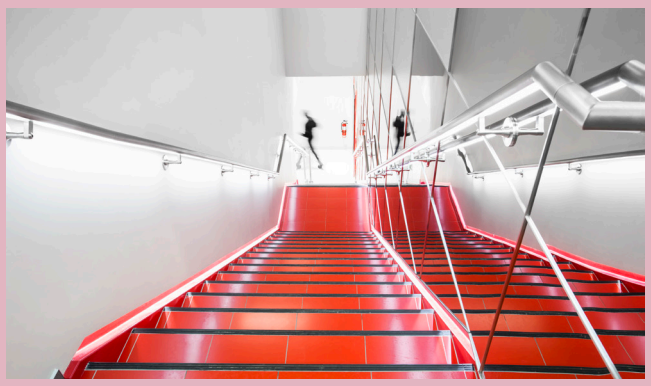
Sponsored by HID

A trend report from IFSEC Global
Connecting the Security and Fire communities



Access control in the connected workplace

The benefits and barriers to enhancing convenience and compliance in connected buildings

1. Introduction

The latest paradigm in commercial building technology is rarely described without using one or more of the words 'smart', 'connected', 'integration' or 'convergence'. While these words have subtly different meanings, they are all synonyms for the concept of linking systems together to function in concert as a coherent whole.

For the access control sector, integration with other systems in so-called 'smart' buildings is the most disruptive technological shift since the IP revolution and, later, the emergency of PSIM. Sharing data and common control interfaces, systems can collectively bolster security, generate operational efficiencies and enhance user experience and comfort. For instance, occupancy data from access control systems can feed into the HVAC system, which can recalibrate heating and air-con accordingly. This translates into energy savings – plus a big step towards compliance with regulations on sustainability and a solid return on investment for system upgrades.

And if this outcome requires integration between systems then integration needs open platforms. Blake Kozak of research company IHS Markit once described the "access control industry as inherently slow to adopt new technologies" when he was principal analyst with the research firm's security and building technologies group. Nevertheless, HID Global, the global provider of access control and trusted identity solutions, has enthusiastically embraced open platforms – whereby software code is published openly so that third parties can readily adapt it for their own platforms – even if some competitors cling to the proprietary or 'closed' models that make integration between systems from different brands impossible.

About the sponsor: HID Global

HID Global powers the trusted identities of the world's people, places and things. They make it possible for people to transact safely, work productively and travel freely. Their trusted identity solutions give people secure and convenient access to physical and digital places and connect things that can be accurately identified, verified and tracked digitally. Millions of people around the world use HID products and services to navigate their everyday lives, and over two billion things are connected through HID technology. They work with governments, educational institutions, hospitals, financial institutions, industrial businesses and some of the most innovative companies on the planet. Headquartered in Austin, Texas, HID Global has over 3,000 employees worldwide and operates international offices that support more than 100 countries. HID Global® is an ASSA ABLOY Group brand. For more information, visit **www.hidglobal.com**.

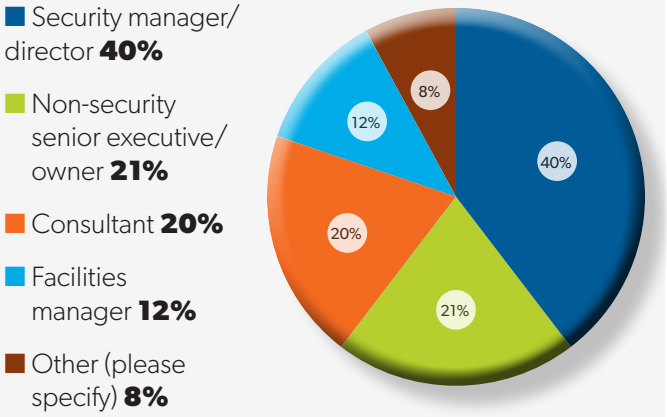
Others are increasingly following suit and open platforms are now *de rigueur* in building technologies generally. With technological limitations no longer a constraint on integration, economic and regulatory pressures are forcing the building management industry to take a much closer look at enhancing the performance of commercial buildings.

HID Global has commissioned this report to establish just how far this process has advanced. Surveying hundreds of security professionals, facility managers and building owners/managers across 54 countries, IFSEC Global sought to ascertain how integrated with one another smart building technologies are in a range of building types, from offices to industrial premises. The industry poll had a particular focus on access control, secure identities and credentials and how they consolidate across disparate systems for enhanced monitoring and user experience as people enter and move around buildings and gain access to different systems.

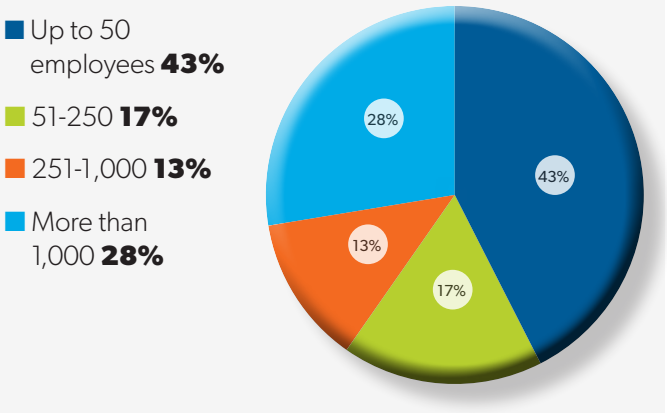
HID Global, which is championing the term 'connected workplace', also wanted to ascertain awareness levels regarding the benefits of integration, to what extent they incentivise system upgrades, whether integration is associated with a heightened cybersecurity threat and viewpoints on what the convergence of physical and IT systems means for training needs and the structure of IT, facilities and physical security teams.

The report also gives HID Global the chance to dispel what they see as myths or misconceptions regarding the connected workplace. Responses to the findings from Ashish Malpani, director of product marketing at HID Global, are interspersed throughout the report.

Which of the following best describes your role?



How many employees are in your organisation?



CONTENTS

2.Defining connected buildings

The lexicon of modern building technologies – 'intelligent', 'smart', 'connected' and so on – is often bewildering and regularly misused. Many terms lack anything approaching definitive definitions. But what does it all mean, in practice, for the effectiveness of building management in general and access control in particular – in terms of security, operational efficiency and the comfort and convenience of occupants?

Intelligence, in the context of building control, is nothing more than the ability of a building to gather information and respond to it autonomously and the concept has been around since the 80s. Most commercial buildings already have intelligent building management systems in place to monitor and efficiently manage energy and water usage. Building owners and facility managers may therefore look at the hype surrounding 'smart' or 'connected' buildings and dismiss it is nothing new.

The truth is there remains no clear definition of a smart or connected building. Several academic papers have, however, attempted to ascribe some definitions to the new vocabulary. From these, we can discern at least a few characteristics that qualify a building for smart status:

- Integrated
- Data-driven
- Adaptive
- Sustainable in terms of energy consumption
- Interactive/intelligent/occupant-aware: automatically responsive to occupant requirements

Buildings of yesteryear often had 'intelligent' functionality in HVAC, access control or lighting systems, but these capabilities were largely siloed with each system locked into separate, proprietary platforms. In contrast, 'connected' buildings link building management solutions together onto a common framework.

