Cybersecurity in the built environment: Can your building be hacked?

Chris Grundy

Received in revised form: 13th June, 2017

E-mail: c.grundy@cundall.com

***Chris Grundy**, MEng, MIET, leads Cundall's IT and audio-visual discipline, a specialist division of global engineering consultancy, Cundall. He works globally with occupiers, developers and landlords to use technology to transform how people operate within and manage buildings. His team consults on workplace transformation and smart building technology, creating value while reducing cybersecurity risk. He has extensive experience in IT and the built environment from over 15 years of delivering major projects including corporate headquarters, campuses, estates and data centres.*

Abstract

The use of information generated by building systems is changing the way workplaces are designed and operated. Drivers such as staff mobility, preference and wellbeing are leading to an unprecedented level of integration between building systems, their occupants and building managers. To achieve the benefits of integration while mitigating business risk, real estate managers need to consider the three pillars of information security: confidentiality, integrity and availability.

Keywords: business risk, information security, cybersecurity, cyber-physical security, security framework, confidentiality, integrity, availability, regulation, legalisation, borderless buildings, Internet of Things, IoT, smart buildings, GDPR

INTRODUCTION

Chris Grundy

Corporate real estate directors/managers can now have a real-time view of the assets they are managing, along with an insight into how space is being used. This is enabled through devices and different building systems communicating information with each other — the 'information age of buildings'.

Until recently, most real estate professionals would only consider the availability of building systems — ie they must operate, and in some cases on a 24×7×365 basis. The idea that they should also know the health/trust level (integrity) of their systems and that their systems hold personal data that needs protecting is not immediately obvious.

This paper explores the following topics:

- Information age of buildings — shift from siloed to integrated building systems.
- Business risk.
- How current/emerging trends in workplace and building design impact cybersecurity considerations.
- A security framework for corporate real estate professionals to follow and key questions to ask of their teams, designers and building operators.

INFORMATION AGE OF BUILDINGS

The era of separate building systems such as building management systems (BMS),

Corporate Real Estate Journal
Vol. 7 No. 1, pp. 39–50

2043–9148

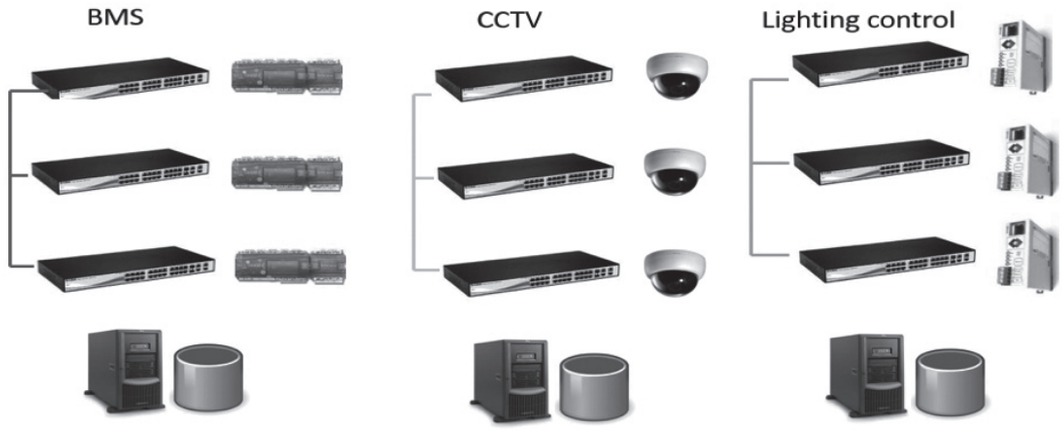

Figure 1 Separate and siloed systems

security and lighting control is coming to an end. New designs are replacing siloed systems with a network of interconnected systems. This shift is represented in Figures 1 and 2.

In addition to the level of integration now being observed, other trends are increasing both the volume and type of information being produced within buildings. These trends include:

- Mobility — a single device such as a smartphone or card for staff interaction within buildings.

