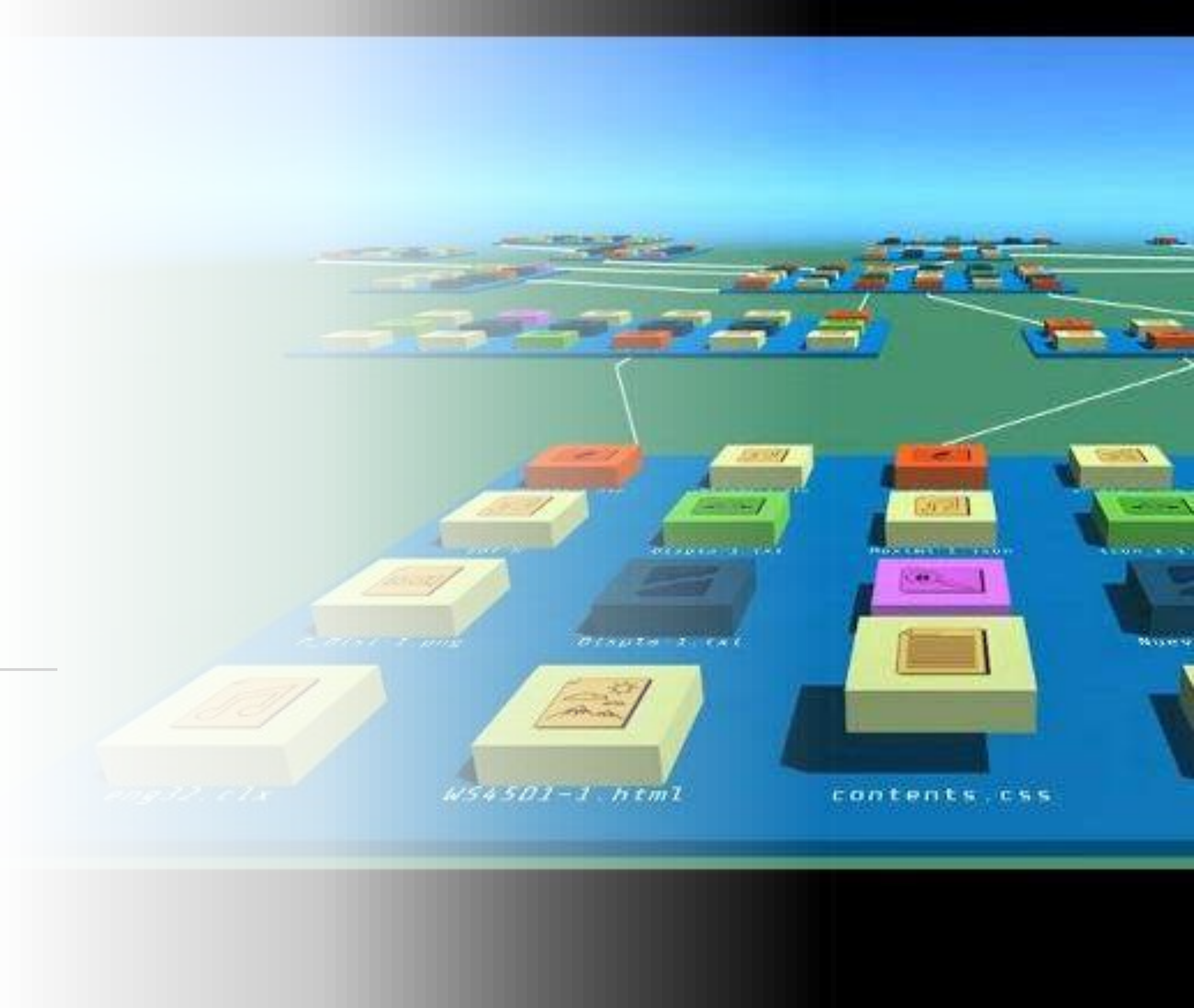
Smart Building Cyber Security

Geraint Williams, CISO

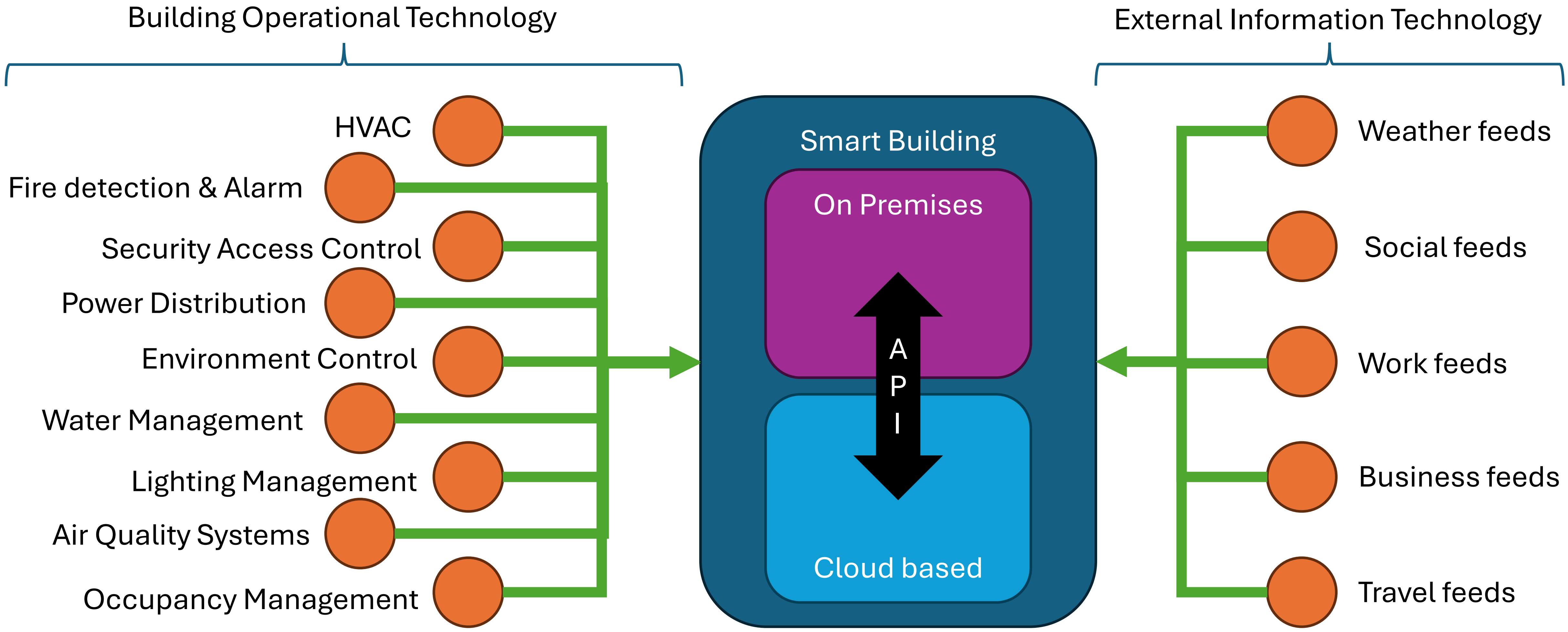
