brivo®

2024 Top Global Security Trends

Empowering CSOs and security teams to enable technology and AI

Table of Contents

Embracing Innovation

A New Era for Security Professionals in 2024

Last year was dominated by evolving technology, from robotics to blockchain to quantum computing. Yet none were as hyped as AI. While AI and automation may not be new, they clearly now hold powerful potential for all kinds of applications, and security is undoubtedly one of them. Data analysis, facial recognition, authentication, proactive security models and more will all be enhanced by AI in the future.

The good news is that security professionals are well-positioned to adapt to these changes. The security industry is now bursting with innovation. It's far from the 'stagnant' market it used to be. Take the shift to cloud-based solutions as an example. Over the past few years the move away from on-premise physical systems in favor of integrated systems in the cloud has been significant. This is a global trend, even if the pace of change may not be universal.

There are also multiple drivers for this change. Today, customers have higher expectations of what their access control should do. Physical security requirements are more demanding. And digital transformation remains a driving force for technology modernization, despite the term seeming a little old hat by now.

As a result, our industry finds itself at a turning point and we need a fresh approach to our annual survey of security professionals for 2024. This year, we spoke to more people than ever before, taking in a wider group of respondents, from Chief Security Officers (CSOs) making the big decisions, to the Security Practitioners and Facilities Administrators implementing them. We also widened the scope of industries we surveyed, including financial services, technology & IT, retail, logistics, health & wellness and manufacturing.

TOP 3 SECURITY TRENDS

✓ Security Teams Prioritize Integration

Security teams are prioritizing integration for tech modernization

✓ High Expectations for AI

AI expectations are high, but require greater skills and data to realize the full potential

✓ Greater Need for Budget & Authority

CSOs have a seat at the table, yet change is slow due to lack of budget and authority

In a year of technological advancements, AI emerges as a frontrunner, promising transformative potential across industries, especially in security. Security professionals are ready to embrace change, leveraging trends like cloud-based solutions and rising customer expectations. Adaptation is essential as digital transformation reshapes security landscapes to meet evolving demands and expectations.

Trend 1

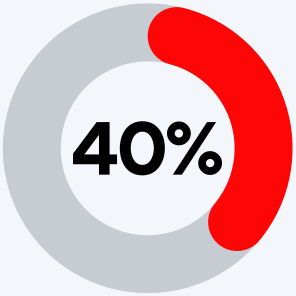
Security teams are prioritizing integration for tech modernization

How do security professionals feel about the state of their access control and physical security? Nearly two out of every five respondents do not have full confidence in their system's ability to keep their employees and facilities safe in 2024 (Figure 1) . When looking at the security professionals who are on the front lines, i.e., those who describe their role as "practitioner", this rises to almost half, 49%.

It seems there is more caution and worry outside of management teams and boardrooms. There may be several reasons contributing to this lack of confidence, ranging from disconnected systems and legacy solutions, to changing perceptions of security in the age of AI. Yet the key takeaway here has to be the large portion of practitioners that are not fully confident in their security systems.

Similarly, the need to integrate security systems with cross-functional areas was the top priority for small businesses and large enterprises. Linking physical security across other parts of the business, like the employee experience, HR software or facility management applications, is a running theme throughout this report. The good news security teams aren't complacent.

SECURITY EXPERTS CONFIDENCE IN SAFETY SYSTEMS



LACK TRUST IN THEIR SAFETY SYSTEM

FIGURE 1

Security Operations Centers -SOCs- are now a higher priority than ever before, reflecting a push for centralization in a "single pane of glass." This is not just a security trend, it's common across all of enterprise IT. For example, one recent survey found that 57% of enterprise professionals plan to implement a tool to centralize data. The same report found 64% of professionals see greater efficiencies and 75% see business growth as a result of this centralization.[1]

Security teams resolute in addressing trust issues through system integration and modernization for enhanced effectiveness

[1] CPD, Customer Data Maturity Study

2024 Top Security Tech Goals

- Integrating security systems with other cross-functional areas within organizations
- Modernizing legacy security systems
- Building a Security Operations Center (SOC)