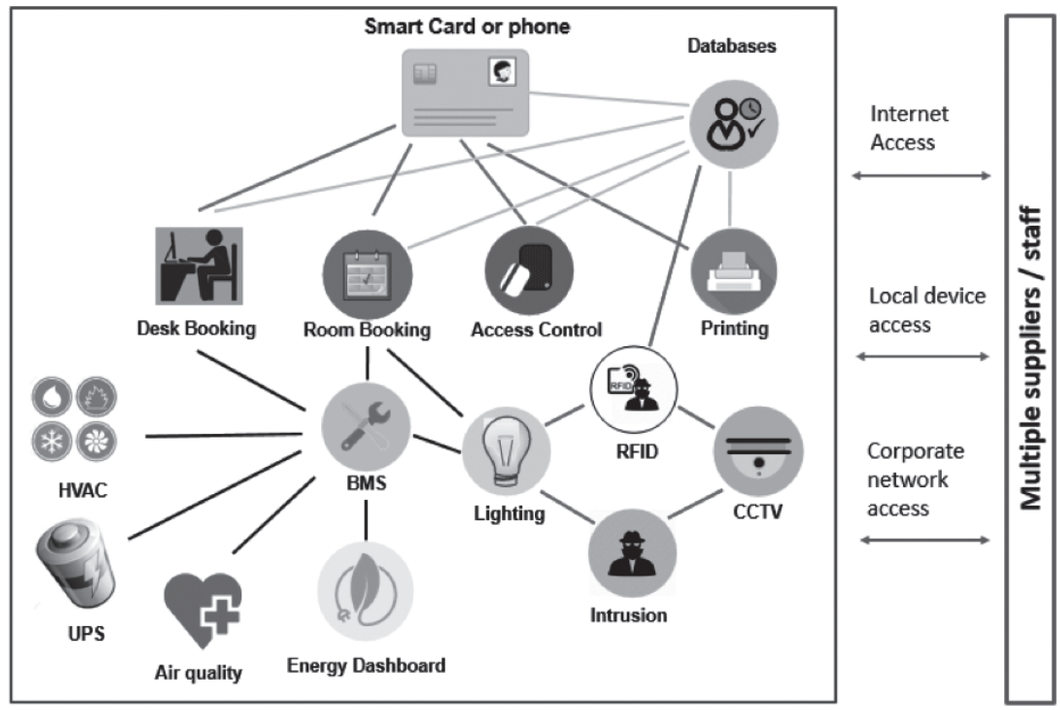

Figure 2 Example interconnected systems

- Internet of Things (IoT) — the growth in devices connected to the internet.
- Tracking of people and devices within buildings to understand how space and facilities are used in real time.

INFORMATION AGE: CIA TRIAD

The integration shown in Figure 2 enables benefits for both occupants and building managers but raises new challenges in the control of information and subsequently the cybersecurity of buildings and estates.

To achieve the benefits listed in Table 1, real estate directors/managers and their advisers need to consider the three pillars of information security: confidentiality, integrity and availability — more commonly referred to as the CIA triad.

CIA, in corporate real estate terms, means:

- **Confidentiality** — keeping personal and building system data secure.
- **Integrity** — ensuring data is correct and not modified, to avoid systemic failure as interconnected systems rely on correct data. Ensuring building security — correct operation of systems such as access control, CCTV and fire alarm.
- **Availability** — ensuring data and building systems operate on a 24×7×365 basis.

In addition to CIA, building systems that provide safety-critical functions should also not be undermined. Buildings need to provide a safe environment for their occupants.

Later in this paper, a framework is presented that real estate directors/managers can use for a holistic approach to cybersecurity. In the following sections, the risks to a business are considered if a framework is not appropriately implemented.

BUSINESS RISK: CYBER-PHYSICAL — BLURRING OF THE LINES

Security is a risk management discipline. To adequately identify risk, real estate professionals need to appreciate that there is a blurring of the lines between physical security and cybersecurity. Both disciplines should be considered at the same time. As an example, consider Figure 3 where a CCTV system that is remotely or locally managed onsite with a default administration password is compromised.

