The 2024 State of Physical Access Trend Report

Brought to you by IFSEC Insider & HID

IFSEC INSIDER | HID

Introduction

It has been nearly two years since our last State of Physical Access Control Report and much in the world has changed since then. Not least the aftermath of a global pandemic which has, for many of us, transformed the way we live and work forever.

What's clear beyond a doubt is that the days of everyone working in the office 9am-5pm, five days a week are over.

Broadband internet and the proliferation of smart devices have been steadily paving the way for a more flexible work environment. The convenience of cloud-based solutions for document storage and access, as well as instant messaging and video conferencing platforms, were already reshaping the traditional work configuration. However, Covid-19 has simply accelerated the pace of change.

Before 2020, around 1 in 8 of working adults reported working from home at some point during the week. In the most recent survey carried out between November 2023 and January 2024, 44% of workers reported working outside the office, comprising 28% who were hybrid workers (in the office and at home) and 16% reporting working from home only.[1]

Inevitably, this shift towards flexible/hybrid working patterns is presenting massive challenges for the physical access control industry, reflected in the responses to our 2024 State of Physical Access Control Report. However, it is also creating huge opportunities too.

According to Omdia's latest research data, the global electronic physical access control equipment market was estimated to be worth $6.7 bn in 2022 and is forecast to grow at a CAGR of 7.5% to $9.6bn by 2027.[2]

Indeed, what we are seeing is a transition within the industry, from simply controlling who enters and leaves the building using physical cards to providing data that can help businesses work more efficiently using newer forms of technology, such as biometrics and mobile phones.

At the heart of this is transition is convenience – a key concern of most of our respondents who want to be able to improve how their systems work for users without compromising on security, whether physical or digital.

In the pages that follow, we aim to gauge the current state of the physical access control report with in-depth analysis of a wide range of topics covered in our global survey. Topics such as who within organization is making the decisions on upgrading the access control systems, what are the most important features of a new system and which are the key trends shaping the industry in the near future.

We would like to extend our thanks to all those who provided us with the responses required to put this report together. Your insight remains invaluable for IFSEC Insider to continue to produce material which we hope is of benefit and interest to the entire industry supply chain. We would also like to thank our sponsors HID for their help compiling the data for this report as well as their industry insight.

Report written by Chris Price, Associate Editor, IFSEC Insider

[1] Characteristics of home workers, Great Britain: September 2022 to January 2023, https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/characteristicsofhomeworkersgreatbritain/september2022tojanuary2023

[2] The central role of access control to the transition to smart buildings, https://www.ifsecglobal.com/access-control/the-central-role-of-access-control-to-the-transition-to-smart-buildings.

About HID

HID powers the trusted identities of the world's people, places and things.

Everyday millions of people use its products and services to securely access physical and digital places. HID's technology is used to open doors, enter countries, access digital networks, verify transactions and track assets - all possible using easy-to-manage solutions such as smart cards, mobile IDs, passports as well as fingerprint readers and facial recognition.

HID's technology aids businesses in securely identifying, verifying, and tracking billions of items globally.

Along with its partners, HID is pioneering in the hardware, software and services that allow people to navigate the physical and digital worlds with confidence.

The company works with governments, universities, hospitals, financial institutions and some of the most innovative companies on the planet - helping them to create trusting and trusted physical and digital environments so that they and the people who use them can fulfil their potential.

Founded in 1991, HID is headquartered in Austin, Texas. It has over 4,500 employees worldwide and operates international offices supporting more than 100 countries. HID is an independent brand within the ASSA ABLOY Group. For more information, visit **www.hidglobal.com**.

About the respondents

This year's State of Physical Access Control Report was conducted between November 2023 and January 2024. Promoted by both HID and IFSEC Insider, the survey was distributed via email, publication partners, social media and internal teams.

Designed as a global report, it was translated into French, Spanish and Mandarin. A total of 1,223 responses were received with answers to 32 questions, although not all respondents replied to all of the questions. For several questions there were also multiple answers to choose from, meaning that some responses totaled over 100%.

In terms of geographical breakdown, the largest percentage came from English-speaking countries. Just over 2 in 5 (41%) of respondents were from the UK ahead of the United States (7%) Canada (2%) and Australia (1%).

However, global representation particularly across the Middle East and Africa regions was also strong with 5% of responses coming from Nigeria, 3% from South Africa, 2% from Saudi Arabia and 1% from Egypt. In Asia, India accounted for the largest percentage of responses (6%) while Pakistan and China were responsible for a little over 1% each.