Modern Networks

modernnetworks

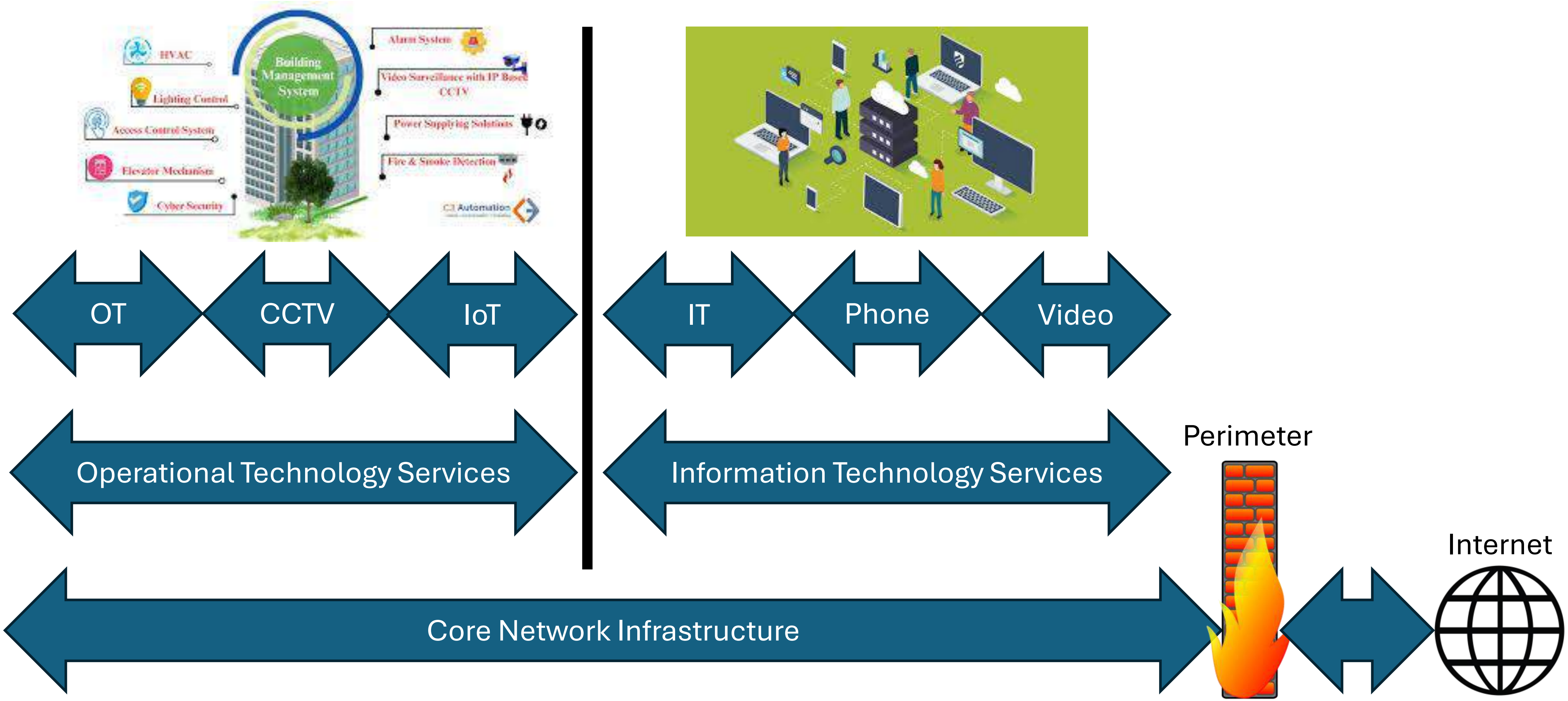
It may not be hacking Jurassic Park but .... !



