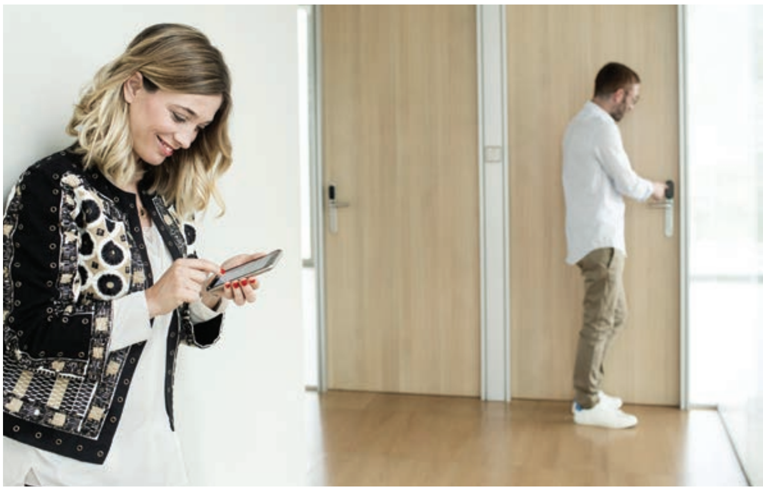
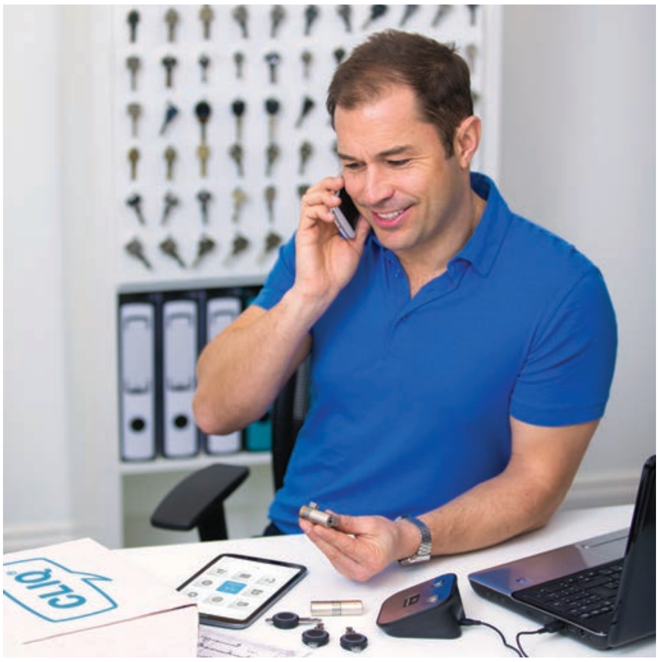
ASSA ABLOY

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



The Wireless Access Control Report 2018

How standards, sustainability, mobile and the cloud continue to shape the future



Introduction

In the early 1980s McKinsey projected that 900,000 mobile phones would be in use around the world by the turn of the century. The management consultancy undershot spectacularly: 900,000 new subscribers were buying mobile phones *every three days* by 1999. Why? Because they failed to anticipate dramatic innovation and falling costs.

Wireless communication has come a long way since then, including in the access control arena. Communicating via NFC and, more commonly, Bluetooth Low Energy is a plethora of wireless readers, locks and tags currently available on the market. This report — the third edition of the *Wireless Access Control Report* sponsored by ASSA ABLOY — reveals only 6% of installed electronic access systems are fully wireless. However, a further 31% include a mixture of wired and wireless systems, and a significantly higher proportion of organisations have wireless systems installed compared to those surveyed at the tail end of 2015 for the 2016 report (see p4).

Transparency Market Research[1] has forecasted robust growth in the global wireless access control market between now and 2025, when revenues will reach US$1.66bn at a CAGR of 7.9%. North America, which accounted for 31.3% market share as of 2016, is expected to be the largest revenue contributor. Published in January 2018, *Wireless Access Control Market – Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2017–2025* notes demand growing strongly in the residential market, although the commercial arena is still expected to account for 56% of revenues by 2025.

Perhaps these optimistic projections will still fall far short of the true rate of growth ahead because, like McKinsey and mobile phones, a research firm can fail to anticipate innovation and falling costs.

Growth has of course already been driven by advances in wireless technology, the popularity of electronic door locks and innovative functionality, notably in smartphone-mediated access. Requiring no power or signalling cables, wireless systems are also much less disruptive to premises' infrastructure.

These ASSA ABLOY-sponsored reports, based on a poll of hundreds of professionals involved in the procurement, operation, deployment or maintenance of access control systems, set out to gauge perception of, and demand for, wireless technologies in a market where hardwired systems still have an edge in the installed base.

Do respondents view wireless access control more positively than they did five years ago?

The inaugural edition, published in 2014, quizzed security professionals, facilities managers, IT professionals and other relevant professionals on their existing access control systems and the pros and cons of wired versus wireless technology[2]. Two years later we examined training requirements; how wireless systems were sourced and how

[1] https://www.prnewswire.com/news-releases/global-wireless-access-control-market-is-anticipated-to-reach-us-16570-mn-by-2025-transparency-market-research-670709443.html

[2] https://www.ifsecglobal.com/wireless-access-control-market-2014/

CONTENTS

wired and wireless systems compare from a security and cost-effectiveness perspective; the prevalence of exclusively mechanical systems; and demand for securing IT servers, safes, gates, cabinets and outdoor structures with battery-powered locks.

This latest, 2018 edition revisits the benefits of wireless technology as championed by its providers, and demand for using battery-powered locks to secure assets which are difficult or impossible to secure with hardwired systems, like those examples highlighted above.

We also explore fresh terrain. Do our respondents view the technology more positively than they did five years ago? In what ways does selling wireless solutions make it easier for service providers to install systems and win business? This report also explores demand for, and perceptions of:

- access control as a service (ACaaS);
- the merits and risks of Bluetooth as an alternative to NFC;
- the value of sustainability and energy efficiency in procurement; and
- the growing value of integration — both between systems and across multiple sites.

IHS Markit returns again to provide expert commentary. We are grateful for the contributions of Jim Dearing, senior analyst for security & building technologies at the global research firm.

For ASSA ABLOY, director for commercial access solutions on the EMEA portfolio Russell Wagstaff sets out to interpret the survey results and challenge any misconceptions — as ASSA ABLOY sees them — that emerge about wireless access control technology in 2018.

About ASSA ABLOY
ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience.

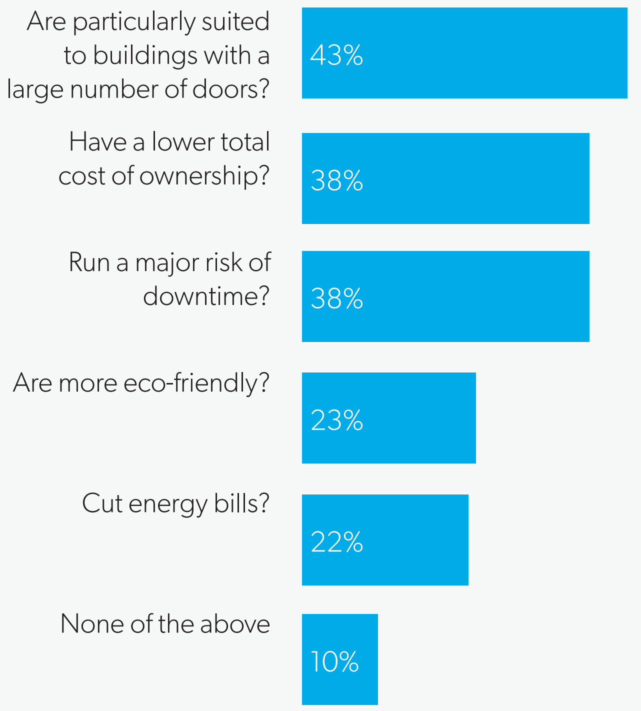
About IHS Markit
IHS Markit is a source for critical information and insight for numerous industries, including leading positions in finance, energy, transportation and technology. More than 5,000 analysts, data scientists, financial experts and industry specialists provide insights for 50,000 customers in over 140 countries, including 80% of the Fortune Global 500.

IHS Markit's Access Control Intelligence Service
IHS Markit Since its inception back in 2005, IHS Markit's electronic access control research has featured the most detailed market analysis available to the industry. Recent topical research published on the service:

- Access control as a service (ACaaS) – Report analysing the growing market for providing electronic access control solutions in return for recurring monthly revenue subscriptions.
- Cybersecurity – Electronic Access Control – An unprecedented study on the growing cybersecurity threat to modern electronic access control systems.
- Mobile Credentials – A report that analyses the current "readiness" of the access control reader install base for mobile access plus brand new data on the number of mobile credential downloads.

A growing, maturing wireless market

Compared to wired locks, do you agree that battery-powered wireless locks...



In homes, in commercial premises, in public buildings and beneath the streets, wires and cables have always been the arteries of our electric-powered society. And while cabling remains the optimum means of powering a system's central hardware, there are many benefits to connecting devices on the periphery "over the air" instead.

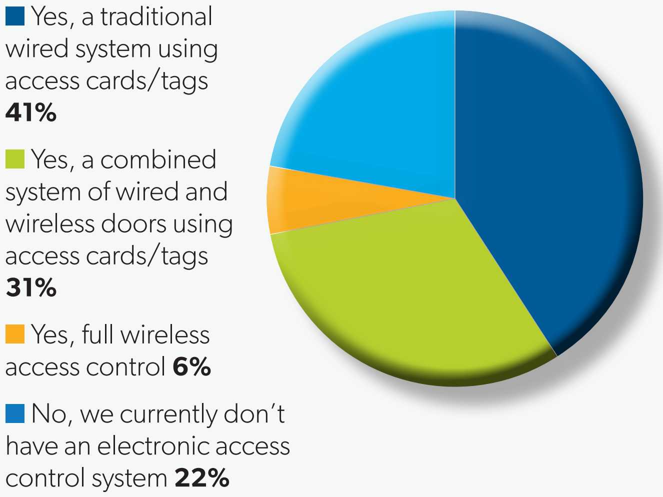
With the global wireless access control market growing briskly at a CAGR of 7.9%, such benefits are increasingly recognised by facilities managers and security departments. Wireless is "the next natural step in fire safety/security," in the words of one professional who responded to our survey.

Mirroring the usual trajectory of emerging technology, wireless systems have over time become less expensive, more reliable and more versatile. Nearly two thirds (63%) of respondents "have a more positive view of wireless than five years ago because the technology has improved". Similarly, 60% of service providers agree that installing and selling wireless technology has become easier over the same period.

60% of service providers say installing and selling wireless technology has become easier

Security professionals — by definition — are disinclined to take big risks in procurement. They're more likely, we can speculate, to invest in a technology if they see it widely and successfully deployed elsewhere; being among the first wave of adopters carries the risk of teething troubles.

