BUILDING Cyber Security

Enhancing Cyber Protections

A SAME Industry/Government Engagement

www.buildingcybersecurity.org

Society of SAME American Military Engineers

Aug 2022

What is Cyber and Smart for Buildings?

Operational Technology (OT)

Programmable systems or devices that interact with the physical environment . Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

Cyber Physical Systems (CPS)

An integration of sensing, computation, control and networking of physical objects and infrastructure, connecting them to the Internet and to each other. – Basis for smart technologies.

BUILDING Cyber Security

What is the Cyber Security Threat?

- Bad Actors using weak IT security to exploit or compromise systems
  - Steal data, intellectual property, financial information
  - Extract payment through ransomware incidents
  - Exploit or compromise technologies to disrupt service, create unsafe condition or destroy an asset
- Most compelling risk is a cyber attack on a system that can threaten the life, safety, or property of citizens
- Government have limited protections and response capabilities

The Cyber Global Landscape

- **Increased Volatility in Cyber Insurance Industry – "Is coverage even available without validated cyber performance?"**
  - **Merck** prevails in court ruling over insurer for $1.75 billion "all-risk" policy to recover from 2017 cyber attack
  - **Lloyds of London** expands insurance exclusion clauses for "Cyberwar" activities impacting companies.
  - **U.S. General Accountability Office**, "The extent to which cyber insurance will continue to be generally available and affordable remains uncertain.

- **2022 Cyber Threat Headlines**
  - **CNN** (2/2/22) – "US officials prepare for potential Russian cyberattacks as Ukraine standoff continues"
  - **Allianz Risk Barometer – "**Cyber perils are the biggest concern for companies globally in 2022"
  - **Gartner** – "Cyber enabled weaponized operational technology may cause human casualties"
  - **Dark Reading** – "Lights Out: Cyberattacks in Germany Shut Down Building Automation Systems"

Cyber Threat Trend – From stealing data, to gaining access, to threatening human safety

USA TODAY™ - October, 12, 2021

”The next big cyberthreat isn't ransomware. It's killware. And it's just as bad as it sounds.”

- **The nation’s top homeland security official is worried about an even more dire digital danger: killware, or cyberattacks that can literally end lives.**
- **“The hack of a water treatment facility in February 2021 demonstrated the grave risks that malicious cyber activity poses to public health and safety. The attacks are increasing in frequency and gravity, and cybersecurity must be a priority for all of us.”**
- **“Soon, CEOs won’t be able to plead ignorance or retreat behind insurance policies.”**

The U.S. Government Response

- **March 2022 - President Biden's Statement on our Nation's Cybersecurity**
  - "This is a critical moment to accelerate our work to improve domestic cybersecurity and bolster our national resilience."
  - "Potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we've imposed on Russia
  - "Evolving intelligence that the Russian Government is exploring options for potential cyberattacks.
- **March 2022 - SEC Proposes New Cybersecurity Disclosure Rules on Incident Reporting, Risk Management, Strategy, and Governance**
  - "SEC determined that investors would benefit from "more timely and consistent disclosures" by public companies of several categories of cybersecurity-related information: (1) material cybersecurity incidents, (2) risk management and strategy, (3) governance, and (4) cybersecurity expertise among board members."
  - New rule require disclosure whether (1) the company has a cybersecurity risk assessment and management program (if so, the rule would require a description); (2) the company engages third parties in connection with the program; and (3) the company has policies and procedures in place to evaluate cyber risks associated with third-party service providers.
- **February 2022 DHS Cyber Security and Infrastructure Agency (CISA) – "Shields Up" Program**
  - "All organizations—regardless of size—adopt a heightened protection posture when it comes to cybersecurity and protecting their most critical assets."

The Trends…

Millions of New Attack Vectors are Added Every Day

Cyber-attacks are sited as

No. 1

in the top 10 global business risks
according to the World Economic Forum

“Cyber attackers will have weaponized operational technology environments to successfully harm or kill humans.”

