ALLIED UNIVERSAL®
There for you.

G4S
An ALLIED UNIVERSAL Company

World Security Report

2,352
Chief Security Officers

31
Countries

World Security Report

Table of Contents

Value Under Threat:
Security in a Polarized World

We are pleased to share the second edition of the *World Security Report*, which provides valuable insight into the security industry and the challenges it faces. We surveyed a total of 2,352 chief security officers (CSOs) from 31 countries representing companies with combined revenue of more than $25 trillion. Additionally, the report gathers views from 200 global institutional investors who manage over $1 trillion in assets.

When the first report was published in 2023, the world was in a period of increased economic and geopolitical volatility following the COVID-19 pandemic and the Ukraine war entering its second year.

Fast forward two years and the world is still grappling with an increasingly polarized global environment, cohesion feels more elusive, trust in authorities continues to erode, and significant economic pressures persist. Politics remains divisive and in unprecedented flux, and in 2024 more people voted in elections globally than in any other year in history.

With war in Ukraine continuing and conflict in the Middle East, countries are increasing their defense spending and global businesses are having to consider the potential impact to their operations.

Economic instability looms large, 44% of CSOs say this will be the top security-impacting hazard for the coming year - similar to 2023.

With so much upheaval globally, as well as economic and social instability, it is perhaps unsurprising that CSOs expect external threats to increase significantly compared with 2023. Anticipated internal or insider threats, in contrast, are slightly down since 2023.

The financial impact of security incidents remains significant. More than a quarter (26%) of companies experienced a loss of revenue following an internal or external security incident in 2024. According to investors, a significant internal or external security incident could decrease the value of a publicly listed company on average by 32%, up 3% since 2023.

The threat of violence to senior company executives has increased according to 42% of CSOs. Concerns are growing that societies are becoming more violent, and this is spilling over to affect the people and assets of businesses.

Global institutional investors place significant importance on executive protection, with a resounding 97% saying it is important that companies they invest in provide this to help protect senior leaders. Executives are regarded as critical, with over two-thirds (68%) of investors stating that leadership accounts for 30% or more of the value of the companies in which they invest.

Social and political polarization can be exacerbated by digital activity where misinformation and disinformation are spread and amplified at breakneck speed. This is now recognized as a serious threat. The sharing of both inaccurate information and deliberate false narratives with malicious intent is increasingly linked to physical security incidents. Three quarters (73%) of CSOs reported that their companies have been targeted by a misinformation or disinformation campaign.

At the same time, CSOs are grappling with the increasing scope and complexity of their roles, including more data analysis and technological oversight. The continued convergence of cyber and physical security threats brings additional threats to the physical security of their operations.

Despite the growing use of artificial intelligence (AI) to enhance physical security effectiveness and efficiency, CSOs agree that people remain the backbone of the security industry. Frontline security professionals will always play an integral role in helping keep companies safe, according to 87% of CSOs.

Notably, the results show that frontline responsibilities are increasing. The vast majority (83%) of CSOs agree there are greater demands on frontline security professionals than there were five years ago. CSOs report they are focusing technology spend to galvanize the role of security professionals at the center of physical security operations.

Investments in technology that enhance security team efficiency and effectiveness as well as improve the security professional's experience, are top of mind. CSOs are also prioritizing investment in training and upskilling their security workforce.

Both security decision makers and institutional investors think that physical security should have a higher strategic priority than it currently does, according to 82% and 92%, respectively. Given the external landscape, it is not surprising that 66% of CSOs expect physical security budgets to increase in the next 12 months.

While exploring and understanding the underlying causes of security incidents, we also want to determine what companies can do to reduce risk. Consistent with the 2023 findings, companies that use a single third-party security provider for 80% or more of their security requirements, not only experience fewer incidents but their confidence to deal with them is significantly higher.

The *World Security Report 2025* underlines the strategic importance and considerable value of good physical security to businesses around the world.

We hope you enjoy reading it.

Steve Jones
Global Chairman and CEO
Allied Universal

Ashley Almanza
Executive Chairman
Allied Universal, International

Research Results

2,352 chief security officers (CSOs) - or those in equivalent positions - at medium and large global companies across 31 countries with combined annual revenue of more than $25 trillion were anonymously and independently surveyed.

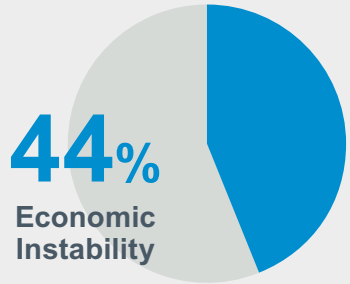
200 global institutional investors with more than $1 trillion of assets under management were also independently and anonymously surveyed. Bold text throughout the report indicates the exact answer chosen by respondents.

2,352 CHIEF SECURITY OFFICERS | **31** COUNTRIES

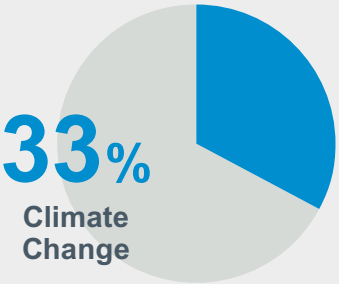
MORE THAN **$25** TRILLION COMBINED REVENUE

200 GLOBAL INSTITUTIONAL INVESTORS | MANAGING MORE THAN **$1** TRILLION IN ASSETS

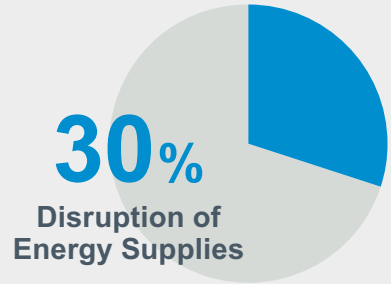
TOP THREE SECURITY-IMPACTING HAZARDS AFFECTING COMPANIES IN THE NEXT YEAR



44% Economic Instability



33% Climate Change



30% Disruption of Energy Supplies

Anticipated Increase in Physical Security Budget

66% EXPECT PHYSICAL SECURITY BUDGETS TO INCREASE IN THE NEXT YEAR

Company leaders are more concerned with cybersecurity than physical security according to 80% of CSO respondents. In addition, 87% of CSOs agreed that frontline security professionals or guards will always play an integral role in helping keep organizations safe.

Executives Impact on Company Values

THE CONTRIBUTIONS OF KEY EXECUTIVES REPRESENT **30%** (OR MORE) OF A COMPANY'S VALUE

Revenue Loss After Security Incident

26 % OF COMPANIES LOST REVENUE FOLLOWING A SECURITY INCIDENT

Impact of Security Incidents on Company Values

A SIGNIFICANT INTERNAL OR EXTERNAL

/// SECURITY INCIDENT ///

COULD REDUCE THE VALUE OF A PUBLICLY-LISTED COMPANY

BY AN AVERAGE OF **32%**

ACCORDING TO GLOBAL INSTITUTIONAL INVESTORS

Chapter One

Emerging and Evolving Threats:
Economic and Geopolitical Impacts

When the first *World Security Report* was published in 2023, the world was experiencing heightened economic and geopolitical volatility following the financial disruptions caused by the COVID-19 pandemic and a major war in Europe. The events of the past two years have only intensified these challenges and new emerging threats.

Economic instability (e.g. recession, high inflation) was the most concerning security-impacting hazard in 2023 for chief security officers (CSOs) and remains so, with 44% saying they expect this to persist.

Climate change events (e.g. long-term shifts in weather patterns, extreme temperatures) and **disruption of energy supplies** are also significant concerns for 33% and 30% of CSOs, respectively.

War and political instability, as well as **civil unrest** (e.g. strikes, protests and riots), are in the top five hazards for the coming year at 29% and 28%, respectively. This points to further pressure on social cohesion, political changes and a breakdown in trust between institutions and citizens.

97%

of global institutional investors say it is important that companies they invest in provide physical protection for executives

42%

of CSOs say the threat of violence towards company executives has increased

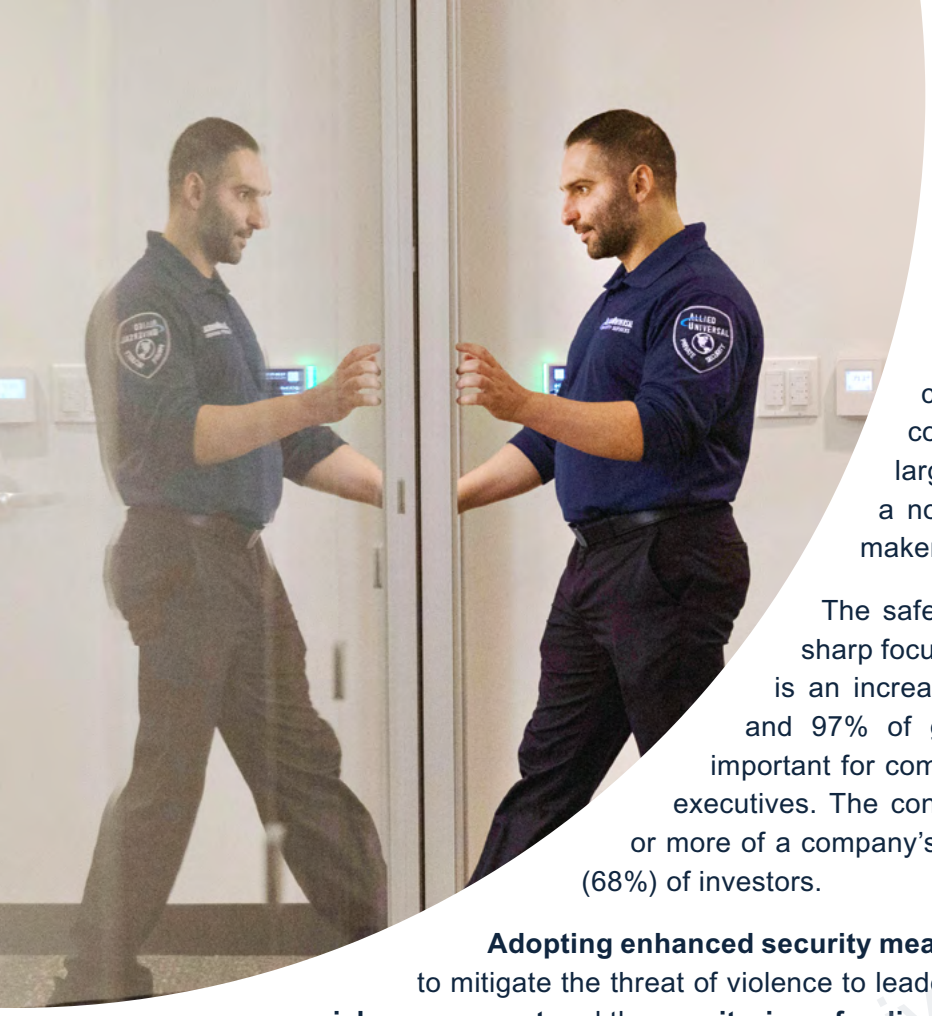
Top Measures to Mitigate the Threat of Violence to Leaders

49% **Enhanced Their Security Procedures**
Enhanced background checks, on-site firearms or explosives screening

45% **Risk Assessment for Leaders**
Pre-event assessments, travel risk management

44% **Monitoring Online Threats**
Social media, dark web, etc.

40% **Security Training and Preparedness for Leaders**
Self-defense, awareness and/or de-escalation



External Threats

External threats are expected to increase significantly in the next 12 months compared to 2024 and become a greater concern for CSOs than previously, now largely on par with internal threats. This marks a noteworthy shift requiring security decision makers to adapt their strategies accordingly.

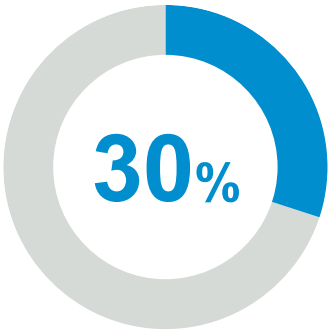
The safety of company executives has come into sharp focus, with 42% of security chiefs saying there is an increased threat of violence toward executives and 97% of global institutional investors agree it is important for companies to invest in physical protection for executives. The contributions of key leaders represents 30% or more of a company's value, according to more than two-thirds (68%) of investors.

Adopting enhanced security measures is the top tactic taken by companies to mitigate the threat of violence to leaders, 49% of CSOs say. This is followed by **risk assessment** and the **monitoring of online threats** at 45% and 44%, respectively.

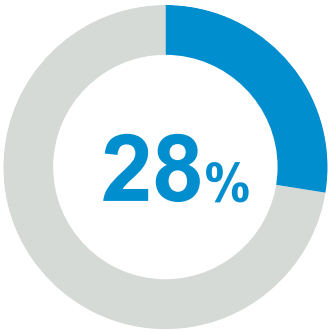
Fraud - a largely financially motivated crime - has grown and remains the most anticipated external threat. Thirty percent (30%) of security chiefs expect this threat to impact their organization, compared with 25% in 2023. Fraud is a physical security incident that, according to 62% who experienced it, was the primary factor driving increased security budgets.