Working in concert, such integration can offer the following benefits:

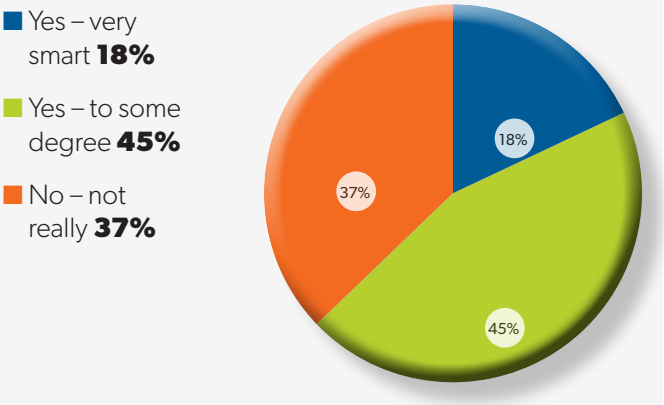
- Long-term cost savings
- Deeper insight into performance of building and occupants
- Single management interface
- Improvements in productivity and occupant comfort/convenience
- Open architectures mean future-proofed systems
- Identity-aware irrespective of authentication mechanism
- Enhanced security: easier to track activities of occupants within a building, across multiple systems

View from the vendor

"The connected workplace is where the building services the employee. It's about valuing convenience: where the workplace knows who you are and provides services based on your location, access level or the work you want to get done at that particular time. Most buildings don't really serve this experience because it's expensive, given today's technology." **Ashish Malpani**, *director of product marketing, HID Global*

Would you define your building as 'smart'?

(ie, Network-connected systems that generate, analyse and respond to data automatically for a more efficient, people-focused environment)



3. How connected are buildings in 2017?

A majority (63%) of our survey respondents felt their building was 'smart' to at least some degree. This represents a 13% increase on 2016 when the same question was posed for a previous IFSEC Global report on smart buildings, indicating brisk growth in the prevalence of connected building tech. Eighteen percent thought their building was 'very smart' – plenty of room for growth there then. Indeed, global spending on smart building technology has been forecast to grow from $7bn in 2015 to $17.4bn by 2019 (IDC Insights: Business Strategy: Global Smart Building Technology Spending 2015–2019 Forecast).

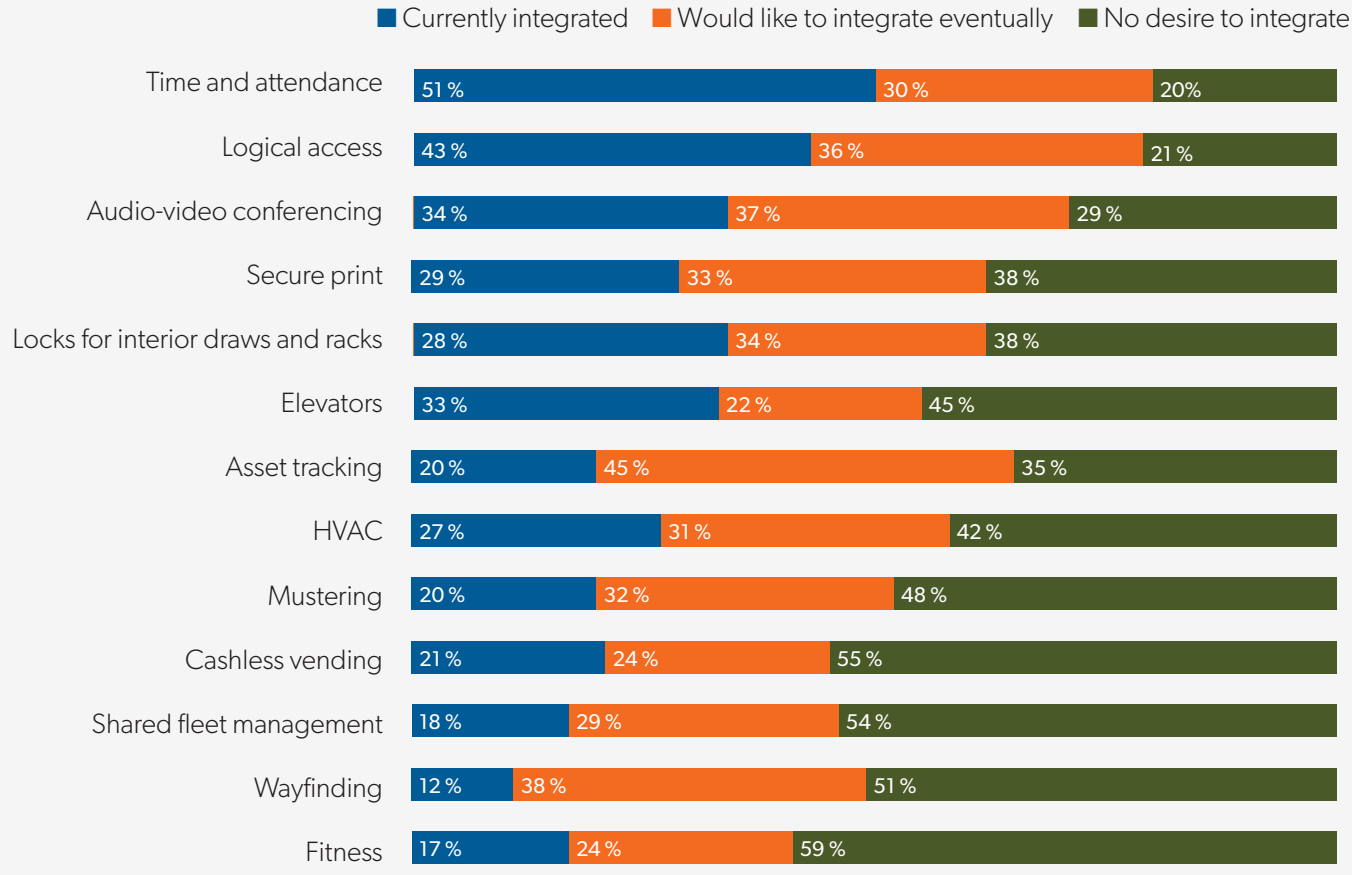
This must come, it should be noted, with the caveat that conceptions of what 'smart' actually means vary – although the survey did offer the following definition: "network-connected systems that generate, analyse and respond to data automatically for a more efficient, people-focused environment".

"We're in the process of integrating KNX, Tridium, Bacnet IP, Crestron, AMX and Polycom with IoT sensors and building management."

UK-based consultant in the construction industry

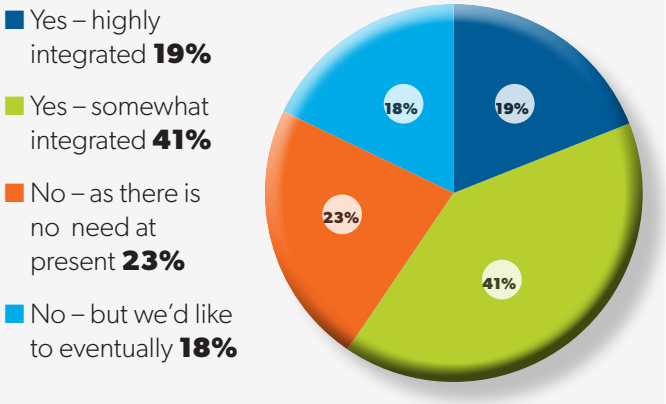
Respondents were asked which of their building systems were integrated with other building systems and, where they weren't, which ones they intended to integrate eventually. Time and attendance led the way with about half (51%) of all systems integrated. The following building systems were also integrated in at least a quarter of buildings surveyed: logical access, audio-video conferencing, elevators, secure print, locks for interior draws and racks and HVAC. Cashless vending, mustering and asset tracking were integrated in about one in five instances.