In this example, a cyber vulnerability has led to cyber-physical actions: break-in and theft of data.

BUSINESS RISK: EXAMPLES

A real scenario of data breach happened in 2013 to the American retail company Target. The attackers managed to enter the company's network by stealing the credentials of a third-party HVAC vendor and the lack of security protocols to monitor activity allowed them to take customers' data, including 40m credit cards and debit cards.[1]

Table 1: Information age of buildings — benefits

Feature	*Benefit*
Mobility	Seamless roaming of staff within and between offices
Preference	Localised control of staff environment
Utilisation	Optimisation of an asset, release or reassign
Well-being	Monitoring air quality and people's activity/inactivity
Maintenance	Proactive and informed regimes
Energy efficiency	Granular information tracked to occupancy, use and ambient conditions

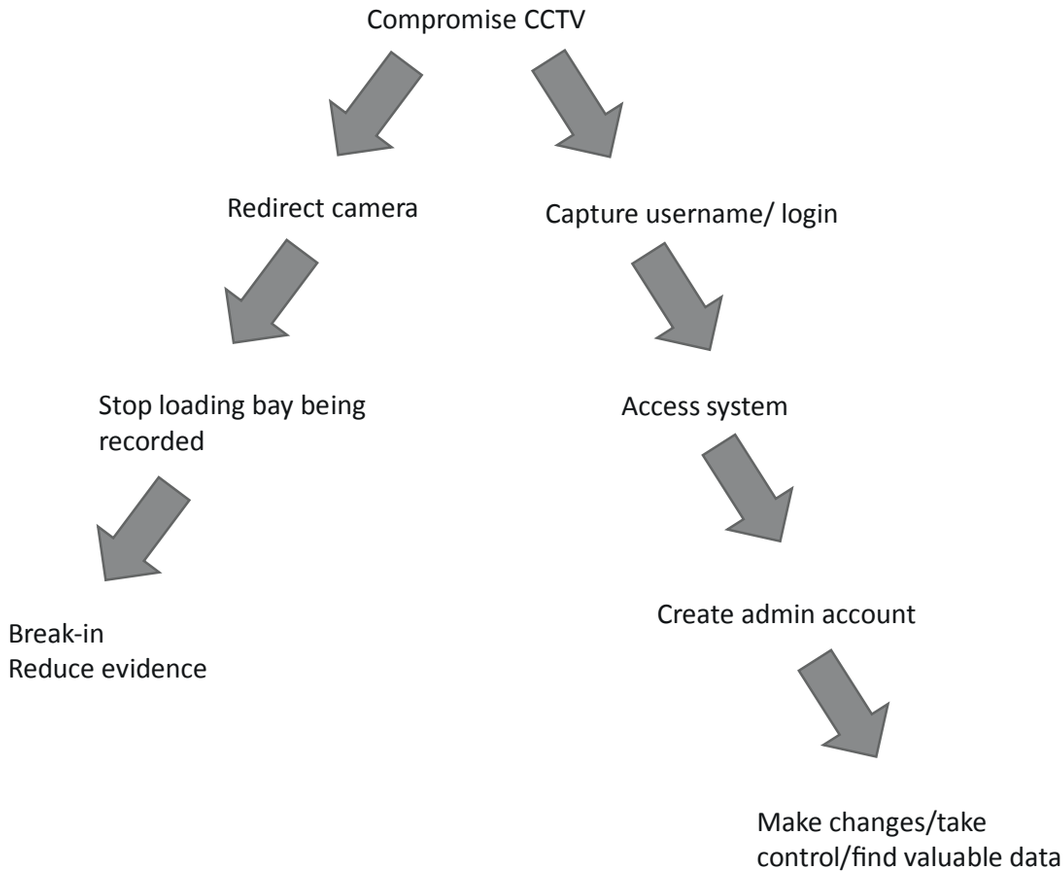

Figure 3 Blurring of lines — cyber-physical

In 2013, researchers found that Google's building management system (BMS) at its Australian office was connected to the internet without the latest software patch installed. Researchers obtained the administrative password and accessed the BMS.[2]

Not all cyber or cyber-physical risks may lead to theft of data, as illustrated in Table 2, but the risks can broadly be categorised as:

- **Override security controls** — steal intellectual property.
- **Nuisance** — drive up energy bills and break building systems.
- **Disruption** — turning off building systems.
- **Ransom** — take control of building systems.
- **Life safety/panic** — threaten duty of care to staff and visitors.
- **Staff information** — steal personal information, research members of staff.