Theft of company physical property and **malicious damage to company property** are expected to impact operations according to 28% and 27% of CSOs, up considerably since 2023. Of the companies who experienced this incident last year, **theft of company physical property** is the second biggest driver of budget increases cited by 60% of respondents.

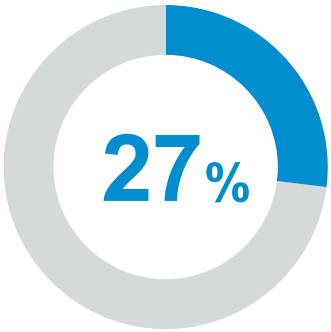
External Incidents Most Expected in the Next 12 Months



Fraud



Theft of Company Physical Property



Malicious Damage to Company Property

Internal Threats

Leaking sensitive information is the most anticipated internal threat for the coming year, 32% of security chiefs say, followed by **unauthorized access to company resources or data** at 28%. Both are slightly less of a concern than in 2023.

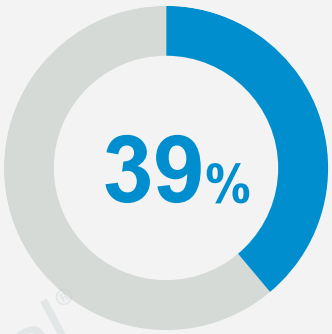
CSOs were asked what they believe drives intentional insider threats, and a clear financial theme emerges. Two of the top three factors are **financial stress or personal debt** and **financial dissatisfaction** at 37% and 36%, respectively. Most concerningly - given the rise of inaccurate information on social media - the biggest driver was the influence of misinformation or external radicalization, according to 39% of CSOs.

Internal Incidents Most Expected in the Next 12 Months

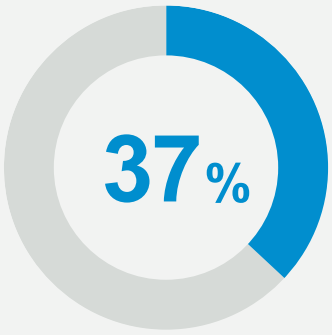
32% Leaking Sensitive Information

28% Unauthorized Access to Company Resources or Data

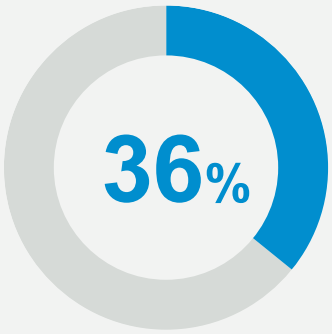
Top 3 Factors CSOs Believe Drive Intentional Insider Threats



Influenced by Misinformation or External Radicalization



Financial Stress or Personal Debt



Financial Dissatisfaction
Low pay, lack of bonuses or incentives

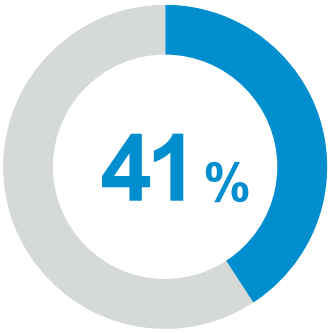
Misinformation and Disinformation

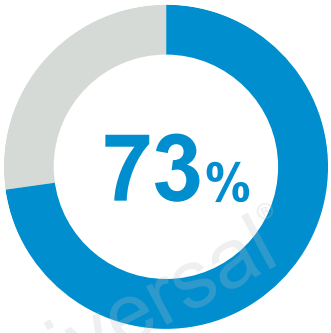
Misinformation (incorrect information) and disinformation (purposely false information) are putting companies and their executives at increased risk. The results highlight how widespread and harmful this phenomenon has become. A staggering 73% of CSOs say their companies have been targeted by a misinformation or disinformation campaign in the last year.

Such events are characterized by real-time information on social media platforms, which can ignite social unrest events or violent incidents. This is a significant concern to companies: misinformation or disinformation motivates at least half of threat actors targeting businesses, according to 41% of security chiefs.

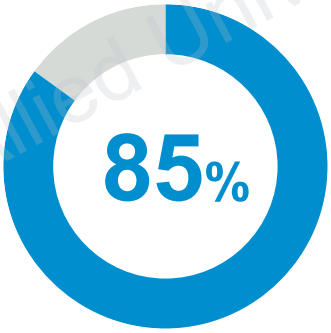
Misinformation and disinformation are closely linked with fringe, activist and extremist groups who use it to promote their cause and gain new followers. Investors remain highly cautious, with 85% agreeing that activist groups increasingly pose a physical security risk to corporate facilities and executives.

MISINFORMATION OR DISINFORMATION MOTIVATES AT LEAST HALF OF THREAT ACTORS TARGETING BUSINESSES ACCORDING TO 41% OF CSOs





73% OF CSOs SAY THEIR COMPANIES HAVE BEEN TARGETED BY A MISINFORMATION OR DISINFORMATION CAMPAIGN



ACTIVIST GROUPS INCREASINGLY POSE A PHYSICAL SECURITY RISK TO CORPORATE FACILITIES AND EXECUTIVES ACCORDING TO 85% OF INSTITUTIONAL INVESTORS

Supply Chains

Geopolitical tension will compromise the security of supply chains over the next 12 months, 78% of CSOs said. Again, this emphasizes how global affairs can impact corporate physical security and indicates that supply chains are a vulnerable target exploited by threat actors, particularly in-transit between manufacturing and distribution centers, which tend to be better protected. Notably, those who experienced supply chain attacks last year said they were a top driver of increased security budgets, according to 60% of security decision makers.

Industry Expert View

Joe M. Olivarez, Jr.

Chief Security Officer and Executive Vice President - Health, Safety, Security, Environment & Enterprise Quality at Jacobs

For years, we've heard security described as a "business enabler," but there wasn't a lot of substance behind it. That's all changed. We're operating in an environment where executive and board-level expectations are higher than ever. The complexities of businesses continue to evolve, and the aperture of security risks has widened.

Chief security officers (CSOs) are now being asked to do more - and I'm not just talking about within the security space; I'm seeing a greater number of CSOs take on responsibility for operational resilience and risk management across a range of functions. That means we have to be prepared to answer questions beyond broad security risks. We must be able to speak to business, commercial and entry risks with a true understanding of the impact these risks may have and help corporations make decisions accordingly.

To drive the greatest value and ensure effectiveness, CSOs must understand how their business operates and align with the company's goals. To meet rising expectations, it's incumbent upon them to deepen their geopolitical expertise, so we can better support leaders and shape strategic, data-informed decision-making. This is essential when it comes to managing global supply chains - gone are the days when you could source things from one place.

The *World Security Report* data around security-impacting hazards, particularly climate change, shows why there is the need for resilience to be a foundational part of each function. I see some security teams separated from their continuity and resilience teams, which is a missed opportunity. It's critical to bring your intelligence and operational capabilities together to deliver strong overall resilience and crisis management.

Executive protection is a growing area of focus. Yes, this has climbed up the agenda because of the media attention, but I think that CSOs are also very aware that threats to their executive team don't always have to be intentional. It could be a case of being in the wrong place at the wrong time - and that's where the net has widened. Unfortunately, we're seeing a rise in indiscriminate crime and violence globally, which increases the risk of leaders being inadvertently impacted. It's important to understand that executive protection is not only a threat mitigator, but it also creates greater efficiencies for executives to execute effectively in this dynamic world.

Many companies are happy to maintain a lower profile and use that to their advantage in protecting their executives. Being mindful of the internal and external information available, as well as having a strong partnership with corporate communications, is critical to managing the public narrative.

This is a key point, especially in light of the growing spread of misinformation and disinformation, as highlighted in the data. While organizations can't control every external narrative, they can take greater ownership of their own story - and doing so is more important than ever.

That's why the partnership between corporate communications and security teams is so vital. For example, aligning on the timing, content and audience of a public announcement allows for a proper threat assessment, so we can manage risk appropriately. This kind of coordination ensures we're not only telling our story effectively, but we're doing so with awareness of the broader risk landscape.

There's no doubt that CSOs are operating in an increasingly complex global environment, but that doesn't mean they can't deliver high-value outcomes for their company and people. An effective CSO is intentional about creating opportunities - not just managing challenges.

All views and opinions expressed in this article are Joe M. Olivarez, Jr.'s own.

Biography

Joe Olivarez is the chief security officer and executive vice president - Health, Safety, Security, Environment & Enterprise Quality at Jacobs, which has 45,000 employees and operates in over 40 countries providing end-to-end services in advanced manufacturing, cities and places, energy, environmental, life sciences, transportation and water.

Olivarez was selected in 2014 to be the first global security leader in the company's 60-year history. Due to his leadership, his remit has expanded and he now has responsibility for developing strategic direction, governance and assurance, research and ideation and knowledge sharing in the areas of health, safety, environmental, security, resilience and enterprise quality.

Prior to joining Jacobs, Olivarez spent 11 years with Baker Hughes Incorporated, where he was instrumental in transforming the program from a department to a function.

Prior to that, Olivarez was vice president at an international investigative and security management consultancy, serving a variety of corporations. He also spent 10 years in government and government defense security, including National Aeronautics and Space Administration (NASA) as a special agent.

Olivarez received a Bachelor of Arts in criminal justice with an emphasis in legal research from Stephen F. Austin State University and Master of Business Administration from the University of Houston Executive Management Program.

Olivarez is currently the president of ASIS International and a serving board member.

Physical Security:
A Strategic Imperative and Value Driver

In an increasingly volatile and polarized world, physical security has become a critical strategic imperative, a corporate value driver, and a barometer of a company's financial health and market perception.

This is powerfully demonstrated in the views of both chief security officers (CSOs) and global institutional investors, reinforcing the role of physical security at the center of corporate resilience.

Physical Security Should be a Higher Strategic Priority for Businesses

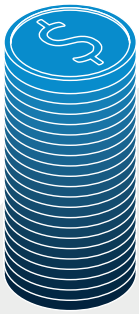
CSOs Agreed **82%**

Institutional Investors Agreed **92%**

In fact, 92% of institutional investors surveyed said physical security should be a higher strategic priority for businesses, compared to 82% of CSOs. This indicates that institutional investors are even more concerned about physical security than those at the forefront managing it day to day.

Impact of Security Incidents on Revenue

The financial ramifications of security incidents can be significant. Following an internal or external breach, 26% of CSOs reported revenue losses, and companies on average lost at least $9 million in revenue.



COMPANIES LOST AN AVERAGE OF $9 MILLION IN REVENUE DUE TO A SECURITY INCIDENT

Corporate Value Impact

Security incidents can inflict considerable damage on corporate value, and the impact is most visible for publicly listed entities. On average, an internal or external incident can impact the value of a publicly listed company by 32% according to surveyed institutional investors. That's 3% higher than two years ago.

Nearly a quarter (23%) of publicly listed companies surveyed experienced a decline in stock price in the last year as a result of an internal or external security incident.

The survey findings demonstrate to executive leadership that security is not just helping to protect assets, but helps safeguard shareholder value and company reputation. This perspective from the investment community reinforces the idea that robust physical security is no longer an optional add-on, but a fundamental pillar of corporate governance and risk management.

However, in terms of the risks different threats pose, the two groups - security chiefs and institutional investors - are not always in agreement. While they both consider **fraud** to be the most concerning external threat, institutional investors also rate **fraud** as the top internal threat, while CSOs ranked it fourth. CSOs are much more concerned with **leaking sensitive information** as their top internal threat - highlighting the convergence of physical and digital threats.

63% OF GLOBAL ORGANIZATIONS SAY THAT PHYSICAL SECURITY INCIDENTS RESULTED IN A REVENUE LOSS OF AT LEAST 10%

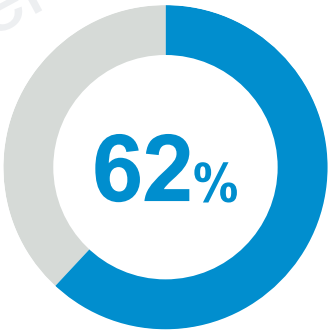
Physical Security Budgets

Two thirds (66%) of CSOs anticipate their physical security budgets will increase in the next year with 26% expecting budgets to grow significantly, demonstrating a proactive approach to enhancing their security posture.

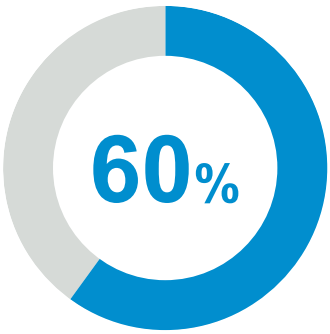
Top budget priorities include investment in **new security technology and infrastructure** (47%), followed closely by **employee security training and upskilling** (45%) and **conducting security risk assessments and threat intelligence analysis** (44%). Companies that experienced **fraud**, **theft of company physical property** and **supply chain attacks** last year said they were the external physical security incidents most likely to drive an increase in security budgets.

Investments planned by CSOs demonstrate a strategic commitment to enhancing physical security capabilities through a blend of technological advancement and developing the skills of their security professionals.