Smart Building



Smart Building Converged Network



OT

CCTV

IoT

IT

Phone

Video

Operational Technology Services

Information Technology Services

Perimeter

Internet

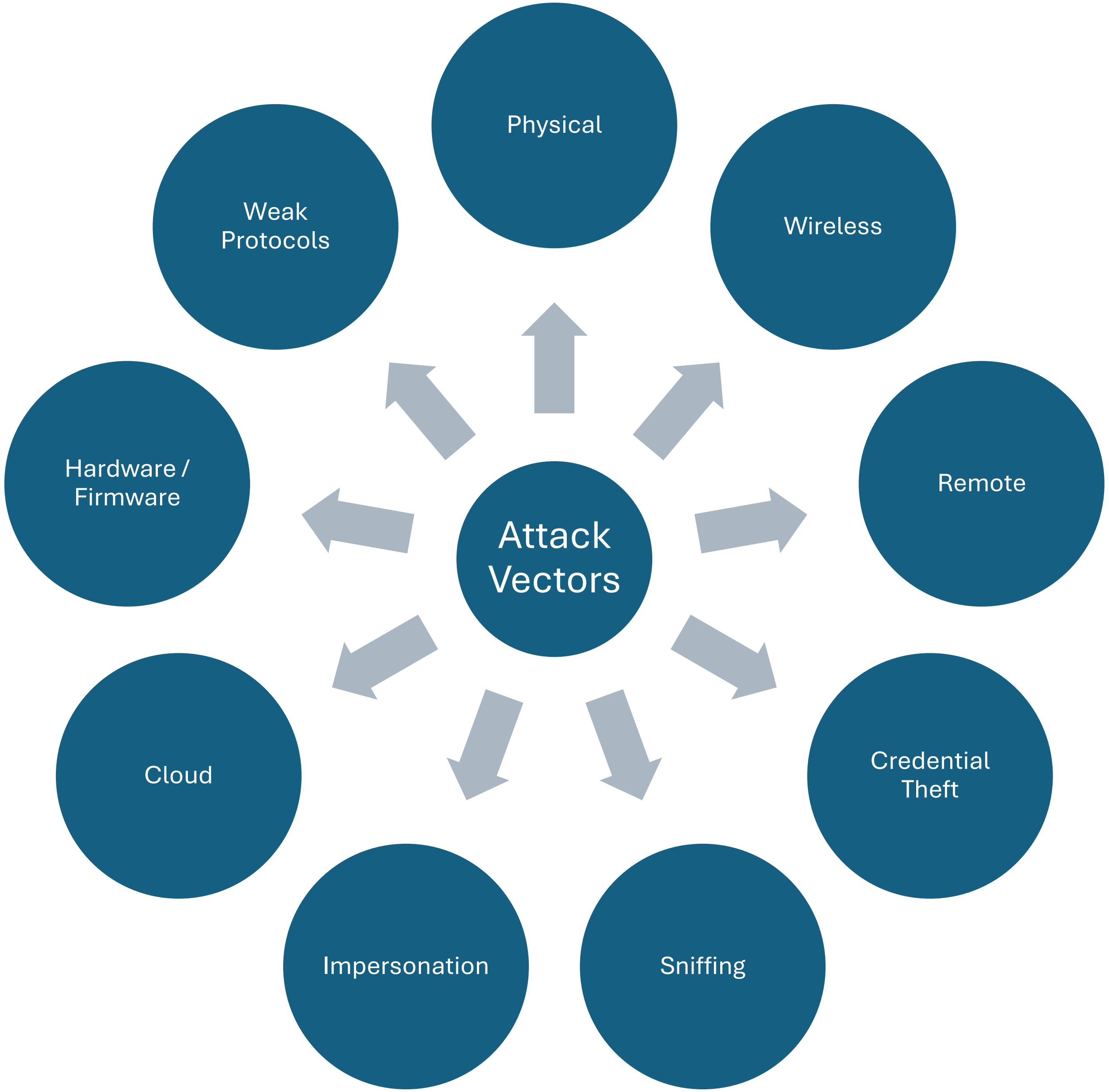
Core Network Infrastructure

Attack Surface

The attack surface of a smart building encompasses all potential vulnerabilities that malicious actors could exploit to compromise its systems and data.

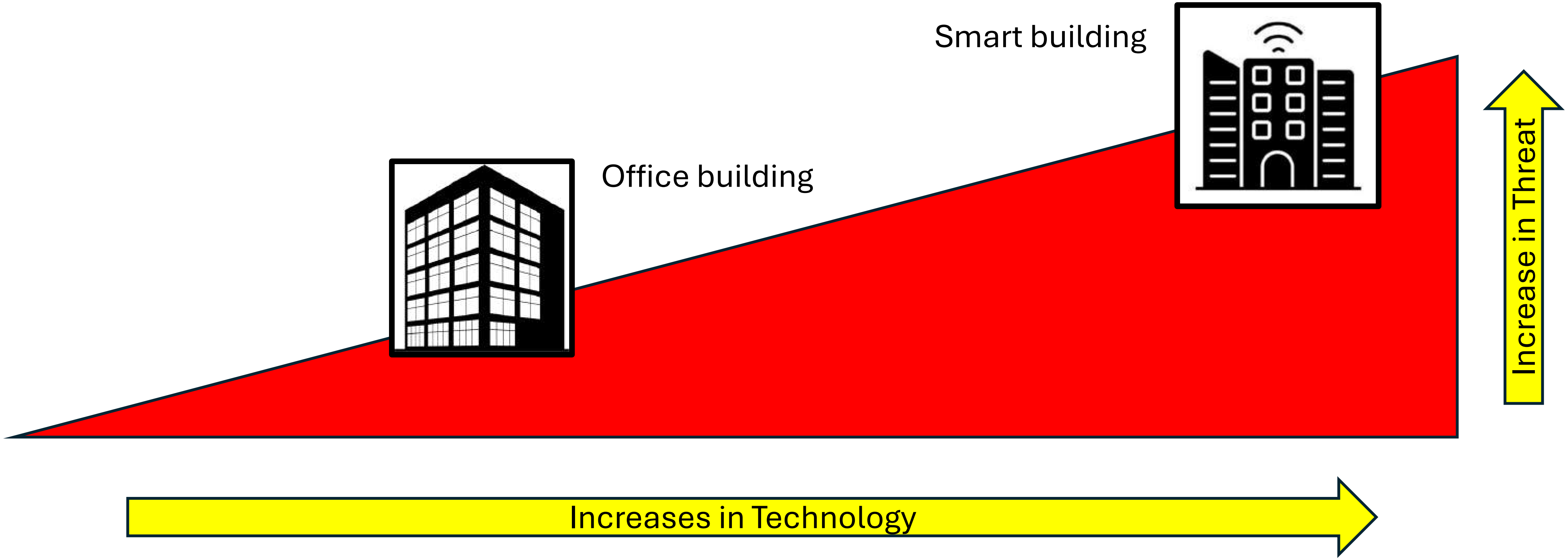
This includes the vast network of interconnected devices like IoT sensors, control panels, and cloud platforms, as well as physical access points and human interactions.

A larger attack surface means more potential entry points for attackers, increasing the risk of breaches and disruptions.

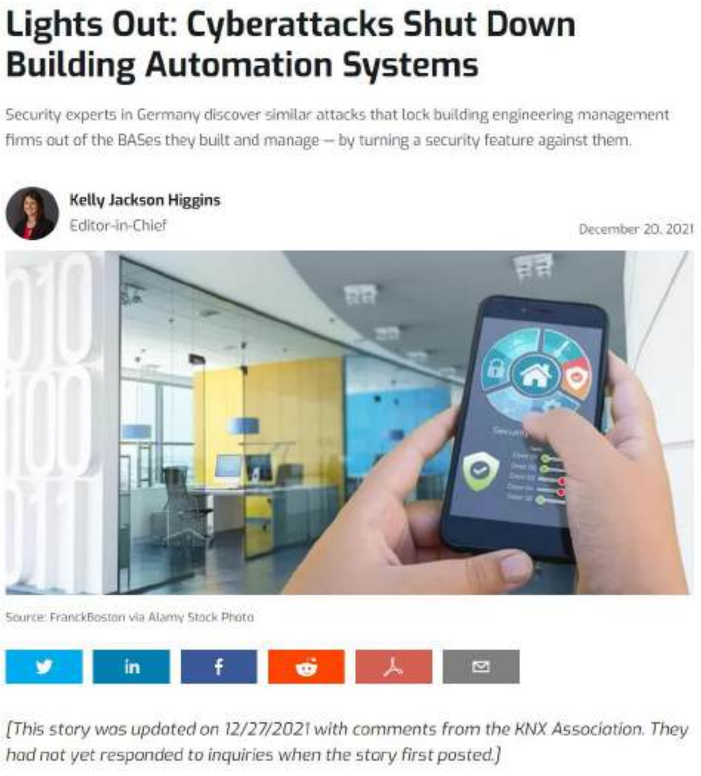


The threat

- The more deployed technology, the more likely a cyber threat will impact the building