Does your organisation/business already operate an electronic access control system?



The technology is certainly well established. A significantly higher proportion of end users have wireless systems installed compared to those that completed the survey in late 2015, for the previous edition of this report. The share of fully hardwired systems has fallen from 57% to 41%, while the proportion of systems that comprise both hardwired and wireless components has risen from 24% to 31%. The proportion of fully wireless systems has climbed marginally, from 5% to 6%.

As electronic access control in general has become more

IHS insight

"Wireless locks are more popular in the Americas than any other geographic region. Any situation when is undesirable or too expensive to cut into a door leads to a preference for wireless locking solutions. These locks have fewer components plus they can by installed at any stage during construction, meaning they are a better fit for retrofit projects. Wireless locks are around 20% more expensive than their wired counterparts on average.

"However, the cost of the additional labour required to make cuts into doors and wire a system can increase the total project cost per door by up to 40%. These labour savings are the main reason behind wireless locks' popularity in developed economies, as wages are higher on average."

Jim Dearing, *senior analyst for security & building technologies, IHS Markit*

ASSA ABLOY insight

"Among the many advantages of wireless discussed in the report, I would highlight two. Firstly, removing the need to cable every door makes it much easier and more economical to bring many more doors into your access system. So wireless technology can upgrade your building's security in an instant.

"Secondly, the energy-efficiency of wireless doors delivers significant cost savings. The standard batteries locks use have long lives, and only fully 'power up' when there's a credential to read. Wired doors are generally connected to the mains 24/7."

Russell Wagstaff, *director for commercial access solutions, ASSA ABLOY EMEA*

reliable, cost-effective and versatile, organisations grow keener to electronically secure higher numbers of entrances. Where once they may have only secured a building's main entrance or perimeter, now they might also secure internal doors to limit access to specific tenants or those with higher authority.

Cabling vs. batteries

The case for installing wireless locks becomes more compelling still, because wiring is disruptive and potentially costly to install — more so in some cases, depending on a building's power infrastructure. A hardwired system may require installers to fit wiring for components including magnetic locks, an automated door closer, a smartcard reader and perhaps even a security camera with a network connection to a centralised monitoring system. It's therefore surprising, perhaps, that only 44% of respondents think wireless solutions are particularly suited to buildings with a large number of doors — and that end users were more likely to agree than service providers.

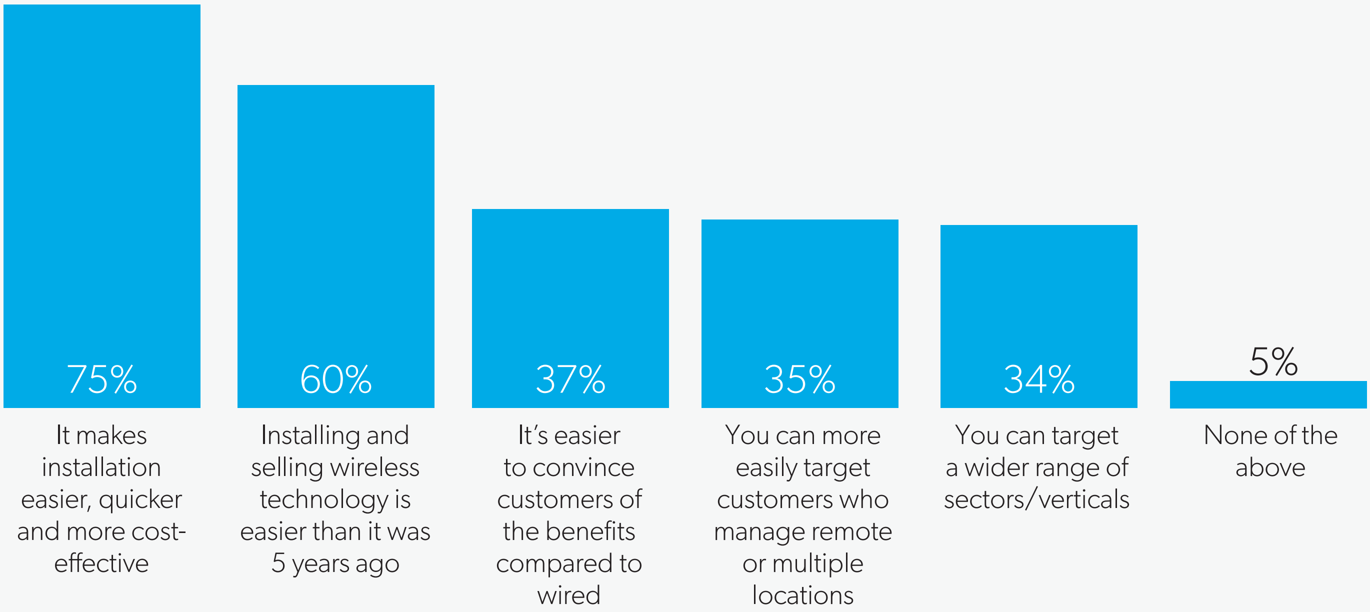
Vendors of wireless systems regularly champion battery-powered locks as simple and inexpensive to integrate with legacy hardware, a major plus given how important integration has become in physical security (as the results on p18-19 attest). About one in three (34%) across the supply chain agree that wireless access control integrates easily with legacy wired locks. A greater proportion (41%) of installers agreed with this statement.

Installer business model

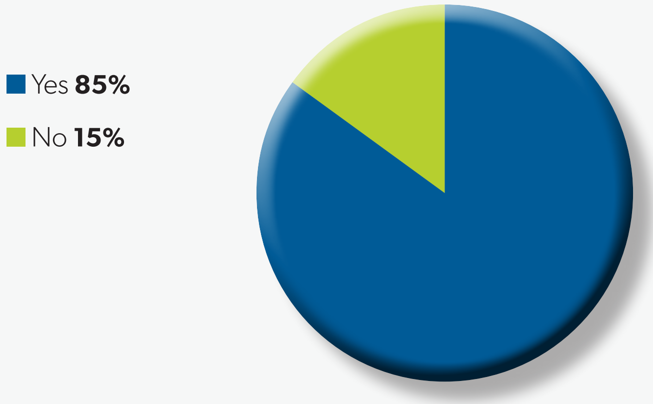
Does wireless access control also broaden the range of sectors installers and integrators can realistically target? Around one in three (34%) responded affirmatively, a similar proportion to those who agreed they can more easily target customers with remote or multiple locations (35%).

The vast majority of service providers — by which we mean installers, integrators, consultants and so on — that we surveyed already sell, install or recommend wireless products. Small wonder when you consider a large

Installers/integrators: Which of these would you agree with about selling wireless solutions?



Service providers: Do you sell, install or recommend wireless products?



majority (75%) agree that wireless systems make installation easier, quicker and more cost effective, with slightly more installers (78%) — obviously more informed on the process — agreeing. One such installer notes there is "less cabling to awkward areas." Another says, wryly: "Installing is easy; getting it right is a bit of magic." A third comments that "standalone wireless access control can be deployed very quickly and is a good first pass, secure environment."

Some might argue wireless systems also reduce the likelihood of repeat visits to repair damage caused by pinched wires and the like. But if service providers are largely sold on the benefits of wireless, they still don't find it easy to convince customers of the technology's merits: only 37% agree "it's easier to convince customers of the benefits compared to wired".

IHS insight

"There are two types of wireless solutions used in electronic access control: those that leverage existing Wi-Fi infrastructure and those that require their own dedicated wireless network.

Due to end user concerns over the reliability and battery consumption of Wi-Fi solutions, in many commercial use cases these wireless systems will operate on their own dedicated wireless networks. This means that in addition to installing wireless locksets, the installer also needs to set up and install wireless hubs throughout the building. The range of these hubs is limited and the building may require electrified access in many areas, meaning installation will require many hubs to cover all required doors. This all adds to the total system cost and erodes the price advantage that wireless solutions often possess compared with wired systems."

Jim Dearing, *senior analyst for security & building technologies, IHS Markit*

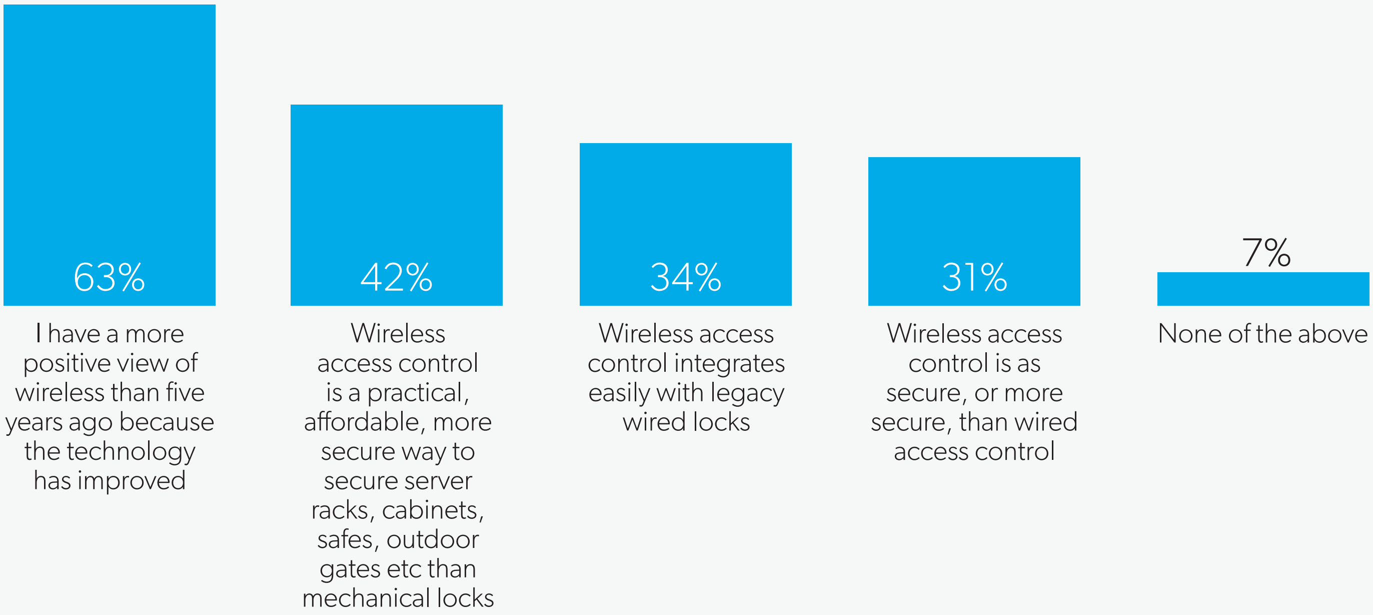
End-user perceptions

Why is this? For one, end users might be deterred by an expectation that they must periodically replace dozens or even hundreds of batteries, possibly across multiple sites.