2024 PHYSICAL SECURITY TECH GOALS SURVEY

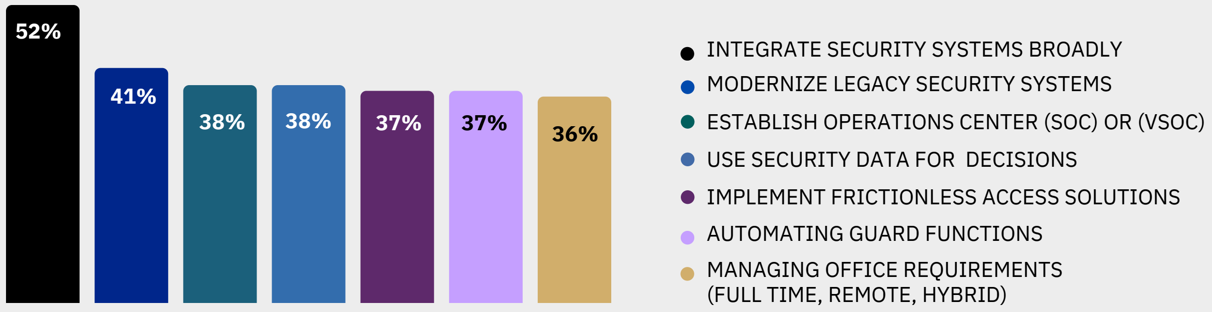


FIGURE 2

The top barriers to modernizing physical security were seen as the challenge of integrating new solutions with existing technology, a lack of alignment between security and other departments, and a lack of budget. Even with the wider scope of this year's survey, this is a consistent trend year over year.

In 2023, the major barriers to new technology adoption included budget constraints and proving return on investment. While some progress has been made, similar challenges persist. Budget constraints remain a concern, especially in economically challenged regions.

However, demonstrating ROI is no longer as problematic. Yet, resistance to new technologies has emerged as a prominent issue, possibly indicating a faster pace of industry change and technological advancement.

As businesses continue to evolve in the digital age, the ability to showcase Return on Investment (ROI) has become increasingly streamlined and accessible. However, despite these advancements, a new challenge has surfaced in the form of resistance to adopting technologies.

IDENTIFYING BARRIERS: ADOPTION OF NEW PHYSICAL SECURITY TECHNOLOGY

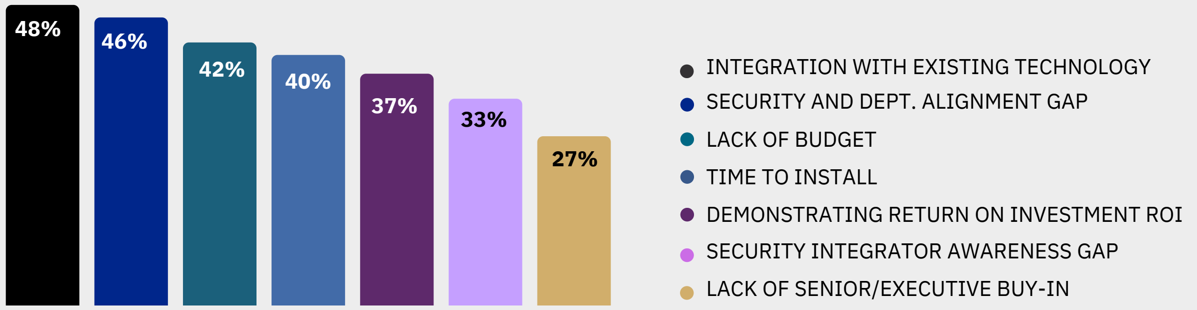


FIGURE 3

This resistance highlights an acceleration in the rate of change within industries and the rapid advancement of technology. Embracing this shift and overcoming resistance can position organizations, including security integrators, to stand out during a period of rapid change and industry noise.