Cyber attacks at properties



Lights Out: Cyberattacks Shut Down Building Automation Systems

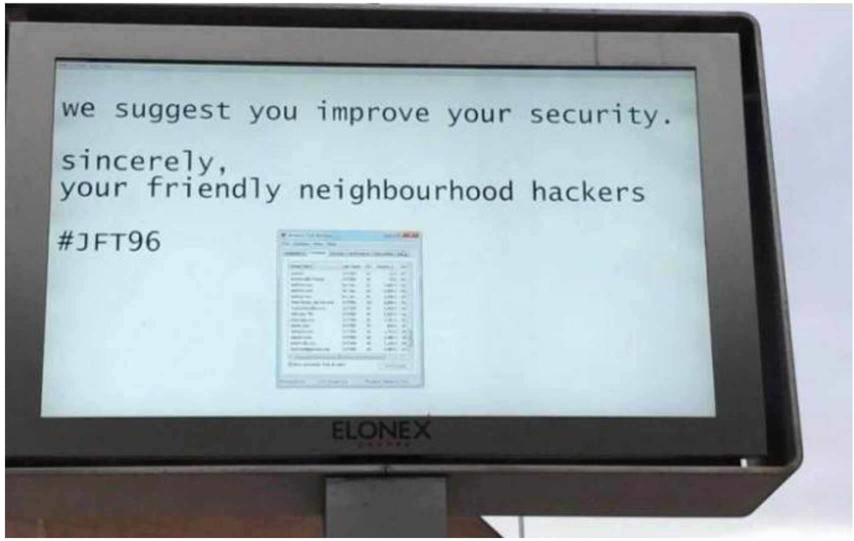
Security experts in Germany discover similar attacks that lock building engineering management firms out of the BASes they built and manage — by turning a security feature against them.

Kelly Jackson Higgins
Editor-in-Chief

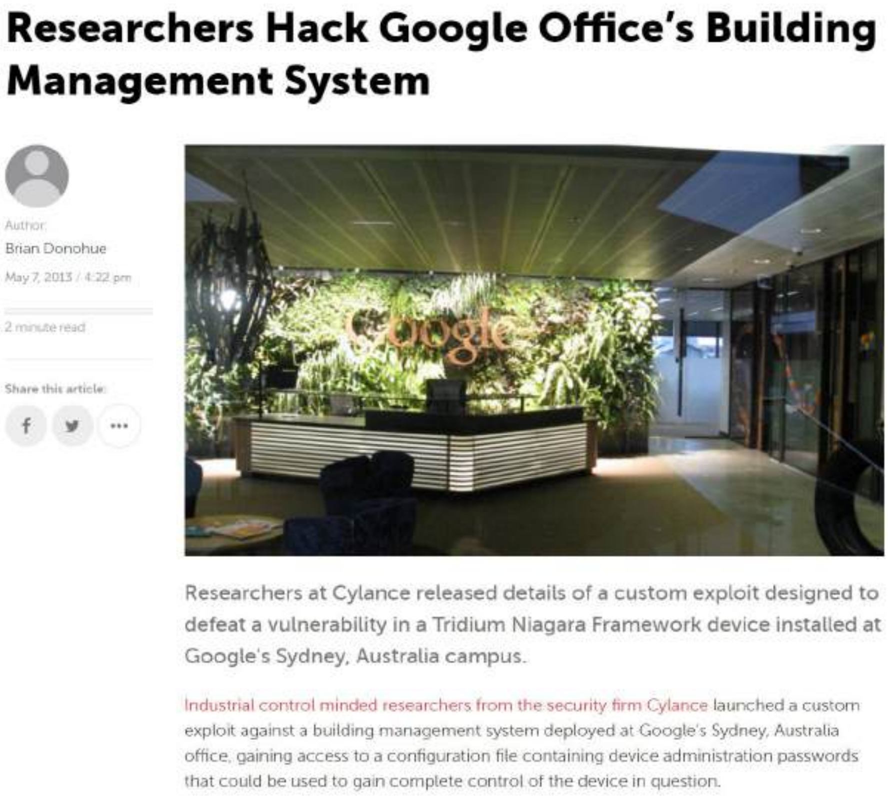
December 20, 2021

Source: FranckBoston via Alamy Stock Photo

[This story was updated on 12/27/2021 with comments from the KNX Association. They had not yet responded to inquiries when the story first posted.]


we suggest you improve your security.
sincerely,
your friendly neighbourhood hackers
#JFT96
ELONEX

A large digital billboard outside a Liverpool shopping centre was apparently defaced by hackers on May 2017