Perhaps some of the "myths" ASSA ABLOY attempted to dispel in a 2014 campaign[3] still persist — namely, that wireless systems cost more to run, can't integrate with existing wired systems, don't support multiple keys, and aren't cost-effective.

[3] https://www.assaabloy.com.au/en/local/au/news_and_events/news_archive/busting-the-myths-about-wireless-access-control/

Which of these statements do you agree with about wireless access control?



On the whole, end users are not widely enthused about the advertised benefits of wireless access control. Fewer than half think wireless systems have a lower cost of ownership, are more eco-friendly, or even cut energy bills. Presumably there is a widespread perception that replacing batteries is at least as expensive as a wired system's contribution to electricity bills. Most alarmingly, perhaps, for developers of wireless solutions, one in three think they run a "major risk of downtime".

Perhaps some myths ASSA ABLOY attempted to dispel in a 2014 campaign persist

Security concerns are a recurrent theme among respondents. One installer said they "have had people comment on the security/hacking aspect." Someone from a manufacturer agreed the "security of wireless systems is perceived as problematic." Another manufacturer's employee echoed these sentiments even as they acknowledged the technology's merits in the hotel sector — a fast-growing market for wireless systems (see below): they are "effective to manage and low cost — hence the adoption by hotels — but inherently insecure," they said.

Battery-powered systems can still operate if mains power is lost, which many see as a benefit, yet one head/director of security believed they are "prone to unauthorised intrusion in the event of a power cut."

An installer expressed the view that wireless locks "are less controllable, due to polling, unless this has changed. I'd like to click on a screen and the door open immediately — not always possible with wireless battery locks."

One UK-based consultant offered these thoughts: "It sounds a very safe and easy to operate product" but "costs may restrict the market depth." But another, based in India, called wireless systems "cost-competitive". A UK installer was more ambivalent about costs, saying that "depending on location these can be more cost-effective." However, he also asserted that they "can be limited in range."

The ‘non-door’ market

Many respondents still have no intention of securing their doors with wireless access control. Of those that don’t already have wireless electronic locks on doors, twice as many intend to install such locks on doors as the number who do not. Filter the results to organisations that do not secure doors electronically, however, and these proportions are roughly reversed.

When appraising demand for electronically securing assets other than doors, turnstiles and barriers within a building, it’s worth remembering that many organisations don’t actually have safes, server racks, machinery or outdoor gates to protect. With this in mind, the fact that 24% of commercial environments have battery-powered locks on gates and other outdoor structures traditionally protected with padlocks, 23% have them on server racks, 17% on safes and 16% on machinery, suggests wireless electronic locks are already widely used in a broad range of environments. Presumably, cabinets and lockers are more common in commercial buildings than these assets. Nevertheless, 17% represents a sizeable installed base, albeit with considerable scope for growth.

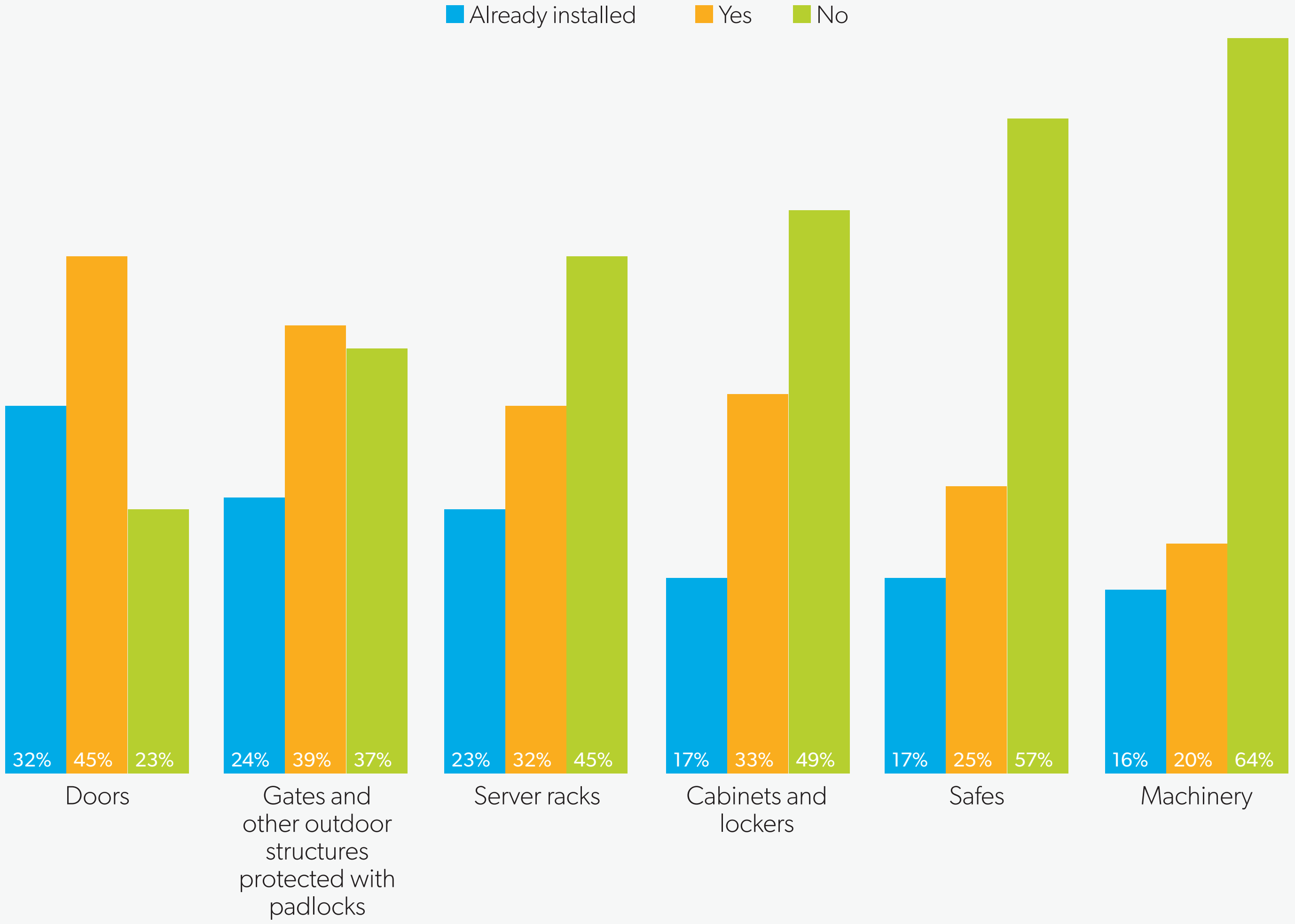
IHS insight

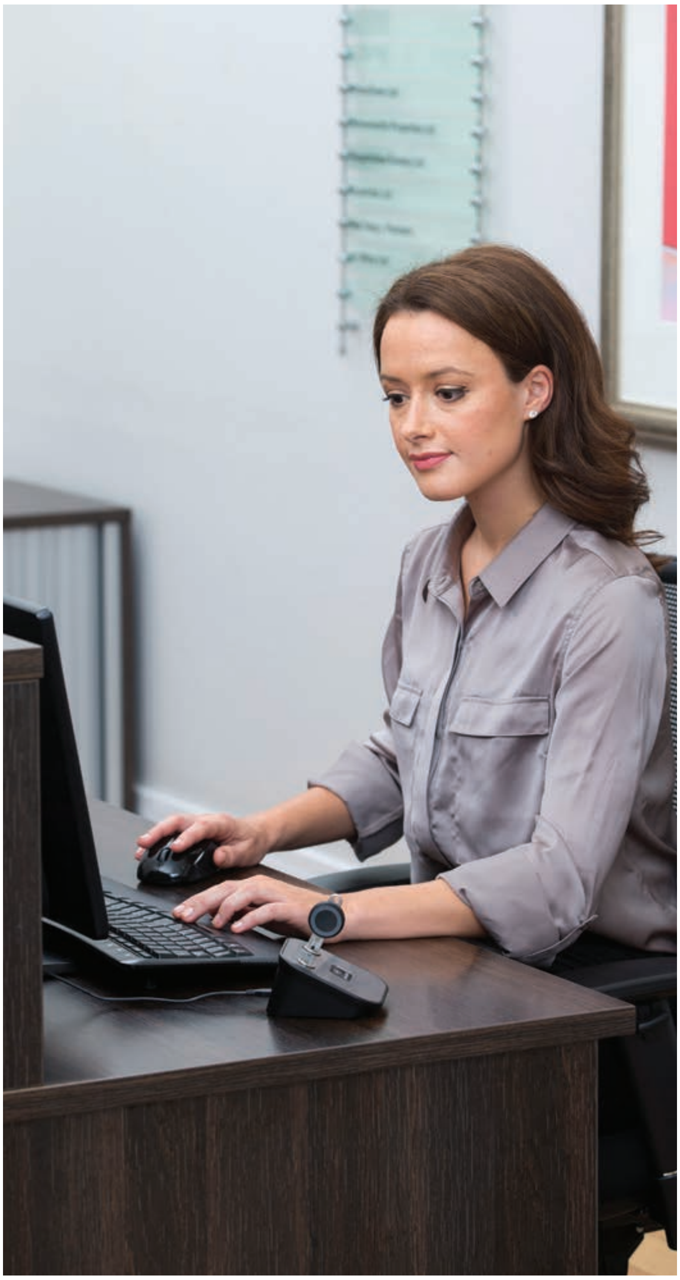
“Standalone battery-powered locking solutions are becoming more popular because they eliminate a number of traditional ‘pain points’ associated with traditional, mechanical master key systems. These systems allow end users to delete lost credentials from the system at no cost, plus allow the possibility of remote or time-restricted access. Standalone battery-powered locking solutions are relatively easy to install and set up when compared to other electronic locking solutions. They are also becoming more affordable each year when compared to their mechanical counterparts.”

Jim Dearing, *senior analyst for security & building technologies, IHS Markit*

‘Non-door’ access control is anticipated by Transparency Market Research to grow at a CAGR of 12.9% to 2025, compared to 7.9% for the wireless market as a whole. For wireless vendors, fully unlocking this market will rest on changing minds among the 58% who declined to agree with

Are you planning to get wireless access control for:





ASSA ABLOY insight

"Partly it's about convenience. The more applications that can be secured and unlocked with a single credential, the better for site users. Facility managers benefit from the wider scope of their access system, which gives them more control.

"In addition, because these 'non-door' devices are wireless, access control can easily extend outdoors, replacing padlocks for gates, machinery locks and storage lockers. With the right lock, these can all be secured within the same access control system as your front door."

Russell Wagstaff, *director for commercial access solutions, ASSA ABLOY EMEA*

this statement: that battery-powered locks are a "practical, affordable, more secure way" to secure such things than traditional mechanical locks. Just raising awareness of the technology generally will help too: one facilities manager admitted to being "unaware such a thing existed".