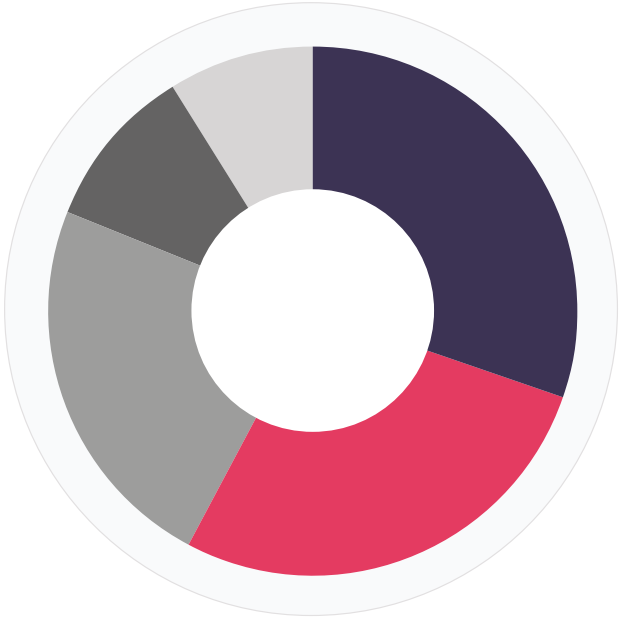
Inevitably the roles of the respondents varied considerably, perhaps reflecting the complexities involved in the decision-making process when it comes to installing physical security systems and devices.

HID

Over 1 in 5 (21%) of those who responded said they were security managers/directors, just ahead of security installers/engineers/technicians and integrators on 19% and security consultants/designers on 16%. However, there was strong representation from other sectors of the security industry too including 6% with executive C-Suite roles such as CISO and CTO and 7% who described themselves as facility managers/directors.

Equally diverse were the industry verticals which the respondents to our 2024 State of the Physical Access Control Report worked in. While Manufacturing and Industrial was the biggest sector on 16%, Professional Services and Government/Public Sector were both well represented on 10% each. Other sectors widely represented included Software, Technology and Communications (8%), Healthcare (6%), Retail (5%) and Banking (5%).

Regarding the size of companies, nearly one third (32%) of respondents worked in smaller organizations employing less than 100 workers with a further 29% employed by companies with between 100 and 999 members of staff (29%). However, nearly 4 in 10 (38%) answered that their organizations had over 1000 employees, almost the same percentage as in the last Physical Access Control Report of 2022 (39%).



Primary job roles

- (**21%**) Security End-users
- (**19%**) Security Installers, Integrators & Engineers
- (**16%**) Security Consultants/Designers
- (**7%**) Heads/Directors of FM/Property
- (**6%**) C-Suite (CISO, CT)

1,223

total contributors to the survey

The current state of physical access control technology

Traditional credentials still in use

To understand the current state of the physical access control market, we asked respondents which credential technologies they currently support for access control. What's clear from the replies is that although we are seeing a gradual shift towards mobile, traditional credentials remain widespread throughout the industry.

For example, one in three (33%) companies still support 125-KHz low-frequency proximity cards with 28% stating they still have systems in place which are compatible with traditional magnetic stripe technology (although this is down on the 2022 Physical Access Control Report which showed 35% support).

Furthermore, technologies such as first-generation MIFARE Classic and HID iCLASS® are still being supported by 19% and 15% of organizations respectively (compared with 18% and 26% in our 2022 survey.)

This is despite the fact that these much older systems represent a much greater security risk than more recent credentials. Not only are hackers able to clone older, unencrypted technologies more easily, but legacy systems are also overlooked when it comes to the latest security updates.

QR codes which rose to prominence with the public during the Covid-19 pandemic as a way of issuing credentials to visitors without the need for a physical touchpoint to check in are supported by 28% respondents – the same as in our previous survey. Other newer credentials include MIFARE DESFire EV1/ EV2/EV3 which is supported by 16% of organizations.

Seos® – a highly secure access control technology from HID that uses mutual authentication and cryptography – is supported by 18% of respondents, either in card form or mobile. That's up from 10% in our previous Physical Access Control Trends Report. Other mobile credentials are also supported by 15% of organizations.

Sanjit Bardhan
Vice President and Head of Mobile at HID

Physical ID still widespread – but mobile gaining ground

From QR codes to automatic number plate recognition systems and from biometrics to location tracking, there certainly isn't any shortage of modern technologies available for organizations wanting to identify individuals.

And while it's clear that companies have multiple access control solutions in place, our survey shows that physical ID badges remain widespread across the board. In fact, they are still actively in use within 63% of organizations.

Nor is the physical ID badge the only technologies being relied upon. Time and attendance systems, where employees check in and out for payroll and other administration functions, remain popular - in active use at 60% organizations. Equally widespread are parking/gate control systems (also 60%) for monitoring drivers entering and leaving a building's car park.