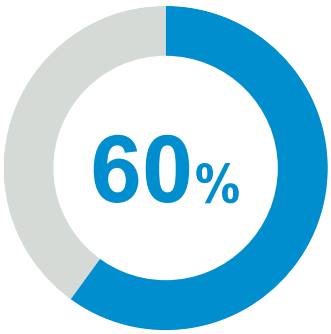
Experienced External Physical Security Incidents That Most Influenced an Increase in Security Budgets



Fraud



Theft of Company Physical Property



Supply Chain Attacks

97%

of institutional investors state that it is important for companies they invest in to provide physical protection for executives

Physical Security Vendor Involvement

Third-party security providers are critical to many successful security programs. Companies that use a single third-party security provider for 80% or more of their physical security requirements not only experienced fewer security incidents, but their confidence to address them is significantly higher at 79%, compared to 51% among those with low vendor involvement.

Confidence in Dealing with Physical Security Threats

Companies with high physical security vendor involvement (80%+) are more confident in dealing with both internal and external threats compared to those with low vendor involvement (70% or less).

High Involvement	**79%**
Low Involvement	**51%**

Industry Expert View

Tim Weir

Vice President of Resiliency at DXC Technology

At its core, security is not simply about deterrence or compliance, it's about corporate citizenship. Organizations that protect their people and assets are ultimately protecting their reputations, their communities, and their long-term license to operate. In this sense, security has always been strategically important to organizations where people matter.

What is changing today is not the need for security, but the scope of what leaders must prepare for. In boardrooms across industries, executives are no longer only concerned with theft, perimeter breaches, or traditional crime. Increasingly, they are focusing on the low-probability but high-impact events that can disrupt entire organizations and even economies.

I call them the "Four Fs": floods, flu, fire, and fury (threats like civil unrest and workplace violence that are becoming all too common). Unlike smaller incidents that can be contained or absorbed, these events represent systemic shocks. And for those charged with securing critical infrastructure, abandoning a site in the face of crisis is simply not an option. Presence must be maintained. Continuity must be assured. People must remain safe.

To better withstand the Four Fs, companies are initiating what I call the "digitization of guards," which means blending and empowering frontline team members with technology to help them make more informed decisions while keeping them out of harm's way. This is part of the "industrial security" approach that spans digital, operational, and human domains and has security professionals working shoulder-to-shoulder with CIOs, CISOs, and increasingly, GISOs (government information security officers). We are not siloed specialists; we are partners in holistic enterprise risk management.

That's the approach, but what's the cost? The true cost of a security incident – like one of the Four Fs – is notoriously difficult to quantify. A facility may suffer only minimal physical damage, and the operational response may be exemplary. But if stakeholders lose confidence, the damage can cascade.

As risks and the team responsible for managing them have grown, so too have budgets. Where that money is spent matters more than how much is spent. In my view, the top two budget priorities should be (1) investing in the right technologies and (2) upskilling the workforce because with the right combination of tools and trained people, investments in security infrastructure will deliver their full potential.

To save budget, I'm an advocate of using a third-party security provider. Outsourcing is not simply a cost play, it's about resilience. External providers bring the ability to rotate staff, share best practices across clients and maintain undivided attention on risk. Most importantly, they are not distracted by the competing priorities that internal teams often face. Security providers are strategic partners, embedded in an organization's resilience framework.

And, ultimately, security is about resilience. Resilience is what allows organizations not only to endure but to thrive during and after the Four Fs.

After three decades in this industry, one truth has become undeniable: security is no longer peripheral, it is central to enterprise value. It enables trust. It ensures continuity. It protects reputation.

All views and opinions expressed in this article are Tim Weir's own.

Biography

Tim Weir is the vice president of resiliency for DXC Technology. He is responsible for the protection and resiliency of DXC people and assets across the world. Weir has significant experience in senior leadership roles spanning more than two decades.

Before joining DXC, he was a principal at an international risk management firm and a Global Fellow with the Science and Technology Innovation Program at the Wilson International Center for Scholars.

As a managing director with Accenture, he held ultimate responsibility for overseeing the protection of personnel and significant assets in more than 120 countries. He has also served by appointment on several government and private sector councils for both domestic and international affairs. He is a graduate of the University of Maryland.

Chapter Three

The Changing Security Workforce:

Culture, Competence and Capacity

In a decade defined by geopolitical disruptions, polarization, continued economic instability, ever-evolving threats and the exponential rise of AI, people remain the beating heart of the security industry.

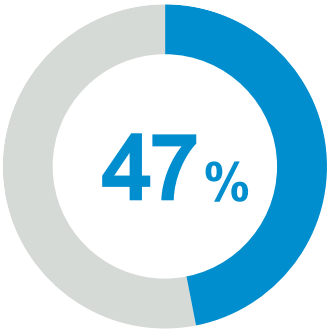
The findings support the enduring importance of frontline security professionals, with 87% of CSOs agreeing they will always play a vital role in keeping organizations safe.

People Are Here To Stay

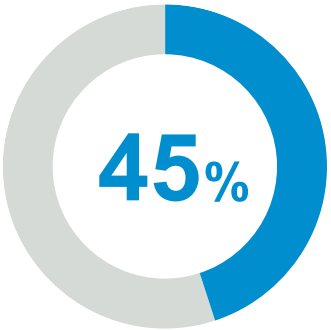
Chief security officers (CSOs) are prioritizing continuous training, fostering a strong security culture across the entire organization and integrating technology to enhance the human capabilities of their teams.

Responses indicate that in the foreseeable future, security chiefs do not expect technology to replace the nuanced judgment, adaptability, emotional intelligence and human interaction essential in security professionals. Underscoring this point, people skills remain more important than physical attributes of strength, according to 84% of respondents.

Top Security Budget Priorities for the Next 12 Months



Investment in New Security Technology and Infrastructure



Employee Security Training and Upskilling

People remain essential and while technology plays a transformative role, it is the dedicated frontline workforce, supported and augmented by technology and training, that help safeguard assets.

Security decision makers are strategically leveraging technology to support their teams, with 51% of CSOs noting they are adopting new technology to enhance security team efficiency and effectiveness.

Human Cost

Security chiefs face considerable challenges. While the frontline workforce operates under intense pressure, recruitment of qualified officers remains a persistent obstacle compounded by high staff turnover driving up training costs.

CSOs are acutely aware of the increasing demands on the workforce, with eight in 10 (83%) acknowledging that there are greater demands on frontline security professionals today than there were five years ago.

83% OF CSOs

AGREE THAT THERE ARE GREATER DEMANDS ON FRONTLINE SECURITY PROFESSIONALS THAN THERE WERE 5 YEARS AGO

CSOs said their top three workforce challenges are recruitment and retention, skills gaps and training needs as well as the ability to adapt to new technologies.

There is a human cost too, with concerns raised about mental health strains, violence, assaults and fatigue.

In response, CSOs are focused on developing and supporting their people. Training and upskilling are top budget priorities with 45% of global security leaders prioritizing this in the coming year.

Industry Views

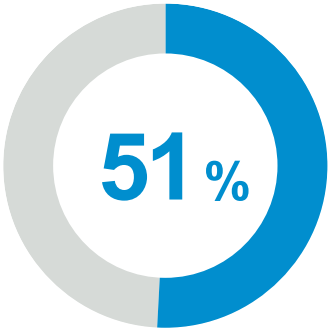
Recruitment and Retention

> We are currently facing significant challenges with frontline security personnel due to a lack of trained personnel, high employee turnover, and increasing pressure to maintain high security standards in an increasingly complex environment. - Anonymous CSO

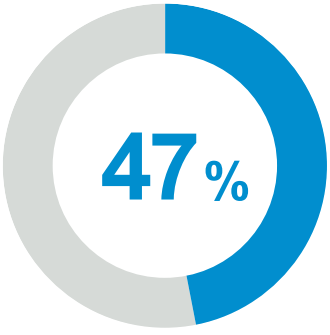
Skills Gaps and Training Needs

> Security professionals must constantly keep up with the latest threats and attack methods, which require continuous updating of their knowledge and skills. - Anonymous CSO

People-Related Factors Driving Adoption of New Security Technology



Enhancing Security Team Efficiency and Effectiveness



Improving Security Employee Experience

The Role of the CSO

While CSOs grapple with workforce challenges, their own roles are broadening in scope and complexity, requiring a more strategic and holistic approach to risk management.

Responsibilities have expanded to include complex data analysis and far greater technological oversight of physical security systems, requiring CSOs to work with IT and cybersecurity colleagues, as the lines between physical and digital threats increasingly converge.

Industry Views

Workforce Well-Being and Morale

> Frontline security personnel are often overburdened, especially in large facilities or environments with multiple critical points. This can result in fatigue, decreased concentration and, ultimately, human error that affects the effectiveness of the service. - Anonymous CSO

Security Culture

> A robust security culture is proactive, collaborative, and education-driven, crucial for safeguarding client data and assets effectively.
> - Anonymous CSO

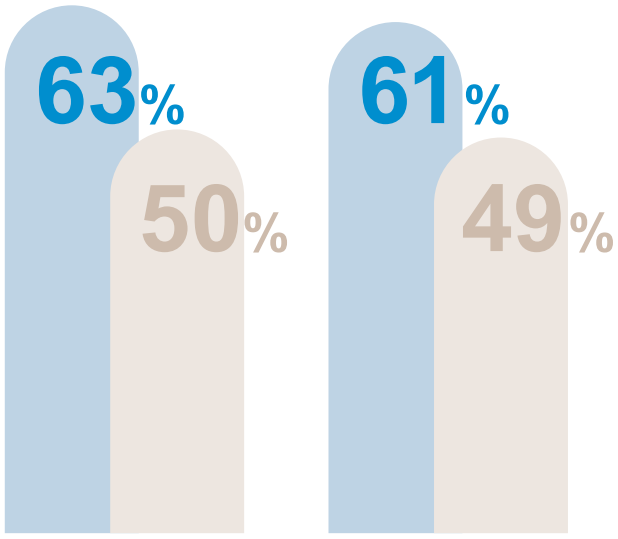
Security Culture Matters

CSOs consider security culture to be a foundational element for effective organizational security, recognizing its positive impact on the workforce. The survey found that 64% of CSOs have a **strong** or **well-adopted** security culture.

A strong security culture encourages a shared understanding and collective commitment to help protect company assets. It also directly influences employee behavior and engagement, which are vital in helping to prevent incidents.

Confidence of CSOs to Address Incidents

Companies surveyed that described their security culture as **strong** or **well-adopted**, were much more confident in their ability to deal with internal and external incidents than those that described their culture as **mixed adoption, low engagement** or **weak**.



AI and Tech: A Reality Check

Security decision makers view technology as an indispensable strategic asset and consider it a key component in a resilient security program. Of those surveyed, 47% say that technology (and the infrastructure that goes with it) are top budget priorities for next year.

Security decision makers are aware of the growing convergence between cyber and physical security, a shift that has fundamentally transformed their roles over the past five years. A weakness in one domain can directly impact the other. For instance, a cyber breach could compromise physical access controls and, conversely, a physical intrusion could lead to cyber vulnerabilities.

Security chiefs express concerns about the speed of technological change and their ability to keep pace along with the potential for new technologies to expose vulnerabilities. Their roles are rapidly evolving to include greater technological oversight as the lines continue to blur between physical and cyber.

Companies Top Security Budget Priority in the Next 12 Months

47%

investment in new security technology and infrastructure

Industry Views

Advanced Adoption

> We have achieved a high level of AI-driven physical security maturity, with continuous monitoring, improvement, and innovation.
>
> - Anonymous CSO

Basic AI Use

> In a fairly early stage, but will be introduced more and more in the near future.
>
> - Anonymous CSO

No Replacement for Humans

Security decision makers are actively adopting technology with an AI element. They do not see AI as a replacement for security professionals, but rather as an analytical and advisory tool to boost and complement human capabilities.

71% surveyed say they are using AI for assistive or oversight tasks where the ultimate decision maker is a person, in surveillance and monitoring, while 69% are using it for access control and identity verification.

The most crucial area of AI investment over the next two years for 45% of those surveyed is **AI-powered video surveillance and analytics**, followed by **AI-powered intrusion detection and prevention** and **AI-driven threat detection and risk assessments** for 44% of security leaders.

Technology in Use

Unsurprisingly, security decision makers are planning to use technology to reduce the likelihood of security threats (93%) and nearly half (49%) said they plan to use technology to enhance human capabilities to improve threat detection and help prevent incidents. Over a third (38%) reported plans to fully automate the function of containing security incidents to allow a response. A resounding 93% said they plan to use technology to improve incident response to reduce impact and accelerate recovery.