Another end user said they had no such installations planned, "primarily because of issues with wireless security" — a recurring reservation among potential end users of wireless access control in general. Another said that "in the future" they might consider installing electronic locks in these scenarios because "we have a global footprint and would look at new technologies when less developed areas have identifiable baseline protection."

In summary, there are plenty of battery-powered locks already protecting assets other than room and building entrances; demand for further installations is strong; yet a modest majority of end users without such deployments are not entirely convinced the benefits warrant the investment.

Bluetooth & smartphone access

Similar proportions of respondents endorse both the benefits and the drawbacks of Bluetooth. And while 16% didn't recognise any of the benefits posed, 14% didn't recognise any downsides put to them.

The most commonly cited benefit (by 56% of respondents) was the ability to remotely permit access to non-employees and revoke credentials instantly.

The biggest misgiving was the perceived cybersecurity risk. "Bluetooth is an open standard and therein lies your security issue," wrote someone who worked for a manufacturer, while an installer said the application is "in its infancy and can be a huge security risk if poorly installed and set up."

However impregnable their core systems, enterprises are increasingly — and justifiably — concerned about the vulnerabilities of devices connected to their network from outside their security perimeter. Nearly half (45%) of chief information officers, tech executives, and IT employees saw mobile devices as the biggest weak spot in their defences, according to a 2016 survey by Tech Pro Research[4]. A separate, Crowd Research Partners report found around one in five (21%) businesses had suffered a mobile security breach, most frequently via malware and malicious Wi-Fi.

Ultimately, organisations can never rely on all employees having robust protections installed and regularly updating their operating systems, let alone having enterprise-standard defences.

One solution is to eschew the BYOD (bring your own device) trend in favour of CYOD (choose your own device), whereby users select devices from a pre-approved list. If employees are restricted to company-owned and managed phones and tablets, IT administrators can maintain blanket enterprise-level protection and have full visibility of all devices in the network.

About three-quarters of 700 senior IT professionals told IDC their organisations already had, or planned to implement, CYOD programmes for employees[5]. However, CYOD is obviously a bigger drain on an organisation's hardware budget.

Mobile access in the hotel trade

The hotel trade is arguably the most promising sector for mobile access. By requiring customers to download an app, keyless smartphone entry gives hoteliers a channel through which they can subsequently send customers special offers and engage in other ways. Customers, meanwhile, can optimise their stay — anything from modulating room temperature to ordering room service — without calling or queuing up at the reception desk.

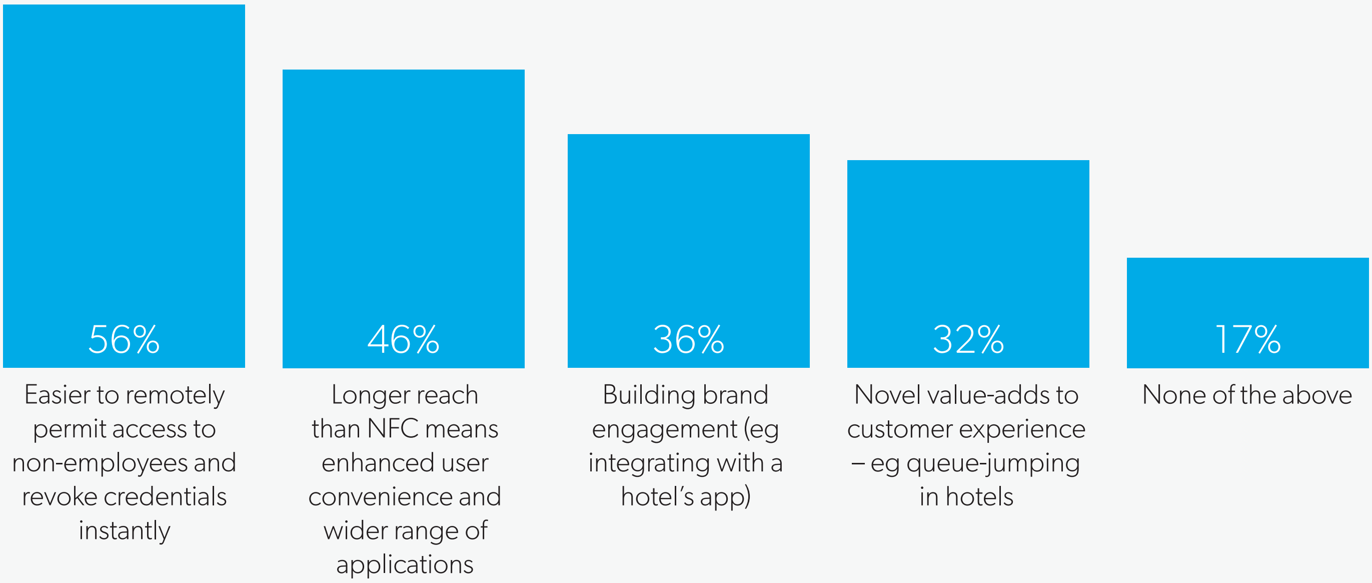
Starwood, Hilton, Marriott and InterContinental Hotels Group have introduced or are developing keyless entry applications. Alyssa Waxenberg, VP of mobile at Starwood Hotels & Resorts, has called its own app, SPG Keyless[6], "transformative for Starwood's hotel associates, allowing

[4] https://hbr.org/2016/09/your-biggest-cybersecurity-weakness-is-your-phone

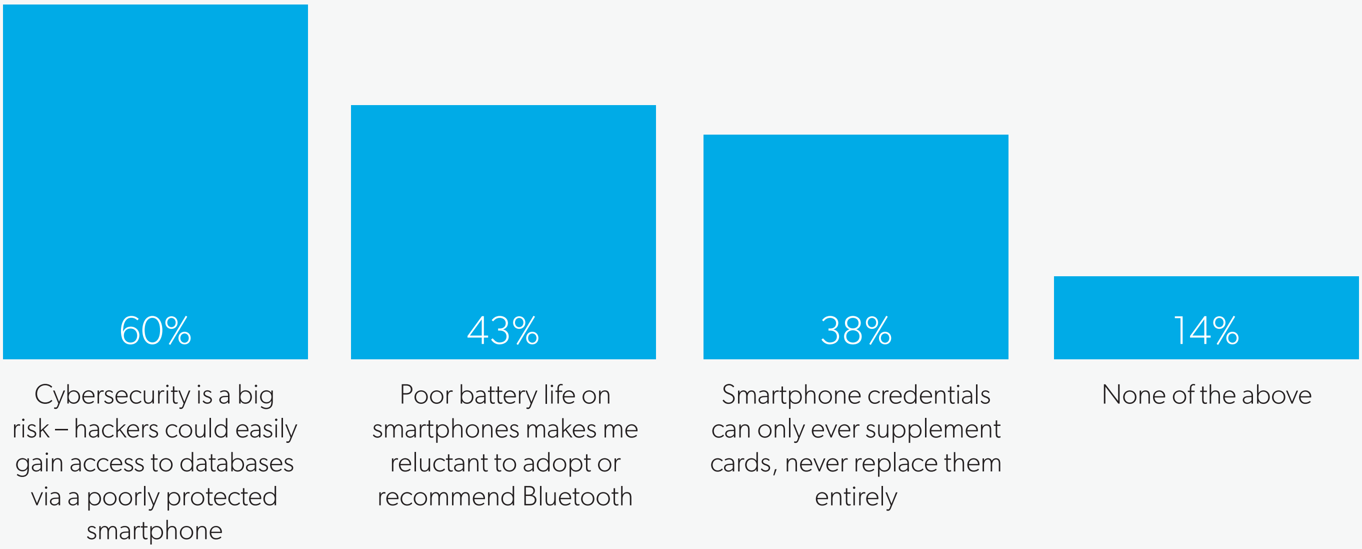
[5] http://www.idc.com/getdoc.jsp?containerId=prUS41706116

[6] https://www.spgpromos.com/keyless/

Do you agree that Bluetooth access control has the following benefits?



Do you agree that Bluetooth access control has the following drawbacks?



them to better-engage with guests. Rather than the first interaction being the swipe of a credit card, hotel associates can now focus on ways to better personalise guests' stays." Hilton said use of its Digital Key[7] app added 10 percentage points to the average "efficiency of arrival" rating submitted by guests and five to "overall hotel experience".

But a majority of our survey respondents neither agree that "building brand engagement" (36% ticked this option) nor introducing "novel value-adds to customer experience" like queue-jumping (32%) are, at least at present, compelling benefits offered by Bluetooth-enabled mobile access. One installer said there is a "licensing issue – not an easy task for a smaller company or even residential application."

Nearly half (46%) agree that "having a longer reach than NFC" enhances user convenience and widens the scope of potential applications for Bluetooth. While NFC can only work at a distance of a few inches, Bluetooth's range extends to several feet. Bluetooth (specifically Bluetooth Low Energy or BLE in this context) has also become the dominant wireless standard for mobile access because, unlike NFC, its use doesn't hinge on securing permission from handset manufacturers or mobile network operators.

Slow to embrace mobile

Nevertheless, hotel sector aside, smartphones are not widely used as a physical access credential. In 2016, according to Gartner's *Predicts 2017* report, less than 5% of organisations enabled the use of smartphones for access to offices or other premises. From giving us real-time directions to driving the dating scene and settling the restaurant bill, smartphones are already central to our daily lives — and they're used widely in logical access control as part of two-factor authentication, notably in internet banking. So why does the decades-old plastic card remain the dominant credential in corporate environments?

[7] http://hiltonhonors3.hilton.com/en/hhonors-mobile-app/digital-key.html

IHS insight

"In addition to being able to issue and revoke mobile credentials instantly (and remotely), a number of other benefits spring to mind:

- **Convenience:** Smartphone usage is widespread globally, even in less developed countries. This means that there already exists a larger potential customer base compared to competing credential technologies.
- **Added security:** An employee is far less likely to lend a colleague their mobile phone than a smart card.
- **Improved privacy:** Most smartphone users add some kind of authenticator to 'unlock' or access data on the device. This helps preserve the identity of a mobile credential holder, especially if the device is lost or stolen.
- **Financial savings:** Depending on pricing, mobile credentials could lower the cost of credentials for end users. This is because the marginal cost – the cost of creating an additional mobile credential – is essentially zero."

Jim Dearing, *senior analyst for security & building technologies, IHS Markit*

Where access control is concerned, security departments have historically been tasked with fulfilling two major tasks as inexpensively as possible: tracking time and attendance; and preventing unauthorised entry. Rightly or wrongly, cards, fobs and keycodes are seen as doing these jobs adequately. Security professionals are unwilling to jeopardise security by adopting innovations perceived as unproven.

Why is the decades-old plastic card still the dominant credential in corporate environments?

Vendors have a tough job convincing organisations that the benefits are compelling enough to justify the investment, and that the risks are negligible. Where vendors talk of enhanced user experience and operational efficiency, more conservative security professionals might see unnecessary cost, risk and complexity. Nearly everyone owns a mobile phone, true, but those phones come with a range of operating systems, capabilities and compatibilities, and cyber protections. By contrast, everyone gets the same, standard access card and this simplicity appeals to many.

