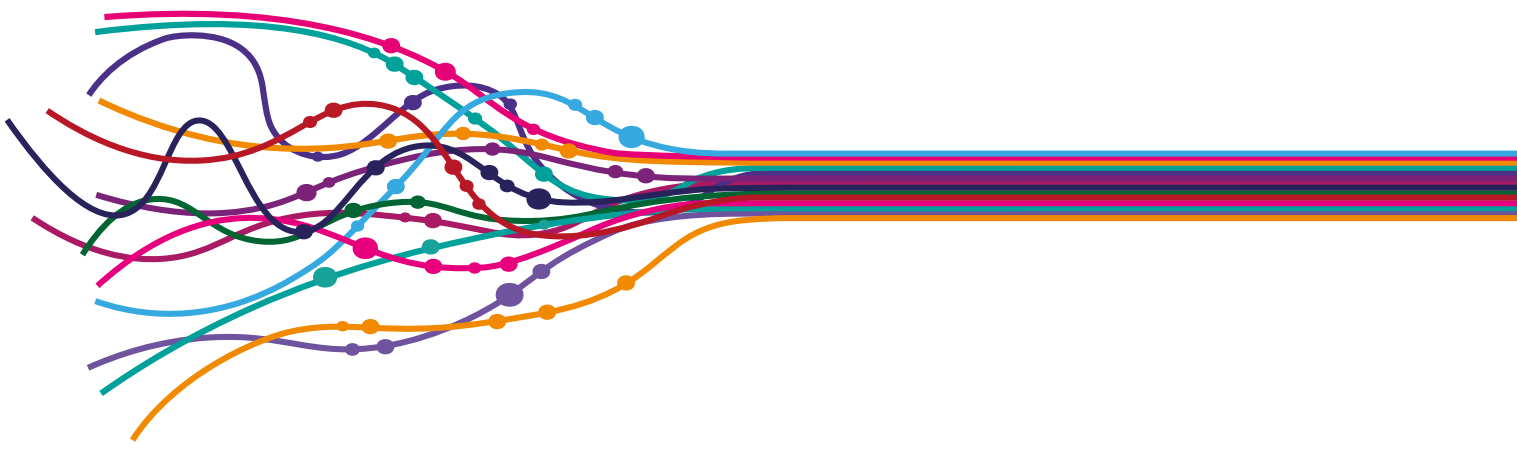
Cyber-threat and the FM solution

urgent technology

Cases of cyber-attacks and corporate espionage are on the rise. In 2017 one notable high-profile cyber-breach was that of the UK's National Health Service (NHS), in which computers throughout the UK were frozen by an attack of 'ransomware'. The increasing adoption of the Internet of Things (IoT), which connects devices throughout a building or even an entire city, brings may operational benefits by automating building services, but also opens up the real risk of organisations being hacked through their Building Management Systems (BMS).

As the lynchpin behind the maintenance of a building's operational integrity, today's facilities manager (FM) plays an important role in protecting systems against hackers as well as meeting the latest regulatory standards.

This white paper explores the threats posed by cyber-security breaches, and explains how the FM can become the guardian of an organisation's security and data.



1

Introduction

In September 2017 one of the world's biggest accountancy firms, Deloitte, admitted it had been hacked, and according to reports[1] the cyber-security attack had gone unnoticed for months. It is thought that the hacker was able to access the global email server through an "administrator's account" that, in theory, gave them privileged, unrestricted "access to all areas". The incident is all the more notable given the fact that in 2012 Deloitte was ranked the best cyber-security consultant in the world.

Earlier that same month Equifax, the US credit monitoring agency, admitted the personal data of 143 million US customers had been accessed or stolen in a massive hack in May, with around 400,000 UK consumers and 100,000 Canadians also affected.

Not even the tech giants are immune to hacking. In 2013, Google's Wharf 7 office in Sydney, Australia, was hacked via its BMS by two security expert researchers who were able to access the building control panel showing the layout of water pipes in the third floor at its Australian headquarters.[2]

According to one of the researchers who uncovered the Google system online: "We could have taken over the operating system and accessed any other control systems that are on the same network as that one. We didn't do that because that wasn't the intent... But that would be the normal path if an attacker was actually looking to do that."

Direct attacks are not the only risk. In 2014 Yahoo, the world's second largest e-mail service provider, was the victim of a major coordinated attack in which both usernames and passwords were compromised. In this incident, the information was stolen from an unsecured, third-party database.[3]

Equifax admitted the personal data of around 400,000 UK consumers had been accessed or stolen in a massive hack in May 2017.