As systems become more interconnected (see Figure 2), multiple building system risks can be exposed. An example being where a security consultant obtained control of room HVAC, lighting, TVs and blinds at the St. Regis Shenzhen Hotel.[3]

BUSINESS RISK: REGULATORY PERSPECTIVE

Many of the benefits listed in Table 1 rely on the use of personal information to locate, identify and provide options to building

Table 2: Example building system risks

Building system	*Example actions*
CCTV	Divert cameras away from criminal activity or delete footage.
	Capture sensitive information (passwords, business details).
HVAC	De-activation of cooling/heating to damage equipment.
	Extreme temperatures make working difficult and have an impact on productivity.
Lighting	Turn off lights: safety and productivity issues, public panic.
	Energy management functions disrupted.
Access control	De-activation/addition of users, increase authorisation.
	Remote release of secure doors for unauthorised access.
Lift	Denial of service on lift destination system.
	Override lift access control.
Digital signage	Inappropriate content to offend or cause panic (bomb alert).

occupants. The definition of personal information is being updated by governments to include location, online identifier or unique physical attribute such as a biometric.

Building systems hold personal information. An example includes an access control database with name, photo, biometric and vehicle registration. Location-based systems may hold staff GPS/similar coordinates, while audio-visual content management systems can hold video and audio recordings.

In the information age of buildings, real estate directors/managers need far greater visibility of what information they have, where it flows, who can see it, how it is stored and monitored. If data protection and retention is not appropriately considered, real estate directors/managers may find that their building systems could be a weak point for a cyber or cyber-physical attack.

New legislation such as general data protection regulations (GDPR) being introduced across Europe (including the UK) in 2018 will include updated definitions of personal information as described above, and will apply to companies operating in the European Union. The UK Information Commissioner's Office (ICO) has indicated that GDPR will apply to buildings, including location tracking and sensor technology. GDPR and other regulatory regimes include a key principle of accountability — that is, a data controller (typically either tenant or landlord) needs to demonstrate compliance and report data breaches within 72 hours.[4]

Buildings can be considered easy targets for organised criminals who wish to research an organisation as part of a targeted attack. For example, an access control system could provide the name, photo, location, department, privilege and potentially biometric information of a member staff. Such a breach of personal information, if not discovered and notified, could lead to large fines for the organisation.

Therefore, real estate directors/managers will need to be more proactive in their approach and adopt 'privacy first' or 'privacy by design' principles that will be a requirement of updated legislation. There will be a balance between holding and processing data to achieve the benefits in Table 1, while doing so in a cost-effective and risk-adverse manner.

BUSINESS RISK: BORDERLESS BUILDINGS AND THIRD PARTIES

Buildings are becoming 'borderless'. Like IT systems, buildings can be connected to the internet or to a corporate network, accessed

via smartphone apps, and managed by multiple third parties.

Benefits such as remote management are enabled by borderless design but, to do this, real estate directors/managers need to ask questions of their third-party building management companies. Security vetting of these companies is required, particularly as transfer of building management does not transfer cybersecurity and information security risk. There is a real risk of third parties being a weak link either through remote management/data breach of their operations or via service engineers with infected laptops connecting to building systems as part of maintenance. In the case of Target's data breach, the HVAC vendor's credentials stolen represented the weak link.[5]

BUSINESS RISK: UNDERMINING INVESTMENT

Case study 1: False confidence in resilient electrical systems

The author was responsible for the review of a new building and associated IT infrastructure in 2016. The review included two uninterruptible power supplies (UPS), each connected to a building management system operating over a building management network. The UPSs supported a critical transactional process.

