing systems, halting operations for a week**
- **AW services 18 military sites including five DAF installations →**
- **Thankfully, no direct impact to water or wastewater services but attack demonstrates vulnerability in critical infrastructure**



Water and wastewater systems will continue to be vulnerable target for adversaries; Need increased focus / resources on water resiliency

Vectors of Attack/Exploitation

Connected Building Systems

Operational Technology (OT)

Programmable systems or devices that interact with the physical environment (i.e., ICS, BMS, fire control systems, physical access control mechanisms)

Cyber Physical Systems (CPS)

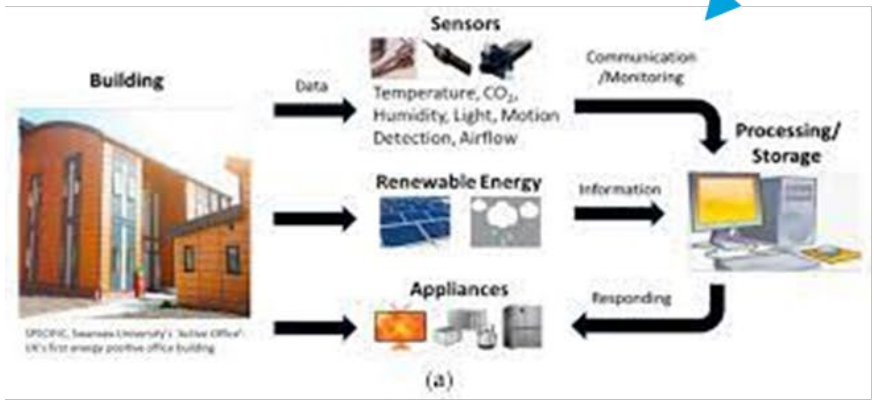
Integration of sensing, computation, control, and networking of physical objects & infrastructure, connecting them to the internet and to each other – **basis for smart technologies.**

Emerging OT in Engineering

Occupant Experience - Collaboration

Enhanced Wired/Wireless Bandwidth

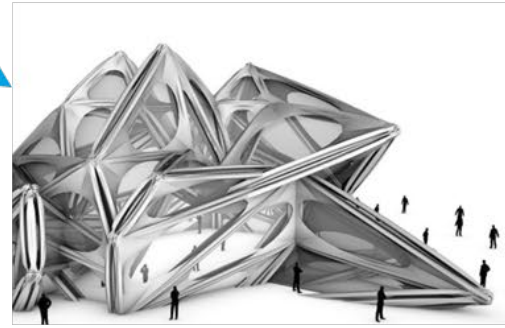
Robotics



Sustainability/Cost Reduction – Building sensors

Marketing Digital Twins

Occupant Experience
Audio Visual



Planning - Generative AI

What's a Bad Day?

WARNING – Urgent -Requires Immediate Attention

Your building management systems have been compromised and encrypted by RSA-2048. We have control over all elevators, cameras, cypher locks, fire suppression, lighting, gas lines, SCADA systems and HVAC

DO NOT CONTACT AUTHORITIES OR PUBLICLY RELEASE THIS INFORMATION

You will need a private key and password to recover these systems. Any attempt to detach or recover these systems without the key will result in an unsafe condition.

You can get your private decryption key in 3 easy steps:

1. You must send 10.0 BitCoin to the address Wa_____
2. After you sent Bitcoin, leave a comment on our site at http:_____ to confirm receipt
3. We will respond to you with the decryption software and run it in your SCADA or building systems.

Failure to carry out these steps within 6 hours from 2pm EDT on March 25, 2021 will result in an unsafe condition

What Does an Asset Owner Do?

Immediate - Will I be warned?

- Evacuate the Building? Avoid the elevators? Will that create panic?
- Where will we go? For how long? Who is responsible for the cost?

Which Law Enforcement Authority to Call?

- Will the local police know how to respond? Should I call the FBI? How quickly can they respond?
- What law that has been broken?

Who pays the Ransom?

- How did this happen? Who is liable? Will I still be compromised? How safe will occupants feel? Will they return?

What Needs to be Done…Now

Establishment – A formal engineering "Standard of Care" for cyber safety in the engineering, construction, and facility management profession

Adoption – Minimal Cyber Safe Building Occupancy Requirements

Development - Prioritized cyber safety performance standards and processes for the engineering and construction industry to enhance human safety in

1. Project drawings, specifications, Digital Twins
2. Product reviews during construction
3. Incorporation of Cyber Commissioning
4. Facility Operations Manual and Training

Integration of Cyber Safety in Planning

Owner's Project Requirements (OPR) is a written document that details the functional requirements of a project **and the expectations of how it will be used and operated**.