The Trends…

Growing Cyber Threats Represent a Clear and Present Safety Risk

75% of CEO's will

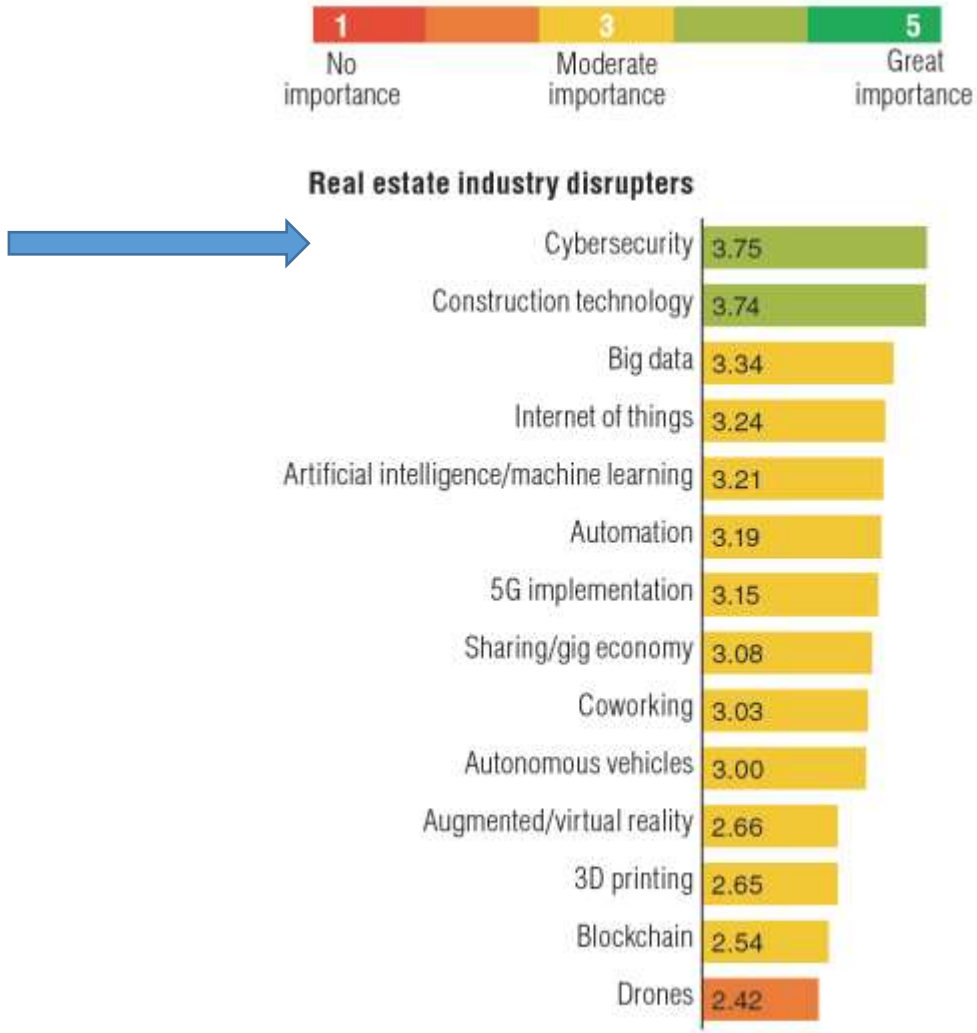
be personally **liable for cyber-physical security incidents** by **2024**

According to Gartner

BUILDING Cyber Security

Smart Buildings…

A global performance framework to guide and incentivize the secure and safe integration of smart technologies into buildings and infrastructure that mitigates cyber risk for occupants is needed now.



Source: *Emerging Trends in Real Estate 2022* survey.