Unsurprisingly, given the shift towards hybrid working patterns, two thirds of organizations (66%) are now actively using logical access (secure computer/network log in for access to cloud and web resources). This is up from 55% in our previous Physical Access Control Trends Survey. Other established technologies currently deployed and being actively used in the market include secure print management and security guard tour applications, both on 43%.

However, while there is no doubt that physical ID badges remain extremely popular, we are inevitably seeing a shift towards newer identification technologies. For example, 39% of companies now actively use mobile identities (up from 32% in our previous 2022 report) and the same number also use biometric technology, whether that's fingerprint, facial or iris recognition for access control (up from 30% in our previous report).

Furthermore, our survey showed that just under 1 in 3 (31%) of organizations are actively using biometrics for two-factor authentication – in other words as an additional layer of security.

Explains Sanjit Bardhan, HID's Vice President and Head of Mobile:

"Typically, most people in offices now use a smartphone and for them it's very natural to use it for access control instead of physical cards because there are less things for them to carry. It's strange for people to use a mobile phone for everything else in a building and yet to have to use a physical card for access control."

According to Mr. Bardhan, using mobile credentials enables organizations, across most vertical businesses, to offer additional functionality to users. He adds: "Increasingly we are seeing companies combining physical access control with a more 'digital experience' via mobile. With exponentially proliferating use-cases, which Mr. Bardhan terms as "use-case explosion", mobile credentials fulfill such needs seamlessly and with significantly improved user-experience. For example, with an app, users can book meeting rooms or pay for food from the canteen." Further, mobile access is now being used by organizations to achieve far better business outcomes due to various use-cases and services being addressed via a single platform and device. For example, in Commercial Real Estate, real-estate companies are able to differentiate themselves from competitors and charge more rent too due to these value added services.

Regarding cost, there is, explains Mr Bardhan, very little difference between using physical ID cards and mobile access, except that mobile access has the capability of providing a lot more value for a similar costs. "All of the readers we have sold for the last five to seven years support mobile access and can be configured for the specific mobile customer key. For installers there is no additional work." (For more information, see Technology and Trends section: **Mobile access and digital ID set to become ubiquitous.**)

Asked if they've installed, upgraded or advised on projects which have involved mobile access control solutions in the past 12 months, 65% of respondents to our survey said that they had.

Meeting organizational security needs

What's clear is that levels of satisfaction with physical access control systems (PACS) have risen slightly of late. In 2022, 12% of respondents claimed that their current PACS system did not meet organizational requirements. Two years later and this has fallen to 8%, to the same level that was reported in 2020.

This may indicate that 2022 was an exception, perhaps as a result of Covid-related supply chain issues causing delays in upgrading systems. A higher percentage of respondents also state their system meets all current requirements (38% compared to 33% in 2022) while 7% believe it exceeds current requirements (3% in 2022).

Regarding the age of systems, our report shows that most organizations have relatively new access control technology, with an even split between systems under three years old and between three to six years (31% each). Legacy systems older than six years – which may represent a much higher security risk – account for a much smaller proportion of the market (19%) although 16% respondents were not sure how old their systems were so the real figure could well be higher.

Inevitably software tends to be much newer (42% under 3 years) compared to other system components (readers, credentials and controllers) with only 14% stating that their access control software was over 6 years old. This may potentially be driven by demand for Access Control as a Service (ACaaS) solutions.

In terms of planned upgrades, more than half of organizations plan to upgrade at least some of their components within the next six years: 54% state they are planning to upgrade their software, 53% their readers and credentials and 50% their controllers.

"We believe in creating products for the long–term with adaptability in mind. And while predicting the future perfectly is impossible, there are ways to prepare by prioritizing continuous innovation and offering clear upgrade and migration paths to emerging technologies. Your access control investment should be a secure one, allowing you to seamlessly integrate new advancements like identity positioning and biometrics to stay ahead of the security curve for years to come."

Cristian Cotiga, Vice President of Product Management, HID.

Improving user convenience

When it comes to installing physical access control systems, it seems that ease of use is the number one priority. Asked to name the three biggest challenges they face on a day-to-day basis, the largest number of those surveyed responded 'improving user convenience' (47%), followed by 'making physical access administration easier' (41%).

Not surprisingly, given ongoing cybersecurity concerns, 'protecting against the threat of security vulnerabilities' remains a top priority too, though down slightly from 40% in our last survey to 38% in this one, while 'complying with new regulations' remained the same as the 2022 survey on 26%.