> "We could have taken over the operating system and accessed any other control systems that are on the same network as that one. We didn't do that because that wasn't the intent... But that would be the normal path if an attacker was actually looking to do that."
>
> **Google researcher**

Of particular concern to FMs is the source of the cyber-attack on US company Target, which exposed credit card and personal data of more than 110 million consumers. This was carried out via a malware (short for malicious software) email phishing[4] attack sent to employees at a third-party HVAC firm that did business with the nationwide retailer.[5]

In Ukraine a power station was hacked leaving nearly 80,000 customers without power.

In other cases, the US Department of Homeland Security reported that hackers had broken into a state government facility and made it "unusually warm", while in Ukraine a power station was hacked leaving nearly 80,000 customers without power.[6]

The most worrying incident in the UK was that of the NHS. The country's National Health Service was victim to a global attack of 'ransomware', a type of malicious software designed to either block access or publish confidential information within a computer system unless a sum of money is paid. In that attack, computers at hospitals and GPs' surgeries in the UK were among tens of thousands hit in almost 100 countries by malware that appeared to be using technology stolen from the National Security Agency in the US. In this case, it created a message which popped up on computers in hospitals and GP surgeries simultaneously across the UK demanding money in exchange for access to the PCs.[7]

All these incidents demonstrate that cyber-hacking is no longer the sole concern of the IT department; it is an assault on the entire organisation, from the C-Suite, to HR and FM.

Image: © Samuel Zeller

2

What is the cyber-threat and what are its consequences?

The systems used to automate and maintain building controls can be used to deliver building managers and FMs vital data on a variety of areas; including health and safety compliance, space usage and lift maintenance. They can also be used to monitor services requirements; for example, the use of sensors that connect washrooms to smartphones or tablets that enable cleaning and facilities staff to check remotely when a maintenance visit might be required.

However, all this useful connectivity may come at a price because:[8] "The richer the data sets, the more attractive an organisation becomes to financially or maliciously motivated cyber criminals. Sadly, devices and systems that leverage the power of data, often become the point of network compromise when poorly secured devices are networked and create jump points to critical systems such as fire alarms, HVAC and CCTV systems where data can be stolen or abused".

Yet despite all these growing threats there is evidence that organisations are still doing little to protect their systems from cyber-attacks, and the built environment appears to be particularly vulnerable. A survey by the Electrical Contractors' Association (ECA)[9] and Scottish electrical trade body SELECT found that almost four in 10 clients (39 per cent) did not take any steps to protect smart installations in buildings from cyber-threats.

The Cyber Security Breaches Survey 2017 found that just under half (46%) of all UK businesses experienced at least one cyber-security breach or attack in the previous 12 months.

This research is complemented by the Cyber Security Breaches Survey 2017[10] which found that despite just under half (46%) of all UK businesses experiencing at least one cyber-security breach or attack in the previous 12 months, rising to two-thirds among medium firms (66%) and 68% for large firms, a sizable proportion of businesses still did not have basic protection or had not formalised their approaches to cyber-security.

It also revealed that:

- Under two-fifths have segregated wireless networks, or any rules around encryption of personal data (37% in each case).
- Just a third have a formal policy that covers cyber-security risks (33%), or document these risks in business continuity plans, internal audits or risk registers (32%).
- Under a third (29%) have made specific board members responsible for cyber-security.
- Only a fifth (20%) of businesses have had staff attend any form of cyber-security training in the last 12 months, with non-specialist staff being particularly unlikely to have attended.
- One-fifth (19%) are worried about their suppliers' cyber-security, but only 13 per cent require suppliers to adhere to specific cyber-security standards or good practice.

This lack of planning was evident in the Wannacry ransomware attack on the NHS. According to Sir Amyas Morse, comptroller and auditor-general of The National Audit Office: "[WannaCry was] a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practice."

The consequences of ignoring the threat of cyber-breaches are far reaching and could include:[11]

- Physical damage to equipment or infrastructure
- Theft of high value property
- Loss of revenue
- Bodily injury or death
- HVAC shutdown/manipulation
- Door locks being disabled
- Disabling of physical intrusion detection systems
- Loss of building lighting
- Data centre thermal overloads
- Loss of customer confidence/contracts
- Higher insurance premiums

While the repercussions of the Deloitte data breach have yet to be determined, Equifax shares fell 1.6% in early trading on Tuesday 26 September, and have fallen 27% since the company revealed the breach. Demonstrating the far-reaching impact on the organisation's leadership, following the departure of chief information officer Susan Mauldin and chief security officer David Webb,[12] Richard Smith, chairman and chief executive, has taken early retirement and forgone his annual bonus.

