The Wireless Access Control Report 2023

IFSEC INSIDER

Sponsored by

ASSA ABLOY
Opening Solutions

Contents

Introduction

Welcome to the 2023 Wireless Access Control report, as we once again explore the major trends, opportunities and challenges in the market.

The report that follows here details the responses of over 400 security, facilities management and IT professionals who have influence over purchasing decisions or the administration of physical access control systems. Installers and systems integrators also took part, as they shared insight into the solutions they're most regularly working on.

It's worth noting that trends from our last report, published in 2021, have stayed relatively consistent.[1] While there are some differences in certain segments – mobile access control continues to build momentum – other areas have witnessed smaller, less significant increases.

These findings are interesting in themselves, however. The wider economic environment, as organisations have recovered from the aftermath of the COVID-19 pandemic, alongside macroeconomic factors such as the Russian invasion of Ukraine and well documented supply chain issues, has been challenging. Indeed, as our analyst partners at Omdia highlight in recent industry reports, supply chain disruptions have hit the full electronic security market, as semiconductor prices have jumped 15% in the last year and there has been a shortage of steel – both critical components in access control hardware and electronic locks.[2]

So perhaps it is of little surprise that organisations may not have invested heavily in wireless access control upgrades – cost is the chief obstacle in implementing a more integrated security environment, for instance.

The sector remains a technologically driven environment, though. The key trends ahead continue to focus on mobile access and an investment in cloud-based systems, while integration of access control into not just the security environment but also building management systems (BMS) is required to promote evolution to smarter, more efficient buildings.

If security is the lock, convenience is the key in the physical access control environment. As access control influencer Lee Odess remarked on episode 11 of the IFSEC Insider Security in Focus podcast, convenience is now just as important to end-users as security credentials – access control is now about so much more than letting people in and out of a building.[3] This year's report backs these assertions up. Whether it's moving to mobile access or specifying a system with open credentials, convenience for both the end-user and administrator is a top priority.

Sustainability remains a principle focus for the majority of businesses, too. But how can access control support these goals and objectives? In particular, we asked respondents what aspects of wireless systems they believe can help in this area.

[1] Notable trends from the 2021 report include growing focuses on mobile credentials, the development of integrated physical security systems, cloud-based infrastructure and open standards.
[2] Omdia, Access Control Intelligence Service, **https://omdia.tech.informa.com/products/access-control---2023**
[3] IFSEC Global, What's next for access control? Lee Odess, **https://www.ifsecglobal.com/podcasts/episode-11-whats-next-for-access-control-lee-odess/**

Report produced by
James Moore
Managing Editor, IFSEC Insider

Contributors:
Chris Price
IFSEC Insider
Bryan Montany
Omdia
Asier Elorza
ASSA ABLOY Opening Solutions
Kelly Gill
ASSA ABLOY Opening Solutions
Olympia Dolla
ASSA ABLOY Opening Solutions
Richard Sharp
ASSA ABLOY Opening Solutions

This year's report also explores the issue of cyber security in greater depth than we've done before. We sought to understand the levels of interest, awareness and engagement of various cyber security regulations and guidelines in UK and European markets in particular. Our survey results demonstrate that cyber security is no longer the sole domain of the IT department, with physical security professionals now needing to be at the very least aware of regulations that the connected products they are installing and managing must hold cyber secure credentials.

Our final chapter marks another change compared to previous reports. With evidence suggesting that security professionals often lack influence at the C-suite level or over their own budgets, we asked whether this was also the experience of our own respondents. And if so, how do they think they can improve this situation? Perhaps the insight generated from modern wireless access control systems could be key to unlocking more influence at board level, as security professionals can furnish businesses with a tangible return on investment through data-led decision making.

About IFSEC Insider

IFSEC Insider – formerly IFSEC Global – is a leading news and online content provider for the security and fire safety markets. Alongside daily articles covering the latest in the sectors, IFSEC Insider also delivers valuable insight and analysis on market trends via webinars, podcasts and trend reports for the global security and fire communities.

About ASSA ABLOY

The ASSA ABLOY Group is the global leader in access solutions. Every day, we help billions of people experience a more open world. ASSA ABLOY Opening Solutions leads the development within door openings and products for access solutions in homes, businesses and institutions. Their offering includes doors, door and window hardware, locks, access control and service.

Executive summary: Key findings of the 2023 Wireless Access Control Report

1. Convenience of access control is vital – no longer solely a security platform?

A shift towards electronic access control systems away from traditional mechanical devices continues, but it's no longer just about security. Convenience – such as ease of use for both operators and users – is a key part of the specification process in 2023. The most popular reason for adopting mobile access credentials, for instance, is convenience. Security is now assumed – so how do traditional vendors look to provide an improved user experience that is flexible, adaptable and scalable?

2. Mobile credentials adoption gathers momentum in access control

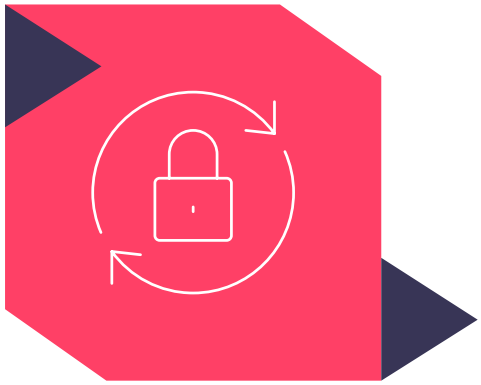
While rarely used as the sole format of credential, the adoption of mobile-enabled access control solutions continues to gather pace: 29% of organisations surveyed said they now used mobile credentials, a 3% rise from our 2021 report. Proponents point towards improved convenience for users and administrators, as well as creating an additional security layer where phones require a method of authentication before they can be used.