When UPS software vulnerabilities were considered, it was decided to move the UPSs from the building management network and locate them on the main IT network. Why, you may ask? While the electrical engineering provided excellent protection to power interruptions, the actual management software and access to the UPSs did not.

It was deemed a lower risk in this specific case to locate the UPSs on the main IT network than have business-critical devices with a basic software authentication vulnerability located on a building management network with minimal information security features, no monitoring, quasi-ownership and internet connection. Effectively, the resilient electrical scheme could be turned off remotely by an unauthorised party.

TECHNOLOGY TRENDS IN CORPORATE REAL ESTATE

Integration of building systems, as described above, is creating benefits for building occupants and managers, while also creating cybersecurity challenges. In the following sections, other technology developments currently found in the design of buildings and offices are considered, with practical advice provided to reduce business risk.

WIRELESS DEVICE GROWTH

Providing wired data connections to devices is expensive. Therefore, there is a trend towards more communication via wireless devices. Wireless devices use radio frequency, which is finite. Real estate directors/managers should ensure that critical functions are based on wired connections. Wireless connections are prone to radio frequency jamming. Additionally, certain frequencies such as unlicensed bands are used extensively, making communication unreliable.

THIN BUILDINGS: CLOUD-BASED BUILDING MANAGEMENT SYSTEMS

There is a trend for companies that occupy multiple properties, or landlords that own multiple properties, to move to a more centralised cloud-based approach for building management systems, minimising the installation of equipment onsite in buildings. While this does have some advantages of scale and estate-wide monitoring/benchmarking, it does require further consideration of the CIA triad, along with reviewing the quality of internet connection for building system availability.

CONSUMER TECHNOLOGY

The technology people expect in buildings is influenced by the consumer space. Often technologies that emerge in people's homes/personal devices find their way into office designs 12 to 18 months later as users become more comfortable with them. Current technology includes biometrics and voice recognition, which is available on the latest generation of smartphones and digital assistants.[6] Such technology has cyber-physical considerations for the security of buildings along with retention of personal information.

INTERNET OF THINGS (IOT): NETWORKS ARE GETTING BIGGER

Internet protocol (IP) data networking is becoming the *de facto* communications medium for devices in buildings. The number of IP devices is increasing. Buildings are being constructed with hundreds or thousands of IP-based end devices/sensors operating over one or more data networks, with software applications talking to each other and sharing multiple databases.

Devices are often rushed to market and, to be cost-competitive, have minimal security features. Such issues can be exploited by using internet-based search engines that can find IoT devices.[7] Such a search tool can be used for positive reasons, however, and may help real estate managers discover their own buildings are connected to the internet without their knowledge.

There are known cases of CCTV cameras with weak security features (default passwords/passwords hard-coded into devices but accessible) being taken control of and forming a large botnet (distributed collection of hundreds or thousands of devices) to send vast volumes of traffic to internet sites to disrupt them. Such attacks are referred to as distributed denial of service (DDoS). Real estate directors/managers may find that some of their own devices within their buildings are part of such botnets.[8]

THREAT LANDSCAPE IS CHANGING

For many years, people's idea of cybersecurity, if asked, would probably be a good password and virus checker. While this is still fundamental, most applied security measures focus on looking for a 'known' threat — they are not looking for an unknown/adaptive threat. This is a challenge the IT community is starting to address through consideration of machine learning and behavioural technology.

If a building is running a critical operation such as a hosted cloud service or processing vast quantities of transactions, consideration should be given to machine learning.

POWER OVER ETHERNET (POE): DENIAL OF SERVICE

Turning things off may be crude, but it is a highly effective way to disrupt a business. Through the established use of PoE, data networks have become the second power distribution system in a building. The use of PoE is also set to grow further with the release of new standards increasing the amount of power that can be transferred to building systems such as lights, cameras, sensors and digital signage screens.

Therefore, if the integrity and availability of data networks within buildings are not considered, the possibility exists to disrupt and take control of networks to shut down large parts of buildings, including PoE lighting and security systems.