Interestingly, one in three, 33%, global respondents report that their security integrator is either not aware of information related to new technology or is holding this information back (Figure 4). This issue is a barrier to adoption across regions, particularly notable in the DACH region (encompassing Germany, Austria, and Switzerland) and in BeNeLux (composed of Belgium, the Netherlands, and Luxembourg), at 36% for both regions. It is also specially high among Security Directors, 51%.

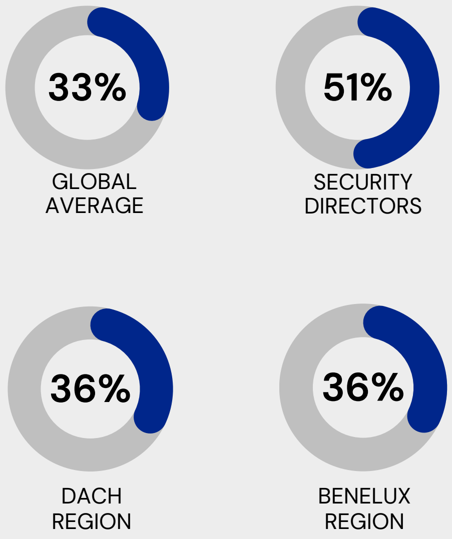
This finding may reflect a disconnect between industry leaders and third parties they should trust, which could be solved with greater communication.

Almost half, 49%, of respondents also said that experienced industry professionals are resisting change to systems they have known their whole career (Figure 5). This is understandable in any profession—why change what already works?

For the security integrator community in particular, change can be difficult when working with organizations that have always approached protection and defense in a certain way. Yet this barrier could also be an opportunity. Integrators should be seen as trusted advisors, helping customers navigate the complexities of new technology and overcome fear of change through support and education. The low confidence of some security professionals in the capabilities of current physical security systems shows just why this is so important.

New technologies can, if implemented correctly and with the right integration, give them an all-important confidence boost. Security integrators should jump on this opportunity and actively demonstrate their understanding of new technologies and their customers' needs from the get-go. Otherwise, they risk being left behind in the industry.

NEW TECHNOLOGY AWARENESS BY SECURITY INTEGRATORS



SECURITY INTEGRATORS LACK AWARENESS OF NEW TECH, ESPECIALLY AMONG DIRECTORS. IMPROVED COMMUNICATION IS CRUCIAL FOR TRUST AND TECH ADOPTION.

FIGURE 4

RESISTANCE TO CHANGE AMONG EXPERIENCED INDUSTRY PROFESSIONALS

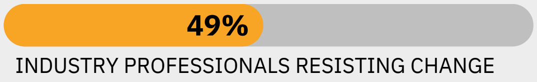
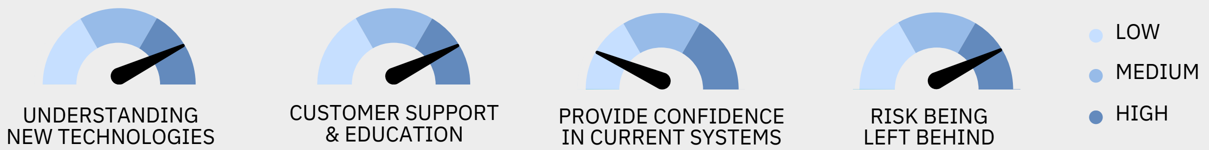


FIGURE 5

Security integrators risk being left behind in the industry without the ability to demonstrate their accute understanding of new technologies

CHARTING SUCCESS

FACTORS IMPACTING SECURITY INTEGRATORS



THIS CHART HIGHLIGHTS HOW SECURITY INTEGRATORS PLAY A CRUCIAL ROLE IN GUIDING CUSTOMERS THROUGH TECHNOLOGY ADOPTION.