3. Wireless access control can contribute to sustainability goals

There is growing awareness of the role physical security systems can play in meeting organisations' sustainability goals. Access control is often the starting point for managing a facility's efficiency, with adjacent building systems such as lighting, power and HVAC responding to the required occupancy level. Respondents believe wireless systems can contribute at source, reducing the need for cables and maintenance requirements.

4. Low awareness of cyber security regulations – despite growth in connected physical security systems in scope

Over half of those surveyed were not aware of four key cyber security regulatory requirements or certifications. Despite 35% of respondents believing that their choice of access control system can strongly contribute to a company's cyber security credentials, there appears to be a knowledge gap for physical security and facilities professionals. With so many physical security devices now connected to corporate networks, it is imperative that systems are protected from cyber-attacks so as not to become the 'weak point' in an organisation.



5. Open standards now a necessity in purchasing decisions

Of key importance to industry professionals is having a wireless access control system that can be integrated into a comprehensive security solution. And it's not just security, but wider building management platform integration that end-users are now looking for as they seek to better track occupancy levels to improve building efficiencies. Those surveyed believe open standards will be vital to this development, with 93% answering they were either 'very' or 'somewhat' important.

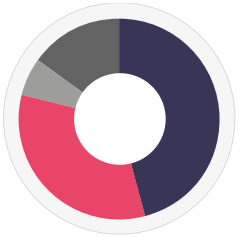
Trends in wireless access control

Wireless technology is transforming all areas of our lives, from the headphones we buy to how we travel on public transport, make payments and access the internet. How we enter, exit, and control access throughout buildings and estates is no exception with Bluetooth Low Energy (BLE) and WiFi 6 becoming increasingly popular standards in the security industry.

Before we assess the major trends in wireless access control, we first asked where the industry was at overall, in terms of the transition from mechanical to electronic access systems.

According to our end-user respondents, only 15% of businesses don't have any electronic access system in place at all. That's down from 23% when we carried out the survey in 2021. Although traditional wired systems remain the most popular access option for organisations at 46%, one in three of those surveyed (33%) now have a combined wired and wireless system in place, up from 30% in 2021.

Furthermore, 6% of organisations already operate an entirely wireless access system that can verify a user's credentials to allow access through a door using wireless electronic locks and readers. With a wireless system in place, different components communicate with one another over a wireless router while locally installed or cloud-based software enables system administrators to establish permissions for users and manage communications no matter where they are in the world.



Does your organisation already operate an electronic access control system?

- (**46%**) Yes, a traditional wired system
- (**33%**) Yes, a combined system of wired and wireless access
- (**6%**) Yes, a fully wireless access control system
- (**15%**) No

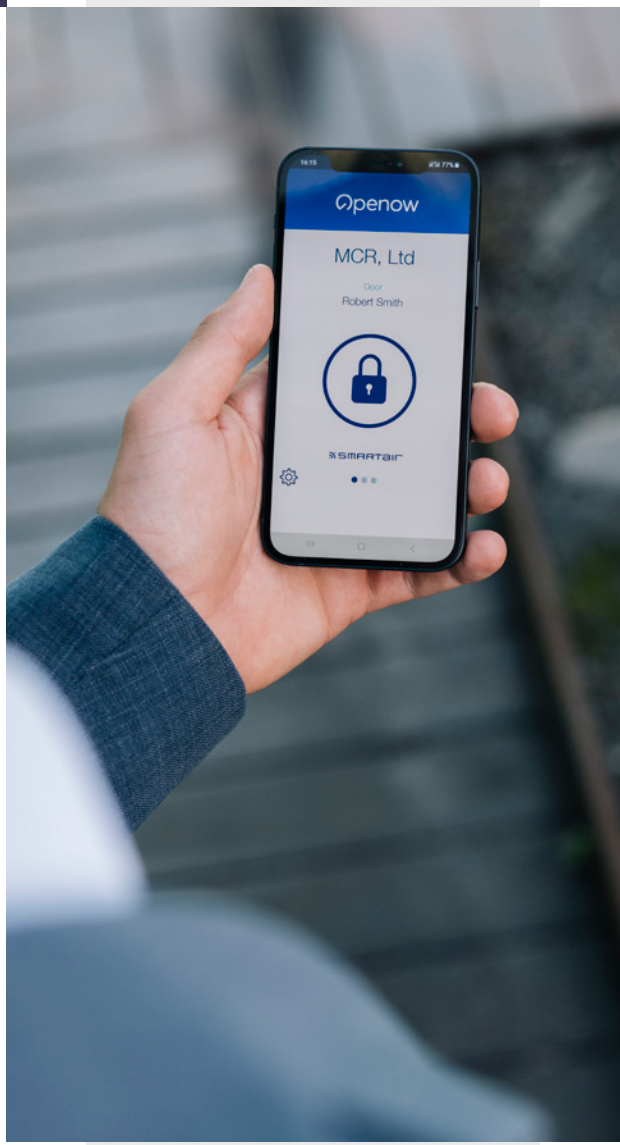
Rise of mobile access

Related to the shift towards wireless technology generally, is the trend towards mobile-based access control – for example using a smartphone as a means of entry into a building.