Being able to issue and revoke ID credentials efficiently – arguably an issue that straddles both security and convenience factors – was cited by 27% of respondents (down from 37% in our 2022 survey) while other top challenges faced by those surveyed included 'managing an existing system near the end of useful life' (23%) and 'knowing the number and locations of employees and visitors' (25%).

Clearly there is also a demand for more integrated systems with the move away from proprietary technology to open platforms, such as Open Supervised Device Protocol (OSDP). Not only does this standard provide much improved operability among access control products, it is also much more secure because OSDP with Secure Channel Protocol supports AES-128 encryption and monitors wiring constantly to protect against tampering.[3]

Over a quarter of respondents (28%) cited 'integrating with other enterprise systems' in their list of top three day-to-day challenges. Perhaps not surprisingly, because as noted in a 2021 eBook for IFSEC Insider, 'physical access control is often the trigger for a transition for connected buildings, and systems integrators and

[3] Turning the spotlight on OSDP, HID Global, https://blog.hidglobal.com/2021/08/turning-spotlight-osdp-open-supervised-device-protocol

vendors are likely to bear the brunt of questions related to open-source technology and native integration.[4]

Knowing who is on the premises

As mentioned above, knowing the number and location of employees and visitors in a building is a major challenge for the security industry – one that is unlikely to have diminished with the rise of hybrid working.

By analyzing occupancy data, companies can identify underutilized areas and make informed decisions as to how to optimize their workplace design as well as improve efficiency (such as reducing heating and lighting in unoccupied areas). Ultimately, they can also use this data to determine which buildings to keep and which should be sold or perhaps sub-leased to other companies. Explains Katarina Björk, Director of Location Services at HID:

"The future of work is hybrid, which brought a new set of challenges for security and space management. Mobile access solutions are key to unlocking that full potential, as they empower businesses to understand how their space is being used, helping them create more efficient and sustainable workplaces."

In our survey, a quarter of respondents cited knowing who is in the building and where they are as one of their top three challenges, over two in five (41%) state they do 'know both the number and location of employees and visitors' while one third (33%) 'know the number of employees and visitors but not their location.' Importantly, all of this data is anonymized and cannot be linked to an individual.

While various methods are used to gather this information, access control systems/badge scanning are the main method, adopted by 48% of organizations. Other methods used to monitor who is on the premises include Time and Attendance Systems (29%), Electronic Rosters (18%) and even Paper Rosters (17%). Less widespread are location tracking systems (14%) and text messaging or mobile phone tracking systems (7%).

Challenges and requirements of upgrading

Not so long ago, the decision-making for an access control system so integral to the security of a facility would most likely have been entirely the responsibility of the security department. However, as the industry moves away from being a standalone technology, the access control system is – much like video surveillance[5] – doing far more than simply providing a barrier to unauthorized individuals.

Instead, as the technology and the software has evolved, access control is – as we have already touched upon

[4] IFSEC Global, Trends, opportunities and challenges in Physical Access Control, **https://informamarkets.turtl.co/story/ifsec-trends-opportunities-physical-access-control/**

[5] IFSEC Insider, The Video Surveillance Report 2023, **https://www.ifsecglobal.com/downloads-resources/the-video-surveillance-report-2023/**

– become more integrated with other areas within an organization including HR, facilities, IT and HVAC (Heating Ventilation Air Conditioning). And inevitably as this shift take place, it has affected the procurement and decision-making process on upgrades to the credentials, hardware components or software being used for access control.

What is clear from the results of our survey is that installers, integrators, consultants and vendors who are dealing directly with the end user increasingly have to balance multiple demands and influences from several departments when upgrading systems.

And although final authority is still most likely to rest with C-Suite executives such as the CISO, CIO and CTO or perhaps even the physical security department, many other departments exert some degree of influence in the decision-making process including Sustainability (38%), Facilities (31%), Procurement (28%) and IT (21%).

Asked to name the three biggest challenges... those surveyed responded 'improving user convenience' (47%), 'making physical access administration easier' and 'protecting against the threat of security vulnerabilities'

Indeed, as our survey shows, we are seeing a growing need for physical security and cyber/IT security departments to work together. Nearly half (48%) of all respondents said that the IT department is 'fully consulted' when it comes to upgrading physical access control systems, despite its overall influence not being as important as other departments.

Furthermore, later in the survey when asked 'which of the following departments regularly have authority or influence in deciding an upgrade', 53% stated the IT department – behind the physical security department (71%), but ahead of facilities (50%), information security (35%), procurement (27%) and C-Suite (24%).

Says Martin Huddart, Senior Vice President and Head of Physical Access Control Solutions, HID:

"To better serve our customers, we heavily invest in cybersecurity, fortifying our core technologies with independent security assessments. Also, to improve our customers' access control administration and

HID

Martin Huddart
Senior Vice President and Head of Physical Access Control Solutions, HID

efficiency we have invested in a new fulfilment center in Europe ensuring short deliveries of access control cards and readers that are easy to deploy."