Most Crucial Physical Security Technologies for Businesses Over the Next Two to Three Years

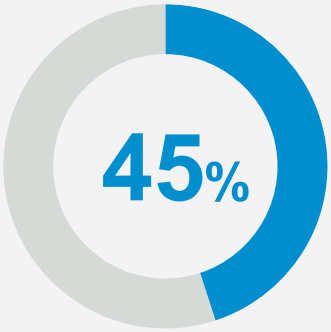
39% AI-Powered Intrusion Detection and Perimeter Security

38% AI-Driven Threat Detection and Risk Assessment

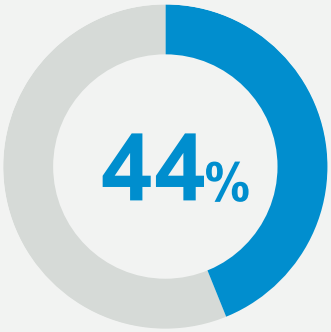
38% Advanced Access Control
Facial recognition, biometrics, voice

38% Advanced Video Surveillance
Cameras with analytics or AI

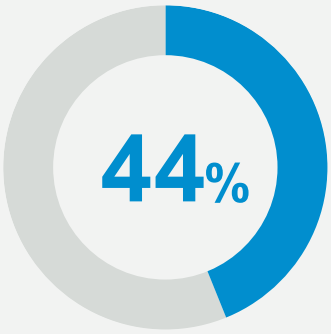
Most Crucial Cutting-Edge Security Technologies for Businesses Over the Next Two Years



AI-Powered Video Surveillance and Analytics



AI-Driven Threat Detection and Risk Assessment



AI-Powered Intrusion Detection and Perimeter Security

Industry Views

AI in Pilot Phase

> We're in an exploratory phase of AI adoption for physical security. Currently, we're testing AI - based access control systems to enhance the security of our facilities. - Anonymous CSO

Advanced Adoption

> My company's adoption of AI for physical security is innovative and strategic, leveraging advanced technologies to enhance threat detection, automate responses, and optimize resource allocation, ensuring a safer and more efficient environment. - Anonymous CSO

Barriers to Implementation

The success of this technological evolution hinges on addressing practical challenges. Significant barriers to AI and technology adoption persist, including implementation costs and a gap in workforce skills that make its effective use more difficult.

AI is valued for its ability to augment human capabilities, freeing up personnel from mundane tasks to focus on higher-level analysis and critical response. AI helps create smart defenses that empower human teams with better insights.

Top Factors Driving Adoption of New Security Technology

52% Reducing Security Risks and Threats

51% Enhancing Security Team Efficiency and Effectiveness

47% Improving Security Employee Experience

47% Enhancing Security for Customers and Visitors

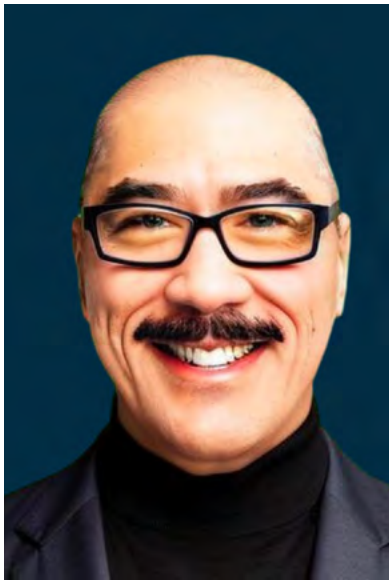
49%

said they plan to use technology to enhance human capabilities to improve threat detection and help prevent incidents

The integration of technology is seen as crucial for enhancing efficiency, effectiveness and for proactive threat mitigation. This widespread intent to integrate new technologies speaks volumes about the perceived value and necessity of digital innovation in physical security.

The biggest challenge that remains is empowering security professionals with the right skills to unlock the power of technology to deliver a robust, proactive security program that strives to reduce risks and helps keep people and assets safe.

Industry Expert View



Brian K. Tuskan

Vice President, Chief Security Officer
Global Safety & Security at ServiceNow

The data doesn't lie - CSOs are doubling down on technology, with 98% planning investments over the next five years. AI, biometrics, robotics, Internet of Things: it's all on the table. But investment in technology alone doesn't solve the real issue, which is execution.

You can have all the technology in the world, but if you don't have the correct processes and the best people with the right skills, your execution will fail. The most advanced racing car will not drive well if the person at the wheel doesn't have the skills to do so and has no idea what it is capable of.

A physical security program requires a sound strategy. It will have greater impact by aligning people, process and technology to build high-performing, agile teams that thrive on complexity and move with purpose. Security employees will have far greater job satisfaction and the team will work better together as a result, with resilience built-in and no single point of failure.

What's clear to me is that the security industry is at a crossroads. Many in senior security roles are still clinging to legacy models that are labor-heavy, they are slow to adapt and apprehensive about cutting-edge technology. Meanwhile, threats are evolving at machine speed and they have no hope of keeping up.

A security program should be scalable and resilient. I have worked tirelessly to replace outdated models with lean, AI-powered operations that scale intelligently, reducing friction and collapsing silos, while driving elite execution across global teams.

AI is here to stay, making this the most exciting time to be working in our industry. Data is everything and AI has completely transformed our ability to interrogate it in multiple ways, which empowers our teams to act on it.

It takes leadership when it comes to the best implementation of technology and it involves partnership across functions in a company to get a deployment right, which takes time. When game-changing technology is integrated effectively, the business and its people will be better protected because of it.

We have been driving the use of AI and automation. It's not about replacing people; it's about augmenting the talent we have to move faster, smarter and more strategically. The direction of travel is the synchronization of people and technology, and it's accelerating.

AI is the force multiplier we've been waiting for - if we implement it responsibly and with purpose. The future of physical security will be defined by those who lean in to AI, not hold back.

Ultimately, in most organizations security is a cost in the budget and we are all looking at ways to save every dollar and spend in the most effective way. When security is viewed as a strategic imperative and there is buy-in at the highest level of an organization, it brings huge benefits.

All views and opinions expressed in this article are Brian K. Tuskan's own.

Biography

Tuskan is a global security leader with a distinguished career spanning law enforcement and corporate security.

As vice president and chief security officer (CSO) at ServiceNow, he leads the Global Safety & Security team - overseeing Executive Protection, Investigations, Threat Management, Event Security, GSOC operations, Intelligence and Security Technology across the enterprise.

Previously, Tuskan served as CSO at Microsoft - Global Security, where he was responsible for all corporate physical security for the company.

With over 12 years of law enforcement experience in Honolulu, HI, and Redmond, WA - most of it in specialized roles including SWAT, major crimes detective, criminal intelligence and undercover narcotics - Tuskan brings operational depth and a public safety mindset to the private sector.

He has been recognized as one of *Security Magazine's* Most Influential People in Security and was ranked the #1 Global Security Executive Influencer by IFSEC.

Tuskan champions innovation in physical security - he's an early adopter of technology solutions. He is leading the industry with the use of gen AI, agentic AI and robotics to transform the archaic physical security field. He is also the founder of Cop to Corporate, a nonprofit helping law enforcement professionals successfully transition to private-sector careers.

Tuskan holds a criminal justice degree from Wayland Baptist University, along with executive certificates from Georgetown University and the University of Washington Foster School of Business.

Asia Pacific

Security-Impacting Hazards

Asia Pacific (APAC) is one of the most impacted regions in the world by a number of hazards and threats. Most notably, **economic instability** is expected to impact the region more than any other, according to 53% of respondents (44% global average).

Climate change is anticipated to impact APAC at the second highest rate in the world, behind Sub-Saharan Africa, according to 37% of security chiefs (33% global average).

External Physical Threats

Focusing on external physical threats, **theft of company physical property** is the most anticipated next year at 30%. APAC is also the highest region globally to assess that **disengagement or dissatisfaction with work** contributes to intentional inside threats at 39% (33% global average).

Geopolitical tensions will compromise the security of supply chains over the next 12 months in APAC more than anywhere else in the world (84% versus 78%).

Company executives are at greater risk of violence than any other region compared to two years ago, said 46% of CSOs (42% global average). Similarly, executives and corporate facilities in APAC are at greater risk from activist groups than anywhere else globally at 83% (77% global average).

More than three quarters (76%) of APAC-based companies have been targeted by a misinformation or disinformation campaign in the last year. That's higher than any other region apart from the Middle East. Misinformation or disinformation motivates at least half of threat actors targeting businesses 48% of respondents said, which is higher than anywhere else in the world (41% global average).

Asia Pacific **53%** vs **Global Average** **44%**

Say **economic instability** is anticipated to be the greatest security-impacting hazard in the next 12 months

Asia Pacific **30%** vs **Global Average** **28%**

Expect **theft of company physical property** to be the top external threat in the next 12 months

Asia Pacific **84%** vs **Global Average** **78%**

Say geopolitical tension will compromise the security of their supply chain over the next 12 months

Next 12 Months

Internal Threats

The top expected internal threat is **leaking sensitive information** at 34%, the second highest region in the world, behind Sub-Saharan Africa. APAC is the second highest region behind Sub-Saharan Africa to say that intentional internal threats are influenced by **misinformation or external radicalization** at 46% (39% global average).

The most crucial cutting-edge technology security chiefs are expected to invest in over the next two years is **AI-powered intrusion detection and perimeter security** (54%). This is higher than any other region in the world.

Internal and External Threats

Asia Pacific **34%** vs **Global Average** **32%**

Top expected internal threat is **leaking sensitive information**

Asia Pacific **46%** vs **Global Average** **42%**

Say the threat of violence toward company executives has increased

Asia Pacific **83%** vs **Global Average** **77%**

Say **activist groups** increasingly pose a physical security risk to corporate facilities and executives

Asia Pacific **48%** vs **Global Average** **41%**

Say misinformation or disinformation motivates at least half of threat actors targeting businesses

This is followed by **AI-powered video surveillance and analytics** and **AI-driven threat detection and risk assessment**, according to 51% and 50% of respondents, respectively. Only security chiefs in Sub-Saharan Africa intend to focus more on these two cutting-edge technologies.

54% SAY THE MOST CRUCIAL CUTTING-EDGE TECHNOLOGY THEY EXPECT TO INVEST IN OVER THE NEXT 2 YEARS IS **AI-POWERED INTRUSION DETECTION AND PERIMETER SECURITY**

(44% GLOBAL AVERAGE)

Physical Security Budgets

More than six in 10 (66%) respondents expect their physical security budget to increase (66% global average). For those who have experienced it, **supply chain attacks** are the threat that will most influence an increase in physical security budgets.

Nearly nine in 10 (86%) security chiefs in the region - and higher than anywhere else in the world - say that company leaders are more concerned with cybersecurity than physical security (80% global average).

Europe

Security-Impacting Hazards

Security chiefs in Europe predict that **economic instability** will be the top security-impacting hazard for the year ahead at 41%. This is slightly higher than in 2023. The anticipated impact of **climate change** and **disruption to energy supplies**, both at 29%, are lower than in 2023.

External Threats

A greater number of external, rather than internal, threats are anticipated next year in line with the global view. **Fraud** is the top expected external threat at 29%, up nine percentage points since 2023, while **theft of company physical property** and **malicious damage to company property** are up six and four percentage points, respectively, at 24% and 23%, compared to 2023.

Europe is the third highest region in the world to agree the threat of violence toward company executives and senior leaders has increased behind APAC and the Middle East at 42%, in line with the global average.

Misinformation or disinformation motivates at least half of threat actors targeting businesses, according to 41% of security chiefs in Europe, in line with the global average.

Seven in 10 companies (70%) in the region have been targeted by a misinformation or disinformation campaign in the last 12 months. However, far fewer respondents say that intentional insider threats are driven by **misinformation or external radicalization** at 29% (39% global average).

Next 12 Months

Europe **41%** vs **Global Average** **44%**

Say **economic instability** is anticipated to be the greatest security-impacting hazard to affect their operations in the next 12 months

Europe **28%** vs **Global Average** **32%**

Expect **leaking sensitive information** to be an internal threat in the next 12 months

Europe **38%** vs **Global Average** **47%**

Say **investment in security technology and infrastructure** is the top physical security budget priority in the next 12 months

Internal Threats

Mirroring the global picture, the top internal threat expected next year is **leaking sensitive information** at 28%, which was the top internal threat in 2023 for Europe. **Fraud** is the second most concerning internal threat anticipated at 24%. This is down five percentage points compared to 2023.

Financial dissatisfaction is the top motivating factor driving intentional insider threats, 34% of respondents agreed (36% global average).