This includes project and design goals, measurable performance criteria, budgets, schedules, success criteria, owner's directives, and supporting information.

The OPR must be developed with significant owner input and ultimate approval

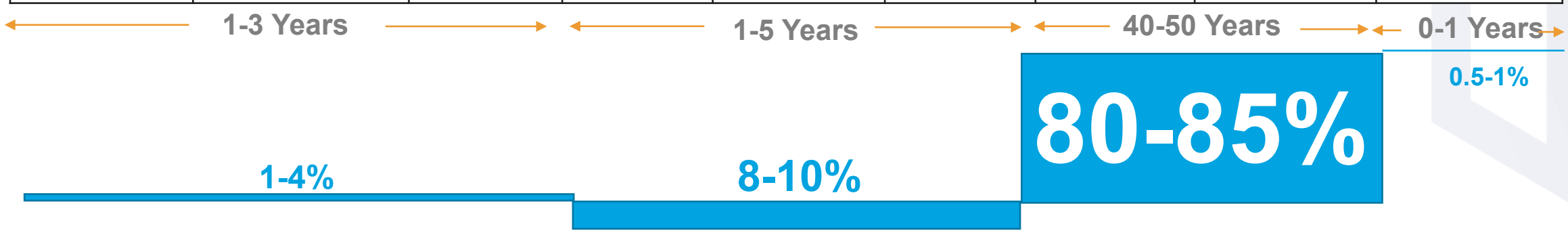
[Resources | BCxA Building Commissioning Association]