Researchers Hack Google Office's Building Management System

Author:
Brian Donohue
May 7, 2013 / 4:22 pm

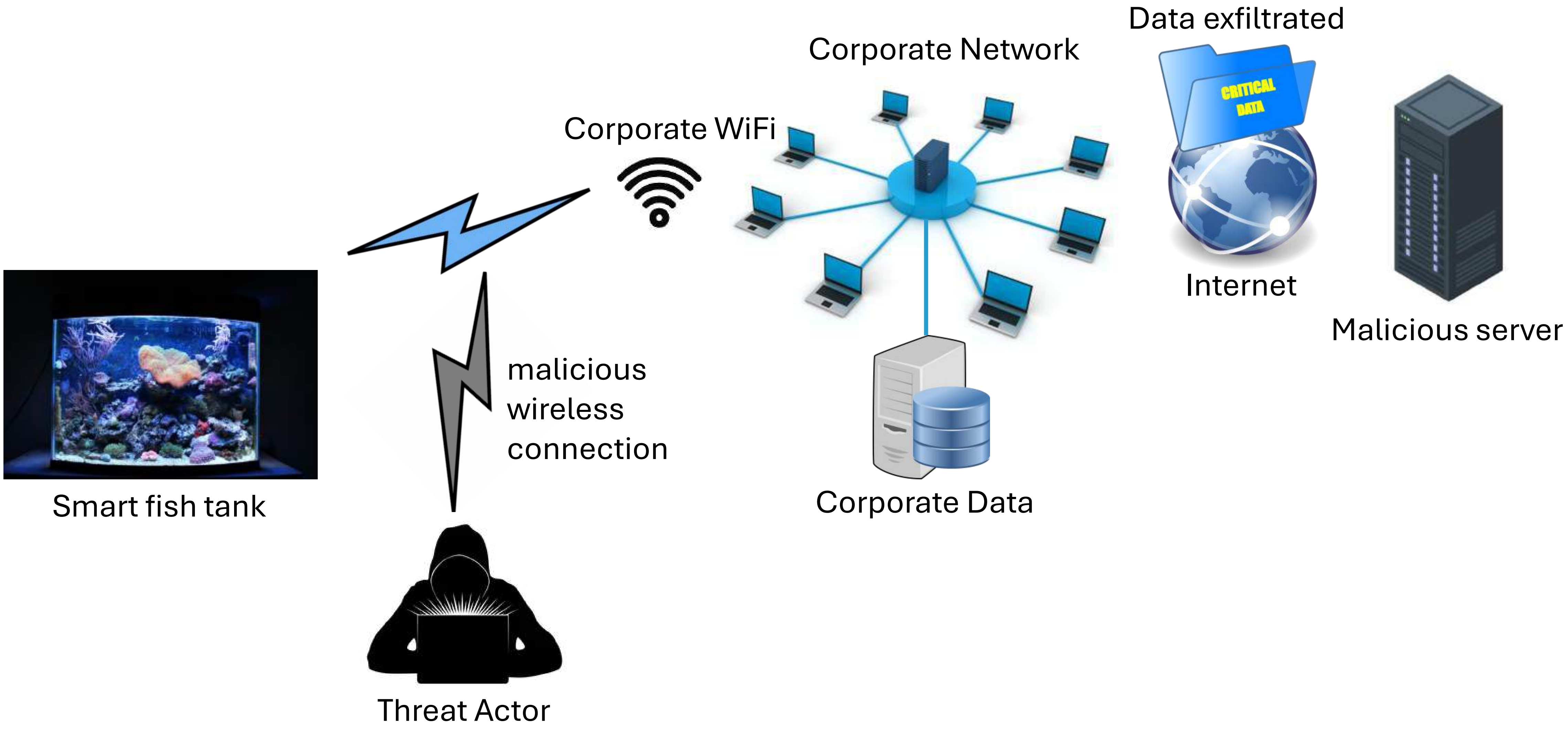
2 minute read

Share this article:

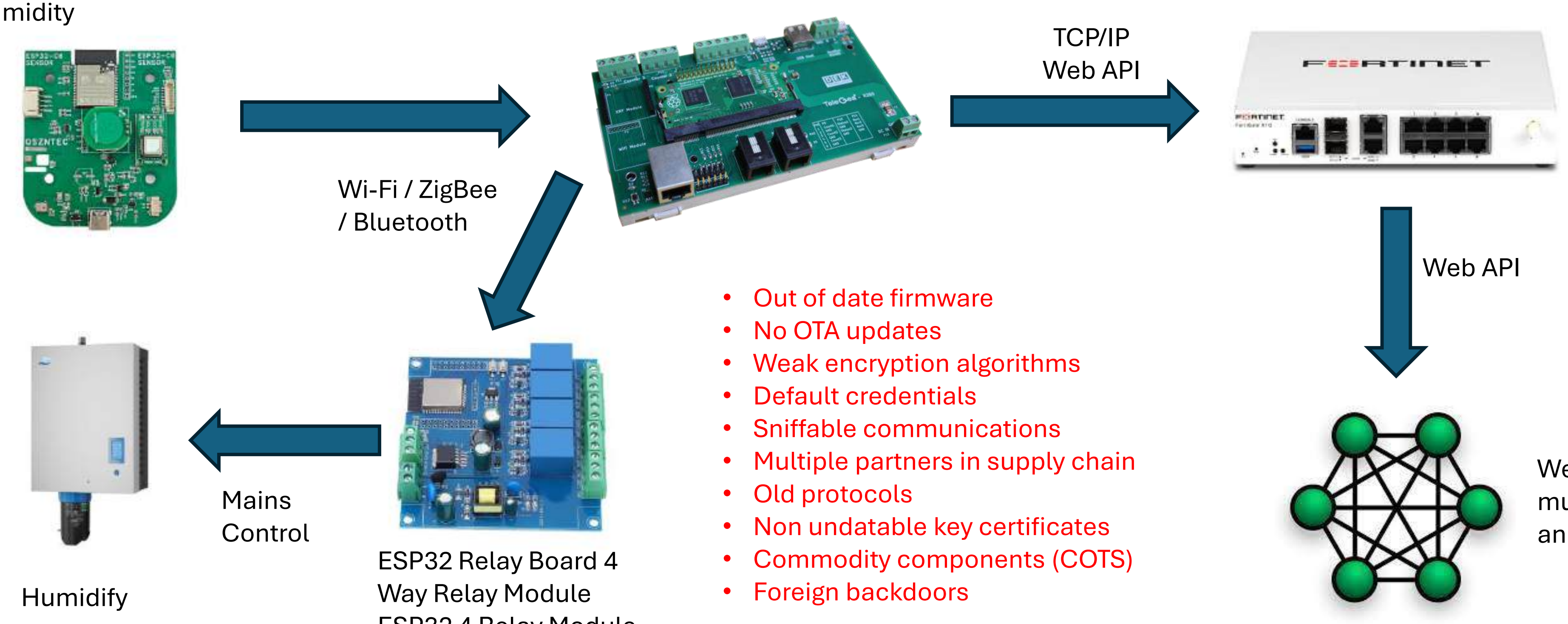
Researchers at Cylance released details of a custom exploit designed to defeat a vulnerability in a Tridium Niagara Framework device installed at Google's Sydney, Australia campus.

Industrial control minded researchers from the security firm Cylance launched a custom exploit against a building management system deployed at Google's Sydney, Australia office, gaining access to a configuration file containing device administration passwords that could be used to gain complete control of the device in question.

The Great Fish Tank Heist



Smart devices breakdown



ESP32-C6 multi-sensor can detect CO2, VOC, IMU, temperature, humidity

Wi-Fi / ZigBee / Bluetooth

Smart hub / IoT Controller

TCP/IP
Web API

Web API

Web Application using multiple webservices and AI services

ESP32 Relay Board 4 Way Relay Module ESP32 4 Relay Module Programmable Resettable Wireless

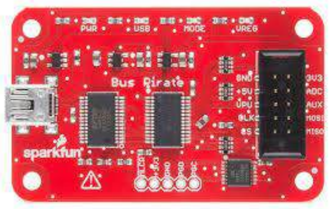
Mains Control

Humidify

- Out of date firmware
- No OTA updates
- Weak encryption algorithms
- Default credentials
- Sniffable communications
- Multiple partners in supply chain
- Old protocols
- Non undatable key certificates
- Commodity components (COTS)
- Foreign backdoors

Amazon hacking tools

RFID Cloning coil



Bus Pirate

Card cloning

Physical Keylogger

SDR Hacking tool

Wireless Pineapple

HackyPi USB Tool
(Rubber Ducky clone)

Flipper Zero

Royal Institution of Chartered Surveyors (RICS)

- RICS identifies digital and cyber risks as significant concerns for smart buildings, highlighting vulnerabilities in operational technology like building management systems, CCTV, and IoT devices.
- These risks stem from outdated operating systems, unsecured networks, and the increased interconnectedness of building systems, potentially leading to data breaches, financial losses, and disruptions to building operations.