Which of these systems are currently integrated with other building systems and which do you want to be integrated eventually?



Regarding those systems not already integrated, survey respondents were more likely to want to integrate them eventually than not in every instance apart from asset tracking, AV conferencing, logical access and – notably, given how widespread integration already is – time and attendance.

Is physical access to the building and/or individual rooms integrated with other building systems and do you want/expect it to be?



Access control integration

When time and attendance and visitor management are integrated with security systems – like ANPR, fire, intruder and CCTV – the result is often streamlined costs. The same outcome can emerge from integration with non-security systems (like HVAC, as we explain on page 9). Overall, three in five (60%) access control systems are integrated with other building systems, with just under a third (32%) of integrated systems classed as 'highly integrated'. This comfortably eclipses the next most commonly integrated technology in the countdown, AV conferencing, on 33%. The second and third most widely integrated systems – time and attendance and logical access – were also access-control related, while locks for interior draws and racks were integrated in 28%.

If access control is more widely integrated than all non-security building tech, this perhaps undermines the perception in some quarters that access control is a conservative industry. This also underlines the fact that most employees today are obliged to carry and/or remember multiple credentials to interact with building management systems. However, with 56% of respondents whose access control systems were not integrated insisting they had no intention to integrate, there is perhaps a strong seam of conservatism among facilities and security staff.

4. The benefits of integration

Done properly, integration can bring a wide range of benefits. But how many respondents recognise these benefits, based on their knowledge and/or experience of integrated systems? About three in five for every benefit posed – around operational efficiencies (62%), 'user convenience' (61%), 'adding value to existing systems' (60%) and 'overall building security' (57%) – so not overwhelming majorities. Clearly, then, vendors and integrators have some work to do to optimise integration and convince end users of its benefits.

A significant portion – 37% – thought that having a smart building could help them attract and retain talented employees. And 42% would be much more likely to choose a particular vendor if they offered an integrated system – for instance where smart elevators or smart parking integrated with building access control.

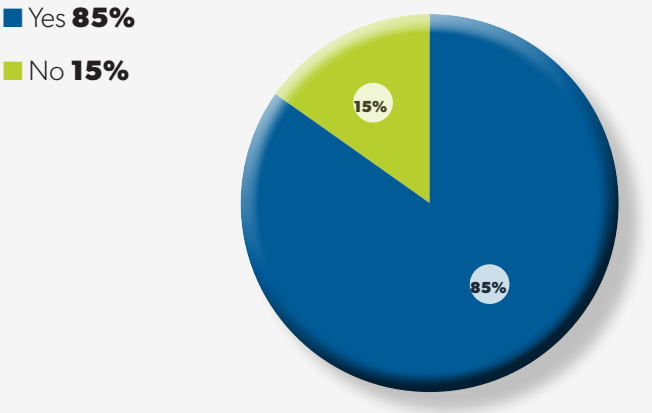
View from the vendor

"As a new employee, if everything else was equal, I would definitely prefer to join a company that makes my life much easier than one where it takes many additional clicks and several minutes longer just to gain access to a system. As an employer, I can really use this as a competitive advantage and a marking tool to attract new talent – especially with millennials entering the workplace." **Ashish Malpani,** *director of product marketing, HID Global*

Ask a government authority, a site owner, a facilities manager and a building occupant to list the primary benefits of smart building technology and you might get four very different answers. In some ways, this underscores the challenges posed by connected buildings, which are defined by more than just the technology driving them.

Of course, low-hanging fruit such as operational efficiency will remain the dominant reason for procuring connected technologies, but as buildings become more seamlessly connected and the internet of things (IoT) continues to move into the mainstream of building management (read more about IoT on page 14) the benefits will become more profound – for building owners, for occupants, and for the environment. As Derek Clements-Croome, Professor of construction engineering in the department of construction management and engineering at the University of Reading, UK puts it: "The building, its services systems and the management of the work process all contribute to the wellbeing of the people within the organisation."

Did you know it was possible to connect someone's ID across multiple systems, through multiple devices, throughout an organisation?



"We are able to do lots of things in a minimum amount of time. We don't have to run around looking to do stuff as everything in integrated into a single unit."

South-Africa-based executive in the IT industry on integration benefits

View from the vendor

"Seos technology from HID Global allows smartphones, wearables and other devices to function as identity credentials. It offers three principle benefits. One is allowing different systems to leverage the same credentials to have their own data on that one credential. Secondly, it's independent of form factor or it supports multiple form factors – from plastic cards or key fobs to wearables and mobile phones. And third, we've shown that this convenience needn't compromise security. The way the technology is architected, the possibility of unauthorised access is next to nil." **Ashish Malpani,** *director of product marketing, HID Global*

Smart retrofitting, sustainability and slashing energy costs

"Let's remember that buildings don't have to be new to be efficient. Today's leading building owners are converting existing buildings into models of sustainability."
Memoori, smart building research

It is estimated that more than 80% of the UK building stock that will exist in 2050 has already been built today. This staggering statistic highlights the need to retrofit these smart technologies into existing building environments.