According to research analysts Omdia, nearly 29.8 million 'mobile credentials' for access control were downloaded globally in 2021 with that number projected to grow at a 44.9% CAGR between 2021 and 2026.[4]

Omdia's research shows that no other equipment type in the Physical Access Control (PACS) market is expected to experience a comparable growth rate during the forecast period. Vendors will frequently cite mobile credentials and mobile access solutions as a prevailing trend and this appears to be for good reason.

Indeed, the growth of mobile access control is reflected in this year's Wireless Access Control survey. While



[4] Omdia, Access Control Intelligence Service, **https://omdia.tech.informa.com/products/access-control---2023**

currently only 5% of organisations surveyed have solely mobile credentials in place, another one in four (24%) use mobile credentials alongside traditional credentials, to a greater or lesser extent. Combining these results suggests that 29% of our respondents offer mobile credentials – up from 26% in 2021.

What's more, 40% plan to implement mobile credentials within the next two years – up marginally from 39% in 2021.

Why might this be? Many proponents of mobile access point towards a more secure and convenient option.

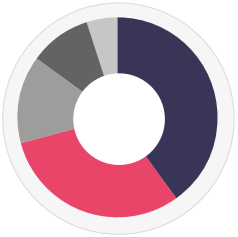
A user will always have their mobile phone with them and is unlikely to misplace it, making it a convenient solution for employees or visitors to access a facility or room. Meanwhile, phones generally offer multiple layers of security including facial or fingerprint recognition, adding biometrics into the security process, or 2FA (two-factor authentication) – though of course no technologies are completely without risk.

In addition, making a move towards mobile-ready readers and access control systems no longer requires a huge 'leap' for the end user. There are many options now available on the market which can integrate with existing systems, and therefore fewer barriers to build-in mobile ready solutions. Organisations may upgrade to 'mobile ready' solutions to futureproof their access control system, without needing to replace their current processes immediately.

Access control analyst lead at Omdia, Bryan Montany, adds: "Even end users that choose not to invest in mobile credentials will still prefer to invest in mobile-capable readers to ensure a potential future transition to mobile credentials."[5]

However, despite this definite shift towards mobile access, it isn't necessarily the right option for all organisations – for example in some parts of the healthcare sector, or areas of pharmaceutical or food preparation industries, where mobile phones may not be allowed for hygiene or security reasons.

Just over three in 10 respondents (31%) claimed that mobile credentials would not be the right solution for their organisation – though this is down from the 2021 survey, when the figure was 35%.



What is the use of mobile credentials in your organisation?

- (**40%**) I'm planning to implement mobile credentials within the next two years
- (**31%**) Mobile credentials are not right for my organisation
- (**14%**) We have some mobile but mainly use traditional credentials
- (**10%**) We mainly use mobile but have traditional credentials on the fringe
- (**5%**) Our organisation is already using mobile credentials only

"Mobile access is about convenience. And, for unlocking a door, the convenience of a smartphone is unquestionable. In a mobile world, it makes sense to keep secure keys on the device we carry everywhere.

"There are benefits from a facilities management perspective, too. Mobile keys enable you to react faster. Using a mobile management system like SMARTair Openow, for example, permissions can be cancelled or amended over the air without any need for updates.

"Fortunately, many existing access control devices are mobile-ready, with BLE compatibility working alongside standard RFID technologies like iCLASS and MIFARE. Businesses don't have to start from scratch with a whole new installation process."

Asier Elorza,
SMARTair Managing Director, ASSA ABLOY Opening Solutions EMEIA

[5] Omdia, Access Control Intelligence Service, **https://omdia.tech.informa.com/products/access-control---2023**

Convenience is key

Asked to rank the most important considerations for opting for mobile credentials from 1 to 8, convenience was in first place ahead of cost and security factors such as not being able to share mobile credentials with unauthorised people easily or finding it more difficult to clone mobile access.

Users also considered the fact that mobile credentials are a more sustainable option than key cards. Overall, sustainability ranked fifth out of eight places for mobile credentials.

Convenience wasn't just the top answer when respondents were asked to rank the most important factors for mobile credentials/virtual keys in order. Asked which statements they most agreed with, nearly 6 in 10 (57%) said 'using a mobile phone instead of a separate access card is more convenient', higher than 'mobile credentials are more flexible than hard credentials' (42%) and that 'mobile credentials are a better solution for external staff, visitors and remote workers' (38%).

Only 10% said they 'would not switch to mobile credentials because cards, fobs and tags already do everything I need' while a further 9% said the switch to mobile credential was not logistically feasible because of phone battery requirements.

Overcoming challenges

While the report clearly shows an appetite to use mobile credentials in their access control systems, barriers still remain for many organisations. Asked to name the biggest challenge they face, respondents cited the need to 'replace existing locks and/or readers' (43%), closely followed by 'pushback from employees not wanting to use their own smartphones' (34%) and concerns that 'employees' smartphones could provide security risks' (29%).

Surprisingly, perhaps, cost was less of a direct factor (only 19% said mobile access was too expensive), though it may have been a consideration among those who said that replacing existing equipment was their biggest challenge. This is slightly lower than the 22% who cited cost as a challenge in the 2021 Wireless Access Report and much lower than IFSEC Insider's Physical Access Control 2020 Report, in which 86% of end-users cited 'cost' as being among the top three obstacles to upgrading their access solutions.

Top 5 advantages of mobile credentials

Perhaps this is because some electronic access control systems now regularly receive software update patches, meaning that implementing a mobile access solution doesn't necessarily involve a complete 'rip and replace' process of the entire access system? For example, with readers that are BLE-enabled, users can switch to mobile credentials when it is appropriate for them to do so, without needing to replace the reader in the future.

