Balancing AI/Smart Tech with Cyber Safety to Ensure Business Continuity

Stacey Shepard - BCS Board Advisor/
President, Shepard Global Strategies

20 June 2025

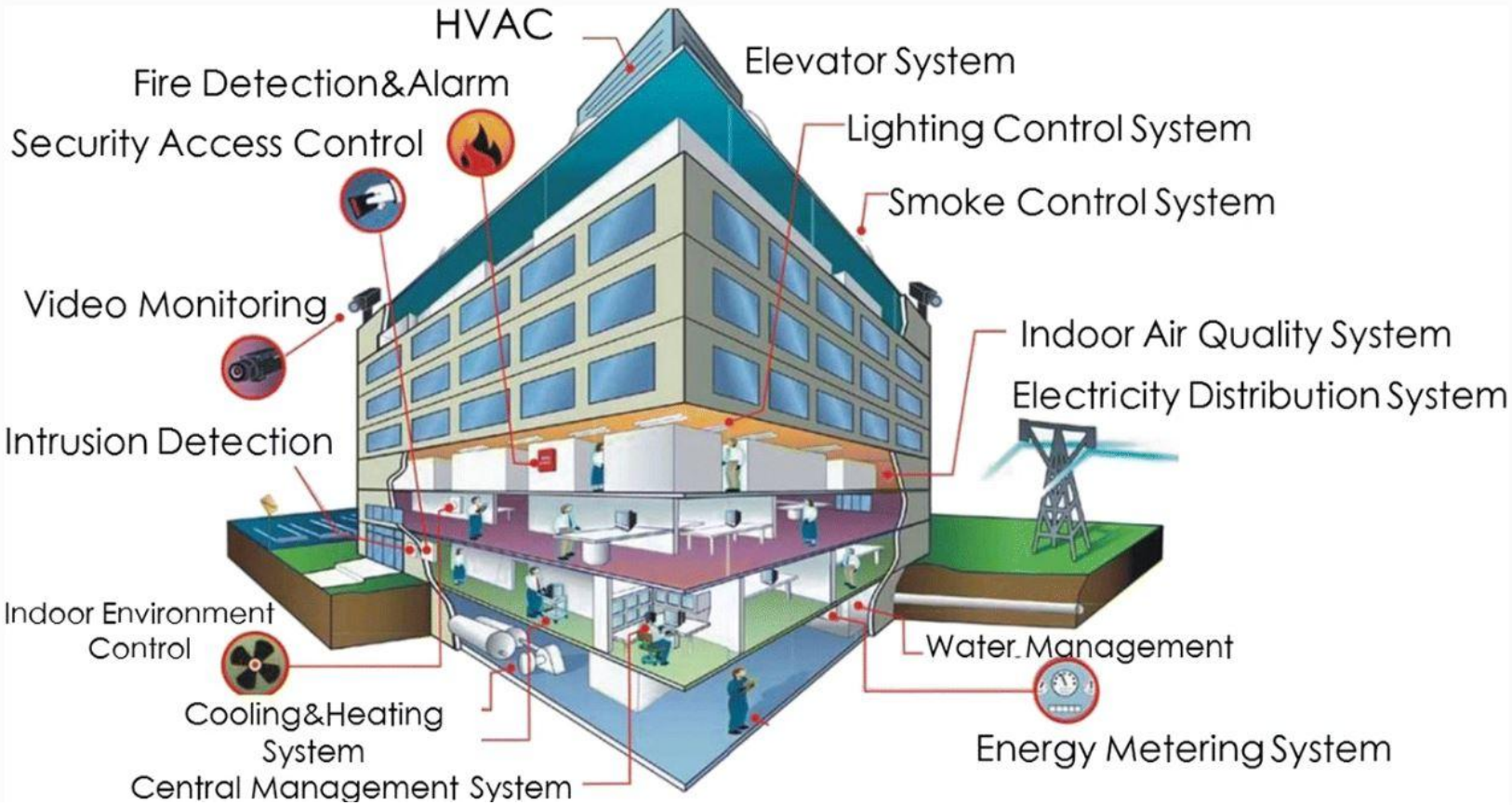
BUILDING Cyber Security

www.buildingcybersecurity.org

IT Technology Community
A Community of IFMA

FM TECH WEEK

The Digital Challenge: A Connected World



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.**

BUILDING Cyber Security

Connectivity Enables Tangible Benefits

HOWEVER……

THERE'S ONLY A FEW PEOPLE THAT HAVE ACCESS TO MY SYSTEM… RIGHT?