Key Risks and Concerns:

Cybersecurity:

- Smart buildings, with their increased reliance on interconnected systems, present a larger attack surface for cybercriminals.

Data Breaches:

- Sensitive information like lease data, BIM models, and access control data can be compromised.

Operational Disruptions:

- Cyberattacks can impact building management systems, potentially disrupting HVAC, lighting, and access control, affecting safety and comfort.

Financial Losses:

- Data breaches and ransomware attacks can lead to financial losses for building owners and occupants.

Reputational Damage:

- Security breaches can damage the reputation of building owners and property managers.

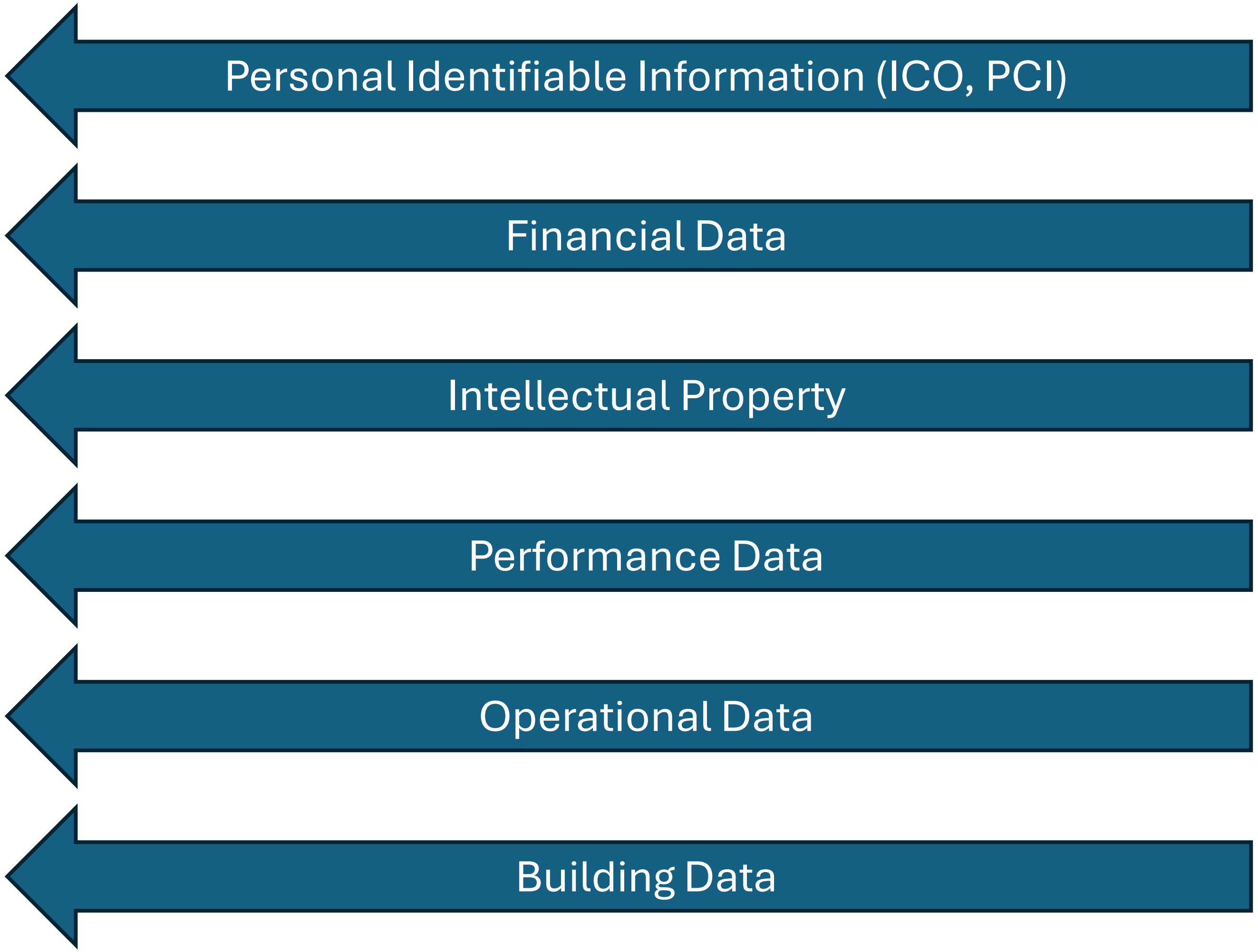
Outdated Systems:

- Many smart buildings use outdated operating systems that are no longer supported by vendors, creating vulnerabilities.

Lack of Cohesive Strategy:

- Disjointed cybersecurity initiatives across different stakeholders can increase risks.

Data breach is more than just PII



Personal Identifiable Information (ICO, PCI)

Financial Data

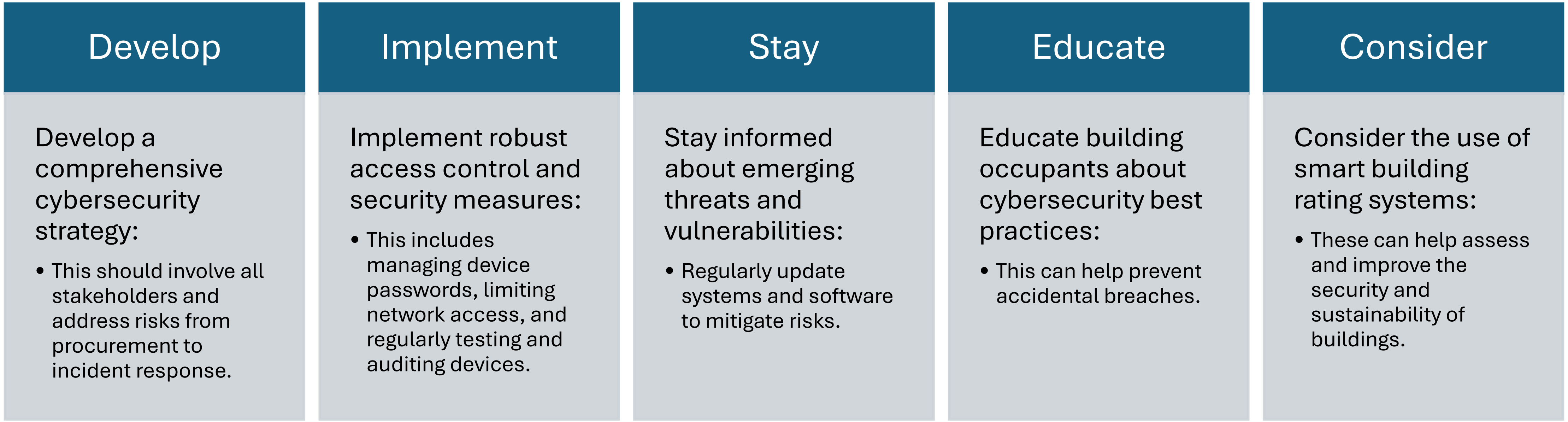
Intellectual Property

Performance Data

Operational Data

Building Data

RICS Recommendations:



Develop

Develop a comprehensive cybersecurity strategy:

- This should involve all stakeholders and address risks from procurement to incident response.

Implement

Implement robust access control and security measures:

- This includes managing device passwords, limiting network access, and regularly testing and auditing devices.

Stay

Stay informed about emerging threats and vulnerabilities:

- Regularly update systems and software to mitigate risks.

Educate

Educate building occupants about cybersecurity best practices:

- This can help prevent accidental breaches.

Consider

Consider the use of smart building rating systems:

- These can help assess and improve the security and sustainability of buildings.

By addressing these risks and implementing proactive measures, building professionals can ensure that smart buildings are not only technologically advanced but also secure and resilient.

Layered approach to certification

Industry standards

- Smart Score
- Wired Score

Cyber Security standards

- ISO27001
- Cyber Essentials

Cyber Essentials and ISO27001

Feature	**Cyber Essentials**	**ISO/IEC 27001**
Purpose	Basic protection against common cyber threats	Comprehensive information security management
Scope	Technical controls only (e.g., firewalls, patching, access control)	Covers people, processes, and technology
Approach	Prescriptive checklist	Risk-based, customisable framework
Certification Process	Self-assessment (or audit for Cyber Essentials Plus)	Independent audit and ongoing surveillance
Complexity	Simple and quick to implement	Complex and resource-intensive
Cost	Low (especially for small businesses)	Higher cost due to audits and documentation
Recognition	UK-focused, government-backed	Internationally recognised (ISO standard)
Best For	Small to medium-sized businesses starting with cybersecurity	Medium to large organisations needing robust, scalable security governance
Renewal	Annual	Typically, every 3 years with surveillance audits in between

Cyber Essentials

- Cyber Essentials is a UK government-backed scheme designed to help organizations guard against the most common cyber threats.
- It focuses on five key technical controls:
  - Firewalls
  - Secure configuration
  - User access control
  - Malware protection
  - Patch management

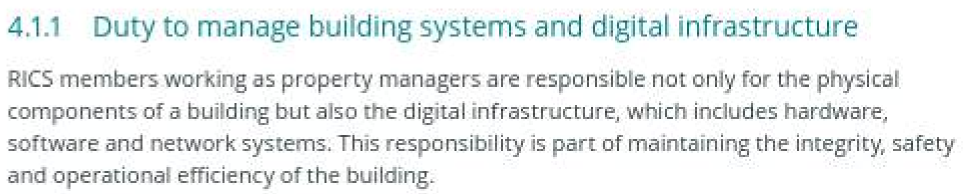
ISO27001

- ISO/IEC 27001 is an international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).
- It includes:
  - Risk assessments
  - Security policies
  - Staff training
  - Incident response
  - Continuous improvement

Smart Building & Cybersecurity Standards Matrix

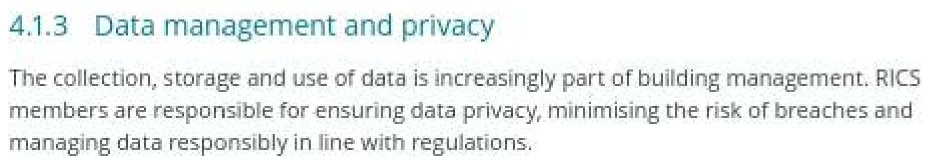
Category	WiredScore	SmartScore	Cyber Essentials	ISO/IEC 27001
Connectivity	Internet service provision, mobile coverage	Seamless digital experience for users	Not covered	Covered under Annex A.7, A.13
Infrastructure	Physical telecom infrastructure	Smart infrastructure readiness	Not covered	Covered under Annex A.11
Technology Resilience	Redundancy, disaster recovery	System uptime, failover capabilities	Patch management, malware protection	Annex A.12, A.17 (Business Continuity)
Cybersecurity	Basic resilience against cyber threats	Secure-by-design systems	Firewalls, secure config, access control, malware protection, patching	Comprehensive ISMS, risk management, access control, cryptography, etc.
User Experience	Digital services (Wi-Fi, portals)	Occupant-centric features (e.g., app control, personalization)	Not covered	Covered under awareness/training (A.7), and service delivery (A.8)
Future Readiness	Scalability, adaptability	Innovation and integration of future tech	Not covered	Covered under continual improvement (Clause 10)
Governance & Risk	Not a focus	Not a focus	Basic risk mitigation	Core to the ISMS (Clauses 4–10, Annex A)
Certification Type	Building-level, scored	Building-level, scored	Self-assessment or audited (Plus)	Audited, internationally recognized

RICS, Property Managers and Ownership of Risk



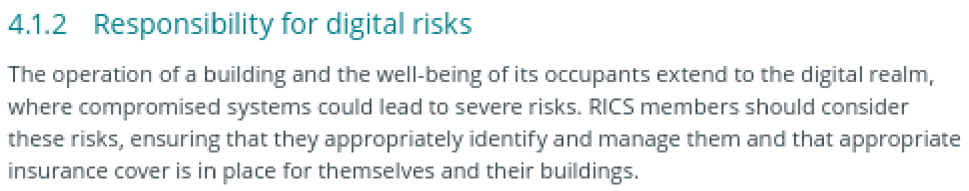
4.1.1 Duty to manage building systems and digital infrastructure

RICS members working as property managers are responsible not only for the physical components of a building but also the digital infrastructure, which includes hardware, software and network systems. This responsibility is part of maintaining the integrity, safety and operational efficiency of the building.