Nevertheless, as corporate infrastructures are upgraded, mobile access technology matures and the installed base grows, many naysayers will relent, according to research by two authoritative sources. Gartner, which predicts that 20% of organisations will use mobile credentials for physical access by 2020, argues that smartphones can capture and match biometric data centrally, negating the need for separate biometric readers and reducing the total cost of ownership. It also suggests mobile access provides greater flexibility in terms of adapting access rights in real time based on risk analysis. It's also worth noting that people are vastly more careful about guarding their expensive phone than a cheap plastic access card. And even when a phone is stolen, password and biometric restrictions can prevent a thief from gaining entry to premises.

IHS Markit projects that 44 million mobile credentials will be downloaded by 2021, up from one million in 2016[8]. In *Access Control Intelligence Database – Mobile Credentials – 2017*, the research firm argues that, because mobile credentials are not competing against physical cards but are offered as a complementary alternative, "the potential market is [actually] much larger"[9].

The reason they aren't seen as a replacement is partly down to a perennial bugbear of smartphone users. Over the years smartphones have improved steadily on almost every metric — becoming lighter, sleeker, more powerful — except one: battery life. (Battery performance has improved but in a context of ever-more power-hungry handsets and software.)

Asked if "poor battery life on smartphones made them reluctant to adopt or recommend Bluetooth," 43% said it did. The other 57% may well have reasoned that people are pretty fastidious about recharging regularly and rationing power, and that no organisation would countenance not having cards or fobs as a back-up anyway. Dr Billy Wu, an Electrochemical Science and Engineering lecturer at Imperial College London's Dyson School of Engineering, told *TechRadar* that a game-changing breakthrough in battery life might still be a decade away. Thirty-eight percent of those polled in our survey say they cannot envisage smartphone credentials ever fully replacing cards.

The growth trajectory of mobile access will likely mirror that of the cloud. As organisations shift away from proprietary, closed systems to open platform, cloud-based IT infrastructure, integrations with peripherals like smartphones will become more viable.

[8] https://technology.ihs.com/596242/access-to-apples-nfc-chip-could-spur-new-growth-in-mobile-access-control-credentials

[9] https://technology.ihs.com/596141/access-control-intelligence-database-mobile-credentials-2017

The cloud and access control 'as a service'

In its 2016 report *Technology Insight for physical access control*, Gartner predicted that 20% of large organisations will use cloud-based physical access control systems by 2020[10]. Why is demand growing so strongly?

First, it's important to make a distinction between two cloud models: an internal cloud and software as a service (SaaS). In essence, it's about who manages the data. SaaS — or access control as a service (ACaaS) in this context — is a software application operated by an external service provider, which also hosts and stores the data in its own data centre. ACaaS outsources your entire data operation — storage, governance, and control — to a third party.

An internal cloud also locates an organisation's data off-site, but it manages as well as generates the data itself. Also known as a corporate cloud, the internal cloud harnesses virtualisation mechanisms, shared storage and network resources.

Cloud pros and cons

Running in-house servers is arguably more expensive, in a more unpredictable way, than either cloud model. One-off investment is needed to buy servers when organisations scale up, while system faults necessitate unforeseen expenditure on maintenance.

Conversely, ACaaS is more like a subscription model and capacity can be quickly scaled up or down by moving a customer into different pricing tiers. There are no unanticipated maintenance costs and it also unburdens in-house IT teams of the hassle of daily data backups, maintenance checks and complex network routing. For internal cloud systems, if workloads grow you can migrate your virtual server from one host to another. No surprise then that nearly three quarters (74%) of respondents agreed that cloud environments — particularly ACaaS — are more scalable than internal servers.

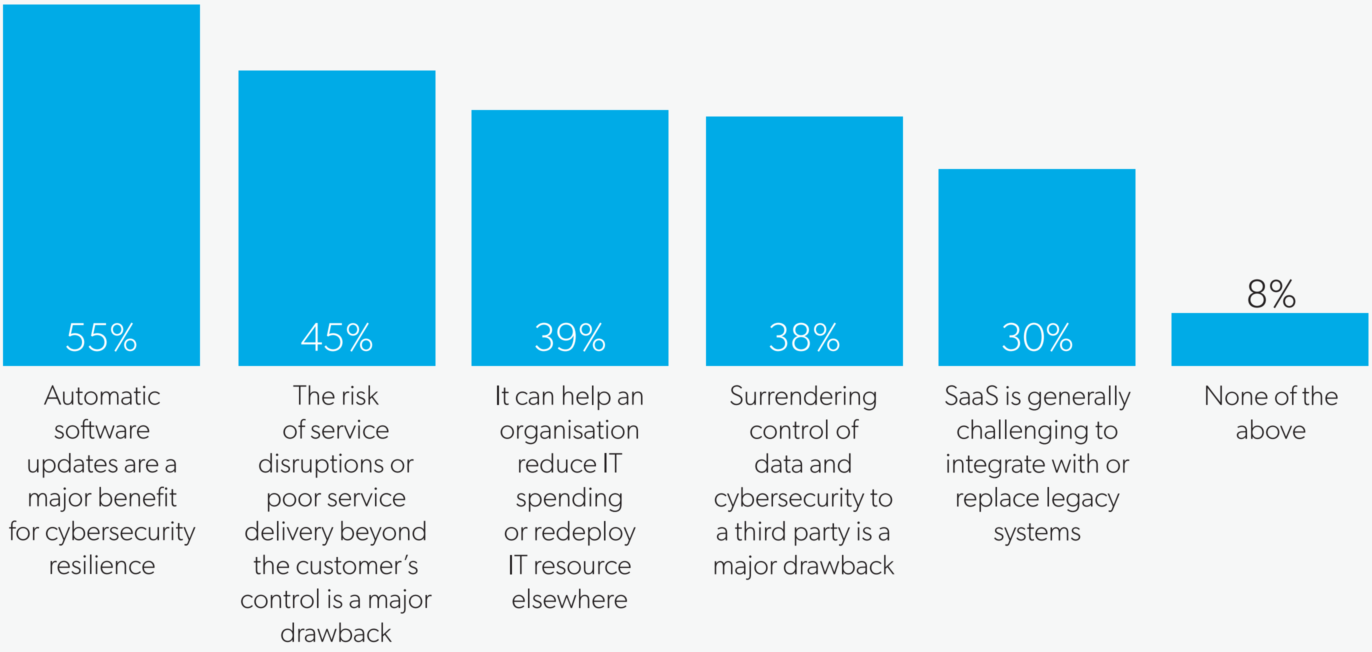
Technavio projects the global ACaaS market to grow at 22% CAGR during 2018–22

Using their own dedicated resources and infrastructure, organisations with an internal cloud bear higher capital costs and have fewer economies of scale. However, it does enjoy some of the benefits of the cloud (like scalability), but not ones associated with outsourcing like reducing the burden on IT. Then again, the organisation does not (whether you think this is a good thing or not) surrender control of its data and cybersecurity protections to a third party.

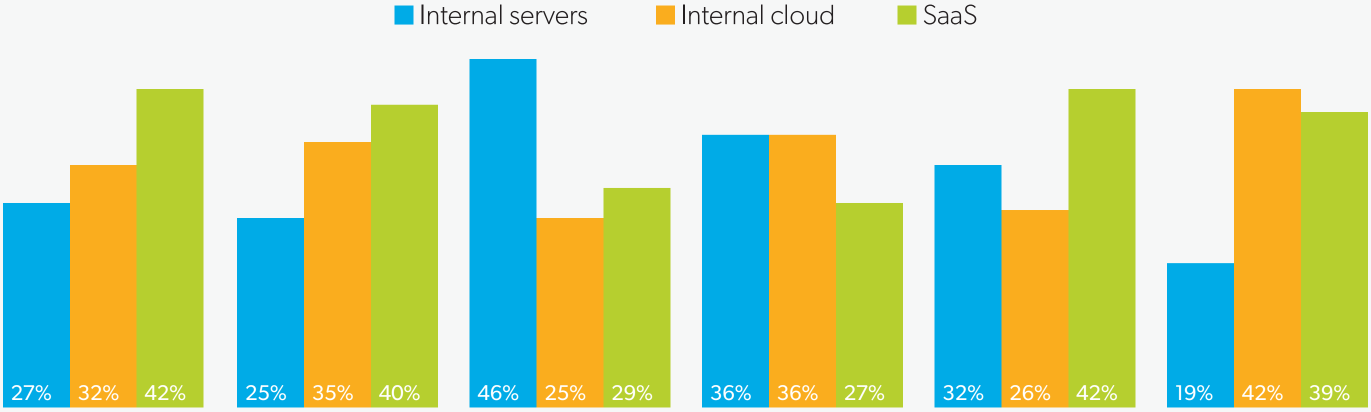
Remote from the user's location by definition, the cloud arguably provides superior remote access, via a unified interface. This also makes it particularly useful for managing multiple sites.

[10] https://www.gartner.com/doc/3451120/technology-insight-physical-access-control

Which statements do you agree with about SaaS (Software as a Service)?



Which of these models in your opinion is most likely to...?



	Internal servers	Internal cloud	SaaS
Be most flexible and scalable (quicker/ cheaper to add/ remove locks/ functionality as company grows/ streamlines)	27%	32%	42%
Be most cost-effective	25%	35%	40%
Be most cyber-secure and helpful in attaining compliance	46%	25%	29%
Best suit large/ enterprise organisations	36%	36%	27%
Best suit small to medium-sized businesses (SMEs)	32%	26%	42%
Best suit remote locations (like utilities, telcos etc with more than one site)	19%	42%	39%

Access control imposes a much lighter burden on bandwidth than, say, Video as a Service (VaaS). Many organisations already outsource security systems infrastructure to major providers with specialist infrastructure such as Chubb or G4S. Mindful of the shifting zeitgeist, those yet to adopt ACaaS are nevertheless upgrading hardware with future compatibility with the cloud in mind.

Market research firm Technavio projects that the global ACaaS market will grow at a CAGR of 22% between 2018 and 2022.

Industry view on internal servers vs. internal cloud vs. ACaaS

Surely, then, we can expect industry professionals to agree that ACaaS is superior in a range of areas? Not so: the overall response was fairly ambivalent.

A sizeable majority (55%) agree that "automatic software updates are a major benefit for cybersecurity resilience". This was as emphatic as it got. Only about two in five (39%) think "it can help an organisation reduce IT spending or redeploy IT resource elsewhere".

Not that, conversely, survey respondents ticked negative assertions in greater numbers. Forty-five percent are concerned about a serious "risk of service disruptions or poor service delivery beyond the customer's control". And a similar proportion (38%) think surrendering control of data and cybersecurity to a third party is a major drawback.

Just 30% believe ACaaS is generally challenging to integrate with or replace legacy systems.