Other factors mentioned as challenges for mobile credentials included ensuring 'all employees have appropriate company phones' (28%) and the 'need to retrain staff' (12%). Again, there may be cost implications with both of these factors, but it seems the main challenges are logistical rather than financial for organisations looking to switch to mobile credentials.

Open standards

Of key importance to industry professionals is having a wireless access control system that can be integrated into a comprehensive security solution. Traditionally, security professionals had to monitor separate access control, surveillance and intrusion alarm systems, each operating in different ways.

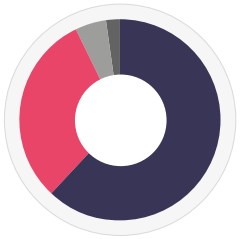
Open standards and architecture which work on common protocols and APIs mean this is no longer the case.

As Omdia's research also demonstrates, the evolution of smart buildings and system integrations has become a growth factor for electronic access control equipment sales more generally. According to its Smart Buildings Intelligence Service, more than 27% of the access control hardware market in 2020 was integrated into either a BMS platform or a physical security information management (PSIM) platform.[6]

Omdia's Bryan Montany adds: "A major trend that has contributed to higher adoption rates of BMS platforms is the need for facility managers to track occupancy levels in buildings. In the wake of the pandemic, facility managers have sought to procure occupancy-tracking data to better understand occupancy levels and ensure that social distancing requirements are adequately followed.

"Data related to the credentials of building occupants can be connected through security integration platforms, BMS platforms, and proptech (property technology) platforms to connect other domains across buildings with real-time, up-to-date information relating to occupancy that can be used to make informed decisions regarding the usage rates of rooms or zones of buildings."

Indeed, such is the importance of security integration that over 9 in 10 respondents said open architecture and interoperability was either very important (62%) or somewhat important (31%) when specifying an access control system – almost exactly the same percentages as our 2021 report which were 62% and 30% respectively.



How important are open standards when it comes to choosing or recommending a security system?

- (**62%**) Very important
- (**31%**) Somewhat important
- (**5%**) Fairly unimportant
- (**2%**) Not important at all

[6] Omdia, Smart Buildings Intelligence Service, **https://omdia.tech.informa.com/products/smart-buildings-intelligence-service**

Greater security integration

But what third party functions or technologies do security professionals want to be able to integrate alongside electronic access/door control using open standards?

Not surprisingly perhaps given the audience of security professionals, CCTV/video surveillance was the top answer (78%) closely followed by an alarm system (72%) and visitor management (68%). Much less popular, though still featured, was integration with HVAC and lighting systems which only one in three (33%) respondents considered important.

According to respondents, the main advantages of having an integrated security system is that it removes the need to keep multiple systems updated (74%), makes compliance easier (48%) and saves employees' time (48%).

However, despite the clear advantages, challenges remain for the security industry when it comes to greater security integration. Chief among them is cost, cited as the biggest factor by 67%. This is up from 59% in 2021's survey, perhaps reflecting the greater cost pressures on businesses due to rising inflation.

Other factors holding organisations back from greater security integration include complexity at 38% and lack of knowledge – up from 26% in our previous survey to 32% in this year's. This suggests that more work needs to be done in educating security professionals across the supply chain about the options available to them and how they are best integrated.

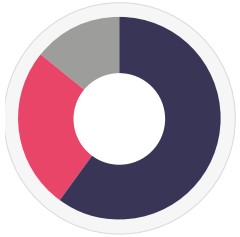
Top 5 factors holding businesses back from integration?

Top three desired functions to control from an integrated environment alongside access control

Access control and the cloud

As well as the trend towards greater security systems integration, there is also a move towards cloud-based applications – particularly when it comes to hosting surveillance footage and analytics software in the cloud.

We are seeing the same shift in access control, although it is a much more fragmented picture. While over half (51%) of respondents stated they still use local internal servers for access control – down from 65% in the 2021 survey – just over one in five (22%) host their system locally but use a cloud-based access management system. And 12% rely on third party cloud-based services, such as ACaaS (access control as a service) – slightly up from 11% in last year's survey.



Which model is your electronic access system based on?

- (**51%**) Local internal servers
- (**22%**) Locally hosted, cloud-based management
- (**12%**) Third party software-hosting in the cloud

Unlike more traditional access control systems, SaaS or ACaaS models involve using a cloud-based software application from an external provider, which may or may not also be the systems provider. Options include a hosted model which allows users to retain full control over administrative procedures using a remote data server and a managed solution where administration and management responsibilities are handled by the third-party provider.

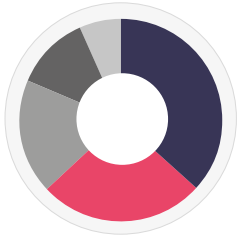
According to our survey, the main reason why organisations choose an external SaaS or ACaaS provider is for automated software updates and patches (39%). However, other benefits include the ability to offer access control systems in real-time (38%), unlimited scalability (29%) and a subscription-based business model. In other words, rather than having to invest heavily in access control systems which may not be suitable for their long-term needs, many organisations like the flexibility of an external solution that can be scaled as they grow or even reduced if their business needs to contract.

Biggest concerns about security in the cloud

Overall, many organisations can see the business benefits of cloud-based security systems. When asked which business goals they looked to achieve from the cloud, 52% stated the ability to manage security from any location at any time, while 44% cited the benefits of being able to manage IT infrastructure costs more effectively.

However, at the same time as seeing the benefits, many organisations are fully aware of the potential risks of managing security in the cloud. Chief among these is the risk of a cyber security breach. This is cited as the biggest concern by over one in four respondents (28%) – slightly up from 27% in the 2021 survey.