FIGURE 6

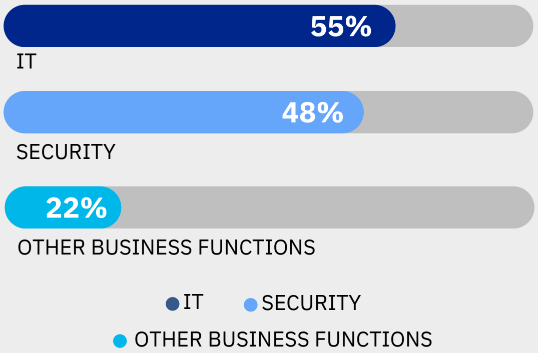
Trend 2

AI expectations are high, but require greater skills and data to realize full potential

As AI and automation continue to gain prominence in the security industry, there's an increasing demand for enhanced skills and access to comprehensive data. We sought to understand how professionals across different functions perceive the looming potential for disruption in their organizations amidst this transition towards AI and automation.

IT is the business function that most expect will be disrupted by AI and automation in the next three years. This finding is unsurprising given the potential advances of AI for general IT are well hyped. Yet security was seen as a close second 48% (Figure 7). This highlights that professionals are recognizing the significant benefits that GenAI, Machine Learning and Natural Language Processing will have in the near future for physical security use cases. Expectations are clearly high.

EXPECTED DISRUPTION BY AI & AUTOMATION

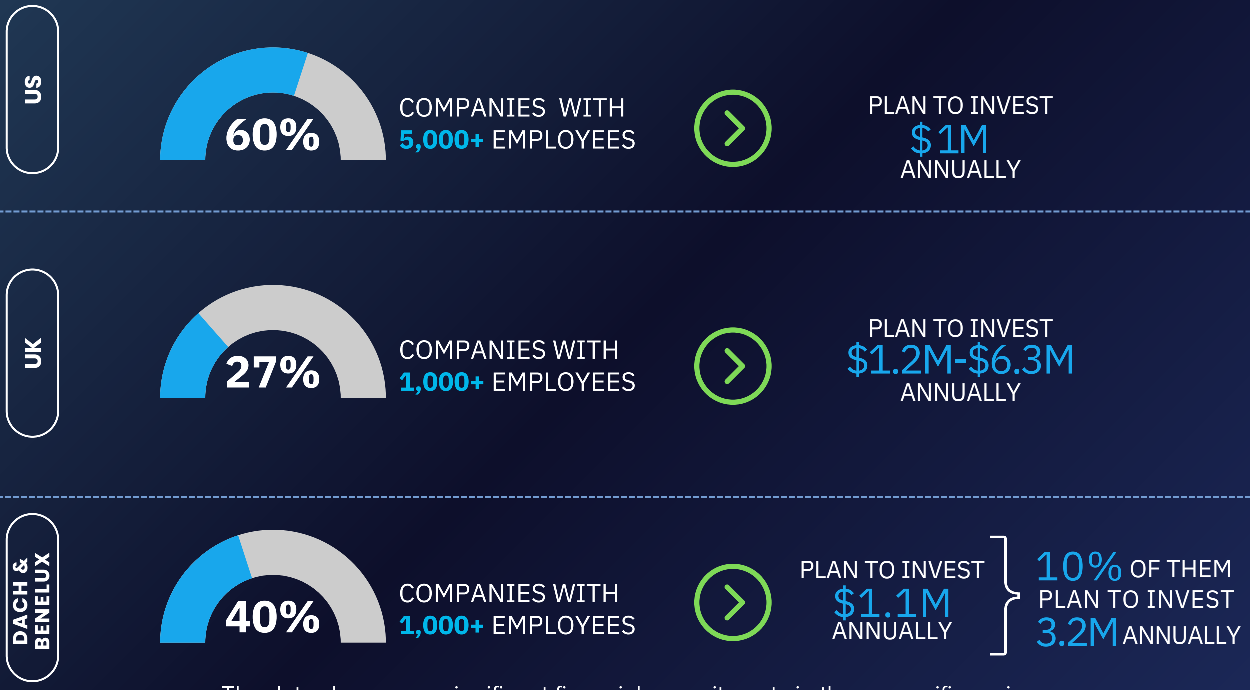


HIGH EXPECTATIONS FOR AI AND AUTOMATION DISRUPTION, LED BY IT AND SECURITY.