Perhaps there is simply a knowledge gap with the cloud, which after all remains a relatively new data management model. We might speculate that if a respondent has no strong opinion on a positive or negative statement, they will likely decline to tick the box. Indeed, one respondent admitted to being "not really qualified to answer this." That said, respondents were offered the chance to choose "none of the above" and only 8% did so.

Perhaps the most interesting comment came from an employee of a manufacturer, who considered the needs of industry in the years ahead: "Edge-based, zero-touch computer solutions (as opposed to internal cloud) are likely to be both the most cost-effective and most scalable IT infrastructure solutions as we move into the IoT age: powerful computing solutions, where they are needed most without the potential cost, delivery, support and security issues associated with using either internal or external cloud solutions."

IHS insight

“Access control as a service has enabled businesses without resources to afford the high initial costs of installing an electronic access control system, therefore improving their facility’s safety. Some smaller businesses may also be unable to afford a full-time or 24-hour-a-day security staff in light of continually rising labour costs. An ACaaS system can help these users achieve a sufficient level of building security.

“The traditional barrier to wider adoption of cloud/ACaaS is that open architecture is inherently insecure. An on-premise solution offers a safer environment because it runs on a closed network. This stems from the perception that data security is ensured by its location, not by the means through which the data is accessed. Often this perception that on-premise solutions are more resistant to attacks has led to vulnerabilities in installations, leaving company data vulnerable. Communication between access control equipment or to a local server can be encrypted and the network secured with a firewall.

“However, problems with single-factor authentication, weak passwords or poor security protocols can make the system vulnerable. The method used to connect equipment to a server is just as important as the application-level connection to that server.”

Jim Dearing, *senior analyst for security & building technologies, IHS Markit*

Internal servers had a strong lead over ACaaS, and was marginally ahead of the internal cloud, for best suiting large/enterprise organisations, presumably because they have sufficient scale to support their own infrastructure. Conversely, ACaaS was deemed the most suitable for SMEs.

On-premises infrastructure fared worse than both internal and external clouds on each one of the other three measures posed in our survey. It came a particularly distant third for suiting remote locations like utilities and telcos, who often occupy more than one site.

On-premises access control systems were subject to many more “brute force” cyber-attacks

“Sent to the cloud, where it is collected, aggregated, and delivered via reporting applications to both local and corporate decision-makers, data can significantly increase visibility into remote building performance,” according to Cara Ryan, writing on Sourceable in 2016[11]. “With cloud technology, all staff from the CFO to the maintenance director can have near real-time visibility into energy use and occupant comfort across the enterprise.” Ryan, now offer manager for smart building services at Schneider Electric, added that through the cloud you can “compare performance of energy and time and attendance — and how they dovetail — and other variables across sites to drive continuous improvement.”

In our survey, both internal clouds and, particularly, ACaaS were seen as more cost-effective than on-premises environments.

Cybersecurity

If internal servers now seem like yesterday’s technology, then many in the security industry still believe they are the best defence against today’s most pressing threat: more respondents (46%) think on-premises storage was more cyber-secure and helpful in attaining compliance than a corporate cloud (25%) or ACaaS (29%).

Yet Alert Logic’s *State of Cloud Security Report*, published in 2012 when the cloud was even more immature, said “the variations in threat activity are not as important as where the infrastructure is located. Anything that can be possibly accessed from outside — whether enterprise or cloud — has equal chances of being attacked, because attacks are opportunistic in nature.” Their report found that web application-based attacks hit on-site environments as well as service provider environments, albeit the latter happened to a greater proportion of organisations (53% versus 44%).

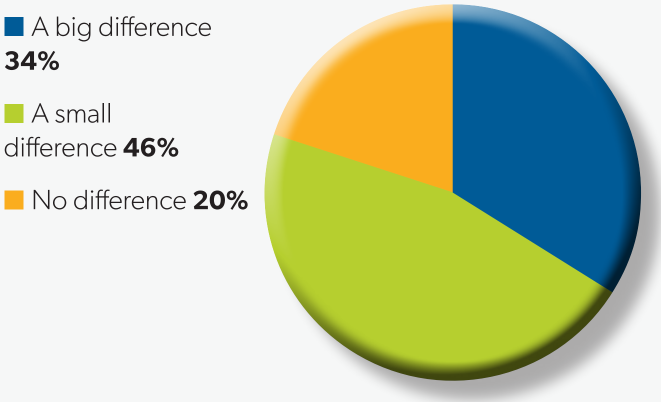
However, on-site environments suffered a far higher average number of attacks: 61.4 attacks against just 27.8 for cloud systems. Predictably, on-premises systems were also subject to far more “brute force” attacks. David Lithnicum, chief cloud strategy officer at Deloitte Consulting, wrote on TechTarget: “Those who build cloud-based platforms for enterprises typically focus more on security and governance than those who build systems that will exist inside firewalls.[12]”

[11] https://sourceable.net/cloud-can-help-manage-multi-site-facilities/

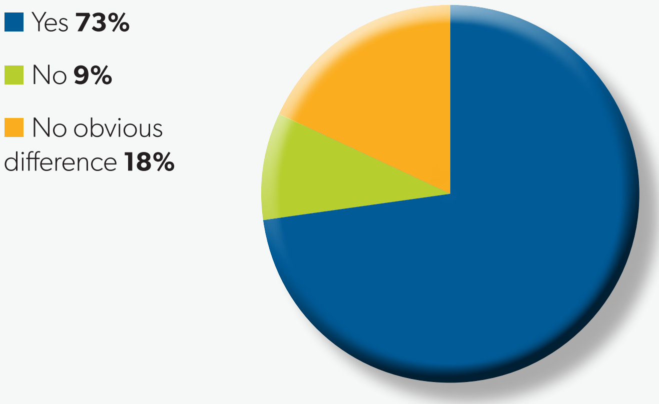
[12] https://searchcloudcomputing.techtarget.com/opinion/Clouds-are-more-secure-than-traditional-IT-systems-and-heres-why

Sustainability & energy efficiency

How much of a difference to whether you buy/recommend a product/solution would an Environmental Product Declaration (EPD) make?



Has sustainability/energy efficiency become more important in procurement decisions over the past 5-10 years?

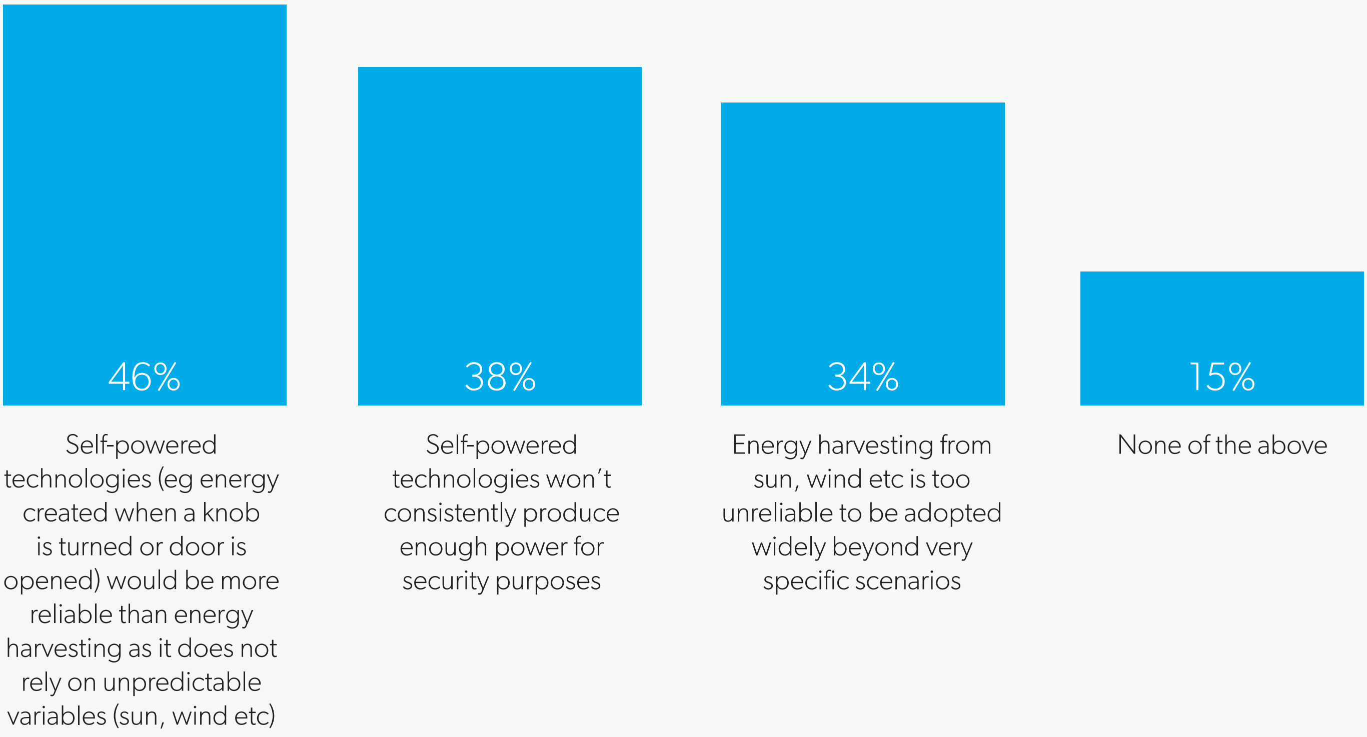


Defined by the Cambridge Dictionary as where "goods and services should be produced in ways that do not use resources that cannot be replaced and that do not damage the environment," sustainability offers three obvious benefits to organisations when it comes to procurement: better compliance, enhanced reputation and lower energy costs. Our findings suggest sustainability is now a major consideration when it comes to procurement. Seventy-three percent agreed that sustainability or energy efficiency has become more important in procurement decisions over the past 5–10 years.

In lifecycle assessments, an environmental product declaration (EPD) reports the environmental impact of a product or system, including factors like the environmental impact of raw material acquisition, energy use and efficiency, and materials and chemicals used. EPDs are created in accordance with ISO 14025, ISO 14040 and ISO 14044. Asked if the availability of an EPD would make a difference to whether they would buy/recommend a product/solution, four in five (80%) say it would, with about one in three (34%) saying it would make a "big difference".

Nothing reduces energy costs more than self-powered technologies. Rather than harvesting power from external sources like the sun, wind or sea, self-powered tech generates its own power with, in the case of door entry, every turn of a door's handle. The benefits, in theory, are significant: no wiring, no need to buy or dispose of batteries, no routine maintenance checks, no energy costs whatsoever. Nevertheless, one of our respondents asserted that "self-powered tech is an expensive undertaking but will become more popular as the development thereof gets better."

Which of these statements do you agree with about innovative sustainable energy solutions?