36% SAY
(45% AND 44% GLOBAL AVERAGES)
AI-POWERED VIDEO SURVEILLANCE AND ANALYTICS AND AI-POWERED INTRUSION DETECTION AND PERIMETER SECURITY
ARE CRUCIAL CUTTING-EDGE TECHNOLOGIES THEY EXPECT TO INVEST IN OVER THE NEXT TWO YEARS

Internal and External Threats

Europe **34%** vs **Global Average** **36%**

Say **financial dissatisfaction** is a driver of intentional insider threats in Europe

Europe **29%** vs **Global Average** **39%**

Say the influence of **misinformation or external radicalization** is the biggest driver of intentional insider threats

Europe **42%** vs **Global Average** **42%**

Say the threat of violence toward company executives has increased compared to 2 years ago

Europe **70%** vs **Global Average** **73%**

Of companies in Europe have been targeted by a misinformation or disinformation campaign

Physical Security Budgets

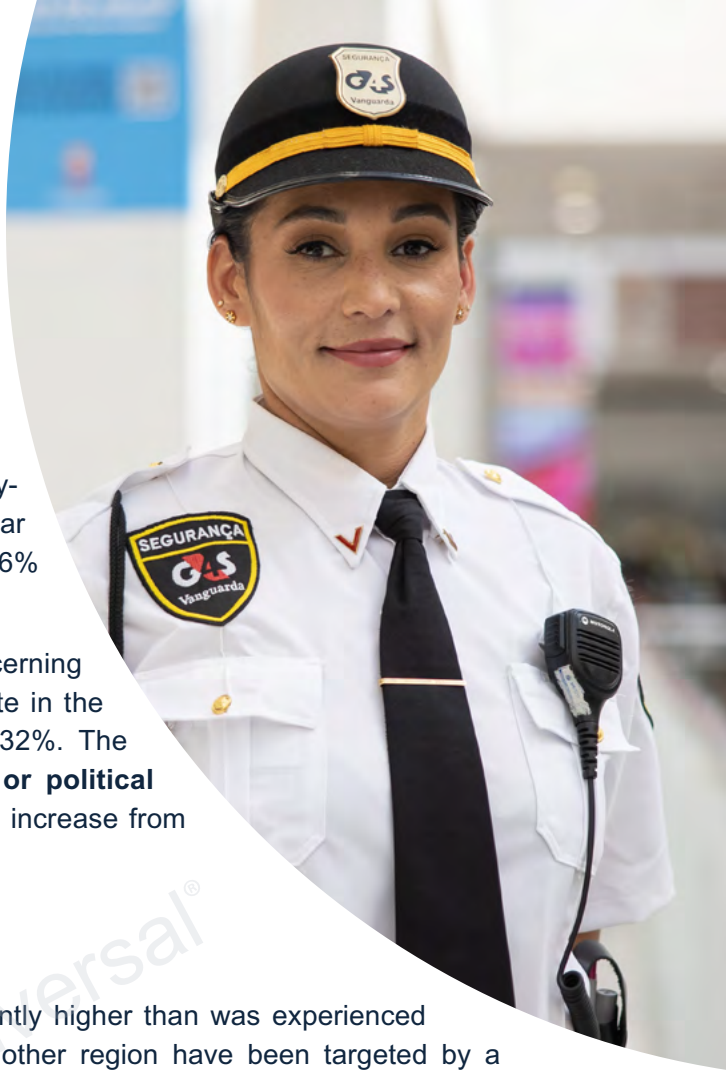
Security decision makers in Europe intend to spend less on cutting-edge technologies than any other region in the world. However, the top investments they will make over the next two years in this space are **AI-powered video surveillance and analytics** and **AI-powered intrusion detection and perimeter security** at 36%.

Fewer CSOs in Europe than anywhere else in the world, and tied with North America, expect to see an increase in their physical security budgets over the next 12 months at 58% (66% global average).

While **investment in new security technology and infrastructure** is the top physical security budget priority over the next 12 months at 38%, this is the lowest rate of all the regions (47% global average).

58% OF CSOs EXPECT THEIR PHYSICAL SECURITY BUDGET WILL INCREASE IN THE NEXT 12 MONTHS
(66% GLOBAL AVERAGE)

Latin America



Security-Impacting Hazards

Economic instability is expected to be the top security-impacting hazard in Latin America (LATAM) over the next year at 41% (44% global average), up significantly compared to 26% that experienced this hazard in 2024.

Disruption of energy supplies will be the second-most concerning hazard according to 31% of CSOs. The second highest rate in the world, after Sub-Saharan Africa and the Middle East at 32%. The two highest emerging hazards are **civil unrest** and **war or political instability**, both according to 26% of respondents, a sharp increase from 18% and 16% respectively who were impacted in 2024.

External Threats

Fraud is the top expected external threat at 30%, significantly higher than was experienced last year, at 16%. At 66%, fewer companies than in any other region have been targeted by a misinformation or disinformation campaign in the last 12 months (73% global average). Fewer CSOs than in any other region, apart from Sub-Saharan Africa, agree the threat of violence toward company executives has increased compared to two years ago at 38% (42% global average).

85%

agree that physical security should have a higher strategic priority within their business

(82% global average)

Next 12 Months

Latin America **31%** vs Global Average **30%**

Say **disruption of energy supplies** is the second most concerning hazard for next year

Latin America **34%** vs Global Average **27%**

Anticipate **fraud** will be the top internal threat in the next 12 months

Internal Threats

Fraud as an internal threat is up markedly since last year at 34% (27% global average). LATAM is anticipated to be the second-most impacted region by this threat, behind Sub-Saharan Africa.

The biggest driver of intentional insider threats was **ideological or political motivations**, according to 36% of CSOs. This was the highest rate in the world for this driver. **Misinformation or external radicalization** was the second-biggest driver of intentional insider threats in the region at 35% (39% global average).

Physical Security Budgets

The most crucial cutting-edge technologies CSOs in LATAM expect to invest in over the next two years are **AI-powered video surveillance and analytics** and **AI-driven threat detection and risk assessment**, according to 46% of respondents and above the global averages for investment in these technologies (45% and 44%).

Physical security budgets are expected to increase by 72% of CSOs. This is well above the global average of 66%, with only Sub-Saharan Africa being higher. Companies that experienced **supply chain attacks** and **armed robbery** said these threats represented the biggest drivers of increased budgets, according to 67% of respondents and above the global averages.

Internal and External Threats

Latin America **66%** VS **Global Average** **73%**

Of companies in LATAM have been targeted by a misinformation or disinformation campaign in the last 12 months

Latin America **36%** VS **Global Average** **31%**

Of CSOs say **ideological or political motivations** were the biggest driver of intentional insider threats in the region

Latin America **38%** VS **Global Average** **42%**

Say the threat of violence toward company executives has increased compared to 2 years ago

Latin America **67%** VS **Global Average** **51%**

Of those who experienced **supply chain attacks,** 67% said it influenced an increase in their security budget.

92% (87% GLOBAL AVERAGE) **OF CSOs IN LATAM AGREE THAT PEOPLE WILL ALWAYS BE INTEGRAL TO KEEPING THEIR ORGANIZATION SAFE**

More CSOs in the region agreed than anywhere else in the world that physical security should have a higher strategic priority within businesses, tied with Sub-Saharan Africa at 85% (82% global average).

At 92%, more CSOs in LATAM than anywhere else, and equal to Sub-Saharan Africa, agree that people will always be integral to keeping their organization safe (87% global average).

There are greater demands on frontline security professionals than there were five years ago, according to 85% of CSOs, higher than any other region apart from Sub-Saharan Africa.

72%

expect their physical security budget to increase

(66% global average)

Middle East

Security-Impacting Hazards

Economic instability will impact the Middle East more than any other hazard, according to 41% of security chiefs, below the global average of 44%.

Perhaps unsurprisingly, the Middle East will be the most impacted region in the world by **war or political instability**, according to 38% of those surveyed; a sharp increase since 2024 when 21% of security leaders said their businesses were impacted by this hazard.

The Middle East will be the second most affected region by **climate change**, on par with APAC but behind Sub-Saharan Africa, according to 37% of security decision makers (33% global average). This is improved from 2024 when 41% experienced this.

70%
expect their physical security budget to increase
(66% global average)

Middle East **38%** vs **Global Average** **29%**
Say **war or political instability** is likely to impact their operations in the next 12 months

Middle East **39%** vs **Global Average** **27%**
Expect **malicious damage to company property** to be the top external threat in the next 12 months

Middle East **33%** vs **Global Average** **32%**
Expect **leaking sensitive information** to be the top internal threat in the next 12 months

Next 12 Months

External Threats

Turning to external physical security threats, the region is set to be the most impacted in the world by **malicious damage to company property** (39%) over the next year and significantly above the global average of 27%.

According to 45% of CSOs in the Middle East (42% global average), company executives and senior leaders are at greater risk of violence compared to two years ago and more so than anywhere else in the world, except APAC.

Internal Threats

The most expected internal threat is **leaking sensitive information** according to 33% of security decision makers (32% global average), this is largely unchanged since 2024.

The biggest driver of intentional insider threats, cited by 42% of CSOs, was the influence of **misinformation or external radicalization** (39% global average). This is the third highest in the world, after APAC and Sub-Saharan Africa. More companies than in any other region have been targeted by a misinformation or disinformation campaign in the last year, according to 79% of respondents (73% global average).

Internal and External Threats

Middle East **79%** VS **Global Average** **73%**

Of companies in the Middle East have been targeted by a misinformation or disinformation campaign in the last 12 months

Middle East **42%** VS **Global Average** **39%**

Say the biggest driver of intentional insider threats was the influence of **misinformation or external radicalization**

Middle East **45%** VS **Global Average** **42%**

Say the threat of violence toward company executives has increased compared to 2 years ago

Middle East **68%** VS **Global Average** **53%**

Say **competitor sabotage** was the physical security incident that most influenced an increase in security budgets out of companies who have experienced it

48% (40% GLOBAL AVERAGE) OF CSOs SAY THE MOST CRUCIAL CUTTING-EDGE TECHNOLOGY THEY EXPECT TO INVEST IN OVER THE NEXT 2 YEARS IS **INTERNET OF THINGS-ENABLED SECURITY DEVICES AND SENSORS**

Physical Security Budgets

The most crucial cutting-edge technology CSOs in the Middle East expect to invest in over the next two years is **Internet of Things-enabled security devices and sensors** at 48% of respondents, which is the highest expected rate globally. That's followed by **AI-powered video surveillance and analytics** noted by 47% of respondents and at the second-highest rate in the world, behind Sub-Saharan Africa.

Seven in 10 (70%) security leaders anticipate their physical security budgets will increase in the year ahead, that's above the global average of 66%. Those who experienced **competitor sabotage** in the last year said it was the physical security incident that most influenced an increase in security budgets at 68% (53% global average). This type of incident influenced budget increases in the Middle East more than in any other region.

North America

Security-Impacting Hazards

North America will be most affected by the security-impacting hazard of **economic instability** in the next year, according to 42% of respondents (44% global average), up significantly compared to 2024, when 28% experienced the impact of this hazard on their business.

60%

say supply chain attacks are the physical security threat that will most influence an increase in security budgets

Climate change will be the second most concerning hazard according to 27% of respondents (33% global average), up considerably compared to 2024, when 20% of CSOs in North America said their company experienced this.

North America **Global Average**

42% vs **44%**

Say **economic instability** is anticipated to be the greatest security-impacting hazard to affect their operations in the next 12 months

North America **Global Average**

29% vs **30%**

Say **fraud** is the most anticipated external threat next year

North America **Global Average**

80% vs **78%**

Say geopolitical tension will compromise the security of their supply chain over the next 12 months in North America

Next 12 Months

External Threats

External physical threats are on the increase. **Fraud** is the most anticipated threat next year at 29%, up from 22% last year. **Theft of company physical property** is expected by 28% of security leaders to impact their organizations, up from 22% in 2024.

Geopolitical tension will compromise the security of supply chains more than anywhere else in the world, apart from Asia Pacific, over the next 12 months according to 80% of North America-based decision makers (78% global average).

Companies that experienced **supply chain attacks** in the last year said it is the external security threat that will most influence an increase in security budgets, according to 60% of those surveyed. An increase in physical security budgets is anticipated by 58% of those surveyed (66% global average).

The threat of violence toward company executives has increased according to 41% of security chiefs, compared with two years ago (42% global average) and three-quarters (75%) agreed that activist groups increasingly pose a security risk to corporate facilities and executives (77% global average).

More than seven in 10 (72%) companies have been targeted by a misinformation or disinformation campaign in the last year (73% global average) and nearly four in 10 (38%) security chiefs in North America say misinformation or disinformation motivates at least half of threat actors targeting their businesses (41% global average).

Internal and External Threats

North America **Global Average**

41% vs **42%**

Say the threat of violence toward company executives has increased compared to 2 years ago

North America **Global Average**

30% vs **32%**

Say **leaking sensitive information** is the most expected internal threat

North America **Global Average**

72% vs **73%**

Of companies have been targeted by a misinformation or disinformation campaign in the last 12 months

North America **Global Average**

38% vs **41%**

Of CSOs say misinformation or disinformation motivates at least half of threat actors targeting businesses

43% SAY

(45% GLOBAL AVERAGE)

THE MOST CRUCIAL CUTTING-EDGE TECHNOLOGY THEY EXPECT TO INVEST IN THE COMING 2 YEARS IS AI-POWERED VIDEO SURVEILLANCE AND ANALYTICS

Internal Threats

The most expected internal threat is **leaking sensitive information** according to 30% of those surveyed (32% global average), up from 26% who experienced the threat last year. Other internal threats such as **fraud** and **theft of company physical property** are both expected to be less of a concern than in 2024.

Intentional insider threats in North America were equally influenced by **misinformation or external radicalization** and **financial dissatisfaction**, according to 35% of CSOs surveyed.