FIGURE 7

AI INVESTMENT PLANS BY ENTERPRISE SIZE AND REGION

Big budgets are set for AI and automation investment in next 3 years



US: 60% COMPANIES WITH 5,000+ EMPLOYEES → PLAN TO INVEST $1M ANNUALLY

UK: 27% COMPANIES WITH 1,000+ EMPLOYEES → PLAN TO INVEST $1.2M-$6.3M ANNUALLY

DACH & BENELUX: 40% COMPANIES WITH 1,000+ EMPLOYEES → PLAN TO INVEST $1.1M ANNUALLY } 10% OF THEM PLAN TO INVEST 3.2M ANNUALLY

The data showcases significant financial commitments in these specific regions.

FIGURE 8

While awareness of the AI opportunity is widespread and budget planning is underway, significant confusion persists. Only 36% of global respondents express strong confidence in their organization's ability to understand and leverage AI and automation. This confidence drops to 28% in the DACH region.

What's more, while many are predicting substantial investment to solve this issue, budget still remains a common constraint. The biggest organizational challenge for AI adoption (cited by 56% of respondents). The second highest concern was the cost to maintain AI applications, called out by just over half 52% of respondents. This report comes at a time of economic uncertainty for some regions, which may be a contributing factor. Investment into new technologies may be seen as at risk when businesses need to reduce spend and conserve cash.

Many, 45%, also perceive risks around inputting data into AI models, as well as limited AI expertise, 41%, as key challenges to adoption. These fears are to be expected with new technologies as education and legislation struggle to keep pace with innovation. Yet these gaps need to be addressed to improve security professional confidence.

Clear policy and data governance processes will help to overcome these challenges. We've already seen good progress on this front, with President Biden's AI Executive Order in the US and the EU AI Act in motion in Europe. It's now up to organizations to reflect this in their internal policy too. Upskilling may be a longer-term commitment and will require a combination of investment, strategic hiring and a culture shift driven from the boardroom down to all levels of the organization.

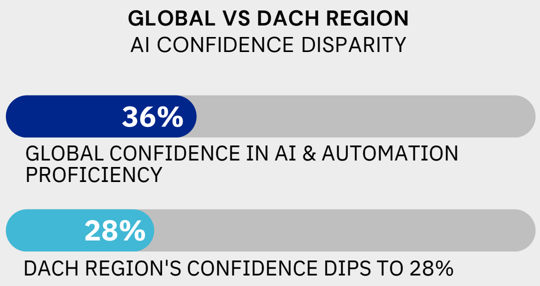


FIGURE 9

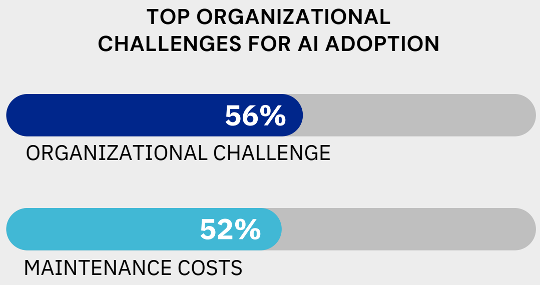


FIGURE 10

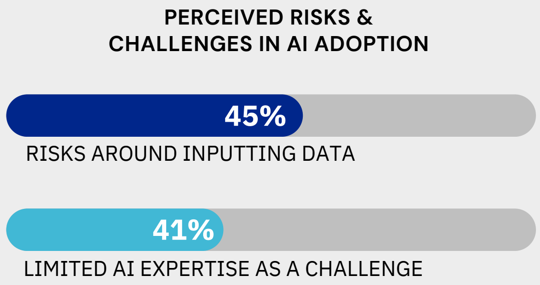


FIGURE 11

There is good news. Even with reservations about how well their organization can execute, respondents are bullish when it comes to AI's potential. They expect that a third of their organization's efficiency gains over the next three years will come from AI and automation. Accordingly, 63% also predict that AI and automation applications will only require minimal human oversight.