*241 respondents

Early attempts at self-powered locks were not entirely practical for commercial environments; a user might have to pump a door handle several times to charge the system sufficiently to gain access. But the latest breed of technology generates enough power with the slightest movement. Even when a door is dormant for days, weeks or months at a time, the lock will still 'wake up' and release the door upon a single handle pull. "Energy harvesting along with batteries or UPS would be reliable enough to be used in security," according to one installer.

Sustainability offers three obvious benefits: better compliance, enhanced reputation and lower energy costs

And yet a sizeable proportion of those polled (38%) imagined self-powered technologies wouldn't consistently produce enough power for security purposes. But while the self-powered mechanism doesn't generate much power, electronic door readers and wireless locks don't actually need much power. They are inactive, and can power down, for long periods. Their only task — reading card credentials and releasing the lock — is completed in less than a second and at the expense of minimal energy. There is a huge gulf in power consumption between access control points and, say, video surveillance cameras.

Solar panels can therefore generate enough power using artificial light alone. But while there are plenty of solar-powered outdoor gates and barriers, the market for internal doors is currently negligible.

External doors can generate thermal energy if fitted with a Peltier engine, which harnesses temperature differentials between the internal and external side of the door to charge a battery. However, again, thermal power is not widely used.

Not far short of half of respondents (46%) consider self-powered technologies a more reliable energy source than energy harvesting, because the latter relies on unpredictable variables. And 34% think energy harvesting from sunlight, thermal and other carbon-free sources is too unreliable to be adopted widely beyond very specific scenarios.

Both energy harvesting and self-powered solutions obviously maintain operation when mains power is lost — a boon in any scenario, notably mission-critical environments. Nevertheless, one manufacturer/service provider said they were "yet to see or be convinced by any deployable solutions."

Integration

Systems integration is a recurring theme in marketing materials for physical security products (although one respondent said that "vendors have not always seemed to grasp" its importance) and in conversations among security professionals. The previous edition of this report, published in 2016, suggested integrating systems was a frequent motive for upgrades. For 53% of respondents, easy integration with CCTV, alarms, time and attendance, lighting and HVAC would make them interested in upgrading to a particular product, more than any other factor we posed. Forty-three percent said easier integration with existing access control systems would make them more likely to upgrade.

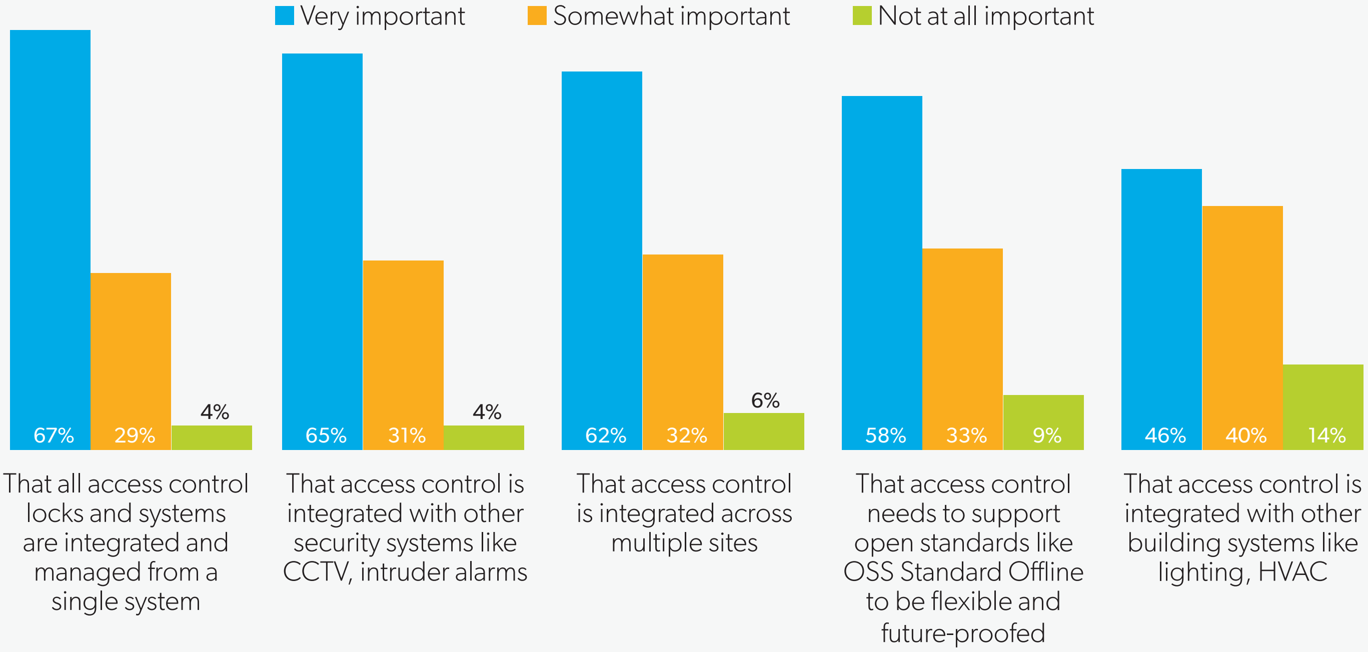
In the 2018 survey, an overwhelming majority (96%) agreed it was important to have access control points and systems fully integrated across the building, with the biggest proportion – 67% – opting for "very important". Responses are similarly distributed with regard to the value of integrating access control with other security systems (96% and 65%).

Some basic degree of security systems integration has long been executed in commercial premises by hardwiring connections between access control, intruder alarms and CCTV. A violation of the access control system, for instance, can trigger an alarm and prompt a camera to start recording the incident. In another scenario, the access control system might automatically lock down the server room if the intruder alarm is triggered. There are cost as well as security benefits; say, if a CCTV–access control integration reduces the number of security guards needed.

A well-executed convergence of logical and physical access, meanwhile, simplifies user management and enhances security. IT staff are thus better equipped to manage risk and compliance, while logical access can be restricted if, for example, someone gains unauthorised physical entry via tailgating.

Organisations are increasingly thinking beyond local or security-only integrations. Overwhelming majorities — with "very important" amassing the biggest shares in

How important is integration in the following ways?



both cases — also think integration with other building technologies (86%) and across multiple sites (94%) is at least "somewhat important".

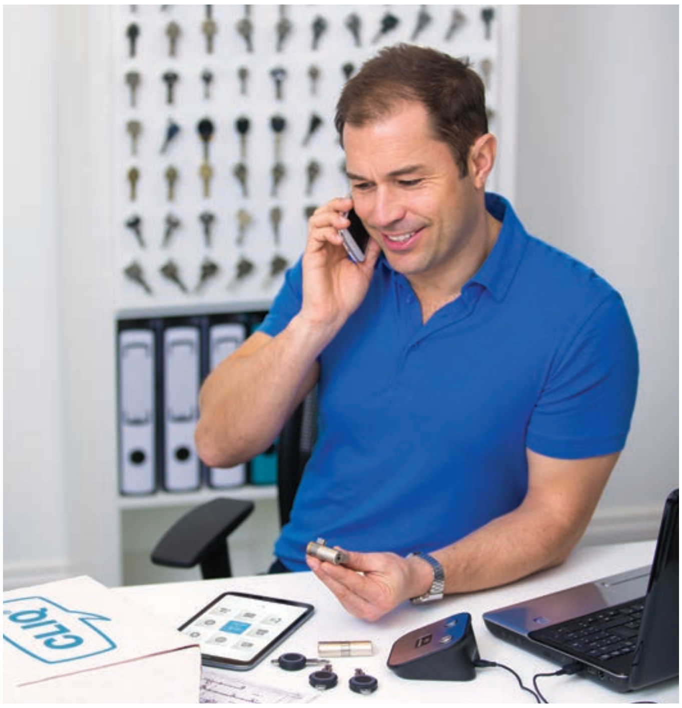
Collaborating with other department heads to drive efficiency gives security professionals a bigger say in the boardroom

Operational efficiency

Integration with other building systems means security systems — and by extension security teams — can contribute to operational efficiency as well as the protection of people and assets. Integrate HR systems with your access control system, for instance, and credentials can be automatically added or revoked when people join or leave the organisation, reducing administrative overheads and even headcount. Fewer interfaces are easier to support and require less training.

Integration can also enhance the experience of building occupants, who could use the same credential to access the car park, the building, their laptop and to buy lunch in the cafeteria.

Technological integration inevitably requires departmental integration, most obviously IT with facilities/security. Increasingly, large organisations appoint chief security officers to oversee combined logical-physical security departments. This is both a huge challenge — in terms of bridging knowledge gaps and delineating overlapping roles — and a big opportunity for facilities and physical security teams.



In protecting people and premises, rather than driving commercial operations, facilities and security personnel have traditionally been peripheral to an organisation's profit-driven goals. Collaborating with other department heads to drive operational efficiencies can give senior security professionals a bigger say in the boardroom. Exploiting this opportunity to its fullest will demand broader training that encompasses IT, cybersecurity and executive/leadership skills. A military or law enforcement background is no longer enough on its own.

In the face of such wide-ranging benefits, what accounts for the 4–14% who didn't consider integration important? Cybersecurity concerns may be a factor. The more integrated systems are, the greater the impact of any successful cyber-attack. Attackers need only gain access via the least protected system to wreak havoc on all connected systems. Indeed, one respondent noted that "integrated systems are a huge security risk".