The most crucial cutting-edge physical security technology 43% of security leaders in North America expect to invest in over the next two years is **AI-powered video surveillance and analytics**, followed by **AI-assisted threat intelligence and automated incident response**, according to 41% of CSOs.

United States

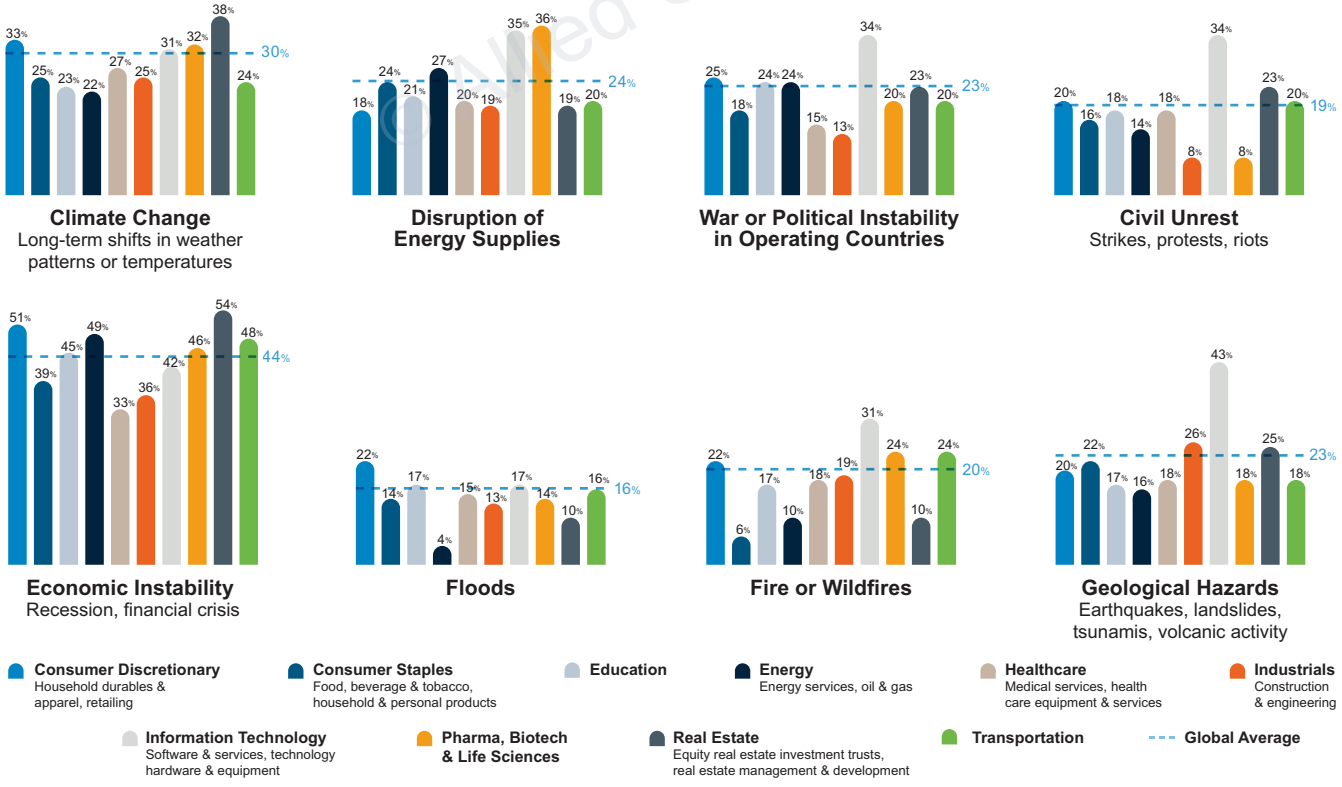
Representing the largest security market in the world, we surveyed 620 security chiefs based in the United States, from large and medium sized companies, across 10 different industries to better understand their similarities and differences.

Security-Impacting Hazards

Economic instability is the top security-impacting hazard for the next 12 months for all U.S. sectors with the exception of **information technology (IT)**, which views **geological hazards** as the top concern at 43% (23% U.S. average). Of all the industries, **real estate** is most concerned about economic instability at 54% (44% U.S. average).

Other hazards on the radar of U.S. companies include **disruption to energy supplies**, of which concern is highest in **pharmaceuticals** at 36% (24% U.S. sector average). Concern about **floods** is highest in the **consumer discretionary** sector at 22% (16% U.S. sector average) and concern about **fires or wildfires** is highest in **IT** at 31% (20% U.S. average).

Expected Security-Impacting Hazards Over the Next 12 Months



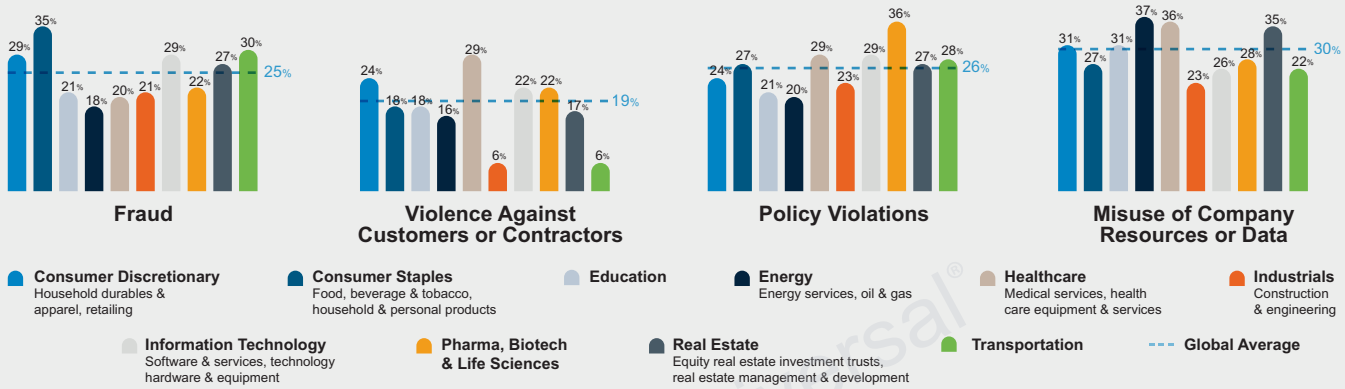
Q: What do you see as genuine security-impacting hazards for your company over the next 12 months?
Base: Chief security officers from large and medium sized companies based in the United States(n=620)

Internal Threats

Violence against customers or contractors as well as **violence against other employees** are two of the top concerns for both **healthcare** and **IT** companies during the next 12 months. **Unauthorized access to company data or networks** is the greatest concern in **education** at 41%, which is significantly higher than all other sectors (27% U.S. average).

Concern over **misuse of company resources or data** is highest in **energy** and **healthcare** at 37% and 36%, respectively (30% U.S. average). Apprehension over **fraud** is highest in **consumer staples** at 35% (24% U.S. sector average).

Expected Internal Security Incidents Over the Next 12 Months



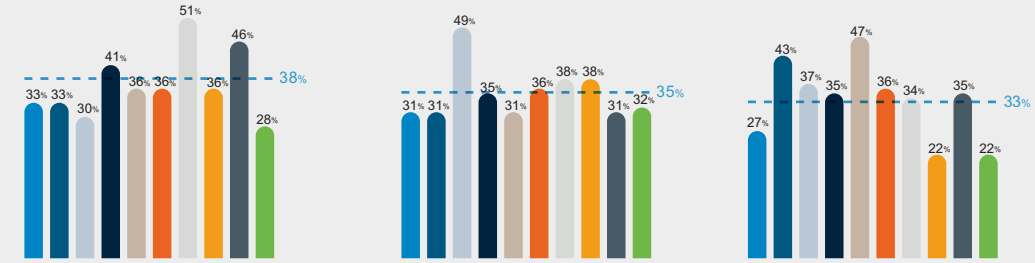
Q: What do you see as genuine internal security threats for your company over the next 12 months?
Base: Chief security officers from large and medium sized companies based in the United States (n=620)

Over half of security decision makers working in **IT**, at 51%, believe that **misinformation or external radicalization** are significant contributors to intentional insider threats (38% U.S. sector average).

Those in **healthcare** and **consumer staples** say **toxic workplace culture** is a key driver of intentional insider threats at 47% and 43%, respectively (33% U.S. average).

At 49%, more security chiefs in **education** than any other sector say that **financial dissatisfaction** significantly contributes to intentional insider threats (35% U.S. average). Those in **real estate** say the same about **financial stress**, at 42%, which is higher than all other sectors (36% U.S. average).

Factors that Contribute to Intentional Insider Threats



Q: Which of the following factors do you believe significantly contribute to intentional insider threats in their environment?
Base: Chief security officers from large and medium sized companies based in the United States (n=620)

External Threats

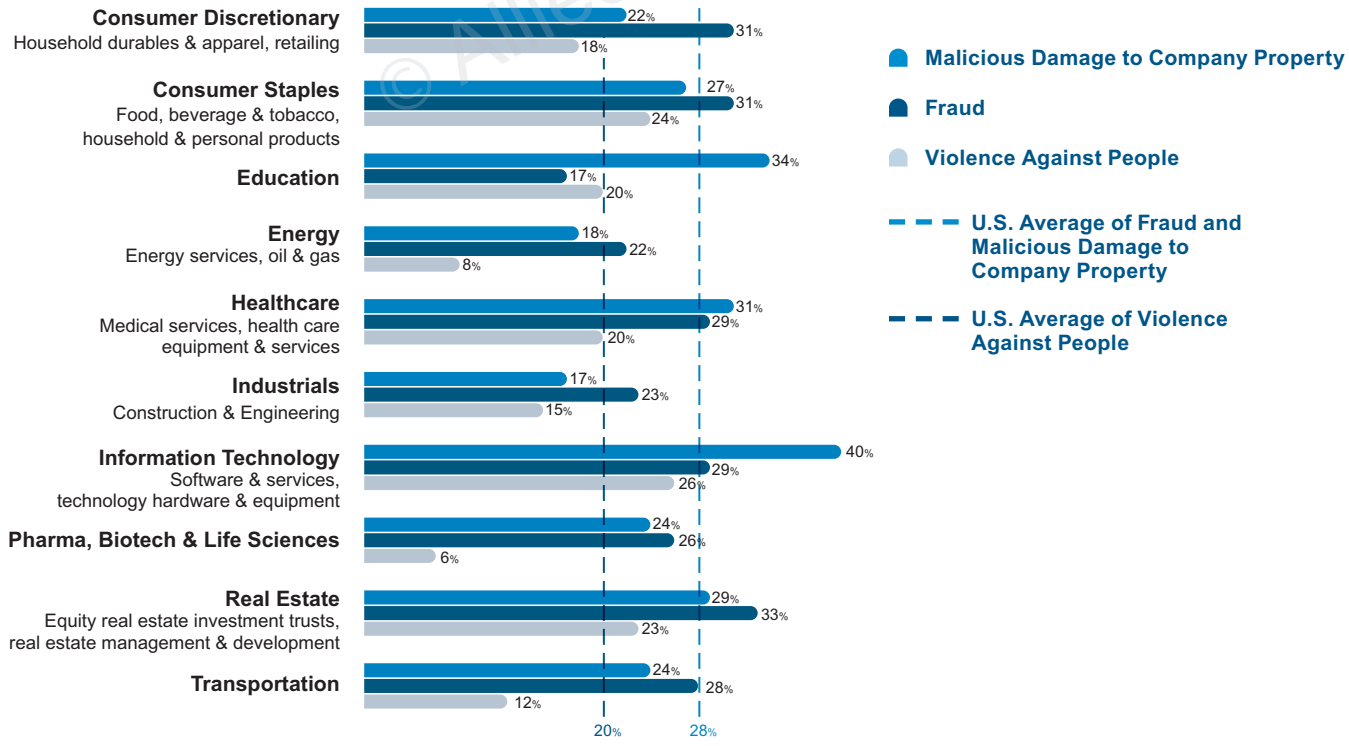
Malicious damage to company property is a top three concern across most sectors over the next 12 months but is highest in **IT** at 40% (28% U.S. average).

Theft of company physical property is most worrying for the **education** sector at 45% but is also a top concern for security chiefs in **industrials, pharmaceuticals** and **transportation** (31% U.S. average).

Fraud is more of a concern in **real estate** than all other sectors at 33%, followed by the **consumer discretionary** and **consumer staples sectors**, both at 31% (28% U.S. average). **Violence against people** is expected to be highest in **IT** and lowest in **pharmaceuticals**.