The Problem

Cost

Network Gaps & Fragmentation

- There are often multiple networks with many vendors connecting at will.
- Internet connectivity needs are increasing with cloud-based services.
- Connections can be unmanaged without enforced policy.

Risk

Aging Infrastructure

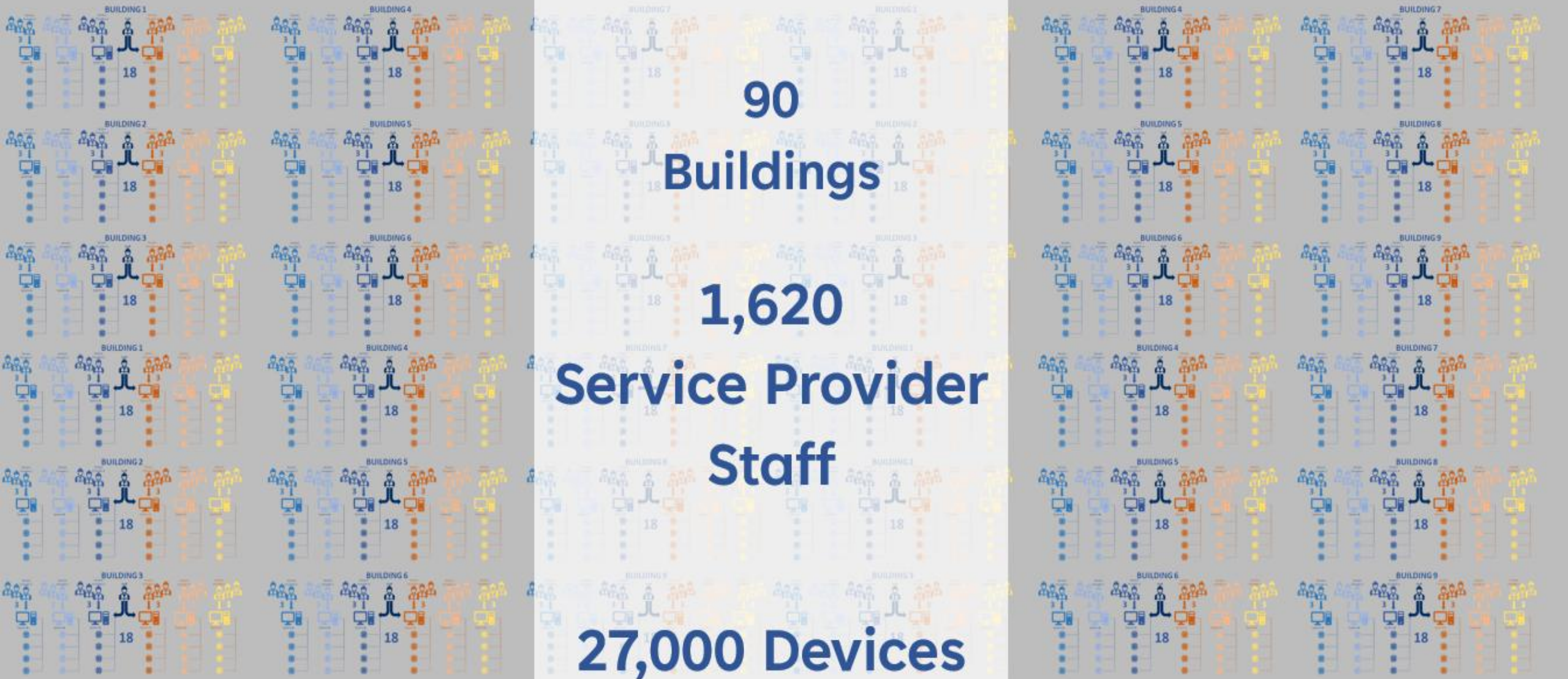
- Building systems and networks are not upgraded on standard IT refresh cycles.
- Old gear leads to vulnerabilities and uptime issues.
- “Band-aids” added to make something work adds cost and risk, like redundant internet connections