Table of Contents

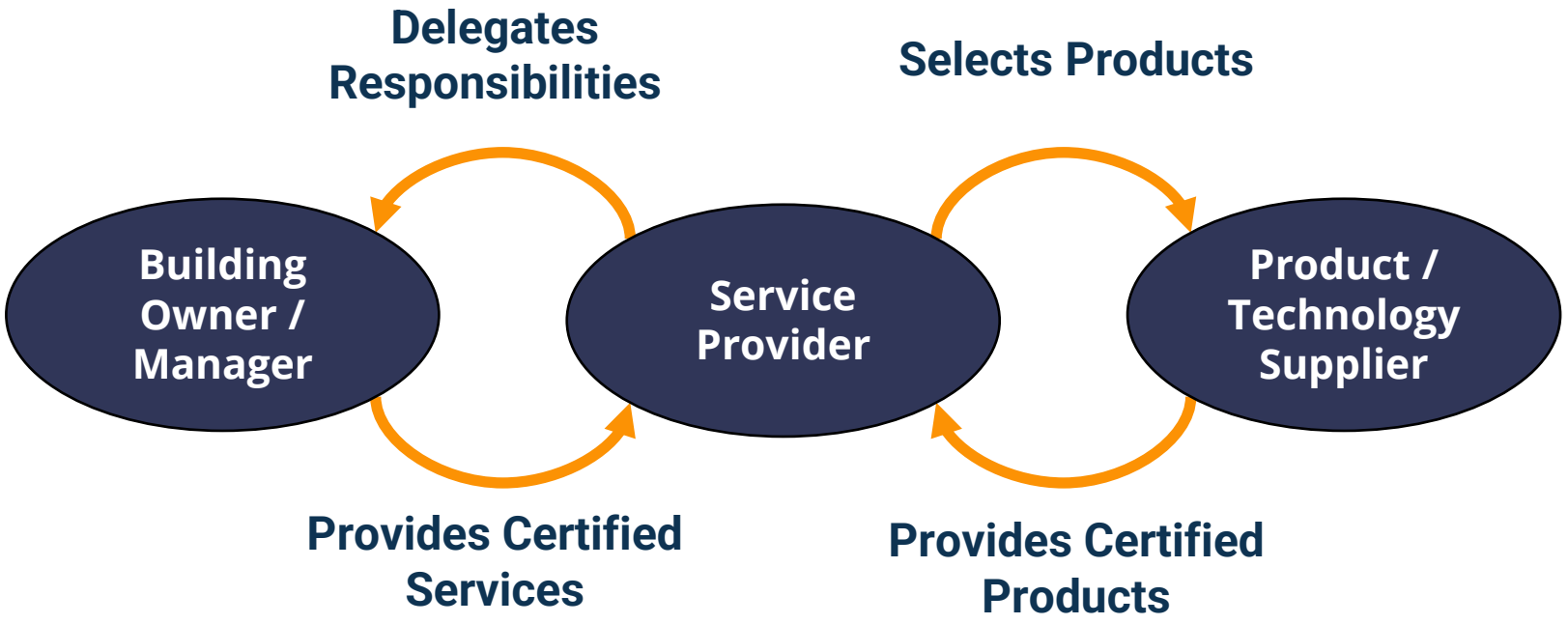
FRCS Cybersecurity

Cyber Safety Facility Life Cycle Costs

Acquisition, Planning and Design			Construction and Transition			Operations		Disposal
Budget, Funding Documents, Basis of Design	35% - 65% -95% Concept and Detailed Design	100% IFC	Product approval and Installation	Startup, Testing, and Validation	Transition	PM, Analytics, Monitoring	Repairs and Replacements	Decommission
OPR to incorporate Cyber Requirements	Focused review controls network design, hardware and software inventory	Formalize a plan for delivery of cyber activities	Equipment/ Device reviews, Acceptance checklists	Harden systems and devices before Cx Performance Testing	Systems Manuals to incorporate procedures to recover from an attack	Implement continuous monitoring for both internal and external threats	Reduce existing vulnerabilities or prevent potential new vulnerabilities	Ensure deletion of stored information



Facility Operations Phase



Cyber Safety Roles and responsibilities

Examples

- Building Owner
- Building Property Managers

Examples

- System Integrators
- Maintenance Providers

Examples

- Building Automation Suppliers
- Control System Suppliers
- Building Physical Systems Suppliers

Society of American Military Engineers

Industry/Government Engagement Established in 2022

- Mitigate cyber risks to physical infrastructure and federal facilities
- Apply industry expertise to enhance cyber security/safety in federal agency construction

Key Focus Areas:

- Identify/assess OT related risks to federal missions, assets, and personnel
- Cultivate cyber risk subject matter expertise both in industry and federal agencies
- Engage federal facility engineering team
- Enhance federal policy development

Award-winning article "Developing an Engineering Standard of Care for Cyber Safety"
https://www.same.org/tmearticle/securing-infrastructure-against-cyberattack/

Results to Date

- Warfighter training programs to detect and respond to cyber attack
- Development of supplemental guidance for planners including use of cyber commissioning

Association for the Improvement of American Infrastructure

The leading minds in infrastructure, dedicated to promoting best practices on the public-private partnership (P3) model.

Cyber Security and Safety Working Group

- **Identify** the cyber risk to human safety, business operations and revenue generation in a P3
- **Protect** the critical connected assets by developing prioritized cybersecurity performance standards and responsibilities to limit access, train personnel, manage data, install protections, and update protections
- **Detect** – Install technologies that will immediately warn of a cyber breach.
- **Respond** – Exercise the roles and responsibilities in the P3 to minimize damage
- **Recover** – Tools in place to quickly restore safe operations of critical systems
- **Govern** – Leadership, contracts, and investments to maintain cyber resilience

Building Cyber Security

Established 2020

A Non-Profit Organization Advancing Human Safety in a Smarter World

Our Mission - Establish and sustain performance frameworks developed by stakeholders across multiple sectors and administered by a non-profit organization to promote cyber protections, offer market-driven options, and develop insurance incentives in an increasingly connected world.

Our Vision - Building Cyber Security will improve human safety globally by incentivizing investments in operational technologies, processes, training, and recovery plans to enhance the security of cyber-physical systems against rapidly evolving threats in technologically advancing societies.

A Solution to Mitigate Cyber Risk

- ✓ Developed unprecedented performance framework of cyber protections for facilities with world's leading standards organizations.
- ✓ Tested framework assessment in COPT buildings and cyber commissioning in new construction
- ✓ Working with founding Member, AON, to establish the insurance incentive
- ✓ Engaged with insurance underwriters to update client risk assessments
- ✓ Partnered with Smart Building System manufacturers
- ✓ Performing cyber assessment and consultation with public entities
- ✓ Updating design guidance for building design industry to engineer cyber safety

BUILDING Cyber Security

A Free Starting Point for Engineers

Building Automation Control Systems (BACS) Prerequisite Questionnaire:

- Questions gauge readiness to start facility cyber security assessment and/or certification
- Applies to both IT & OT BACS components
- BCS cyber security/safety experts and partners available to support your review and assessment
- BCS Members can offer capabilities to mitigate threats

The Way Forward – A Call to Action

A Collaboration Among Professional Engineering Societies, Insurers, and the Cyber Security Industry

1. Adopt a cyber safety "Standard of Care" definition;
2. Develop a professional engineer licensing requirement consistent for all States;
3. Recognize a curriculum 4-year undergraduate cyber engineering degree;
4. Update NCEES Engineering Exams incorporating cyber safety Standards of Care for network and control system engineering;
5. Promulgate engineering and construction best practices to enhance cyber safety, and:
6. Incorporate enhanced cyber protections in all future projects with human safety risk

Please Get Involved

Thank You

Want to get in touch?

Lucian Niemeyer at lucian@buildingcybersecurity.org