Expected External Security Incidents Over the Next 12 Months

Malicious Damage to Company Property, Fraud and Violence Against People



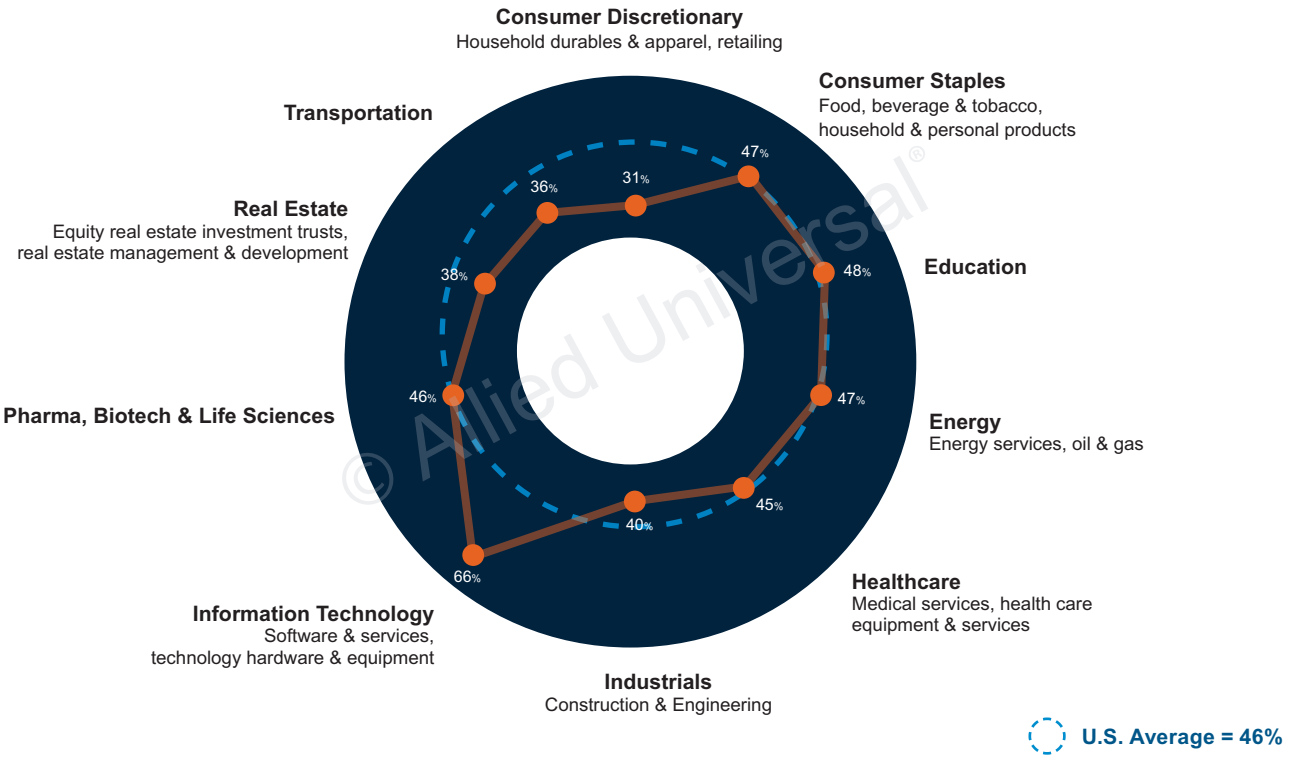
Q: What do you see as genuine external security threats for your company over the next 12 months?
Base: Chief security officers from large and medium sized companies based in the United States(n=620)

Nearly nine in 10 of those working in **IT** and **energy** say their company has been targeted by a misinformation or disinformation campaign in the past 12 months at 89% and 88%, respectively - this is higher than all other sectors (75% U.S. average). In contrast, at 58%, the **transportation** sector was the least targeted by false or deliberately misleading information.

Additionally, 63% of CSOs in **IT** said misinformation or disinformation influenced more than half of all threat actors targeting their company. The sector least likely to say this is **healthcare** at 27% (44% U.S. average).

Two-thirds of security chiefs working in **IT**, at 66%, say the threat of violence toward their company's executives has increased compared to two years ago, which is significantly higher than any other sector (46% U.S. average). In contrast, just under a third of those in **consumer discretionary** say the same, at 31%, which is the lowest of all sectors.

Increase in Threat of Violence Toward Executives Compared to Two Years Ago



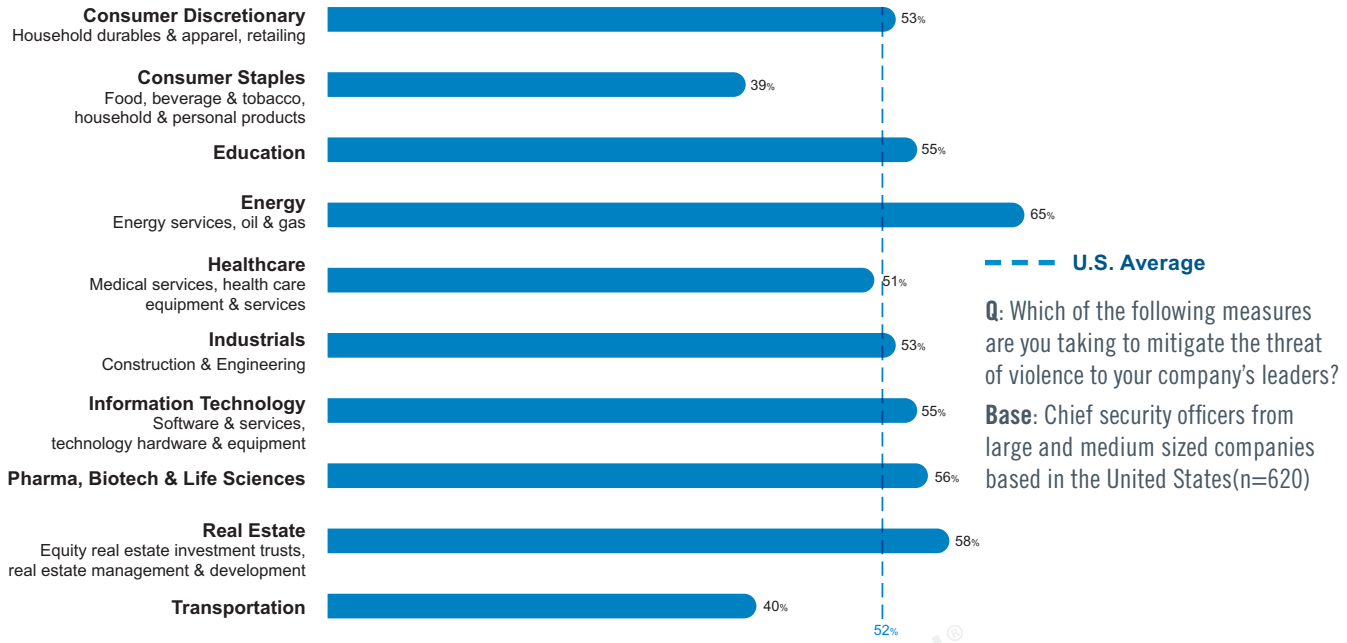
Q: How would you estimate the threat of violence towards your company's executives and senior leaders has changed compared to 2 years ago?
Base: Chief security officers from large and medium sized companies based in the United States(n=620)

Pharmaceuticals is one of the most proactive sectors when it comes to implementing executive protection measures and 62% are far more likely to conduct risk assessments to mitigate the threat of violence toward their leaders (44% U.S. average).

Leaders in **energy** are significantly more likely than the average to focus on enhanced security procedures at 65%, such as enhanced background checks (52% U.S. sector average).

Measures to Mitigate Threat of Violence Toward Executives

Enhanced Security Procedures



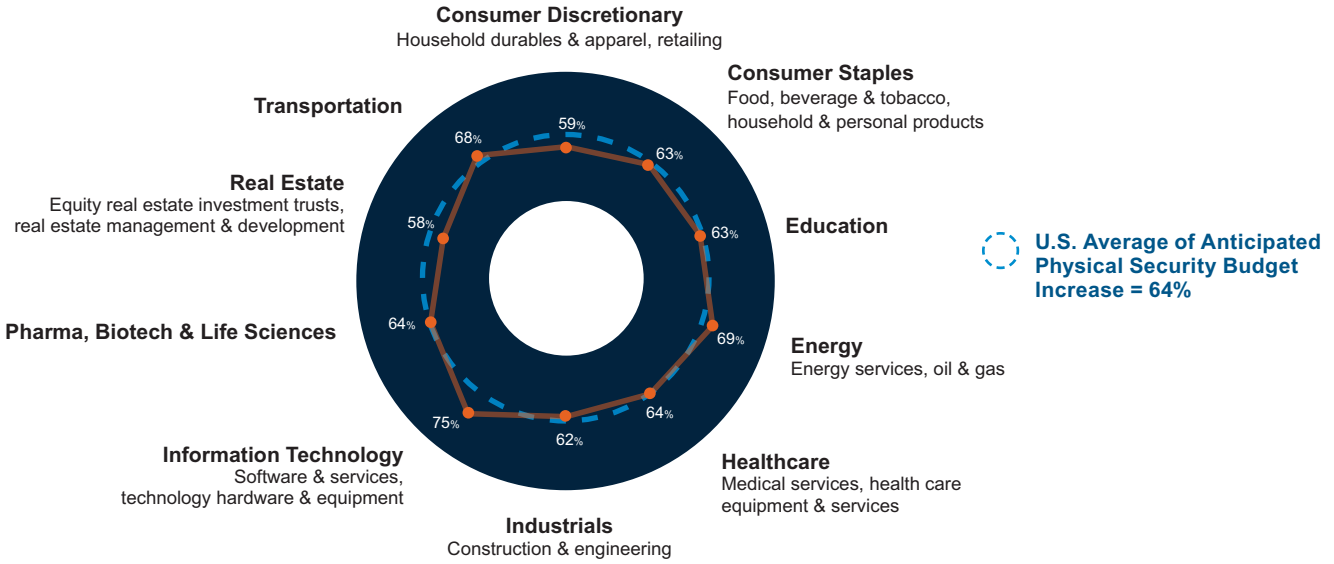
Q: Which of the following measures are you taking to mitigate the threat of violence to your company's leaders?

Base: Chief security officers from large and medium sized companies based in the United States(n=620)

Physical Security Budgets

IT, energy and **transportation** are the three sectors most anticipating an increase in physical security budgets over the next 12 months at 75%, 69% and 68%, respectively (64% U.S. average). **Employee security training and upskilling** is the top security budget priority for the next 12 months overall (46% U.S. average) and is highest in **real estate** at 63%.

Anticipated Physical Security Budget Increase Over the Next 12 month



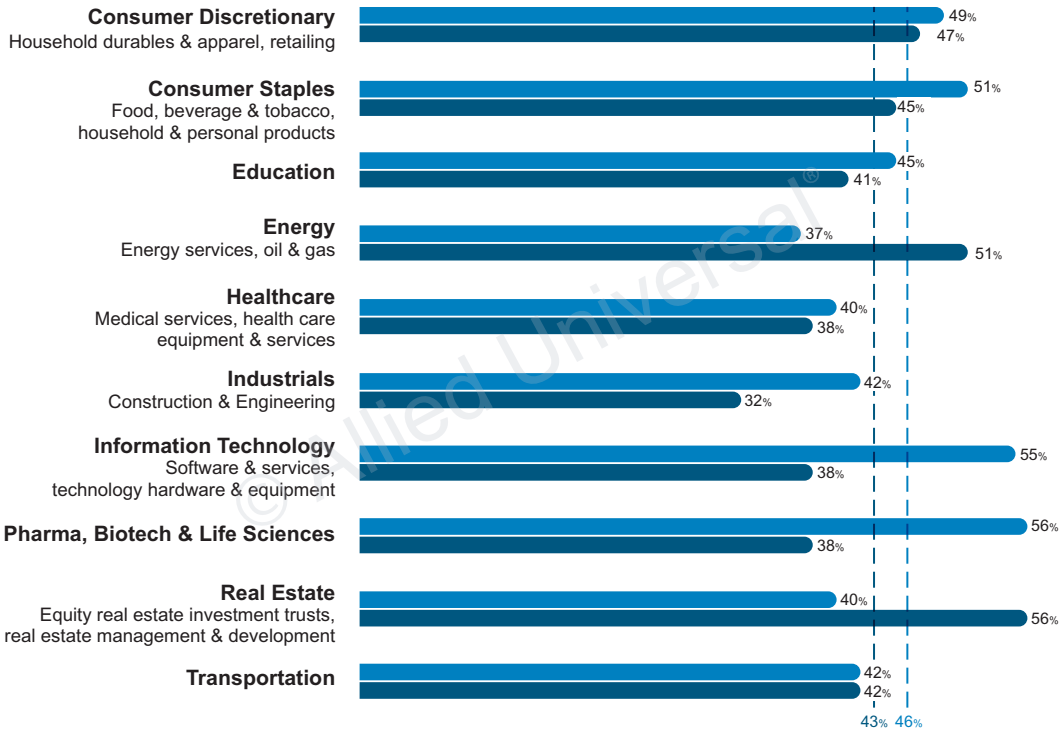
Q: How do you anticipate your physical security budget will change in the next 12 months?
Base: Chief security officers from large and medium sized companies based in the United States (n=620)

IT, real estate and **consumer staples** suffered the greatest negative revenue impact from physical security incidents at -21%, -17% and -16%, respectively (-16% U.S. average). More than a third of **IT** companies, at 37%, said they suffered a 25% or more loss in revenue (24% U.S. average).