Privacy and data protection is another concern, scoring 20%, while other factors such as loss of control (14%) and expense (9%) are much less important considerations. Interestingly, 17% of respondents didn't have any concerns about cloud-based security at all, perhaps indicating a growing confidence in the technology.



What are your biggest concerns about managing security in the cloud?

- (**28%**) Cyber security breaches
- (**20%**) Privacy and data protection
- (**14%**) Loss of direct control
- (**9%**) It's expensive
- (**5%**) Compliance uncertainty

"Managing access in the cloud offers significant security benefits.

"Automated software updates, for example, ensure that software deployed on-site is up to date. There's no need to rely on scheduling the update, as patches can happen automatically, meaning the latest, most secure software version is running.

"According to the UK Government's National Cyber Security Centre, cloud security management can also improve organisational resilience. Indeed, for anyone with concerns about cloud access management in general, it is well worth downloading their excellent (and free) report: 'Security benefits of a good cloud service.' It's packed with great advice on getting the most out of your cloud service."

Richard Sharp,
Director, Product Line Management, Digital Access Solutions, ASSA ABLOY Opening Solutions EMEIA

Cyber security and access control

Cyber security is no longer a 'nice to have'; it's a must for any organisation or individual that relies on digital systems and data. Furthermore, new products placed on the EU market must comply with a number of mandatory cyber security rules in order to retain the CE mark – to be allowed to be sold in the EU.

For this year's survey, we wanted to understand the level of awareness that security professionals currently have of several pieces of legislation.

While we are predominantly focused on physical (or electronic) security in this report, and there remains a difference in job role between the cyber and mechanical security departments, it is clear that 'gap' is getting ever-closer. It's not enough to have an efficient, convenient and secure access control system if it doesn't have the right digital (cyber) protection. If the digital part is insecure or flawed, the system is vulnerable, and the same goes for the mechanical part.

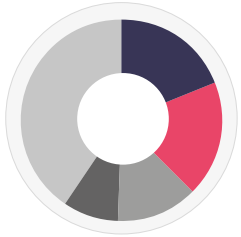
Cyber-physical attacks are on the rise, where attackers may breach a system remotely, and then exploit this vulnerability in a physical sense.[7] This may involve taking control of an autonomous vehicle, or bringing down an organisation's security system to gain physical access to a highly secure area.

It is critical, therefore, that the physical security department collaborates and communicates with its cyber and IT counterparts. Certainly, IT professionals have greater influence than ever before over purchasing decisions where equipment or devices will be connected to the corporate network – the main reason we opened the survey up to this area.

Governments and industry associations are increasingly aware of the cyber threat, too.

Concerns were highlighted in the UK Government's own Cyber Security Strategy, released in January 2022. Though the strategy noted the progress made, it admitted "there remains a significant gap between where government cyber resilience is now and where it needs to be... brought into sharp focus by the sheer volume of cyber attacks... and the evolving capabilities and techniques of the broad range of malicious actors conducting them".[8] This threat extends to the private sector – 2.7 million cyber-related frauds were found by the National Cyber Security Centre in the 12 months to March 2022 in the UK alone.[9]

Yet, despite the many policies and regulations now in place, affecting everything from smart home security devices to enterprise access control systems, awareness of them remains low among our respondents.



Are you aware of the following certifications/regulations related to cyber security?

- (**26%**) European Cybersecurity Act
- (**25%**) Network Information Security 2 (NIS2)
- (**18%**) Product Security and Telecommunications Infrastructure (PSTI) Act 2022
- (**12%**) European Cyber Resilience Act
- (**55%**) I am not aware of any of the above

[7] Verizon, Cyber physical attacks: an emerging threat, **https://www.verizon.com/business/resources/articles/s/cyber-physical-attacks-are-an-emerging-threat/**
[8] UK Cabinet Office, Government Cyber Security Strategy 2022 to 2030, **https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030**
[9] National Cyber Security Centre (NCSC), NCSC Annual Review 2022, **https://www.ncsc.gov.uk/collection/annual-review-2022**

Over half (55%) are not aware of any of them at all, while only the European Cybersecurity Act and NIS2 are familiar to more than quarter of those who answered our survey.

Worryingly, only 12% of respondents say they are fully prepared for the implications of cyber security legislation with exactly one in three (33%) saying they are not prepared at all and a further 33% investigating/exploring the implications.

However, nearly two-thirds of respondents believe that their choice of access control systems can support in compliance with cyber security legislation, either playing a 'very important role' (35%) or 'somewhat useful' role (30%).

Below we discuss some of the regulations that professionals should be aware of, or those that organisations must comply with to continue to operate and sell products in the EU.

European Cybersecurity Act

The most well-known piece of cyber security legislation in our survey, the European Cybersecurity Act (CSA) was familiar to just over a quarter (26%) of respondents.

Launched in 2019, the legislation aims to protect against cyber security threats within the EU by introducing a harmonised system for the certification of Information and Communication Technology products, services and processes.[10] Designed to replace national schemes, CSA certification has the following objectives:

- To protect data during the entire lifecycle of the ICT product, service or process
- To verify that ICT products, services and processes do not contain known vulnerabilities
- To record and make it possible to check when data, services or functions have been accessed and by whom
- To restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident
- To ensure ICT products, services and processes are secure by design and by default
- To ensure they are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities

Network Information Security 2 (NIS2)

Initially created to increase the level of protection of socially critical infrastructure within EU Member States, the NIS Directive came into force in 2018.[11] It has since been revised and replaced by Network Information Security 2, or NIS2. All EU member states are expected to comply with NIS2 by 2024.