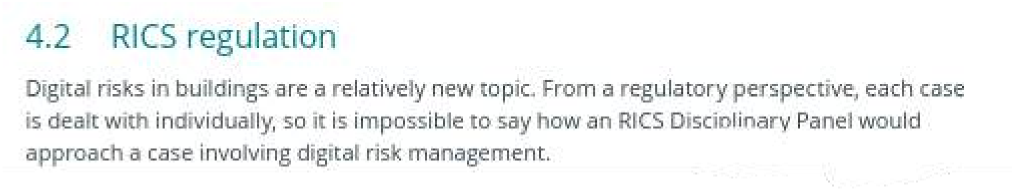
4.1.3 Data management and privacy

The collection, storage and use of data is increasingly part of building management. RICS members are responsible for ensuring data privacy, minimising the risk of breaches and managing data responsibly in line with regulations.



4.1.2 Responsibility for digital risks

The operation of a building and the well-being of its occupants extend to the digital realm, where compromised systems could lead to severe risks. RICS members should consider these risks, ensuring that they appropriately identify and manage them and that appropriate insurance cover is in place for themselves and their buildings.



4.2 RICS regulation

Digital risks in buildings are a relatively new topic. From a regulatory perspective, each case is dealt with individually, so it is impossible to say how an RICS Disciplinary Panel would approach a case involving digital risk management.

https://www.rics.org/content/dam/ricsglobal/documents/standards/Digital-risks-in-buildings-1st-edition.pdf

Secure Smart buildings

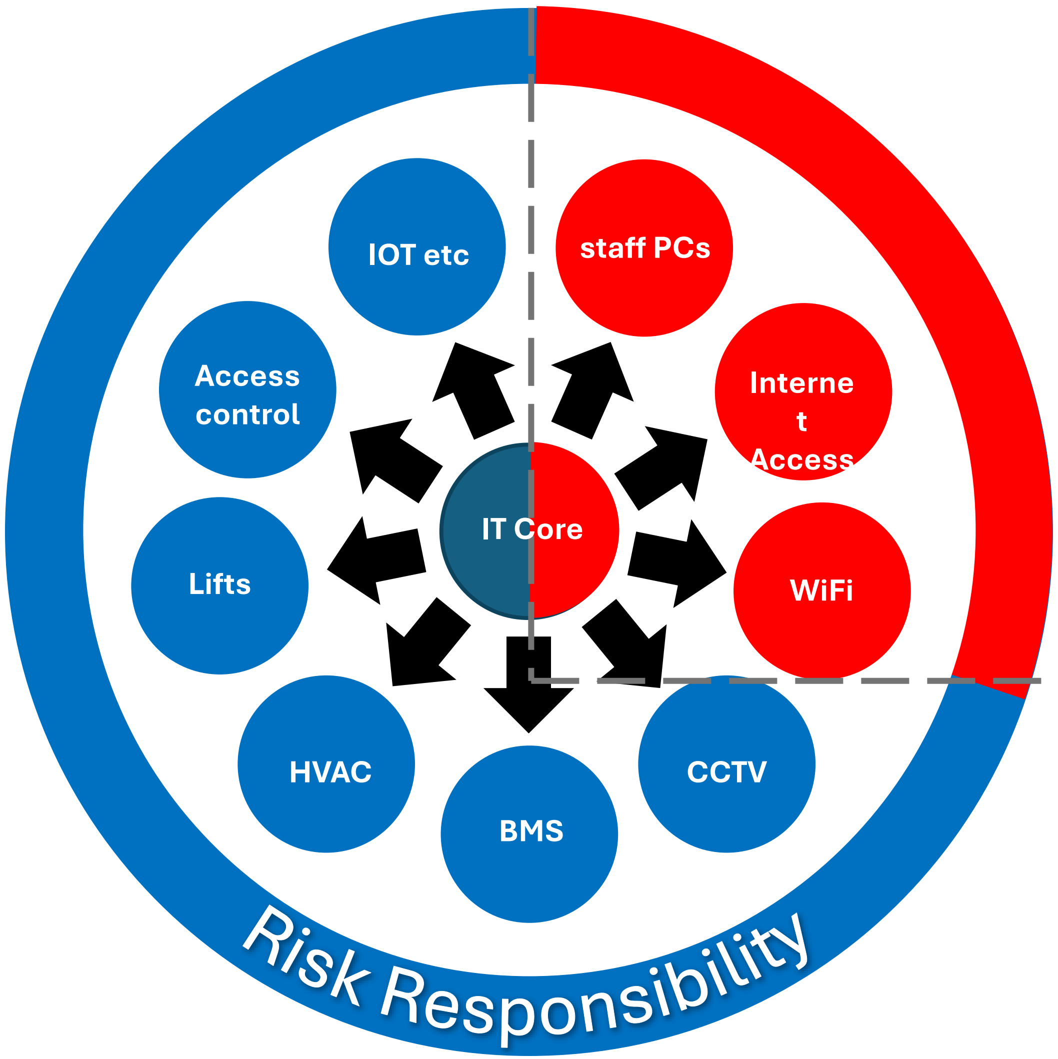
- In the realm of smart buildings, cybersecurity is no longer an optional consideration; it is a fundamental requirement.
- To effectively secure a smart building, cybersecurity must be integrated from the very beginning of the design process.
- The cybersecurity landscape is constantly evolving, with new threats emerging every day. To stay ahead of these threats, smart building systems must be continuously monitored, and both software and hardware components must be regularly updated.
- Even the most advanced security systems can be compromised if the people who use them are not adequately trained. Building managers and occupants need to be aware of the potential risks and trained to recognise and respond to security threats.

Secure Smart buildings

- Modern smart buildings require high-capacity, secure networks that can support the data demands of various systems.
- Security appliances such as firewalls, intrusion detection systems and real-time monitoring tools are crucial components of a secure network infrastructure.
- Physical security is also an often overlooked aspect of cybersecurity in smart buildings. Ensuring that server rooms, network closets and access points are secure from unauthorised access is just as important as securing the data that flows through them.

Modern Network Services

- Asset Management
- Secure Device Build / Endpoint Detection and Response
- Secure Network
- Secure Wireless Network
- Resilient Internet Connectivity
- Patch & Vulnerability Management
- Vulnerability Scanning / Managing Penetration Testing
- vCISO / CSaaS / Risk Assessment



modernnetworks

Scope of Modern Networks

- Management agent staff computers
- Servers
- Core Network
- Wifi Access
- Internet access
- Management agent access control
  - AD
  - Office 365

3rd Parties

- Own staff
- Operational Technology (OT)
- Information Technology (IT)
  - Servers
  - Workstations
  - Remote Access
  - Wireless Technology

WiredScore and SmartScore consultants

Sam Jack

- Cyber Security Engineer

Chris Kenworthy

- Pre-sales Consultant

Questions

gwilliams@modern-networks.co.uk

modernnetworks