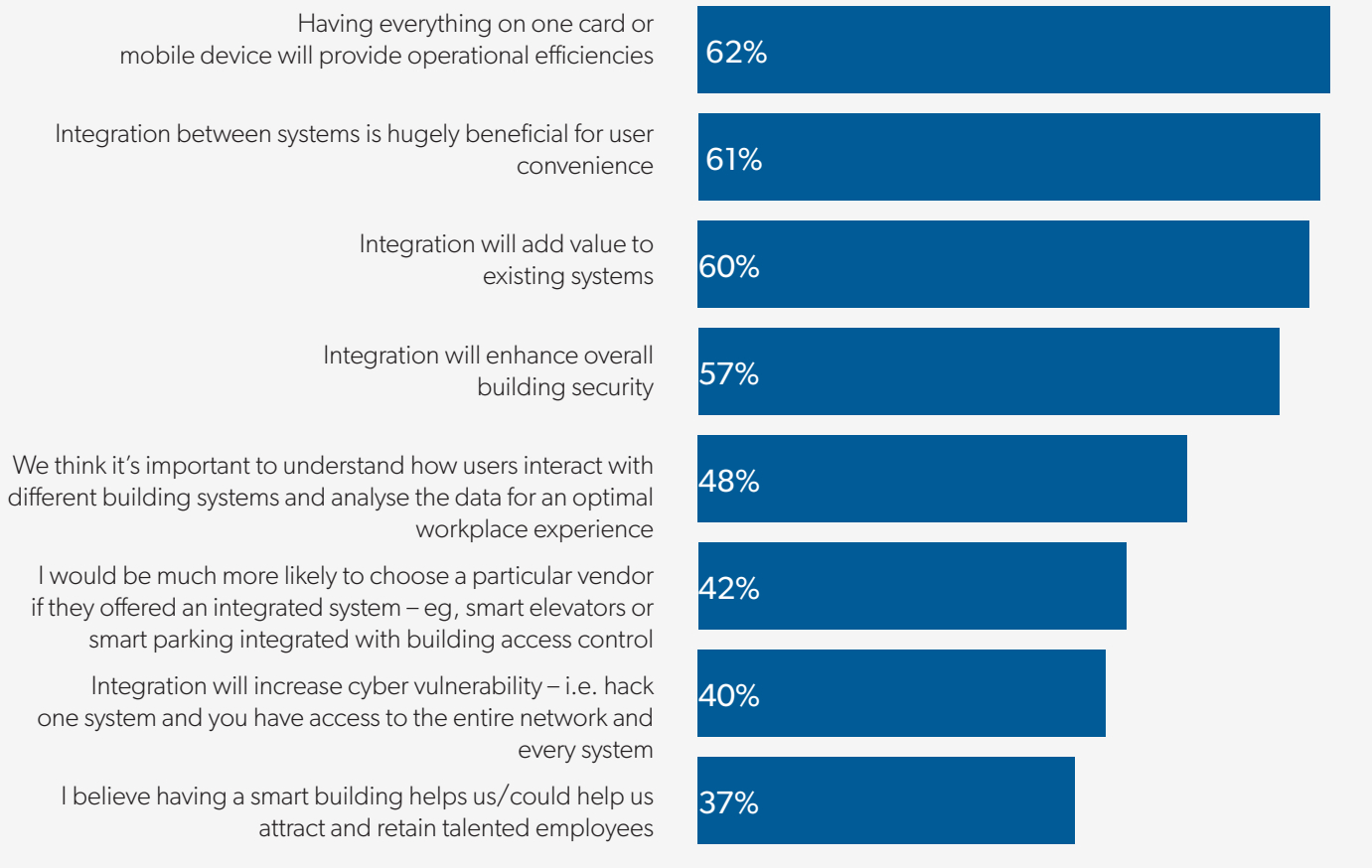
The connected workplace has to bring together disparate ecosystems. Seamless data sharing between physical systems presents a number of technical challenges. For example, the majority of commercial buildings still use pneumatic thermostats, which are non-communicating. There is significant up-front investment to 'connect' these systems, but the rewards can be significant. Research suggests that retrofitting technology can save up to 60% of a building's energy consumption.

According to the International Energy Agency, buildings consume almost 40% of the world's energy. Globally, smart building technology could reduce emissions by 1.68 GtCO2e [gigatons of equivalent carbon dioxide], achieve £201bn of energy savings and slash carbon costs by £31.1bn by 2020. Whereas an upgrade to an isolated building system might generate energy savings of 5-15%, data suggests that smart buildings with fully integrated systems often realise 30–50% – and access control systems can play a big part in this. With governments increasingly incentivising emissions reductions in light of the Paris Agreement on combating climate change, there are clearly compelling reasons to make access control and other building systems more connected.

Connected buildings: operational efficiencies in numbers|

- Buildings are the largest global consumer of energy, ahead of industry and transport. They also contribute to one third of total global greenhouse gas emissions, primarily through the use of fossil fuels during their operational phase
- Whereas an upgrade to an isolated building system might generate energy savings of 5–15%, data suggests that smart buildings with fully integrated systems often realise 30–50% *(Smart Buildings: Using Smart Technology to Save Energy in Existing Buildings, Jennifer King and Christopher Perry, 2017)*
- Building managers report an average of 30% savings in repair costs when networked buildings enable proactive maintenance *(according to Jim Young, CEO and founder, Realcomm, 2015)*

Which of these statements do you agree with?



Most building operators are starting with low-hanging fruit, which can still offer considerable benefits. Mobile technologies, for example, are playing an increasingly pivotal role when it comes to smart building integration – for example, leveraging physical access control systems to monitor time and attendance or managing secure print release. Most respondents were aware of the role that mobile technologies play in integrating existing systems. Eighty five percent said they were aware that it was possible to connect IDs across multiple systems, through multiple devices, across the organisation.

Integration between access control and HVAC (heating, ventilation and air conditioning) can generate huge energy savings. Lighting and heating can be adjusted depending on whether rooms or areas are occupied and by how many people. Unused space can be reallocated internally or rented out based on analysis of occupancy trends. Integration with Building Energy Management Systems (BEMS) can isolate indoor spaces with revolving security doors to reduce heat wastage.

BT slashed its electricity bills by 77% following the installation of a BEMS system by ADT. "We needed to refurbish the HVAC system and wanted to install variable speed drives because we knew there was a potential for energy saving," BT's energy manager for the company's Castle Wharf site told the British Security Industry Association for its guide to access control and sustainability. "Out of hours, there are only a few occupants. As the fans were not speed controlled, this led to a large waste of energy. Also, the car park ventilation was not needed at night and needed to be controlled as well. Additionally, our building management system was not set up the way we wanted and so we decided to use a BACnet-based system. This would allow us to zone the building and introduce time controls to take account of occupancy patterns."

Modern access control systems can monitor and identify patterns in visitor behaviour and share that data with a BEMS system. So sophisticated are modern systems that the presence of occupants whose profiles signal sedentary activities will trigger a higher temperature than for manual workers. Heating can be turned on in advance of visitors' arrival and turned down during periods of inactivity.

The prospect of cutting power consumption through data analysis and machine learning was cited as a strong motivation for upgrading by 36% of respondents to our survey – which brings us to the next section.

View from the vendor

"Our approach is reducing the total cost of ownership. Rather than forcing in new hardware and software and integrating the back end, we are making all these systems identity-aware, so the same identity can be leveraged to make authorisation decisions at all business systems – whether it's an elevator, a parking garage, a vending machine or printer. So all these systems will know who you are and what actions you are asking permission for. Based on your access levels they can grant or deny access." **Ashish Malpani,** *director of product marketing, HID Global*