Asked how they currently work with an organization's IT department, 58% of respondents replied 'establishing best security practices for your facilities', closely followed by 'looking for new technologies together' (55%). Only around one quarter (24%) said there was 'little to no overlap' between the two departments.

This is, perhaps, not a surprising development given that, according to many industry commentators, organizations need to merge their physical and cyber security operations. Partly this is for very practical reasons, as Nick Ingelbrecht, a senior director analyst with Gartner's Technology and Service Provider Research organization in Australia, explains. "Physical security systems have moved from the analogue, closed circuit, siloed physical security systems to IP-based networks and IP endpoints, which means that all these endpoints need cybersecurity protection."[6]

However, it's also for strategic reasons to combat the growing threat in a world where devices are increasingly connected to one another via the Internet of Things (IoT). Says Thomas Kopecky, Co-Founder of Ontic Technologies: "It has become increasingly apparent that companies need to unify their cyber and physical security operation. As recent cyber-physical threats have shown, to dismiss one area puts the other at risk."[7]

Inevitably, as physical security systems have evolved into IP-based products many are now directly attached to the organization's IT network. Not only will IT professionals want to ensure that anything attached to their network adheres to standards such as ISO 270010 - a globally recognized standard to help organizations manage their information security - they also need to assess the risk from hackers via vulnerabilities in, say, an access control unit.

But who pays the bill for these convergence projects, integrating physical and logical access? According to our 2024 State of Physical Access Control Survey, physical security and IT share a technology budget in around 20% of organizations while in around 25% of cases it depends on which department initiated the project.

Improved convenience and ease of use

Despite these challenges, not least balancing different departmental influences and ensuring components meet strict cybersecurity standards, there is a clear demand to upgrade physical access control systems.

Our survey showed that 43% of respondents planned updates or changes to their physical access control solutions (up from 38% in our 2022 report) while 36% said it was 'still to be determined.' Only 21% said that updates and changes weren't being planned for 2024.

Who pays the bill for these convergence projects? In around 25% of cases it depends on which department initiated the project.

[6] Converging physical and cyber security, iStart Technology in Business, https://istart.com.au/news-items/converging-physical-and-cyber-security/

[7] Managing cyber-physical security threats through convergence in a hyper-connected world, https://www.ifsecglobal.com/cyber-security/managing-cyber-physical-security-threats-through-convergence-hyper-connected-world/

Getting systems 'mobile ready' is just one of the reasons to upgrade. Nearly one in three (29%) are either currently in the process of upgrading to mobile-enabled readers or have already upgraded to mobile-enabled readers, but not yet deployed mobile access credentials. A further 16% have already deployed mobile access credentials.

Clearly convenience is the main reason we are seeing this shift to mobile access control. Indeed 56% of respondents cited 'improved convenience and experience for users' as the main reason to upgrade to mobile access control, well ahead of other factors such as 'higher security' (43%), 'more efficient credential issuance and management' (32%) and even 'cost savings' (30%).

However, cost remains a considerable barrier for upgrading, cited as the biggest obstacle by 53% of respondents – up from 38% in 2022 – with a perceived lack of a compelling return on investment and having to learn a new system both on 11%. Other much smaller factors preventing upgrade projects included 'disruption to daily business' (7%) and 'compatibility, or lack of it, with existing legacy systems' (8%).

Asked what were the top three drivers are to upgrade, 'improved user convenience' was once again the top answer, chosen by over half (51%) of respondents, ahead of 'taking advantage of new technology that can improve security posture' (40%) and the 'existing system 'nearing the end of its useful life' (27%).

Unsurprisingly, given that improved user convenience is the biggest driver to upgrade, ease of use is also cited as the top feature required in a new access control system (favored by 58% of respondents). Related to improved user convenience, touchless/contactless capabilities feature highly too (45%) as does the ability for users to use smartphones, tablets and wearables for access control (43%).

Finally, ensuring the system works with both legacy and future components is also a huge consideration with the same percentage (43%) of respondents citing 'integration with existing security platforms' and 44% stating 'ability to add or support new technologies in the future' among their three features required. Meanwhile, open-standards based technologies such as OSDP which are required for interoperability, are cited by 21% of respondents.

Asked what were the top drivers to upgrade, 'improved user convenience' was once again the top answer.

Five technology trends in physical access control – looking ahead

1. Mobile access and digital ID set to become ubiquitous

While physical ID is still prevalent within the access control industry, there is no doubt that mobile access credentials and digital IDs are fast gaining ground. According to this report, nearly 2 in 5 (39%) now actively use mobile identities with respondents naming the touchless/contactless solutions (48%) and mobile access (44%) as the two largest trends shaping the wider access control industry.