Availability

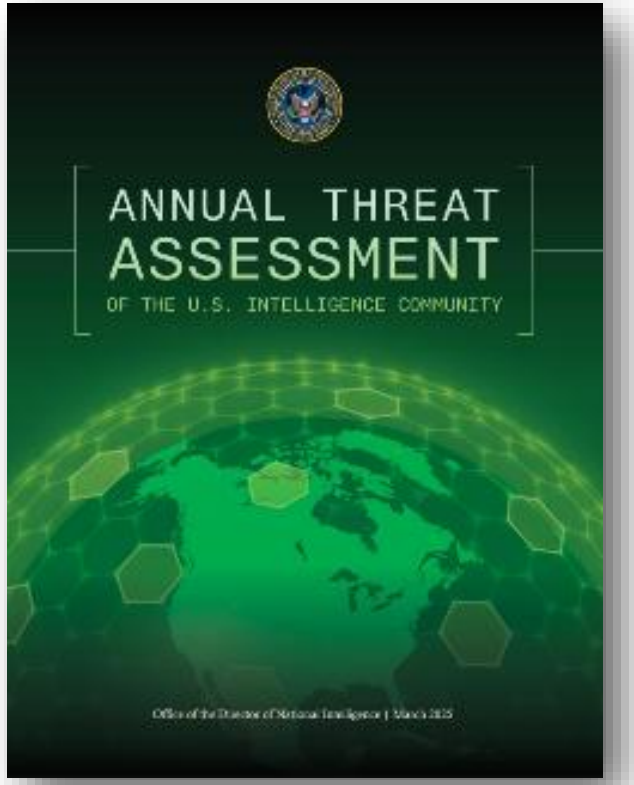
Modern Network Management Needed

- Enterprise grade monitoring, security and maintenance services need to be applied to these networks.
- Standardized services for cost effective risk management is needed.
- An approach tailored to building systems with IT best practices is recommended.

One Client Example



2025 & 2024 Global Threat Reports



Office of the Director of National Intelligence

Attacks By Location

900 million attacks originated from 213 countries:

Top CI Incidents by Region:

1. North America (U.S.)
2. Europe (Germany, France, Spain, Italy, UK)
3. Asia (Japan, India, Korea, Taiwan, Singapore)

Top 3 Verticals Targeted by Threat Actors

384	349	50
Telecommunications	Financial Services	Government

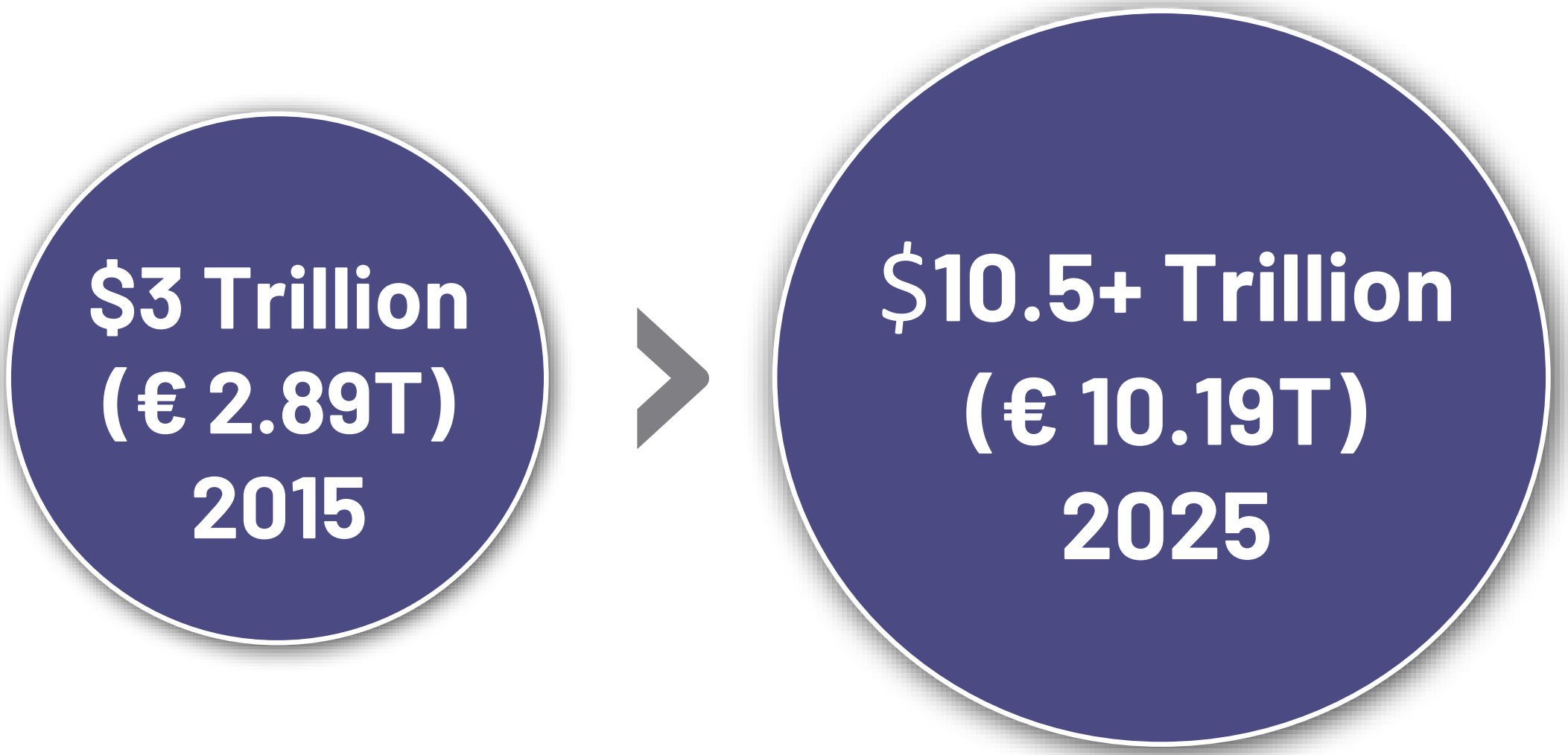
Threat Actor Increase (YoY):