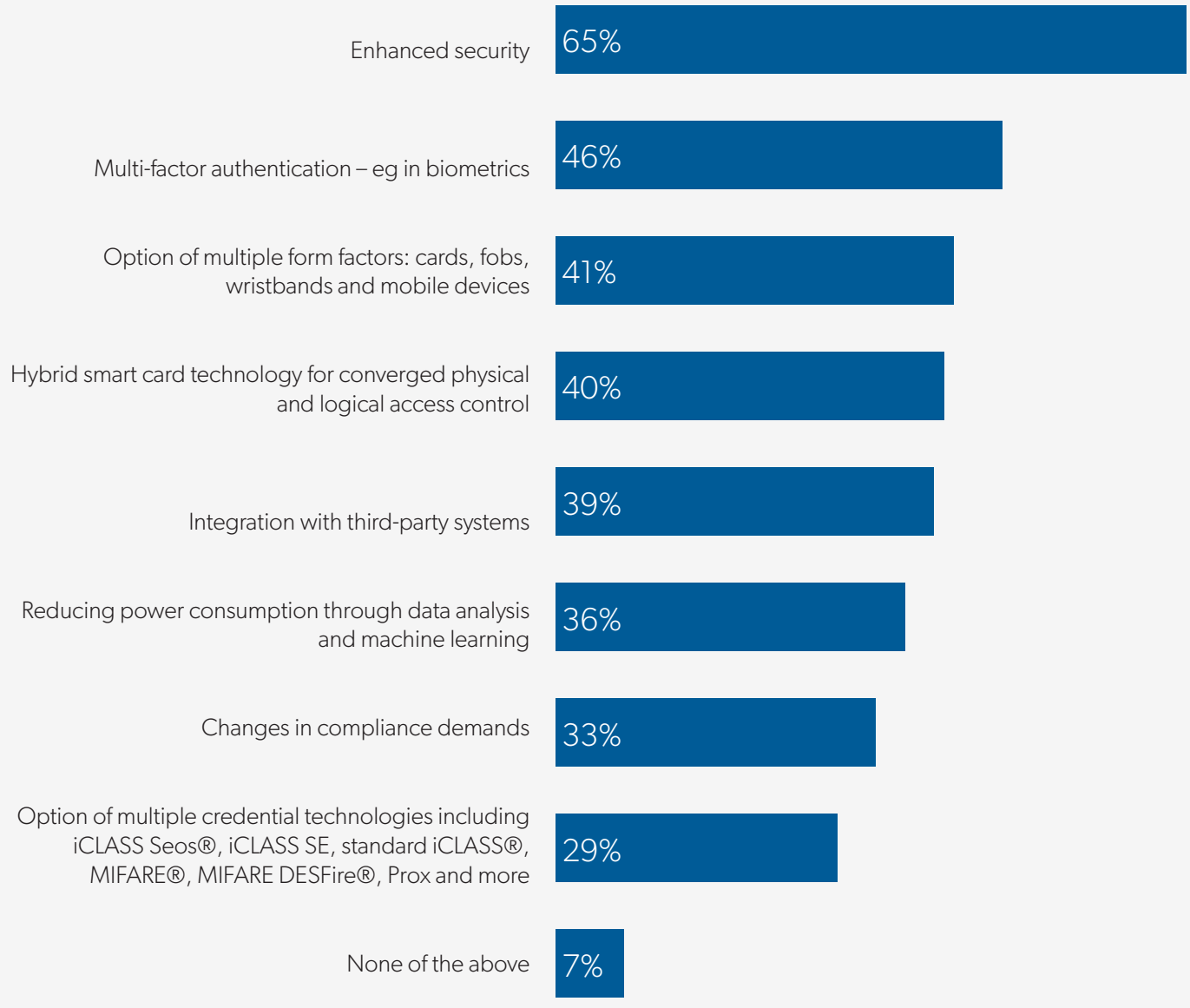
5. System upgrade motivations

Respondents were asked what functionality or needs might persuade them to upgrade their access control systems. Naturally enough, given 37% of respondents are security professionals and access control is primarily a security technology, improving security was the biggest driver for upgrading systems (cited by 65%). The other motivations given – all but one being cutting-edge benefits offered by the latest generation of access systems – were credible motivations for at least three in 10 respondents in each instance. That only 7% ticked 'none of the above' is proof enough that the merits of modern, connected access-control systems are compelling enough to sustain impressive growth in this market. Markets and Markets has projected global growth at a CAGR of 7.49%, reaching $9.8bn by 2022.

View from the vendor

"Investment in new technologies is primarily driven by compliance requirements. But at the same time, the connected building experience will offer a great benefit in terms of convenience for every tenant, every employee. And then upgrading is not just a conversation about security; it primarily becomes a convenience conversation, with security as an integral part. It's also about ROI. If the systems talk to each other, you have more intelligence to optimise building efficiency. That's a shift that will become more profound in the future."
Ashish Malpani, *director of product marketing, HID Global*

Which of these is likely to persuade you to upgrade your access control systems?



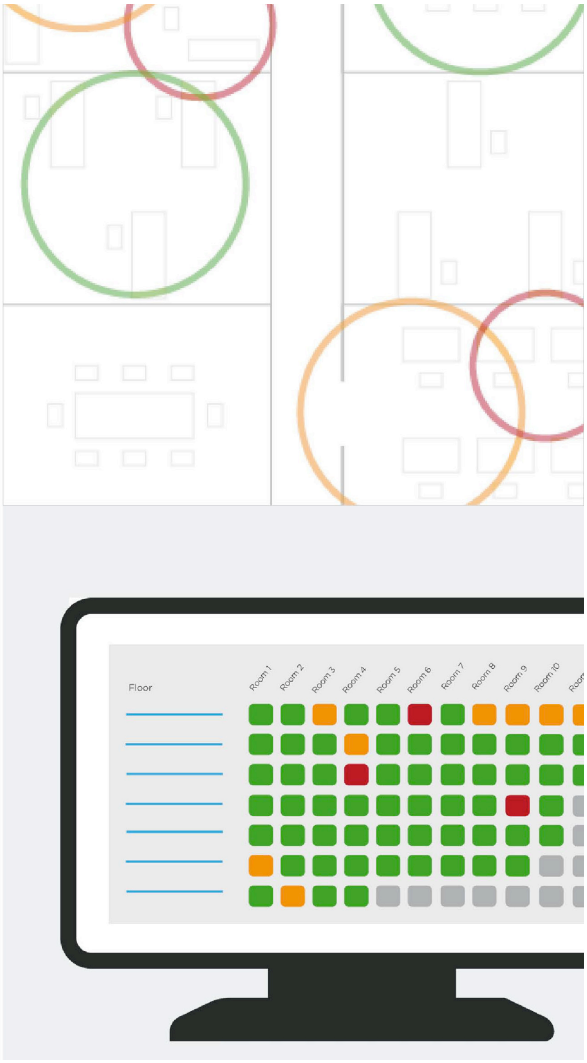
6. Cybersecurity

To realise the full potential of smart buildings, businesses need to overcome a number of hurdles. There is no question that security and data privacy are two of most significant. Our physical and virtual worlds are converging and increased connectivity introduces risks that simply did not exist before. There are proliferating endpoints to secure against hackers, therefore entirely new security frameworks must be adopted that span the full cyber-physical stack.

One senior executive in the education sector even steadfastly refused to adopt smart technology "until all security 'hacking' issues are dealt with." Two in five (40%) said integration would make systems collectively more vulnerable – ie, hack one system and you have access to the entire network.

"[Our systems are] "not 'smart' at all, and won't be until all security 'hacking' issues are dealt with."

Senior executive in the education sector



The prospect of hackers breaching cyber defences via physical building systems is no hypothetical threat. In 2013, the theft of millions of customers' credit card data from US retailer Target was traced back to the heating and ventilation system. In the same year, the US Department of Homeland Security revealed that hackers had hijacked the network of a "state government facility" and made it "unusually warm", while Google's Sydney office was hacked through its building management system. A year later, security consultant Jesus Molina told US cybersecurity conference Black Hat about how he commandeered control of the lighting, HVAC and entertainment systems of 200 rooms at a hotel in Shenzhen, China. Speaking to the BBC, one of these 'benign' hackers, Billy Rios, claimed there are 50,000 buildings currently connected to the internet, 2,000 of which lack any kind of password protection.

However, HID Global, which sponsors this report, believes there is a widespread misconception about the vulnerability of connected buildings to cyber-attack.