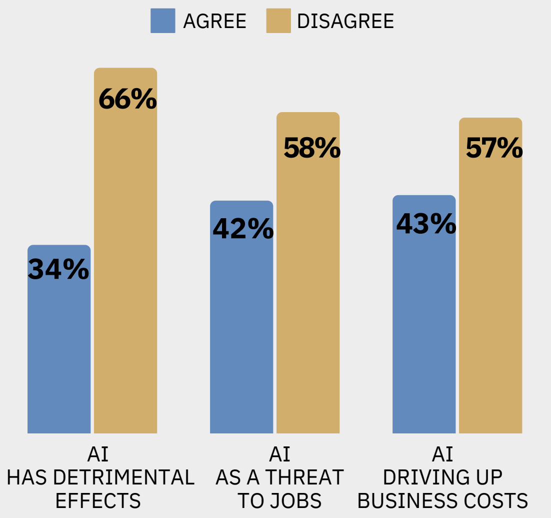
Positive expectations continue when it comes to the more common concerns around AI. Two-thirds of respondents, 66%, reject the idea that AI "hallucinations" could have detrimental effects, while more than half, 58%, do not see AI as a threat to jobs.

A similar number, 57%, disagree with the premise that AI integrations would drive up business costs.

Perhaps these security professionals see the upsides of AI as outweighing potential risk. The data also suggests that security teams don't deem common fears around job loss or hallucinations relevant to the industry. Regardless, the findings point to security professionals being hugely optimistic about the technology's potential.

For security, it's a matter of "when", rather than "if", when it comes to AI. There is clear momentum and desire for it to be a part of physical security technology. Budgets have been set aside in principle and many see clear efficiency benefits. But overcoming key challenges requires a CSO with the authority to make change.

ATTITUDES TOWARDS AI CONCERNS AMONG SECURITY PROFESSIONALS



DATA SHOWS OPTIMISM: MOST REJECT AI CONCERNS

FIGURE 11

AI in Security: A Question of 'When,' Not 'If'

AI integration is inevitable, driven by clear momentum and desire. Budgets are set for efficiency, but change needs empowered CSOs.

Trend 3

CSOs have a seat at the table, yet change is slow due to lack of budget and authority

The introduction of AI into security technology stacks require strong leadership. The CSO is best positioned to provide the oversight needed. We were keen to discover just how this role was perceived among security professionals.

Almost three quarters, 74%, of security professionals agreed that CSOs have had a more important role in recent years. This may be a result of various factors. According to advisory firm, Security Executive Council, some challenges driving the CSO role evolution include:

- COVID-19 causing the re-definition of the workplace
- The great resignation and job cuts increasing the possibility of information theft
- Nation State Attacks becoming more common as geo-political tensions increase

Security needs a dedicated role at a high level to manage the risks and potential for AI. Now that AI is accessible to anyone, there must be organizational policies to govern. CSOs will be vital in guiding teams through integrating this technology securely.

The growing importance of the CSO means they have been more engaged across business units. For example, the data shows an increased alignment between security and HR departments in decision-making. Most respondents agreed that security and HR departments are closely aligned now more than ever before.