Building Cyber Security

Established 2020

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

Our Mission - Establish and sustain cyber performance frameworks developed by stakeholders across multiple sectors and administered by a non-profit organization offering market-driven options and insurance incentives to promote cyber protections in controls and devices in an increasingly smart 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 in May 2022 – assessing results
- ✓ 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
- ✓ Working with investors on start up of for-profit entity for training, certifications, and managed services

BUILDING Cyber Security

What is Needed to Mitigate the Risk?

- Awareness of emerging cyber threats and collaboration between the private and public sector
- Tools - Dynamic design guidance and assessments of asset condition and risk beyond static checklists and audits
- Solution – National adoption of a cyber safety performance framework to monitor, validate, and update protections as the threat grows
- Incentive – an ROI through insurance policies and other financial return

Cyber threats are an urgent matter of Public Safety in Buildings and Infrastructure

SAME IGE Charter

Mission

- **Increase understanding and mitigate cybersecurity risks to physical infrastructure and facilities owned and/or operated by federal agencies**
- **Identify ways that SAME can support federal agency partners in mitigating those risks.**

Key Focus Areas :

- **Identify/evaluate OT related risks to federal missions, assets, and personnel**
- **Cultivate cyber risk subject matter expertise both in industry and federal agencies**
- **Engage leading experts in protection of OT in building management systems**
- **Engage the facility engineering team in federal agencies**
- **Develop content in support of federal policy development**

Proposed updates to targeted documents, starting with specifications (UFGS) and criteria (UFCs) related to Control System Cybersecurity UFC (UFC 4-010-06) and UFGS (UFGS 25 10 10) as well as of the UFCs and UFGS for HVAC controls and Utility Monitoring and Control Systems.

- https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06
- https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-10-10

BUILDING Cyber Security

SAME IGE Goals

Deliverables:

- ❑ White Paper on Reducing Cyber Risk in Smart OT for Federal Facilities and Infrastructure
  - Discuss risks associated with use of smart OT in federal facilities (awareness, thought leadership)
  - Discuss potential cyber risk mitigation strategies (awareness, thought leadership)
  - Curated list of best practices for securing smart OT for federal facilities and infrastructure (awareness)
  - Proposed framework for analyzing risk and the criticality of mitigating vulnerabilities (awareness, advocacy)
  - Design review checklist for protection of smart building management systems. (awareness)
  - Recommended changes to applicable policies and specifications as informed by best practices (advocacy)

SAME IGE Progress

Proposed Milestones:

- ✓ Kickoff Panel – DC/NoVA Post Meeting – 16 Sep 2021
- ✓ Charter approved and IGE Working Group established Oct 20, 2021
- ✓ Commencement of IGE activities – Oct 26, 2021
- ✓ Vector Check – SBC CEO Roundtable – Nov 2021
- ✓ White Paper Preview at NOVA/DC Post public event – Apr 2022
- ✓ Update to Federal Engineering Chiefs and SAME leadership at JETC – May 2022
- ❑ White Paper Submission to SAME Executive Committee – SBC – Nov 2022

SAME's Executive Committee may consider extending and/or expanding the PT to address ongoing or emerging cyber issues or initiatives.

SAME IGE Benefits

- **A/E/C Industry Recognizing Need to Engineer Cyber Safety into Projects**
  - **Firewalls/airgaps are not the answer in an IT/OT convergence**
  - **Collaboration between network and facility designers/engineers on specifications, configuration instructions, submittal reviews, and commissioning requirements**
  - **Using digital twinning and baseline building system performance metrics as the next generation of as-builts for smart technologies**
  - **Specifying new types of data transport architecture to be able to monitor smart technologies (ie Fiber to the edge)**
  - **Consulting with cyber security firms offering platforms for protection of OT**

A/E/C Firms are joining BCS to access cyber safety expertise for development of a cyber practice and the offer of a "Technologist of Record" for buildings and infrastructure

BUILDING Cyber Security

brian.may@buildingcybersecurity.org

Lucian@buildingcybersecurity.org

Lucian Niemeyer
(571) 277-3115

Society of SAME American Military Engineers