View from the vendor

"With Seos, even though one person carries one identity, this identity is manifested in different ways in different systems. Some systems may only need to know your first name and last name. Others might know your first name and email address. Others might know your date of birth. This means that malicious actions can be highly localised and not affect the whole connected building experience. All data is encrypted too. Seos is the highest level of security you can have in the connected building space right now." **Ashish Malpani,** *director of product marketing, HID Global*

It's perhaps ironic that while security concerns might be the biggest inhibitor of widespread adoption, connected solutions are playing an increasingly fundamental role in the protection of infrastructure, both physical and virtual. For instance, it's much easier to track the activities of occupants within a building across multiple systems. This perhaps explains why integration has gone further with security than non-security systems, as the results on page … seem to show.

But realising these benefits is not dependent on technology alone; the expertise of those procuring, installing, operating and maintaining systems is fundamental too.

7. The convergence of physical-logical access: bridging the cultural, educational and structural divide

Our survey findings have discerned a disconnect between the domains of IT and facilities management. Historically, these two areas arose out of two very different business needs. The remit of IT was to manage information flow, while facilities staff managed the building's physical functions.

While those basic remits remain valid, the physical and virtual realms are converging, necessitating greater collaboration between these departments. But, as is often the case in other spheres, the technology is evolving faster than the attendant culture, processes and best practices can keep up with.

Two-thirds (66%) of respondents agreed that IT and facilities/security management teams need to work together more closely when buying, installing and using new technologies.

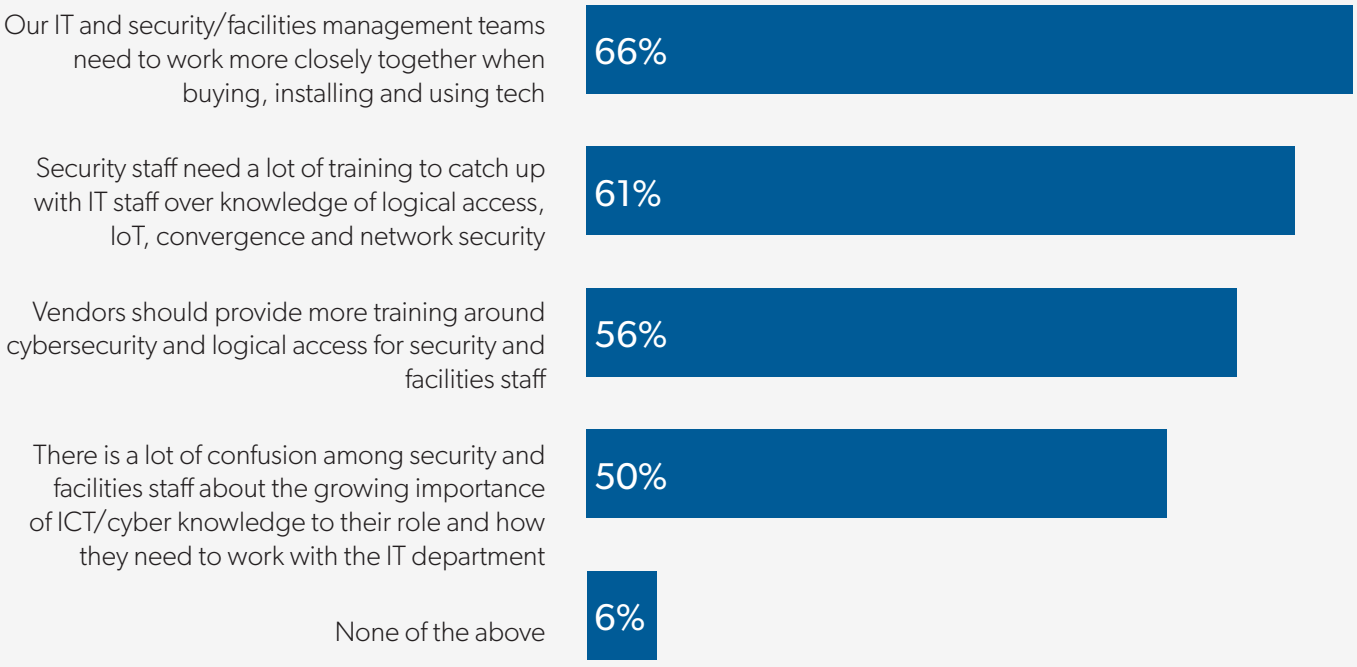
Almost as many (61%) said that physical security staff need 'a lot' of training to catch up with IT staff in terms of understanding logical access, convergence and network security. And exactly half (50%) thought there was a lot of confusion among security and facilities staff about the growing importance of ICT/cybersecurity knowledge to their role and how they need to work more closely with the IT department.

Clearly, then, much work is needed to bridge cultural, educational and structural gaps between these hitherto siloed disciplines.

> **"Security and facilities staff think they can catch up on the IT front. In about 99% of cases they cannot grasp the necessary detail."**
>
> *UK-based systems integrator*

This applies across the supply chain, with vendors scrambling to bolster security following a spate of IoT hacks and integrators in danger of falling by the wayside unless they upskill accordingly and abandon business models designed for the analogue age. Talking about access control as a service (ACaaS), Blake Kozak, an analyst specialising in building technologies at research firm IHS Markit, has said that "most integrators and installers must change a longstanding mindset of selling boxes and components and begin selling services, features and concepts. Additionally, they must know the IT side of the business and be able to

Which of these statements would you agree with?



answer questions regarding redundancy, certifications, hacking, and other buzzwords associated with cloud-based services and ACaaS."

Facilities teams, meanwhile, are trying to make sense of how their roles intersect and overlap with those of IT departments. Where once ex-police officers and military personnel moved seamlessly into the security industry with few or no industry-specific qualifications, the modern head of security is highly professionalised, with multiple accreditations and qualifications, and increasingly needs in their armoury ICT/cybersecurity as well as security management expertise.

But where should responsibility lie for providing training and education in logical access and cybersecurity? More than half (56%) thought vendors should be playing a bigger role than present. One integrator who completed the survey suggested that "security and facilities staff think they can catch up on the IT front. In about 99% of cases they cannot grasp the necessary detail. If you start in IT, learning the facilities and security side of things is far easier. The systems are IT systems first and foremost." However, they also had some harsh words for manufacturers, who often "confuse simplicity and security."