This problem was often considered 'designed out' with traditional distributed controller systems that had local memory to operate and did not need to communicate back to a central server on/offsite; however, many system topologies are now being deployed with PoE and centralised controller. A denial of service (DoS) attack on a building network will affect not just the ability for a controller/device to communicate back to a central server, but fundamentally, whether the device is on.

ENCRYPTION FOR CONFIDENTIALITY — BUT DO NOT FORGET PHYSICAL SECURITY

The use of encryption is increasing in both personal and business life. It is conceivable that in future all communication and data storage will be encrypted. This apparent level of security (confidentiality) can give false confidence, when physical security such as control zones are not considered. Additionally, in advanced situations, encryption can be used to hide malicious actions.

It is important to remember that information is not encrypted when it is created, used, displayed or played back. Therefore, consideration should be given to the following points in high-risk areas such as boardrooms, operation and plant rooms:

- Stray radio frequency from the emissions of electrical equipment.
- Overlooking of office area/computer terminal.
- Pan Tilt Zoom (PTZ) cameras that can be used to look at what an attacker wants to see.
- In sensitive environments, data network backbone data links that may not be encrypted.
- Malicious damage of telecoms links outside buildings.
- Key logging devices with radio frequency transmission.
- Audio recording in meeting rooms/dictation.
- Confidential printing.

The quality of smartphone cameras is now very high. There are cases where pictures of fingerprints on biometric readers have been taken and used to create 3D printed models/prosthetics to bypass fingerprint biometric-based security. Therefore, multi-factor authentication (something you have and something you know) is recommended.

Access to the management consoles for building systems, such as building management system head-ends, may be in back-of-house areas. Consideration should be given to securing physical access to these terminals.

NEW THREATS ARE OLD THREATS — THEY DON'T GO AWAY

Building systems have a long in-use life cycle (up to 15–20 years) and use software applications that will require updates over time to fix vulnerabilities as they are found. This creates the need for real estate directors/managers to implement a process of software updates as part of a security framework. This needs to be done in such a way that automatic software updates from a trusted source do not affect the availability of 24×7×365 systems.

ENCRYPTION FOR DATA INTEGRITY: IS BLOCKCHAIN THE SOLUTION?

Technologies that have emerged in recent years are being continuously developed — specifically, the blockchain protocol, which was first implemented for the digital cryptocurrency 'Bitcoin'. Blockchain is a network of transactions that are recorded in a decentralised distributed database (such as a distributed ledger). Each transaction of data is recorded on a 'block' and creates a chain that cannot be modified.

The IT industry is looking for new ways to deploy blockchain as a cyber-security measure. Recent developments show that it could be used to provide data integrity to business-critical functions such as transport systems, industrial control or building management systems. It may be possible to create cryptographic hashes of critical building components (ie BMS controller, sensors, actuators, etc.). The network of blockchain devices will protect the flow of sensible data inside an organisation's network without concern of it being modified.[9]

SECURITY FRAMEWORK

IT professionals operate in a dynamic environment. Like modern buildings, the systems and information they protect are borderless. IT professionals adopt a framework approach to security, which enables them to take a holistic view. Most large companies will have an information security management or enterprise architecture framework. There are several that exist, such as ISO/IEC 27000 series, along with guidance from National Institute of Standards and Technology (NIST) in the US.[10] Figure 4 shows an adapted version of NIST Framework. Such frameworks are comprehensive and perhaps only some parts will be appropriate for buildings and corporate real estate directors/managers, but they do provide a methodology for considering cybersecurity in the built environment and avoid the 'design, install and forget' scenario that often occurs when an operating view is not considered.

The benefits of adopting a security framework include:

- A holistic view leading to safer buildings.
- Helping define staff policy and training needs.
- Consideration of a contingency plan, with steps to restore building systems to health when they have been compromised.
- A rigorous approach to testing:
  - Going beyond functional testing to test abnormal conditions, or independent penetration testing by ethical hackers.
  - Consideration of behavioural science — people are often the weakest link in security as they are prone to social engineering or targets for phishing.