The Yahoo breaches almost wrecked the sale of Yahoo's core business to Verizon, and resulted in a $350m reduction in the sale price to $4.48bn. It also cost Yahoo's top lawyer Ronald Bell his job and its CEO Marissa Mayer millions in bonuses.[13]

"[WannaCry was] a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practice."

Sir Amyas Morse, comptroller and auditor-general of The National Audit Office

Despite the fact that Target was the victim of a third-party breach, the retailer has paid a very high price. CEO Gregg Steinhafel left the company soon after the incident and earlier this year the company also learned it was going to be fined $18.5 million.[14]

Added to the reputational, fiscal and personal consequences, a data breach also brings a risk of prosecution. The introduction of new European-wide General Data Protection Regulations (GDPR) affects how organisations can collect, use and transfer personal data and applies to any global company which holds data on EU citizens.

This does not just apply to data such as personnel records, but can impact on anyone responsible for the storage, destruction or recycling of equipment that contains data. As such, FMs must understand the new regulations and liaise with the various internal departments to ensure company-wide compliance, as there will be hefty financial penalties for organisations that don't. These penalties can be up to four per cent of annual revenue, or up to £20 million, whichever is greater.[15]

The Yahoo breaches almost wrecked the sale of Yahoo's core business to Verizon, and resulted in a $350m reduction in the sale price to $4.48bn.

3

The FM's role in preventing cyber-attack

To address the cyber-security risks which may affect their organisation, FMs first need to acknowledge that they have a crucial role to play. This is because, due to the evolution of information technology within the workplace, the responsibility for data security has tended to be viewed as the remit of the IT department.

However, over the last few years the global economy has increasingly devoted huge levels of investment into the IoT with worldwide investment in hardware, software, services, and connectivity[16] reaching approximately $737 billion in 2016.

According to Gartner, 5.5m devices are being connected to the Internet each and every day within the built environment, and it predicts that by 2020 that will rise to 20.8 billion.

According to Gartner,[17] 5.5m devices are being connected to the Internet each and every day within the built environment, and it predicts that by 2018, one billion devices will be deployed in commercial buildings, rising to 20.8 billion by 2020.

These trends mean that the IoT is becoming firmly established in operations and the evolution of smart buildings. Today's smart buildings are equipped with a range of IoT devices which automate much of the facility management processes, including lighting, heating, ventilation and air conditioning (HVAC), as well as lifts, escalators and security. Connected technology enables building and facilities managers to deliver higher levels of efficiency, and gives occupiers unprecedented levels of control of their surroundings, for example, enabling them to adjust their preferences for lighting and heating via mobile apps.

However, as Building Management Systems (BMS) evolve into internet-enabled Building Automation Systems (BAS), they are much more susceptible to possible cyber-threats. A technology which enables users to control all the elements of a building, including security equipment such as CCTV and door locks, is also more vulnerable to cyber-attack.

Back in 2012, Professor David Fisk of the Imperial College in London, warned that a cyber-threat on an intelligent building was imminent,[18] and the above examples illustrate how he has been proved right.

Because IoT and connected devices increase the level of risk to an organisation, it's important to establish a best practice strategy to secure data in the Cloud, protect data integrity while in transit over the public internet, and securely provision devices. This strategy should be developed and executed with the active participation of the various players involved with the manufacturing, development, and deployment of IoT devices and infrastructure.[19]

FMs who are concerned that their systems are vulnerable should begin the cyber security process by lobbying those who are responsible for the safeguarding of information to commission a data assessment. This will help an organisation identify what critical information is stored, processed or transmitted, establish why the data might be an attractive target, and establish any regulatory compliance it must adhere to.