Omdia estimates that nearly 50 million mobile credentials were downloaded globally in 2022 and that revenue from the sales of mobile credentials will grow at a 39.8% CAGR rate from 2022 until 2027.[8]

In the latest HID 2024 State of the Security and Identity Report[9], surveyed security professionals state that nearly 80% of organizations will deploy mobile IDs within the next five years while industry partners are even more optimistic in their outlook, stating that 94% of their customers will have deployed mobile IDs by 2029.

Nearly 50 million mobile credentials were downloaded globally in 2022.

[8] The central role of access control to the transition to smart buildings, IFSEC Insider, **https://www.ifsecglobal.com/access-control/the-central-role-of-access-control-to-the-transition-to-smart-buildings/**
[9] HID 2024 State of the Security and Identity Report
[10] HID Global, Employee Badge in Apple Wallet **https://www.hidglobal.com/solutions/employee-badge-apple-wallet**

Stephenie Haldane
Vice President, End User Business Development at HID

For physical access control, mobile credentials are not only more convenient (unquestionably the biggest driver for organizations upgrading their systems) they also enable digital IDs to be stored within a digital wallet. For example, credentials in digital wallets such as Apple Wallet or Google Wallet™ enables smartphone and smart watch users to access a building, log on to their own workstation even print documents, rather than relying on a plastic card. The same technology is also being increasingly used for student ID cards as well as for hotel guests.[11]

When or where an employee badge is used, it is never shared or stored with either Apple or Google servers, helping to ensure privacy to the end user.

Stephenie Haldane, Vice President, End User Business Development, HID:

"Generation Z and Generation Alpha are set to significantly influence the demand and adoption of digital and mobile credentials. As these tech-savvy individuals transition from university to the workforce, their expectation for convenience and seamless integration into everyday activities is already being recognized by competitive industries. These industries are making advanced access control solutions a key part of their recruitment process, highlighting the need for organizations to innovate and adapt their access control strategies to ensure both security and user satisfaction in an increasingly digital world."

[11] Apple, Access Credential Types, **https://support.apple.com/en-gb/guide/security/sec30bdef041/web**

2. Open standards driving smart buildings phenomenon

While open standards have been on the access control agenda for some time, it's only recently that we have started to see their real benefits emerge. For example, although it was first developed in 2008, OSDP only became an International Electrical Commission (IEC) Standard in 2020, since which time it has helped to drive what is fast becoming a smart buildings phenomenon.

Indeed, Fortune Business Insights[12] predicts that the global smart building market size will grow from $96.96 billion in 2023 to $408.21 billion by 2030, at a CAGR of 22.8% during the forecast period. It's a trend that seems to be reflected in our survey too, with 'smart buildings and flexible workspaces' cited by 43% as one of the top three trends shaping the wider control access control industry in the near future, only just behind implementing touchless/contactless solutions (48%) and mobile access/mobile apps (44%). Related to this, integration with other business functions such as HR, HVAC, lighting and desk booking was also listed as one of the top three trends shaping the industry by nearly one in three (32%) respondents.

It's clear that the move towards open standards has become the key driver for much more converged security solutions, where physical access control data is helping not just to decide who should be allowed into the building, but also how that building is best used. Indeed with an increase of workers[13] now identifying as hybrid workers (defined as working from home and travelling to work in the last seven days), it's become much more important than ever for businesses to use occupancy data to help shape their business strategy and optimize costs.

For example, with mobile credentials implemented for access control, it's possible to determine which parts of the building are used on which days and ensure only these areas receive heating, lighting, even power. According to our survey nearly half (48%) of organizations already have access control/badge scanning systems in place to monitor building usage throughout the day, at least to some extent.

However, while the benefits of open standards and interoperability are clear from a business point of view, this converged approach isn't without its challenges. With physical access control increasingly becoming an integral part of a smart building set-up, there are inevitably more opportunities for cyber-criminals to attack an organization's infrastructure. As a result, it's becoming clear that physical systems need to be managed in conjunction with IT. As Dark Reading's Thomas Kopecky says: "Physical security and cybersecurity are intrinsically connected, and it is no longer effective to manage these threats separately. Cyber-physical incidents can quickly lead to physical harm, destruction of property, environmental disasters, and worse."[14]

[12] Fortune Business Insights, **https://www.fortunebusinessinsights.com/industry-reports/smart-building-market-101198**
[13] Characteristics of homeworkers, Great Britain: September 2022 to January 2023, **https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/characteristicsofhomeworkersgreatbritain/september2022tojanuary2023**
[14] Dark Reading, Managing Increased Cyber–Physical Security Threats in a Hyper-Connected World, **https://www.darkreading.com/physical-security/managing-increased-cyber-physical-security-threats-in-a-hyper-connected-world**

3. Sustainability becoming greater influence on business decisions

Whereas once security professionals focused purely on risk mitigation, increasingly security teams are now operating with other considerations in mind. From this survey we can see sustainability is playing a significant role in access control with nearly two thirds (63%) of respondents citing that those with responsibility for sustainability have either some influence or are fully consulted when it comes upgrading physical access control systems.