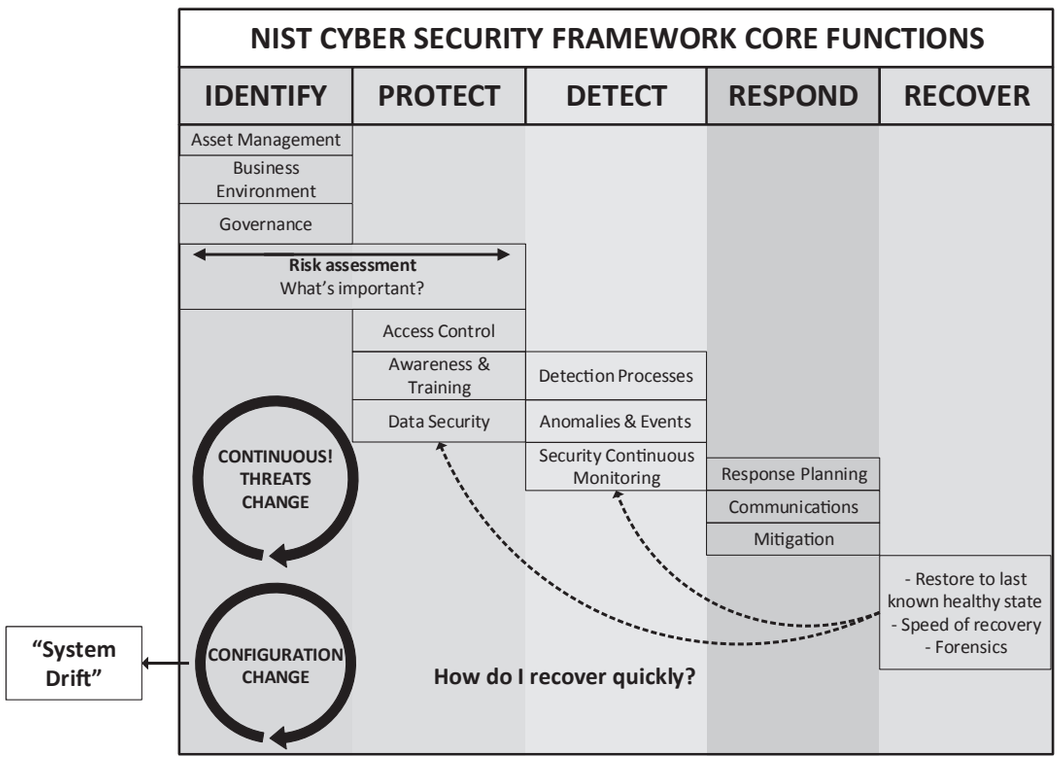

Figure 4 Example security framework

SECURITY FRAMEWORK: ASSIGNING RESPONSIBILITY

Buildings and offices have multiple designers, building systems and operation/maintenance third parties. This mix of companies creates a real problem for cybersecurity, as often no one party has overall responsibility for cyber or cyber-physical security.

To overcome this responsibility paradigm,[11] real estate directors/manager should adopt an approach such as the following:

- Accept that cybersecurity is their problem — this is how regulators see it after all.
- Adopt a security framework to provide governance, structure and focus in both the design and operation of buildings.
- Make greater use of internal IT department resources for assessing risk and mitigation methods.
- Consider the IT department taking ownership for the information security of systems.
- Make cyber and cyber-physical security a key component of procurement for third parties who will manage/maintain building systems.

Case study 2: Impact of not considering a security framework

The author was responsible for the review of the expansion of an existing public building in 2017, including the installation of a new onsite combined heat and power plant (CHP) unit. The specification of the CHP unit included the requirement for remote management. The specification did not define why remote management was required or how this would be achieved securely. The specification simply stated that the CHP unit should be connected to the internet without any measures such as a firewall.

This case study is reflective of a lack of a security framework being applied to a project.