Once the value of data is understood FMs should:

- Encourage the same parties to commission a formal risk assessment to identify the possibilities of reducing any unnecessary storage and processing.
- Assess the likelihood and impact of an attack.
- Formally identify what an appropriate security baseline should be and establish the extent of any gaps between the existing and target positions.
- Conduct an efficient data risk assessment, recommending the adoption of an information security standard and framework such as ISO 27001. This standard helps organisations respond to data risk by establishing a platform for implementing, operating, monitoring, reviewing and improving information security.[20]
- Carry out both internal and external penetration tests on the network; while internal testing is a valuable tool, hiring an outside specialist to attempt to breach your network will identify security holes the in-house team may have missed. Establish a group of 'friendly hackers' that can assess aspects of cyber security within an organisation. If possible, FMs should be part of this process; in particular by pinpointing all the physical aspects of cyber-crime. For example, helping to identify physical items that could cause a risk, such as lighting sensors and other foreign devices connected to the network infrastructure. It's worth noting that some IoT devices are cheap, disposable items and may not have sufficient inbuilt network security.

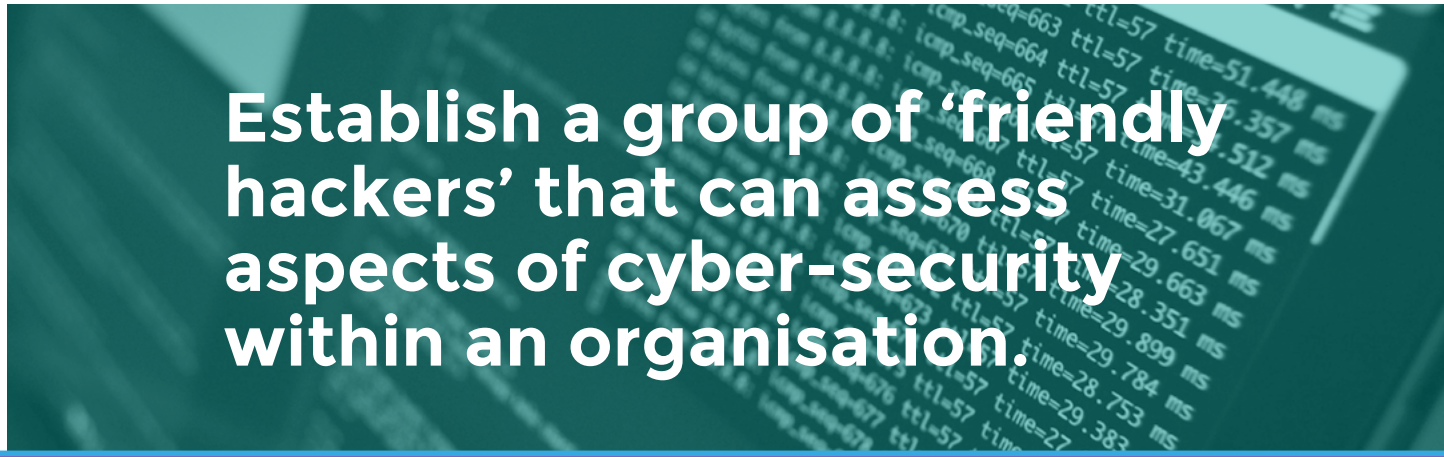
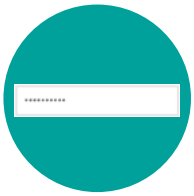


Image: © Lewis Ngugi

Once a risk assessment has been carried out, the organisation must ensure that all the weakest links within the system are detected.

- A particular area of vulnerability is access by end users to any part of the network. Researchers[21] found that 23% of employees used the same password for different work applications, 17% wrote down their passwords, 16% worked while connected to public Wi-Fi networks and 15% accessed social media sites on their work PCs. This is why employee security training should be a priority in educating staff on what habits could compromise organisational security and enable hackers to exploit the BAS or networked systems. Password disciplines should be made more complex, defined to a single user and managed via a password management tool.



Researchers found that **23%** of employees used the same password for different work applications, **17%** wrote down their passwords, **16%** worked while connected to public Wi-Fi networks and **15%** accessed social media sites on their work PCs.

- Data can enter the organisation in many ways, including emails, FTP[22] and external memory devices, such as USBs. It is important to identify these entry points and take steps to secure them. At a minimum, scanning incoming and outgoing email attachments for viruses and other threats and implementing a secure file transfer solution should be considered.

- As the NHS breach demonstrated, Microsoft Office documents and PDFs are a common means of attack, with vulnerabilities detected in Microsoft Office and Adobe Acrobat Reader on a regular basis. Patches are typically released very quickly, but if they are not applied immediately these vulnerabilities could be exploited.