93%	71%	55%
Energy	Manufacturing	Healthcare

FORESCOUT

*"We've got to **shift** the whole focus to stopping the event **before** it happens, and that is the **shift** that most security teams really have to undergo." – Jason Steer, CISO, Recorded Future*

What is the Total Cost of Global Cybercrime?



How Much Does a Single Data Breach Cost?

$4.9 Million (€ 4.7M) 2024

Up 15%
Over 3 previous years

Attack Frequency on Critical Infrastructure?

What Does Bad Day Look Like?

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:

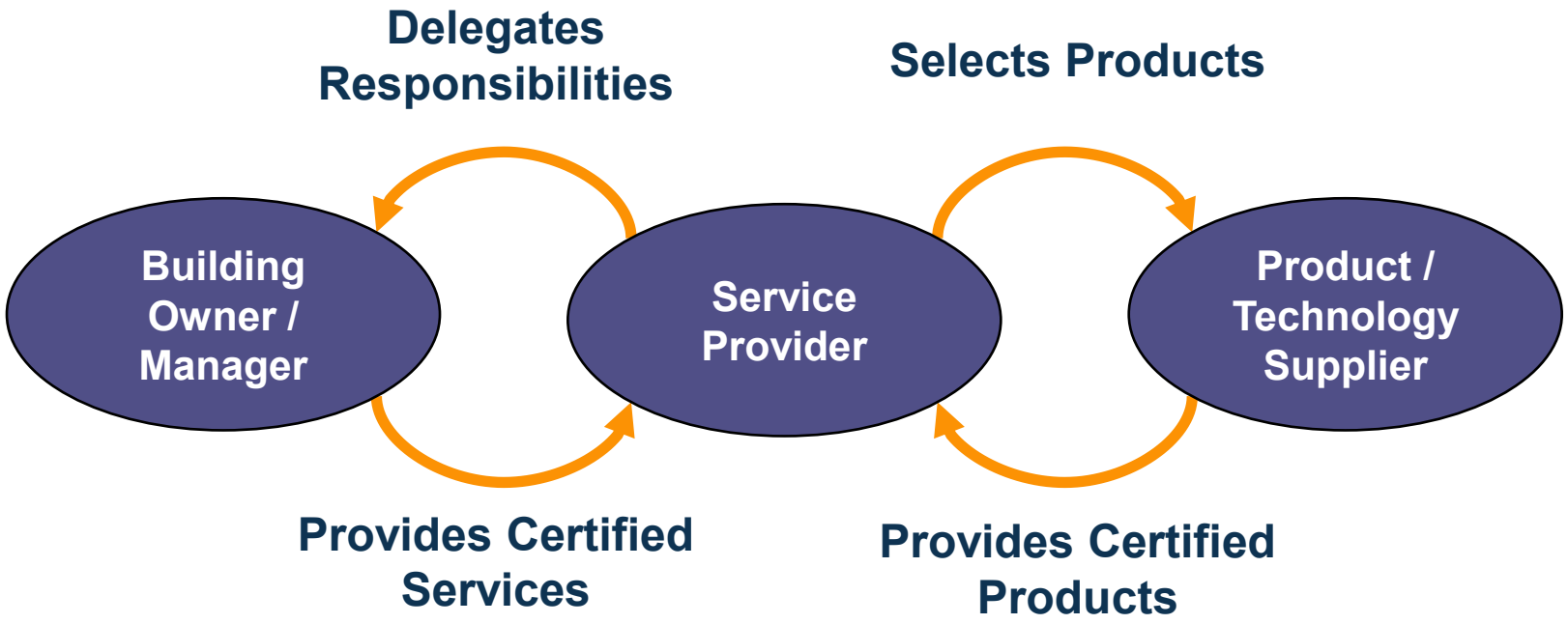
1. **You must send 10.0 BitCoin to the address _____**
2. **After you sent Bitcoin, leave a comment on our site at http:_____ to confirm receipt**
3. **We will respond to you with the decryption software and run it in your SCADA or building systems.**