NIS2 builds on the requirements of the original directive, aiming to protect critical infrastructure and organisations within the EU from cyber threats and achieve a high level of common security across the EU.

[10] For further information about the European Cybersecurity Act, see: **https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act**
[11] For further information about NIS2, see: **https://www.nis-2-directive.com/**

To achieve this, NIS2 requires member states to take several additional measures, including:

- Establishing an incident response plan that co-ordinates with other member states
- Establishing a national Computer Emergency Response Team
- Strengthening co-operation between public and private sector organisations
- Improving information sharing between member states

According to our survey, NIS2 is one of the better-known pieces of EU cyber security legislation with 25% of respondents familiar with the directive.

Product Security and Telecommunications Infrastructure (PSTI) Act

While IoT products offer great benefits to consumers and businesses alike, according to research only one in five manufacturers embed basic security protocols into their products. As a result, the UK government decided there was a need for much greater product security.

Passed into law in December 2022, with manufacturers being required to comply by 29 April 2024, the PSTI Act is actually two acts merged into one. One is focused on the security of products that can connect to the internet, such as network CCTV cameras and alarms, the other specifically around telecommunications infrastructure.[12]

Three key areas require compliance, based upon the EU Standard produced by the European Telecommunication Standards Institute (ETSI) – ETSI EN 303 645. These are:

1) Clear information on the support period for the product at the point of sale
2) No default passwords
3) Reporting of security issues

Awareness of the legislation among our respondents remains low overall at 18%, perhaps reflecting the fact that the law hasn't been on the statute books for very long. However, this percentage is a little higher in the country where the Act is applicable, with 25% of UK respondents who answered this question aware of the legislation.

[12] IFSEC Insider, The Product Security and Telecommunications Infrastructure (PSTI) Act 2022 – What does it cover? **https://www.ifsecglobal.com/cyber-security/product-security-and-telecommunications-infrastructure-psti-act-2022-what-does-it-cover/**

European Cyber Resilience Act

The least well-known piece of cyber security legislation in our survey with only 12% awareness among respondents, the European Cyber Resilience Act (CRA) aims to bolster cyber security rules to ensure more secure hardware and software products. The first working draft was announced in September 2022.[13]

Purposefully aligned with the PSTI Act in the UK, the European Cyber Resilience Act (CRA) has two main functions:

1. Ensure that products with digital elements are placed on the EU market without known vulnerabilities and that manufacturers take security seriously throughout a product's life cycle

2. Create conditions allowing users to take cyber security into account when selecting and using products with digital elements.

"ASSA ABLOY helps billions of people to experience a more open world with innovative solutions that enable safe, secure and convenient access to physical and digital places. As part of our role in supporting our customers, we welcome the European Commission's approach to improving the security of not only companies and their resilience against cybercrime, but also the security of digital connected products that are placed on the EU market. As Europe moves towards an increasingly cyber-based environment, we believe that ensuring connected devices operate in a safe and secure way is essential for users.

"At ASSA ABLOY, we prioritise security, whether it's mechanical or digital. We understand that security is what sets us apart and enables millions of users to trust our business."

Kelly Gill,
CTO, ASSA ABLOY Opening Solutions EMEIA

[13] For further information about the European Cyber Resilience Act, see: **https://www.european-cyber-resilience-act.com/**

Wireless access control – Supporting a more sustainable future?

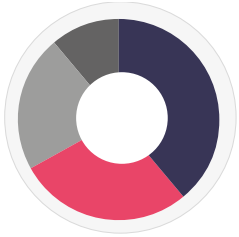
Sustainability is becoming increasingly important to organisations. It is a business imperative that can help them save money, reduce risk, and even improve their reputation.

According to McKinsey, more than 90% of S&P 500 companies in the US now publish ESG (Environmental, Social and Governance) reports in some form, while the Securities and Exchange Commission (SEC) in the US is considering new rules that would require more detailed disclosure of climate-related risks and greenhouse-gas emissions.[14]

The UN Environment programme estimates that buildings use about 40% of global energy, 25% of global water, 40% of global resources and are responsible for one third of greenhouse-gas emissions.[15]

In 2017 the Harvard Business Review declared energy efficiency one of the 'key levers for business success.' It has also become an important criterion for environmental certification schemes such as LEED and BREEAM.

As a major part of a building's infrastructure, the access control solution is often regarded as the 'key' to unlocking more sustainable practices when in use.



How much will your choice of access control technology be affected by sustainability concerns?

- (**39%**) To a great extent
- (**28%**) To some degree
- (**22%**) The most important factor
- (**11%**) Not at all

"In Europe, sustainability becomes a license to operate for all companies no matter their size. First, the European Commission recently published requirements about the corporate sustainability due diligence duties that will apply to EU and non–EU companies that have a substantial size where they have to constantly prove that business strategies are compatible with limiting global warming to 1.5°C in line with the Paris Agreement.

"Second, product regulations like the Construction Products Regulation are currently being revised to integrate as part of the mandatory CE marking process environmental sustainability performance.

"At ASSA ABLOY, we are committed to science–based targets with ambitious targets reducing our Scope 1,2 and 3 emissions. We are also preparing to ensure that our processes and all the necessary elements are in place to comply with the upcoming regulatory sustainability requirements."