When asked which are the top three drivers to upgrading your physical access control solution, 15% answered 'to support the company's sustainability goals' with features such as 'low energy consumption hardware' cited by 12% of respondents (slightly up from 11% in our 2022 survey). Energy saving solutions were also cited as one of the top three trends shaping the wider access control industry in the near future by 14% of respondents. Though it should be noted that other trends such as mobile/contactless access, cloud hosting and smart building technology scored more highly.

The fact that sustainability is starting to play a more important role when it comes to making business decisions certainly shouldn't come as any great surprise. In the United States, more than 90%of S&P 500 companies now publish ESG (Environmental, Social and Corporate Governance) reports in some form, as do approximately 70% of Russell 1000 companies[17], while 83% of consumers think companies should be actively shaping ESG best practices.[18]

According to HID's 2024 State of Security and Industry Report[19], end users are increasingly demanding that suppliers provide footprint transparency in terms of their operations, product sourcing and research and development practices. In fact, 87% of respondents to its survey say that sustainability ranks as "important to extremely important" to their customers, while 76% say they have seen the importance of sustainability increasing for their customers.

One area it is clear where organizations could do more to improve sustainability is when it comes to reducing plastic. And while it is possible to issue bamboo cards rather than plastic, Steven Commander, Director of Consultant Regulations and Relations at HID, argues that it is now time for organizations to move towards mobile credentials both for environmental and convenience reasons.

"While a badge offers easy visual identification, from a sustainability perspective there's an obvious reason why we should be getting rid of the badge and that's because we need to get rid of plastic," he says. "A virtual badge is less eco-toxic, generates less CO2 and helps companies achieve their environmental goals."

[17] McKinsey and Sustainability, Does ESG really matter and why? https://www.mckinsey.com/capabilities/sustainability/our-insights/does-esg-really-matter-and-why
[18] PwC, Beyond Compliance: Consumers and employees want businesses to do more on ESG https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/consumer-and-employee-esg-expectations.html
[19] HID 2024 State of Security and Industry Report https://www.alliedmarketresearch.com/facial-recognition-market

4. The rise of artificial intelligence for analytics use cases

As with other areas such as video surveillance, the use of Artificial Intelligence capabilities in physical access control is becoming more common as AI technologies and expertise are developed. Asked if they are looking to incorporate AI/machine learning into their access control solutions, 38% of respondents to our survey stated they were (although the same percentage said they were unsure of the benefits). Only 23% said they didn't have any plans to incorporate the technologies.

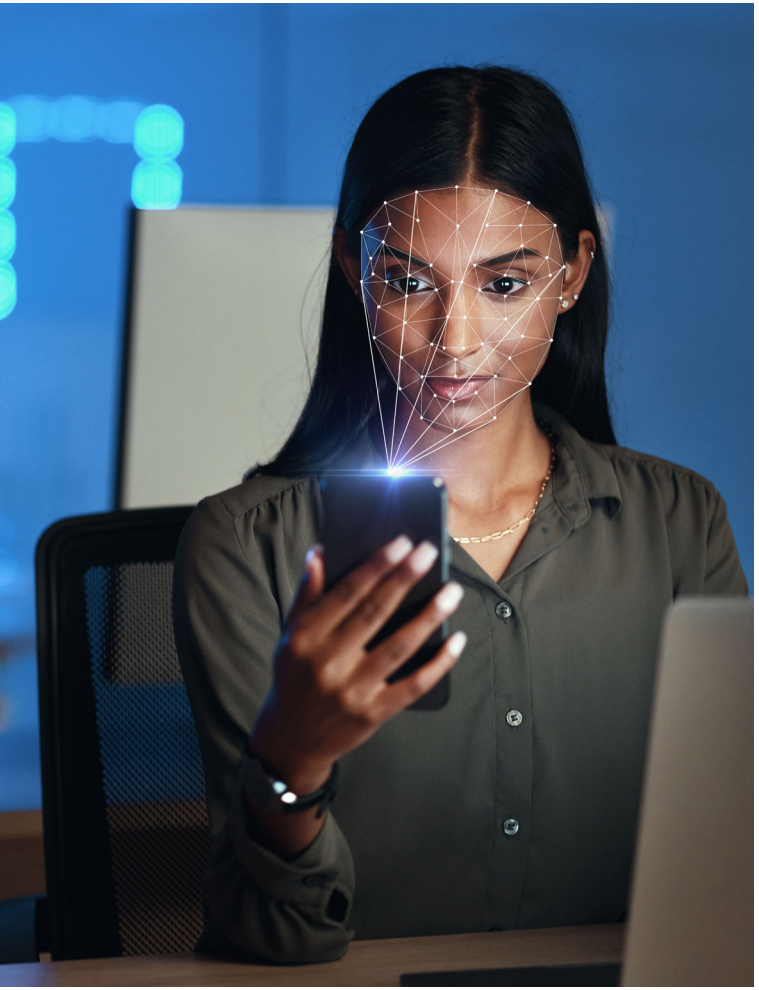
Similarly, HID State of Security and Identity Report[20], states that many security professionals see AI's analytic capabilities as the 'low-hanging fruit'. And rather than looking to AI to inform the entirety of the security system, they see analytics as a way to operationalize AI in support of immediate outcomes. In this scenario, 35% of end users reported they will be testing or implementing some AI capability in the next three to five years, with 15% already using AI-enabled biometrics.