- The Cloud is another potential route through for hackers because much of the data on a modern BMS is cloud-based. BMS are designed to offer functionality rather than security. As such, there is a concern that the cyber-protection solutions are less mature. This is why it is worthwhile for FMs to check with their BMS vendors to ensure that they have the most rigorous security protocols in place. Another important recommendation here is to keep your BMS separate from the main corporate IT systems.

- Conversely, the Cloud can afford a greater opportunity to protect your systems. A Computerised Maintenance Management System (CMMS) can be hosted in the Cloud. As well as automating both preventative and reactive maintenance management activities, a CMMS can provide complete visibility of the systems, enabling facility managers to be able to see the real-time status of any particular maintenance request in order to optimise the performance of their building assets. The added benefit is that the third-party centre which manages the servers and storage systems will have all the necessary security in place to make sure that vital maintenance data is never lost or destroyed.[23]

4

Conclusion

Cyber-threat is a major issue for every organisation, and with the advent of an ever more connected and digitised workplace, it is now a prime concern for the facilities and building management team. The facilities management department could become extremely vulnerable if these risks are misunderstood. However, this also represents an opportunity for the FM to demonstrate their value to the business by becoming the guardian of an organisation's security and data.

As eminent futurologist and Unwork CEO, Philip Ross, said: "With technology moving at such a fast rate, there is a risk to the profession of being left behind if it falls into the remit of the CIO or the IT director. As digital technology becomes a big disruptor in buildings there is an opportunity for facilities management to grab it and own it, but the risk is – if you don't act fast, you'll lose it to the domain of the IT director."[24]

FMs and their organisations face significant challenges in the future in combating the cyber-threats posed by the convergence of physical assets within a building with data and, as illustrated above, the ill effects that a cyber-attack could have on their organisation. This is why a wide-ranging and proactive approach should be taken to ensure that the FM can reap the undoubted benefits of workplace digitisation while ensuring that facilities are not open to undue risks.

In the future facilities management and IT must always remain alert to the latest cyber-threats, and FMs must work together with their software supply chain to help reduce the likelihood of data breaches.

"With technology moving at such a fast rate, there is a risk to the profession of being left behind if it falls into the remit of the CIO or the IT director. As digital technology becomes a big disruptor in buildings there is an opportunity for facilities management to grab it and own it, but the risk is – if you don't act fast, you'll lose it to the domain of the IT director."

Philip Ross, CEO, Unwork

References

[1] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

[2] www.wired.com/2013/05/googles-control-system-hacked/

[3] https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-hackers-stole-data-from-500-million-accounts-in-2014-idUSKCN11S16P

[4] https://en.oxforddictionaries.com/definition/phishing

[5] http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

[6] www.bbc.co.uk/news/technology-35746649

[7] https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

[8] Andy Compton, Managing Director of Information Security Consultancy, Blackfoot UK: www.blackfootuk.com/

[9] www.eca.co.uk/news-and-events/news/2017/jan/survey-four-in-10-buildings-at-major-risk-from-cy

[10] Cyber security breaches survey 2017: Department for Culture, Media and Sport

[11] www.parsons.com/Media%20Library/cybersecurity-BMS-FINAL.pdf

[12] http://www.computerweekly.com/news/450426974/Equifax-breach-claims-another-scalp

[13] https://www.ft.com/content/7541c82a-f843-11e6-9516-2d969e0d3b65

[14] https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

[15] www.fmj.co.uk/new-general-data-protection-regulations-gdpr-mean-organisation/

[16] IDC's Worldwide Semiannual Internet of Things Spending Guide

[17] www.gartner.com

[18] Fisk, D. (2012) *Cyber security, building automation, and the intelligent building, Intelligent Buildings International*, DOI:10.1080/17508975.2012.695277

[19] https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-best-practices

[20] Line of attack, Andy Compton FMJ September 2017

[21] Norrie Johnston Recruitment (NJR); Cyber-security how real is the threat and how can you reduce your risk?

[22] https://techterms.com/definition/ftp

[23] http://www.csemag.com/industry-news/codes-and-standards-updates/single-article/hacking-scandals-show-value-of-cloud-storage/d821749215a9b72df7806211cd6caaa8.html

[24] http://www.fmj.co.uk/pushing-the-boundaries/

Contact Urgent Technology
UK: +44 (0)1908 391160 USA: +1 312 809 3661
info@urgtech.com
www.urgtech.com