APPENDIX

SECURITY FRAMEWORK: KEY QUESTIONS TO ASK

	Key questions
Risk assessment (identify and protect)	What is critical/non-critical? What is life safety? Where is data located and how does it flow between systems/companies? Am I storing data relevant to the tasks to be accomplished? What technology/process is appropriate to mitigate risk? Have I asked my staff for consent to hold personal data? Who are the data controllers and data processors? What is the financial or reputational impact?
Protect	Once risk has been assessed, what administrative, technical and physical controls are required? In a world of multiple designers, packaged procurement and multiple subcontractors, what are the cyber-security responsibilities? Have all information flows been mapped, and is there an alternative way for achieving 'building integration' without exchanging information?
Detect	Once systems are installed/upgraded, who is going to manage, monitor and change system(s) to the new business needs? Business-critical environments — what assurance has taken place to test the effectiveness of security measures? Do third party contracts allow for right to audit?
Respond and recover	What is the plan to restore building systems when they have been hacked and how is this tested?
All phases	What training/policy is required? What is the difference between staff and visitors?

SECURITY FRAMEWORK: ENGAGING WITH LANDLORDS — KEY QUESTIONS

Real estate directors/managers may have many different buildings within their estate and possibly a mixture of owner occupied and leased spaces. Where buildings are leased, not all building systems may be the responsibility of the tenant, but rather the landlord. Ideally, landlords should define how their tenant's systems and data are protected to avoid obscurity.

In this scenario, dialogue with the landlord is required to ascertain the cybersecurity of systems. The landlord should have measures in place, as it will be the tenant who will suffer if the building is compromised in some way.

Therefore, the following questions (in addition to those above) apply equally to landlord or tenant managed systems:

Area	*Questions*
Discovery	Is the building connected to the internet without prior knowledge — use IoT search engines? Are landlords holding personal information on employees, and in what systems? How is personal information exchanged between systems?
Data	Who owns the data buildings generate?
Password discipline	Is there a multi-site password policy?
Software updates	Do building systems have up-to-date software patches?
Connectivity to internet	Who has remote access and for what purpose? Is there a firewall/security appliance and is it configured correctly?
Assurance	If business-critical such as a data centre, what security testing has taken place?

References

(1) Olavsrud, T. (2014), '11 Steps Attackers Took to Crack Target', CIO, available at http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html (accessed 9th June, 2017).

(2) Zetter, K. (2013), 'Researchers Hack Building Control System at Google Australia Office', Wired.com, available at https://www.wired.com/2013/05/googles-control-system-hacked (accessed 9th June, 2017).

(3) Zetter, K. (2014), 'Here's How Easy It Could Be for Hackers to Control Your Hotel Room', Wired.com, available at https://www.wired.com/2014/07/hacking-hotel-room-controls/ (accessed 9th June, 2017).

(4) EU GDPR Portal (2016), 'Frequently Asked Questions about the GDPR', available at http://www.eugdpr.org/gdpr-faqs.html (accessed 9th June, 2017).

(5) Olavsrud, T. (2014), '11 Steps Attackers Took to Crack Target', CIO, available at http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html (accessed 9th June, 2017).

(6) Samsung UK (2017), 'Security — Iris Scanner | Samsung Galaxy S8 and S8+', available at http://www.samsung.com/uk/smartphones/galaxy-s8/security/ (accessed 9th June, 2017).

(7) Shodan (2009), available at https://www.shodan.io (accessed 9th June, 2017).

(8) *Construction Manager Magazine* (2017), 'Cybercrime: The dos and don'ts of smart tech', available at: http://www.constructionmanagermagazine.com/news/cybercr0ime-we-g9etting-too-sm8art-our-own-good/ (accessed 9th June, 2017).

(9) Shah, S. (2017), 'Blockchain: What It Means for Cybersecurity', *Infosecurity Magazine* (2), pp.47–49, available at https://www.infosecurity-magazine.com/magazine-features/blockchain-means-for-security/ (accessed 9th June, 2017).

(10) Boyes, H. (2013), 'Resilience and Cyber Security of Technology in the Built Environment', London, The Institution of Engineering and Technology, p. 36, available at http://www.ecalimited.co.uk/pdfs/ebooks/Resilience%20&%20Cyber%20Security%20of%20Technology%20Tech%20Briefing.pdf (accessed 9th June, 2017).

(11) Ibid.