Olympia Dolla,
Sustainability Program Manager, ASSA ABLOY Opening Solutions EMEIA

[14] McKinsey, Does ESG really matter? And why? **https://www.mckinsey.com/capabilities/sustainability/our-insights/does-esg-really-matter-and-why**
[15] UN Environment Programme, : **https://www.unep.org/news-and-stories/press-release/co2-emissions-buildings-and-construction-hit-new-high-leaving-sector**

Growing environmental interest

Against this backdrop it is perhaps no surprise that we are seeing a shift towards smarter and greener buildings that can help save organisations money and potentially help the planet too. But how can the choice of access control technology genuinely contribute? Do security professionals even think that it can influence organisational sustainability goals?

This year's Wireless Access Control Report certainly reflects the growing importance of sustainability to organisations with nearly two in five (39%) respondents saying their choice of access control technology will be affected by sustainability concerns 'to a great extent'. That's up from 36% in our 2021 survey.

Furthermore, over one in five (22%) state that it is 'the most important factor' when choosing the technology. Only 11% say that sustainability isn't a consideration at all when choosing access control technology.

How can access control tech contribute to sustainability goals?

Asked how access control products should best contribute to meeting sustainability goals, over half of respondents (54%) suggest the use of wireless systems that reduce the need for cabling, while 44% cite the importance of reduced maintenance – up from 40% in our 2021 survey.

Generally, wireless access control systems are more energy efficient than their wired counterparts because they use less power and require less maintenance as

there are fewer parts to install and service. This in turn means fewer journeys made to the business premises by external contractors and technicians.

However, reduced cabling and maintenance aren't the only ways that respondents think access control products can help contribute to sustainability goals. Just over one in three (34%) believe systems should be self-powered (i.e. no batteries at all), while 37% think products should be made with a large proportion of recyclable components and parts.

Having less packaging or easily recyclable packaging was cited as an important factor by 25% of respondents. Meanwhile 20% believed deploying access control systems with sustainability certification, including EPDs or Green building specifications (BREEAM, LEED), could help ensure their organisations met sustainability goals.

In addition to packaging, there are also material savings associated to these systems. If an organisation uses a mobile phone to access a building instead of physical keys, this will also save waste when these products reach their end of life.

Only 8% of respondents thought access control didn't have any part to play in their organisation's sustainability plans, reflecting a growing interest among organisations in smarter and greener buildings.

It should also be noted that access control systems are often the key to a more integrated and efficient building – as explored earlier. Considering that energy efficiency is of particular importance across Europe, automated wireless access control systems can significantly contribute to more energy efficient buildings.

Part of this process may involve integrating access control into a BMS platform, allowing for sustainability objectives to be achieved. For instance, power outlets, lighting or HVAC systems may only be switched on once a desk, room, or specific part of the building has identified that it's required to do so due to an individual using the access control system to enter.

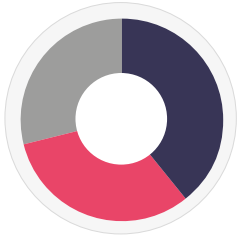
"Considering that energy efficiency is of particular importance across Europe, automated wireless access control systems can significantly contribute to more energy efficient buildings."

Influencers and decision makers for access control systems

Research shows that having influence over the security budget is key to providing effective security solutions.

A November 2022 report from the Security Research initiative (SRI) based on the views of in-house and contract security professionals found that over three quarters (76%) agreed that being able to influence the budget is essential for delivering good organisational security.[16]

Respondents to the SRI report stated that influence over the budget helps to give status to security in discussions with other departments and enables the allocation of resources based on relevant experience. Conversely, a lack of influence leaves security managers unable to purchase basic and essential resources, or to plan effectively, and results in security decisions potentially being made by non-security experts.



Which of these statements do you agree with?

- (**41%**) Security decisions regularly made or influenced by 'non–security' experts
- (**33%**) Security isn't considered a core business function
- (**30%**) Security budget is insufficient

Lack of budget?

Indeed, evidence from this year's Wireless Access Control survey confirms the SRI findings – indicating that security decisions are often made by those without security experience. Over two in five (41%) respondents agreed with the statement 'security decisions are regularly made or influenced by non-security experts' while one in three (33%) said that security isn't considered a core business function within their companies.

Worryingly, 30% stated that the security budget was insufficient – though this was lower than the SRI report, which found that 46% of security managers/directors thought their current budget was insufficient. However, unsurprisingly, the SRI report found that those with the highest influence over the budget were the least likely to view it as insufficient.

As Professor Martin Gill, who led the SRI research, noted at the time: "It is striking that so many security managers do not have the desired level of influence over the security budget, and that so many consider their current budget to be inadequate, especially given that having influence is widely considered to be key to delivering good security."

[16] IFSEC Insider, Latest SRI report indicates security managers "lack influence over the security budget", **https://www.ifsecglobal.com/physical-security/latest-sri-report-indicates-security-managers-lack-influence-over-the-security-budget/**; The full report is available on the Perpetuity Research website: **https://perpetuityresearch.com/3820/report-launch-security-managers-lack-influence-over-the-security-budget-and-how-to-remedy-that/**

Convincing the C–Suite

According to our survey results, 29% believe their security budget does not adequately reflect the risk the organisation faces, such as industrial espionage and increased cyber security attacks, while just over one in four state that security personnel have a lack of direct influence over the security budget.

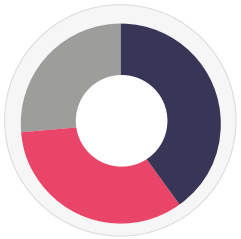
Lack of budget may also be a key reason why nearly 19% of respondents who took part in the report state that the security department feels understaffed and undertrained.