View from the vendor

"Traditionally there are boundaries where physical security is handled by the facilities department and logical security is handled by the IT team. But there are growing numbers of threats that involve both logical and physical access. So education is needed, not just securing the perimeter but internal business systems too. We are starting to see the convergence of logical and physical access. Eventually you will find models that work in certain scenarios. If you take a multi-storey building with multiple enterprise tenants, the building owner, property manager and tenants will each need their own network admins, security admins and physical access admins. If a building is owned and occupied by a single enterprise it makes sense to converge these functions into one team that manages the whole landscape. For a tenanted structure you would still need someone doing facilities management, someone doing IT management… You still need a separation of duties. Perimeter security is managed by the building owner, whereas anything that happens beyond internal doors is the tenant's responsibility." **Ashish Malpani,** *director of product marketing, HID Global*

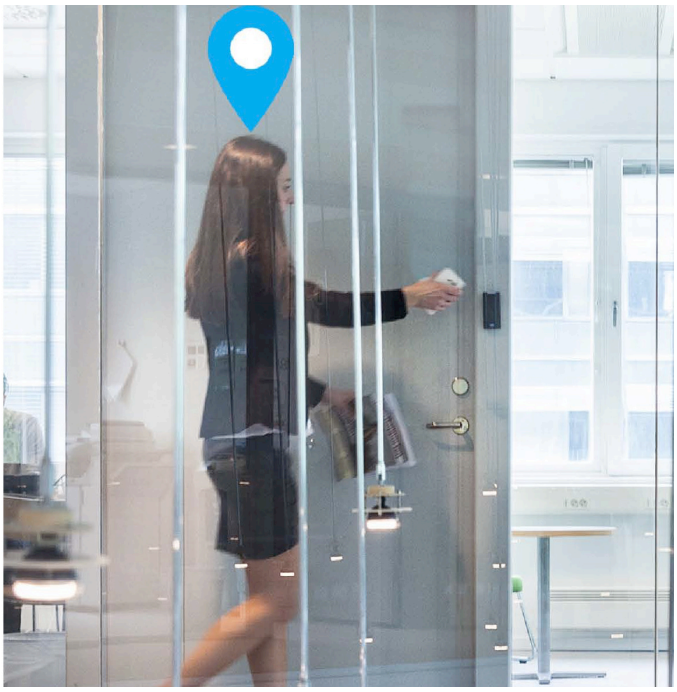
8. IoT: the next revolution

"While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation. As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats."

US Department of Homeland Security

The mainstream media tends to focus on consumer applications when discussing the Internet of Things (IoT). Whether it's the Apple Watch, internet-connected coffee machines or smart TVs, you'd be forgiven for assuming that smart technology starts and ends in the house or as wearable consumer tech. While it's true that 12.8 billion units of connected consumer 'things' are expected to be in use by 2020, the equivalent global growth curve for industrial IoT is expected to see 7.5 billion devices online (Gartner) by that point. But if unit volume is higher in the consumer world then industrial spending will actually far outstrip its consumer equivalent. Consumers are projected to spend roughly £182.45bn per annum globally on IoT technologies by 2020, compared to £643.22bn in the business sector.

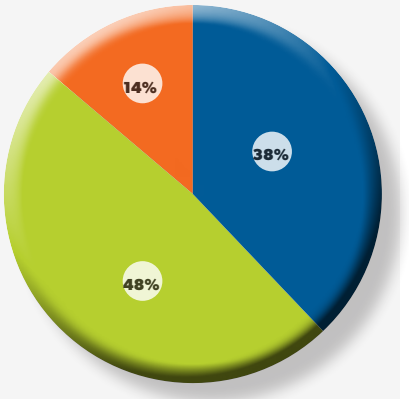
If connected buildings help systems talk to each other in the back end then the internet of things (IoT) promotes connectivity at the front end. The IoT is a brave new world and the consumer tech press has been abuzz with all manner of weird (like smart hairbrushes) and wonderful (like smart bluetooth trackers for finding lost car keys) 'things' in recent years. IoT developers have apparently cleaved to an overriding maxim: don't waste time researching whether internet connectivity will enhance a thing's utility; better instead to put a computer chip in every consumer product imaginable and let the market decide. Hence, the smart salt shaker.



The commercial sector cannot be so blasé, as Ashish Malpani of HID Global explains below.

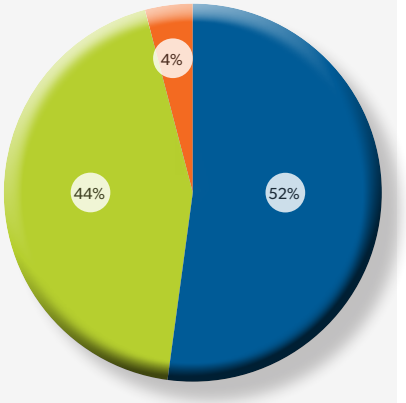
How aware are you of the Internet of Things and its benefits (or risks)?

- Very aware **38%**
- Modest awareness **48%**
- Know very little about it **14%**



How applicable do you think the Internet of Things is to building access control?

- Very applicable **52%**
- Somewhat applicable **44%**
- Not very applicable **4%**



View from the vendor

"IoT is a big buzzword. Everybody sees the potential of having everything talk to each other and taking appropriate actions based on analytics. But people are sceptical about how to deploy IoT systems and whether the benefits justify the investment and risk. Security is a big question mark. Take the hack on US retailer Target. The hackers jumped onto the network via the HVAC system. That's why people are concerned. The security implications are still unknown of having these systems integrated and talking to each other. So although it shows a lot of promise, security professionals are really approaching this with caution, because evaluating risk is their job and right now, very few people really understand the attack vectors. The portfolio of 'things' will have to be risk-evaluated before the IoT is widely deployed." **Ashish Malpani,** *director of product marketing, HID Global*

So for all its enormous potential, the IoT is not yet ready for widespread adoption in the commercial arena. But with global spending on IoT security expected to reach $547m by 2018 – up 58% on 2016 (Gartner) – the industry has belatedly recognised that assuaging security concerns should be its priority if it wants the building management industry to embrace its technologies.

It seems to be a case of when, not if, the connected workplace routinely incorporates the IoT. General Electric estimates that the industrial internet market will add between £8tn-£12tn to global GDP within the next 20 years. By comparison, the GDP of China is just over £7tn.

Given these are such new frontiers, it would be unsurprising if many involved in the protection and management buildings were unfamiliar with the technology and its potential. And indeed, a survey conducted by the Electrical Contractors' Association (ECA), Chartered Institution of Building Services Engineers (CIBSE) and Scottish electrical trade body SELECT found that 40% of professionals who protect and manage buildings admit they are 'unfamiliar' with the term 'internet of things', while 55% agreed there was a 'lack of clear advice or knowledge' on the subject.

Nevertheless, a huge majority of respondents to our survey (86%) said they had at least some awareness of IoT and its benefits and risks. That said, nearly half (48%) admitted that their awareness of these technologies was only 'modest', with a further 14% saying they knew very little about the IoT.

Regardless of their knowledge of the subject, an overwhelming majority – 96% – thought the IoT was applicable to access control to at least some extent, with more than half (52%) ticking 'very applicable'.