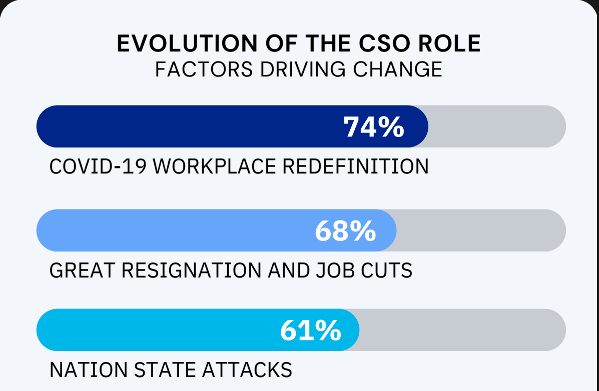


FIGURE 12

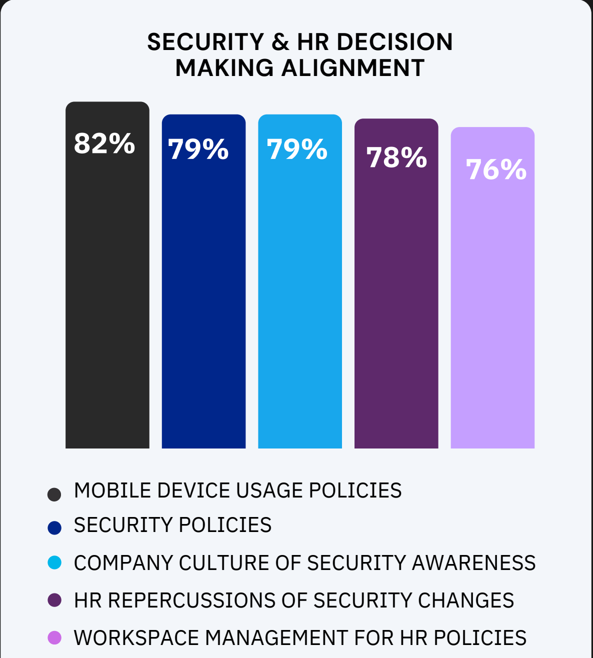


FIGURE 13

Security and HR Alignment.
Policies and Workspace Management include:

- Mobile device usage & Security policies
- HR repercussions of security decisions or system changes
- Management and utilization of the physical workspace and access control

However, if we delve deeper into the role of the CSO, we start to uncover some challenges. From a management perspective, while CSOs have elevated status in most organizations, the budget and decision making authority has not followed in. These executives are responsible for only 42% of an organization's security budget and are more likely to be part of the team making security procurement decisions, 56% agreed. Less respondents agreed that the CSO is the ultimate decision maker, 32%.

Can CSOs be truly effective if they are not fully responsible for the entirety of security budgets and decision making? The trajectory of CSOs' importance is certainly a positive one. While today they might not necessarily have the authority to have the final say, it's clear they are more part of the decision making process than pre-pandemic. Today, the data shows CSOs are more often than not utilized in other areas of the business as well as consulted on critical decisions around security policy. While the buck stops with CSOs for protecting a business, these leaders do need to work with others to drive greater security.

The issue lies in departments making siloed decisions without consulting each other. We may see alignment between HR and the CSO, yet other findings suggest a disconnect between teams. A lack of alignment between security and other departments was cited as a barrier to the adoption of new physical security technology by 46% of respondents. This survey findings highlight the need for greater collaboration. Perhaps a more empowered CSO could drive this change.

More alignment across departments will also will have other positive effects for the use of organizational data in physical security. Security professionals' use of access data today is basic but there's a strong desire to use this data for more complex purposes. It has the potential to inform decisions and drive change. These include anomalous activity detection, applying analytics to physical security policies, tracking access trends and space utilization, and more.

Where do we go from here?

We can be optimistic about the security industry's attitude towards technological modernization and appetite to explore new technologies like AI. Security professionals understand the benefits, want to make substantial investments, and demonstrate more positivity than other industries.

However, there are real concerns around the barriers to change. This includes the reality of integrating new solutions, the skills gap, and a worry that security integrators lack the ability to offer the right help. What's more, while demonstrating ROI is no longer as big a problem, general resistance to change is. This suggests that the argument for better technology has won out, but natural inertia remains.

Key Takeaways

These takeaways demonstrate that the industry is heading in the right direction. There may be some barriers to innovation, yet recognizing these issues is the first step to overcoming them. Security professionals acknowledge the obstacles they face and are on the journey to physical security modernization.

01 A Clear Need to Modernize to Improve Security

Integrated systems, tech stack modernization and a 'single pane of glass' view across solutions can provide a much needed confidence boost for security professionals professionals, especially the nearly 40% that do not have confidence in their security technology today.