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

RESPONSE?

- Do you know the extent of the impact of the attack?
- Do you have an incident response plan?
- Do you evacuate the building?
- Who is responsible for decision making?
- How do you communicate internally if your emails are down?
- What is your external communication policy?
- Who do you notify (clients/ tenants), stakeholders, shareholders, and when?

Who Holds the Risk?



Examples

- Building Owner
- Building Property Managers

Examples

- System Integrators
- Maintenance Providers

Examples

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

Cyber Risk: What is Your Approach?

- Cyber insurance vs Property & Casualty
- Have you read the fine print?
- Do you understand the exclusions/gaps?
- BCS is collaborating with the insurance industry to establish a standard approach to cyber risk assessment

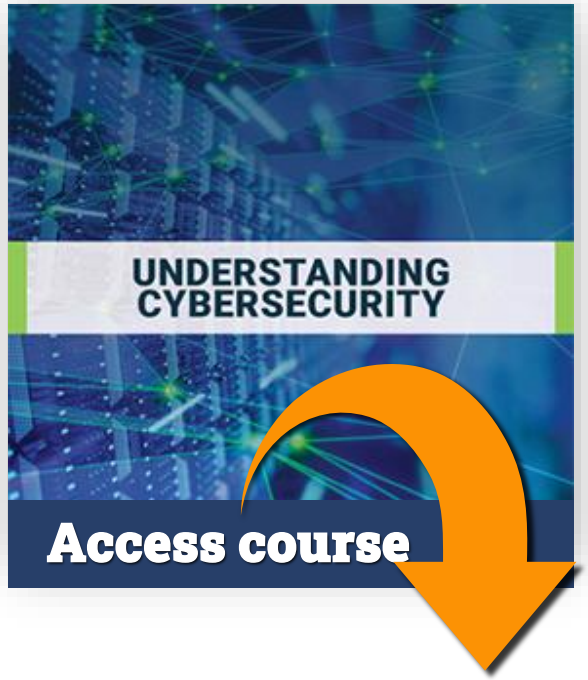
BCS Benefits to Facility Managers

- **Awareness** of emerging cyber threats to building systems, enhancing collaboration between CRE & cyber industry
- **Training** for facility managers to initiate programs and processes to defend against cyber threats
- **Incentives** – identified ROI through insurance policies and other risk mitigation programs
- **Solutions** – cyber safety performance framework to deploy monitor, validate and update building protections
- **Tools** – including an initial checklist and performance framework providing guidance to FMs to evaluate risk and vulnerability of facilities and technologies

Cyber threats can compromise occupant safety and operational continuity in facilities

Training:
Facility Manager Cyber Security

- Check out IFMA's recently published research paper **"Cybersecurity: Securing FM's Digital Transformation"**
  https://ifma.foleon.com/white-paper/cybersecurity/
- IFMA and BCS released first joint Cyber Security Training Course: **"Introduction to Building Cybersecurity for Facility Managers"**
  https://qrco.de/Cyber101
- Courses to walk through BCS 16 Steps
- IFMA and BCS partnering to deliver deeper level of cyber protection instruction in Phase Two