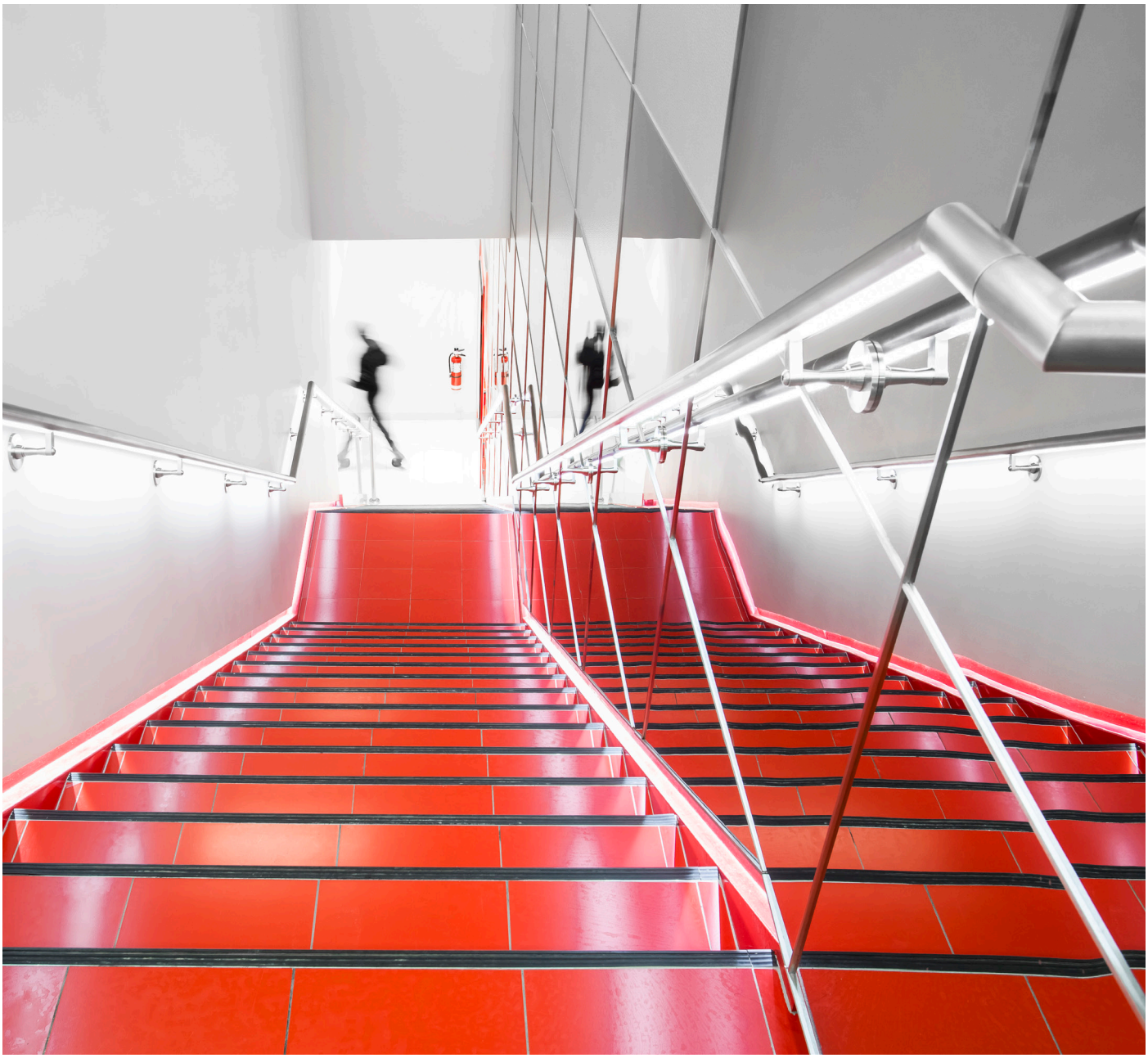
9. Bigger organisations leading the way

The migration to truly connected workplaces is being led by larger organisations, our survey results suggest. Given that today's predominant integration approach requires significant investment in software and hardware, this is not surprising. Some 70% of respondents employed in organisations with more than 250 employees saw their systems as at least somewhat smart, compared to 57% of those with fewer employees; 67% versus 55% respectively had access control systems that were at least 'somewhat' integrated; and every other building system was more likely to be integrated in larger organisations.

Respondents employed by large organisations were also more likely to "think it's important to understand how users interact with different building systems and analyse the data for an optimal workplace experience" (53% versus 45%). All these differences are starker still if you contrast the smallest segment (up to 50 employees) with the largest (more than 1,000).

Larger organisations were also more likely to upgrade based on every single factor posed, by significant margins in some cases.

And respondents were more likely to have concerns about training/knowledge gaps in logical access and cybersecurity if they worked for larger organisations, with 76% thinking that their "IT and security/facilities management teams need to work more closely together when buying, installing and using tech", compared to only 59% among smaller organisations. Smaller organisations can enhance the workplace experience by deploying identity-aware business systems.



10. Conclusion

"The starting point for establishing a model of intelligent buildings is people because they determine the mind force of the building. People are not passive recipients of their environment and adapt physiologically and behaviourally."
Derek Clements-Croome

The connected workplace has arrived – for some organisations at least. For others, the journey into the world of smart buildings has only just begun. At present, just 18% of the UK's commercial buildings are considered 'very smart' by the staff managing them. Our survey highlights a number of challenges that vendors and building stakeholders must grapple with if this technology is to become truly pervasive.

One of the biggest is that of security and data privacy. The number of nodes in a building network is growing and, for the first time, cyber threats are encroaching into the physical world. It's therefore critical that facilities managers implement proper security frameworks, as well as appropriate access control and logical access systems.

Challenges

There are also challenges in how these technologies are deployed in the coming years. The ability to retrofit smart technologies will be vital if they are to have any meaningful impact. A lack of clear terminology, meanwhile, only creates confusion for those from a non-technical background. The industry must rally around an agreed set of definitions, processes and protocols. Loose definitions that are bandied about are impeding progress, making it difficult for stakeholders to keep abreast of the landscape. There also needs to be progress in terms how IT, physical security and facilities teams are structured.

But as the technology spreads, there is evidence that information on best practice is beginning to trickle down. The Institution of Engineering and Technology (IET) recently issued fresh guidance to aid engineers with connected systems integration projects, for instance.

With open platforms now dominant, there are few technological limitations to realising the vision of a truly connected workplace. But our survey findings suggest that a sizeable percentage of those tasked with the protection and management of commercial buildings are yet to be persuaded that the benefits warrant the investment.

Nevertheless, a significant percentage of common building systems – ranging from one in four to one in two – are already integrated. And those who manage those systems yet to be integrated are more likely than not to want to integrate them. The benefits of modern, connected systems seem highly persuasive when it comes to upgrades too, our survey suggests.

As for IoT, stakeholders instinctively see what these technologies can bring to the table. However, until concerns around security and interoperability are addressed, the IoT revolution will have to wait.

In the meantime, the connected workplace is having a transformative effect on organisations that follow best practices. If the aforementioned challenges can be overcome, the potential rewards are enormous. By leveraging technologies already in use by the workforce such as mobile, building operators can both improve security and drive operational efficiencies.

Procurement is also shifting towards flexible, service-based models and away from front-loaded investments. Total cost of ownership is an increasingly important consideration.

Smart technologies promise to aid agile working practices, improve operational efficiency, aid compliance, enhance security, make the experience of occupants more frictionless and convenient and help organisations meet their corporate sustainability goals.

View from the vendor

"The workforce is changing. The notion of privacy is changing. People expect to do with devices in the workplace what they do with their personal devices. If I want to do whiteboarding, I don't have to copy all my files to a USB drive, hook my laptop up to a whiteboard, then figure out the files I want to share. This is how it is today in many organisations. But this multistep process will not work for long. We are seeing change and pretty soon the workforce will demand one-click access to everything. Sometimes you won't even need to click; the system detects you presence without you interacting at all. We want to find the simplest way to provide a unified experience." **Ashish Malpani,** *director of product marketing, HID Global*