Says Steve Belt, Vice President of Engineering, HID Physical Access Controls:

"For example, in advanced condition monitoring, AI and machine learning can be utilized to understand the behavior of an asset in its "normal" state. When this behavior changes, the system can trigger alerts, such as temperature, power, motion, etc. With AI support, the system can also perform predictive maintenance and diagnostics. Ultimately, AI capabilities enable organizations to detect threats more quickly, obtain reporting and analyze huge amounts of data faster, helping them to respond to threats in a timely manner."

Steve Belt
Vice President of Engineering for Physical Access Controls, HID

[20] 2024 HID State of Security and Identity Report **https://www.hidglobal.com/documents/industry-report-2024-state-security-and-identity**



5. Growing role of biometrics – especially contactless solutions

The biometrics market is growing at a rapid pace. By 2031 the worldwide market for biometrics is expected to reach $136.18 billion[21] while the global facial recognition market alone is predicted to grow to $16.74 billion by 2030, up from $3.83 billion in 2020. That's a CAGR of 16% from 2021 to 2030.[22]

Certainly, when it comes to access control there is strong interest in biometrics. Asked to 'name the top three trends shaping the wider access control industry in the near future' nearly one in four respondents (23%) to our 2024 Physical Access Control Survey cited biometrics.

In HID's 2023 State of Security Report[23], 26% stated they currently use biometrics (contact or contactless) while another 33% stated they plan to test or implement a form of biometrics within the next one to five years.

But which of the many biometric technologies are companies looking to implement for access control and are there any regional differences? According to HID's Cristian Cotiga, Vice President of Product Management, PACS, while fingerprint readers remain a popular choice for mature markets such as North America and Europe, "in emerging markets such as Africa, parts of Asia and Latin America – where fingerprint recognition is already widespread - many companies are now moving towards facial recognition."

Unlike traditional fingerprint scanning, the advantage of facial recognition is that it is a contactless technology (this was an especially important factor during the Covid-19 pandemic to prevent contamination). However, there are other forms of contactless biometrics which are becoming more widespread too, including palm readers and touchless fingerprint readers, as well as iris scanners.

When it comes to facial recognition, Omdia projects a growth rate of 20%[24], driven by lower pricing and falling error rates for advanced readers. Indeed, many studies, including NIST's Face Recognition Vendor Test, confirm that modern-day face recognition algorithms can achieve accuracy of around 99.97%.[25] However, only a few manufacturers today offer solutions that deliver accurate biometric recognition in less-than-ideal lighting or with non-frontal face positions.

[21] Transparency Market Research, Biometrics market size **https://www.globenewswire.com/en/news-release/2022/08/02/2490352/0/en/Biometrics-Market-Size-worth-136-18-Billion-by-2031-CAGR-13-3-Notes-TMR-Study.html** [22] Allied Market Research, Facial Recognition Market, **https://www.alliedmarketresearch.com/facial-recognition-market**
[23] The Industry Report: 2023 State of Security and Identity, **https://www.hidglobal.com/documents/industry-report-2023-state-security-and-identity**
[24] Omdia Access Control Database, **https://omdia.tech.informa.com/om032178/access-control-database--2023-analysis**
[25] NIST, Facial Recognition Technology Evaluation (FRTE), **https://pages.nist.gov/frvt/html/frvt11.html**