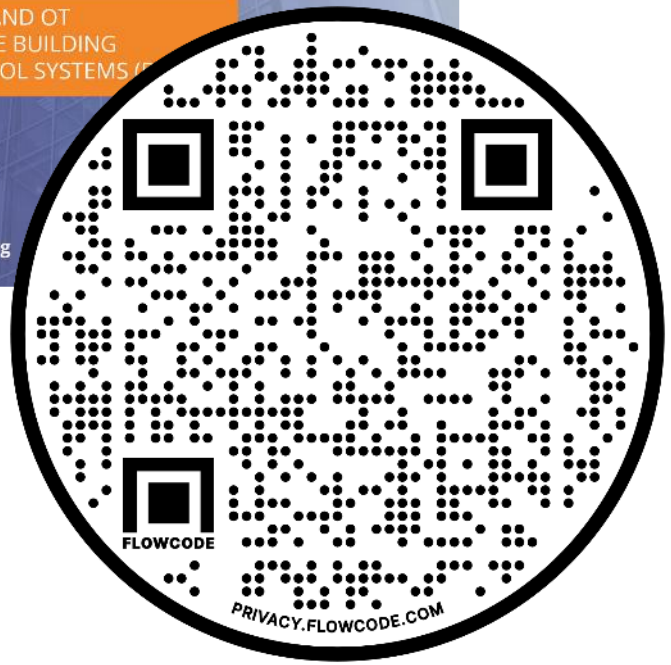


80% of Cyber Attacks are Caused by Human Error

How do you get started?

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



BUILDING Cyber Security

BCS 16 Steps to Securing OT: #1-8

Security Program
(governance, policy, roles)

System Asset Inventory
(hardware + software)

Risk Assessment
(identification of essential functions)

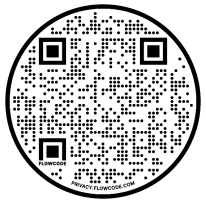
Service Provider Management

Network Access Control
(remote + local)

Network Architecture
(physical + logical)

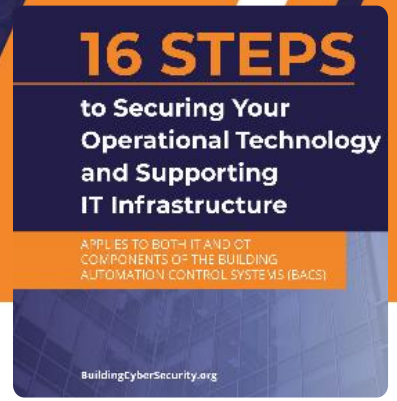
Backup and Restore

Physical Access Control



Watch for 15-minute courses for in-depth review of each of these topics!

BCS 16 Steps to Securing OT: #9-16



System Account Management

Network Infrastructure Management

Change Management

Update As-Build System Documentation

System Security Verification

Incident Response & Recovery

Security Awareness & Skills Training

Data Protection

Watch for 15-minute courses for in-depth review of each of these topics!

www.buildingcybersecurity.org

BUILDING Cyber Security

Final Thoughts

- Cyber attacks threaten both IT/OT risking lives, property, business disruption, revenue, and brand
- In an increasingly technical world – a cyber incident is not a matter of if, but when…
- Cyber Risk, like other corporate risk is either assumed, mitigated, or transferred
- All insurance policies and managed services agreements must be reviewed to understand cyber-related terms and exclusions
- Everyone should have a plan to quickly Identify, Protect, Detect, Respond, and Recover from a cyber-physical attack.

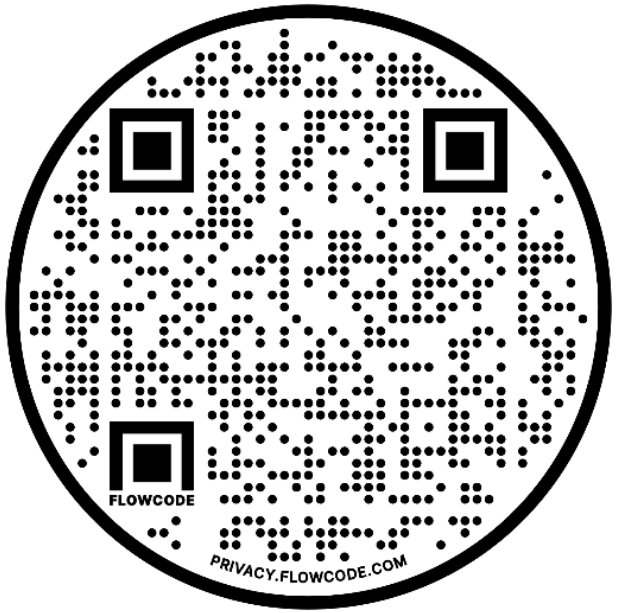
Stay Connected

Stacey Shepard - BCS Advisor/

President, Shepard Global Strategies

stacey@shepardglobalstrategies.com

Lucian Niemeyer – CEO,

Building Cyber Security

lucian@buildingcybersecurity.org