However, a lack of budget and influence isn't the only problem faced by security professionals, it seems. Many respondents also believe that the C-Suite may not understand the risks the organisation faces, perhaps reflecting a concern echoed by many that they don't see it as a core business function.

According to the SRI report, the chances of being allocated an appropriate budget was improved if the security function was seen as core to business (86% agreed), an organisation understands its security threats and risks (85% agreed) and if the security team has a high status (83% agreed).

Increasing security influence

But how can security professionals themselves best influence their organisation's security budget? According to this year's Wireless Access Control report, just over half (52%) cite the need to 'highlight the dangers/risks in not meeting security objectives' while nearly 44% believe that data generated by security systems should be improved to ensure arguments are evidence based.



What solutions are likely to solve the problem of lack of influence/budget?

- (**52%**) Better highlight dangers of not meeting security objectives
- (**44%**) Improve the use of data generated by security systems
- (**34%**) Link physical security budget to cyber/IT budget

Indeed, data gathered from security systems can be used in many other areas of the business, such as managing the hybrid working patterns of the staff and improving energy efficiency by only heating and/or lighting areas of the building which are occupied. Our survey found that 28% of respondents believed that a key to gaining influence was to relate security spend to providing data and improvements to other departments.

Also, one in three believe that the physical security budget should be linked to the cyber/IT budgets, perhaps reflecting a growing concern among the C-Suite about the potential for damage caused by a cyber-attack.

In summary, while 18% of respondents to our survey believe that the security department has sufficient influence and budget to manage the risks that an organisation faces, it's clear the vast majority think there is still much work to do.

"Data gathered from security systems can be used in many other areas of the business, such as managing the hybrid working patterns of the staff and improving energy efficiency by only heating and/or lighting areas of the building which are occupied."

About the respondents

The findings of this report are based on the views of over 400 security, facilities management and IT professionals who responded to a survey which ran through February and March 2023.

The survey was open to a range of roles in security, as well as those who manage, or are responsible for managing, buildings and facilities where they have influence in the use or specification of physical access control systems.

Anyone who selected 'not in the security/facilities profession' as a job role was automatically disqualified from the survey and has therefore not been included in these results. We also filtered those considered 'end-users' into a separate section of the survey initially, for questions directed specifically at their roles. When using the term 'end-users', we are referring to in-house security, IT and facilities professionals, such as managers, directors, or operators/administrators of physical access control systems.

Summary of respondents

The responses are from a wide geographical range. A significant number come from the United Kingdom (35%), while for the first time we had the survey translated to French, enabling us to widen the audience – 14% of the total responses came from France.

Meanwhile, another 19% of respondents were from elsewhere in Europe, 6% from the Middle East, as well as 4% each from the US and India.

Job roles varied, though we can broadly split respondents into four categories, with the remainder answering 'other': 42% were end-users, 18% integrators and installers, 18% manufacturers, vendors, or distributors, and 12% security consultants.

Breaking down the end-user audience a little more, the majority were either security/facilities managers, or security directors/executives; 32% were from small organisations of fewer than 50 employees and another 20% from those with 51-250 employees. Just over a quarter (16%) worked in businesses with 251-1,000 colleagues, and the remaining 32% were from larger organisations with over 1,000 employees.

End-users also represented a wide breadth of sectors. The most well represented included government or the public sector (16%), education (9%), manufacturing/ engineering (9%), property management or residential management (9%), commercial (8%) and finance, banking or insurance (6%). Others included healthcare, entertainment, transport, critical national infrastructure, retail, hospitality, data centre management and distribution or logistics.

Organisations who already trust wireless access control

Project: Clockwise
Type: Office/ Corporate
Location: UK

Clockwise is a UK and European provider of workspaces, with offices, meeting rooms and shared workspaces in multiple cities, accessed by a variety of membership packages. The flexibility of Incedo allowed them to select the ideal electronic lock for each specific opening plus a choice of physical and mobile credentials and easily manage them via a cloud system.

Project: Becorp
Type: Multi–residential
Location: Spain

With over 1,000 individual homes at their new build-to-rent development, Becorp knew mechanical security would create a huge workload. Mobile key technology was a more efficient and attractive solution. Residents use secure mobile keys in a smartphone app instead of a physical credential. SMARTair Openow™ app-based credential management keeps managers in control: Virtual keys can be created and sent from anywhere, with no metal keys to handle.

Project: City of Quimper
Type: Education
Location: France

The city of Quimper in Brittany, north-west France, has a diverse set of doors to secure — at multiple municipal sites including schools. City officials sought a safer solution to integrate with their public safety "Vigipirate" plan. With the installation of eCLIQ cylinders at multiple municipal locations around Quimper, users benefit from carrying all their access rights on a single eCLIQ key. No one wastes time looking for the right key, nor do they have to hold bulky, inconvenient key bunches.

Project: A Place To
Type: Multi–residential
Location: Denmark

Esbjerg's new "A Place To" housing complex focuses on sustainability and aims to maintain a green profile throughout the life-cycle of their buildings. For efficient access control, they looked for an energy-saving solution which would operate without batteries or wires. They chose PULSE key-operated electronic cylinders with energy-harvesting technology to. secure more than 300 apartments.

Project: CHM Savoie
Type: Healthcare/ Hospital
Location: France

To meet their security challenges, the hospital's managers selected Aperio locking technology integrated online with an ARD access management system. Because Aperio locks are wireless, the hospital has introduced many more layers of security and secure doors without incurring excessive Installation or operating costs, including for sensitive offices and drug stores where real-time control is needed.