Integration risks

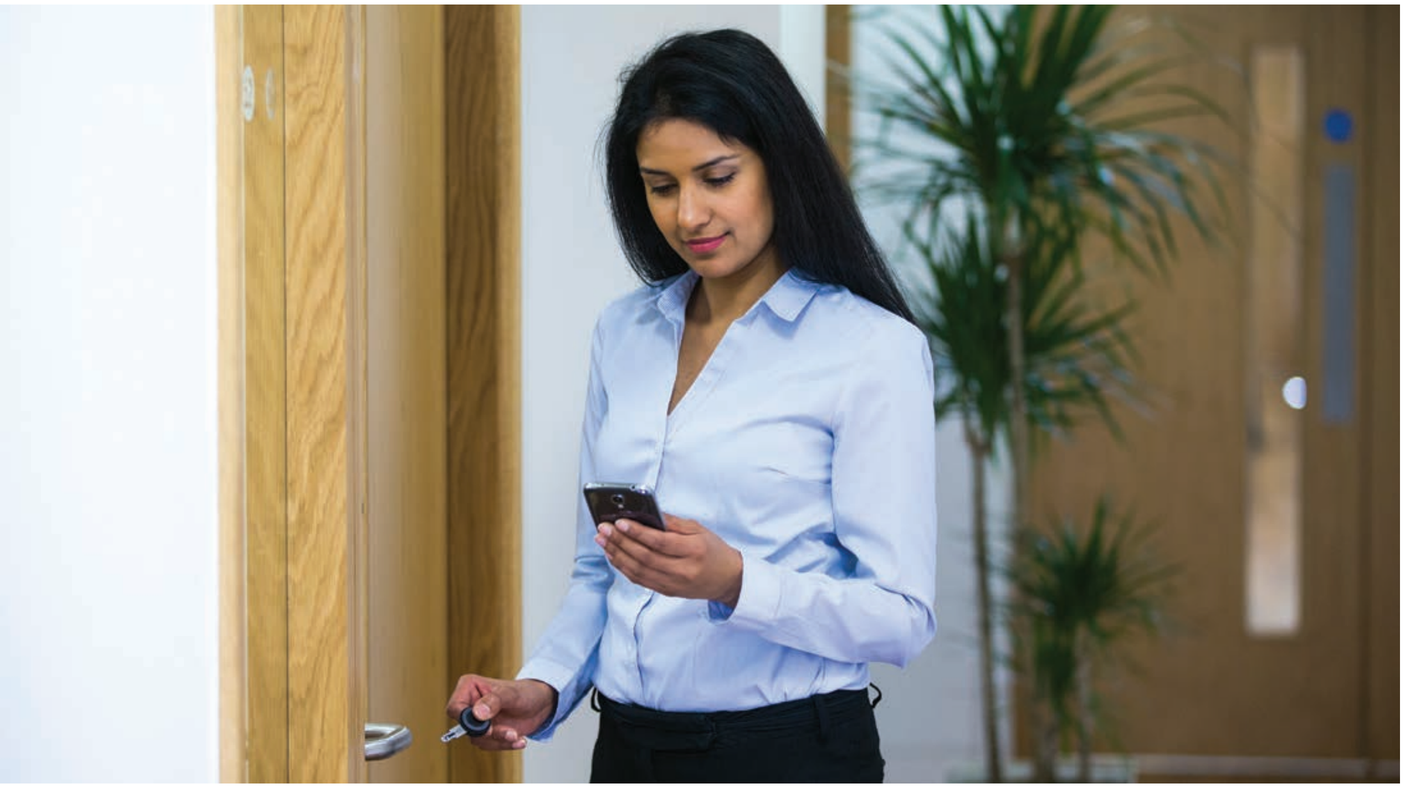
Integration also takes time, effort and resource — and costs easily escalate beyond initial budgets. Done badly, it can reduce the effectiveness of (or even disable) systems. Case studies abound. In 2013, for instance, tyre manufacturer Bridgestone sued IBM for $600m over an integration project that threw Bridgestone's "entire business operation into chaos"[13]. Defending itself, IBM said Bridgestone decided "to ignore IBM's warnings and prematurely roll out the implementation across its entire business" (the dispute still rumbles on at the time of writing).

One security professional we polled commented: "Integrating outside of family/industry systems such as ACS/IDS with BMS for buildings can create issues as the systems are often supplied by different installers etc. I have experience of an attempt for [such] a combined [system] that failed very badly." Suffice to say, organisations must do their due diligence when choosing an integrator and make sure integration specifications are precise, clear and financially and logistically realistic.

Costs can spiral further still if legacy systems are proprietary and therefore unable to integrate with other systems. Organisations might therefore take a view that partial integration is preferable to an expensive, comprehensive integration.

This is why future-proofing figures so much in procurement considerations today. Will the system accommodate the growth and changing needs of a business and the evolution of the hardware and software around it? Sometimes decision-makers buy a system with capabilities beyond current requirements in anticipation they'll eventually be

[13] http://www.businessinsider.com/bridgestone-sues-ibm-for-600m-2013-11?IR=T



needed, calculating this will be cheaper in the long run than adding capabilities later. Recognising this, growing numbers of vendors have developed a modular model.

A majority consider it "very important" for access control to support open standards like the OSS Standard Offline

Open platforms

Most access control developers have migrated, or are migrating, to open platforms in response to demand for greater flexibility, thereby dismantling technological barriers to integration and further fuelling demand. Hence 90% of those polled agreed integrating security systems with each other and with other building technology has become noticeably more important in the last five years.

The primacy of the smart building paradigm, where building systems are interconnected and generate and respond automatically to data generated, is also driving this shift. "Integration and single-seat management is where security systems in general will fit within the growing smart buildings brief the industry is getting from end users," noted one manufacturer employee.

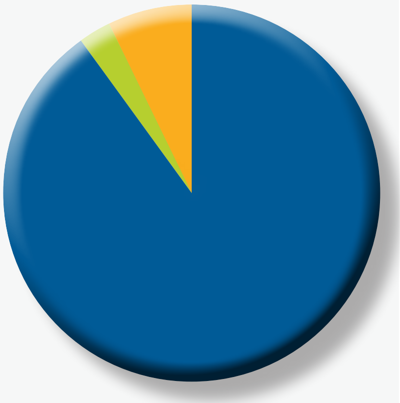
The importance of flexibility and future-proofing explains why major vendors make sure their latest readers and cards support a wide range of chips, such as CLASS, MIFARE® Classic, iCLASS®, MIFARE®, DESFire and Crescendo.

Has integrating security systems with each other and with other building technology become noticeably more important in the last 5 years?

Yes **90%**

No **3%**

No noticeable difference **7%**



A majority (58%) of those polled said it was "very important" that access control supports open standards like the OSS Standard Offline in order to be flexible and future-proofed, with the vast majority (91%) considering it at least "somewhat important". Wireless components that conform to the OSS Standard Offline, which was released by the Open Security Standards Association (OSS) in 2015, are interoperable with smartcards from a range of brands. Established by ASSA ABLOY, Nedap, Primion, dorma+Kaba Group, Deister and ACS, the Open Security Standards Association (OSS) develops standards that foster greater interoperability between access control products[14].

[14] https://www.oss-association.com/

Wireless access control solutions

Aperio®
Available globally, ASSA ABLOY's Aperio® devices enable access control providers to cost-effectively integrate non-wired doors with mechanical locks into new or existing access control systems. Doors merely need to be fitted with battery-powered, RFID-equipped Aperio® locks, cylinders, escutcheons or the new H100 Aperio® handle. Server rack locks (KS100) are also available. All Aperio® devices are then linked to the access control system via a communications hub for online integration, or via update on card for offline integration.

As a result, security and facility managers have greater control, can easily respond to organisational changes and only need to monitor a single security system; users carry a single RFID access card.

SMARTair®
SMARTair® is an access control system that offers an intelligent, yet simple, step up from physical keys. SMARTair® wireless locks are more cost-effective to fit and to operate than standard wired access control doors — and can be installed offline or online. Replacing a lost card is much cheaper and faster than replacing a key. SMARTair® access control doors are reprogrammed, with no need to replace locks or cylinders.

For users, SMARTair® offers smart-card and fob credentials, as well as the new Openow™ mobile app to open doors securely with a mobile phone.

CLIQ®
CLIQ® is a security locking system with high-end security, microelectronics and programmable keys. It combines mechanical and electronic protection to match different security and flexible access needs. Power is supplied by a battery inside every CLIQ® key.

In this wire-free system, each key can be programmed and updated individually to allow access to specific areas at specific times and dates, accommodating changing access requirements and ensuring maximum security.

CLIQ® incorporates flexible access and key management solutions for all kinds of locking applications. Flexible solutions include CLIQ® Connect, which smooths mobile workflows by enabling remote workers to update key permissions with a mobile app. For small to medium-sized businesses, CLIQ® Go enables managers to administer an access system on the move and in the cloud.

Learn more by visiting:
https://campaigns.assaabloyopeningsolutions.eu/wac

Recap & key trends: wireless access control in 2018

Market data in 2018

- Currently, only 6% of installed electronic access systems are fully wireless; a further 31% include a mix of wired and wireless devices
- A significantly higher proportion use wireless access control technology than in our 2016 report: the share of fully hardwired systems has fallen from 57% to 41%
- 'Non-door' deployment of wireless access devices is already significant, according to our survey: 24% of commercial environments have battery-powered locks on gates and other outdoor structures; 23% on server racks; 17% on safes; 16% on machinery; 17% on cabinets and lockers
- Transparency Market Research forecasts robust growth in the global wireless access control market between now and 2025, when revenues will reach US$1.66bn at a CAGR of 7.9%. They predict the 'non-door' market will grow at a CAGR of 12.9% to 2025

Trends

- **Installers are more convinced than customers about the benefits of wireless access control:** Three quarters (75%) agreed wireless systems make installation easier, quicker and more cost -effective but only 37% said "it's easier to convince customers of the benefits compared to wired". Fewer than half of end users believed wireless systems have a lower cost of ownership, for example, highlighting a need for continued market education (see p4-5)
- **Cloud-based physical access control will continue to experience strong demand growth:** ACaaS offers faster scaling and more predictable costs, despite a lack of industry consensus on the cybersecurity advantages and drawbacks vs. in-house management (see p13-15)
- **Sustainability is a major and growing factor in procurement:** Four in five (80%) state the availability of an EPD would influence whether they buy or recommend a solution, and because wireless access control devices need very little energy to operate, interest is likely to grow in self-powered and energy-harvesting technologies (see pp16-17)
- **Open standards like the OSS Standard Offline are critical to future-proofing:** Access control systems need to be flexible, and this means accommodating needs not yet foreseen (see p 20)
- **The uptake of mobile access credentials has been slow – for now:** Security professionals may (understandably) be unwilling to jeopardise security by adopting unproven innovations but change is coming: Gartner predicts 20% of organisations will use mobile credentials for access by 2020, and IHS Markit that 44 million mobile credentials will be downloaded by 2021 (see p 12)
- **Bluetooth is becoming the de facto standard for mobile access:** Its longer reach over NFC widens the scope of potential applications and, unlike NFC, use doesn't hinge on securing permission from a third party (see p10-11)
- **The most commonly cited benefit of Bluetooth is enabling remote access for non-employees and revoking credentials instantly:** Conversely, perceived cybersecurity risk is the biggest misgiving
- **Integration of an access control system with other functions remains key:** For operational efficiency (including reduced training costs) and user convenience benefits, an overwhelming majority of respondents emphasise the importance of having access control points and security systems fully integrated across the building and/or multiple premises (see p10)

IFSEC GLOBAL

IFSEC Global is a leading provider of news, features, videos and white papers for the security and fire industry.

Preeminent in the UK with a truly global audience, we cover developments in long-established physical technologies – like video surveillance, access control, intruder/fire alarms and guarding – and emerging innovations in cyber security, drones, smart buildings, home automation, the internet of things and more. With the help of the industry's foremost thought leaders, IFSEC Global also examines the latest developments and best practice in disciplines like security management, counter-terror and fire-risk assessments.

From vendors and system integrators to security professionals who buy, manage and operate fire and security technologies, we cater to the full supply chain.

IFSEC Global draws on a long pedigree in the security and fire sectors. IFSEC International, which is run by the same group – UBM – that owns IFSEC Global, launched in the UK in 1972. FIREX International, IFSEC's fire-safety-focused sister event, launched later on. Now a truly international brand, IFSEC has regional shows in India, Southeast Asia and the Philippines.