02 Budget Planning for AI Benefits

Planning budgets and fully understanding efficiency gains for AI today will be crucial for security professionals to benefit from AI disruption sooner rather than later. This also includes budget for upskilling staff to tackle the needs for tomorrow.

03 Education & Policy Changes Needed to Guide Technology Adoption

When facing budget constraints and uncertainty regarding AI utilization, one must turn to educational initiatives and internal policy frameworks for guidance and support.

04 CSOs Are Poised to Lead the Change

While we're on the path to progression for the CSO, there's clearly still work to be done. Organizations need to understand the growing importance of this C-level role and invest in it appropriately.

05 Empowering CSOs

It's up to security integrators to support the CSO role and arm them with knowledge and tools to advocate for greater responsibility.

06 Security Integrators Losing Ground As Trusted Advisors

Integrators should also seize the opportunity to become trusted advisors, given a third of professionals aren't yet getting the right support from partners.

07 Security Integrators That Adapt With Technology Will Prevail

Keeping up with the pace of innovation will be the difference between success and getting left behind for integrators.

About the Survey

The survey was conducted in partnership with independent research company Coleman Parkes in October and November 2023. It gathers data from 850 security professionals across eight countries (UK, US, Germany, Austria, Switzerland, Belgium, The Netherlands and Luxembourg) and 20 sectors.

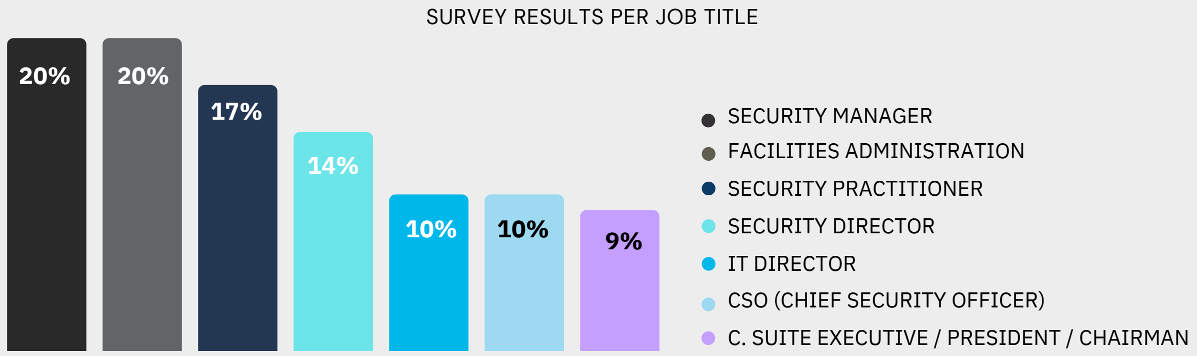


FIGURE 14

Let Brivo Help

- ✓ Cloud-native solutions
- ✓ Data and auditability
- ✓ Centralized access management
- ✓ Integration to video
- ✓ Compliance with new and emerging rules
- ✓ Automatic software updates
- ✓ Unlimited scale – Anywhere in the world
- ✓ Remote management of all facilities
- ✓ SOC2 certification

Sites	Monthly Attendance
San Antonio	19
Houston	35
Philadelphia	99
Phoenix	47
San Diego	35

Departments	Weekly Attendance
Marketing	19
Human Resources	35
Technology	99
Sales	47
Support	35

ABOUT BRIVO

Brivo, Inc., created the cloud-based access control and smart spaces technology category over 20 years ago and remains the global leader serving commercial real estate, multifamily residential and large distributed enterprises. The company's comprehensive product ecosystem and open API provide businesses with powerful digital tools to increase security automation, elevate employee and tenant experience, and improve the safety of all people and assets in the built environment. Brivo's building access platform is now the digital foundation for the largest collection of customer facilities in the world, protecting over 600M+ SQ.FT of real estate across 60+ countries. Learn more at **www.Brivo.com**

Find out more Brivo solutions at

visit brivo.com