Overall, **AI-powered video surveillance and analytics** and **AI-driven threat detection and risk assessment** are the two top cutting-edge technologies that are crucial to companies over the next two years. Use of AI-powered video surveillance is highest in **pharmaceuticals** at 56% (46% U.S. average) and use of AI-driven threat detection is expected to be the most widespread in **real estate** at 56% (43% U.S. average).

Crucial Cutting-Edge Technologies Over the Next Two Years

AI-Powered Video Surveillance and Analytics and AI-Driven Threat Detection and Risk Assessment



Q: Which of the following CUTTING-EDGE technologies would you classify as crucial for your operations over the next 2 years?
Base: Chief security officers from large and medium sized companies based in the United States(n=620)

Regional

Sub-Saharan Africa

Security-Impacting Hazards

In Sub-Saharan Africa, while **economic instability** is expected to be the top security-impacting hazard over the next year at 43%, **climate change** is anticipated to be a greater hazard in the region than anywhere else in the world at 42% (33% global average).

52%
say a driver of intentional insider threats was the influence of **misinformation or external radicalization**
(39% global average)

Next 12 Months

Sub-Saharan Africa **42%** vs **Global Average** **33%**
Say **climate change** will be a top security impacting hazard next year

Sub-Saharan Africa **40%** vs **Global Average** **30%**
Say **fraud** will be an external threat in the next 12 months

Sub-Saharan Africa **39%** vs **Global Average** **27%**
Say **fraud** will be an internal threat in the next 12 months

External Threats

Both external and internal **fraud** are likely to be substantially higher in Sub-Saharan Africa than all other regions at 40% and 39%, respectively (30% and 27% global averages). This was also true in 2023 when they stood at 34% and 37%, respectively.

The number of companies targeted by a misinformation or disinformation campaign in the last 12 months is 74% (73% global average). However, the region is the highest in the world for intentional insider threats that were influenced by **misinformation or external radicalization** at 52% (39% global average).

More CSOs than in any other region agree the **threat of violence toward company executives** has increased compared to two years ago at 33% (42% global average).

Internal Threats

Internal threats are expected to impact more companies in the region than any other. For example, **policy violations** stand at 36% (27% global average). More intentional insider threats than anywhere else in the world were influenced by **financial dissatisfaction** at 52% (36% global average).

52%

say a driver of intentional insider threats was the influence of **financial dissatisfaction**

(36% global average)

Investments

Sub-Saharan Africa **58%** VS **Global Average** **38%**

Say that the most crucial cutting-edge technology they expect to invest in over the next 2 years is **smart security infrastructure for buildings and public spaces**

Sub-Saharan Africa **81%** VS **Global Average** **66%**

Expect their physical security budget to increase

Sub-Saharan Africa **85%** VS **Global Average** **82%**

Agree that physical security should be a higher strategic priority within their business

Sub-Saharan Africa **92%** VS **Global Average** **87%**

Of CSOs in Sub-Saharan Africa agree that people will always be integral to keeping their organization safe

Physical Security Budgets

Physical security should have a higher strategic priority within their business, more CSOs in the region agreed than anywhere else in the world and tied with LATAM at 85% (82% global average).

Supporting that, physical security budgets are expected to increase significantly more here than all other regions at 81% (66% global average). Investment in **new security technology and infrastructure** is the top security budget priority over the next 12 months at 71% (47% global average), which is higher than anywhere else.

In terms of cutting-edge technologies, far more companies in Sub-Saharan Africa expect to invest in **smart security infrastructure for buildings and public spaces** than anywhere else in the world over the next two years at 58% (39% global average). Just over half (52%) also expect to invest in **AI-powered video surveillance and analytics and biometric access control**, which similarly is higher than any other region.

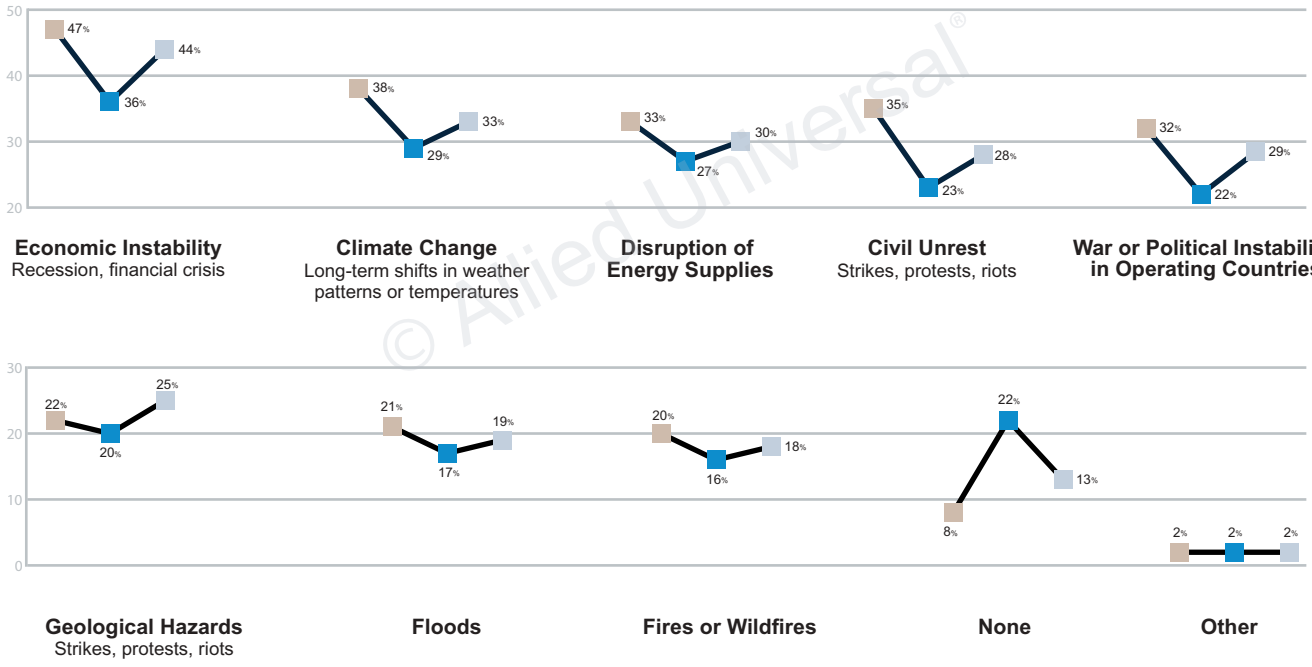
There are greater demands on frontline security professionals than there were five years ago, more CSOs in Sub-Saharan Africa agree than any other region at 90% (83% global average).

Alongside LATAM, Sub-Saharan Africa is the top region in the world for CSOs to agree that people will always be integral to keeping their organization safe at 92% (87% global average).

Charts
Chapter 1

Emerging and Evolving Threats: Economic and Geopolitical Impacts

Security-Impacting Hazards Expected vs. Experienced
Global Average



CSO Survey 2025

Q: What do you see as genuine security-impacting hazards for your company over the next 12 months?

Q: Has your company experienced any of the following security impacting-hazards in the last 12 months?

Base: Chief security officers from large companies (Global n=2352)

CSO Survey 2023

Q: Which of the following do you see as genuine security-impacting hazards for your company over the next 12 months?

Base: Chief security officers from large companies (Global n=1775)

Top 5 Most Expected Security-Impacting Hazards
2025 vs. Experienced in 2024 Regional Comparison

	APAC		Europe		LATAM		Middle East		North America		Sub-Saharan Africa	
	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected
Economic Instability Recession, financial crisis	42% ↑	53%	36% ↑	41%	26% ↑	41%	38% ↑	41%	28% ↑	42%	39% ↑	43%
Climate Change Long-term shifts in weather patterns or temperatures	34% ↑	37%	24% ↑	29%	24% ↑	28%	41% ↓	37%	20% ↑	27%	34% ↑	42%
Disruption of Energy Supplies	26% ↑	30%	19% ↑	29%	29% ↑	31%	30% ↑	32%	22% ↑	23%	41% ↓	32%
War or Political Instability in Operating Countries	28% ↑	33%	22% ↑	28%	16% ↑	26%	21% ↑	38%	19% ↑	22%	22% ↑	29%
Civil Unrest Strikes, protests, riots	25% ↑	30%	22% ↑	25%	18% ↑	26%	28% ↑	33%	17% ↑	18%	27% ↑	33%

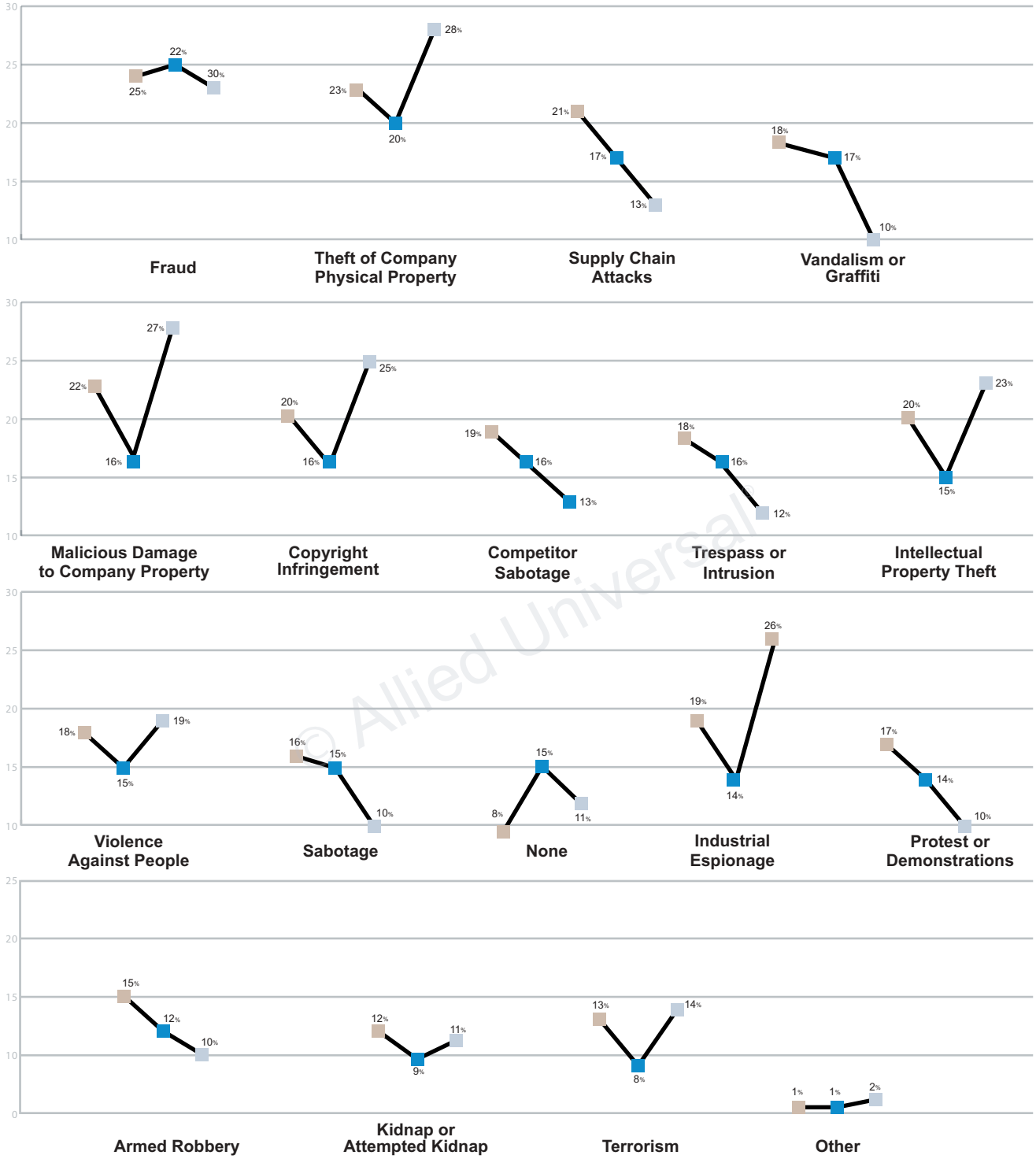
Q: What do you see as genuine security-impacting hazards for your company over the next 12 months?
Q: Has your company experienced any of the following security-impacting hazards in the last 12 months?
Base: Chief security officers from medium and large companies (Global n=2352). APAC (n=464), Europe (n=464), LATAM (n=290), Middle East (n=232), North America (n=678), Sub-Saharan Africa (n=174)

Top 5 Most Expected External Threats
2025 vs. Experienced in 2024 Regional Comparison

	APAC		Europe		LATAM		Middle East		North America		Sub-Saharan Africa	
	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected
Fraud	22% ↑	27%	20% ↑	29%	16% ↑	30%	23% ↑	33%	22% ↑	29%	36% ↑	40%
Theft of Company Physical Property	18% ↑	30%	19% ↑	24%	18% ↑	26%	19% ↑	31%	22% ↑	28%	33% ↑	31%
Malicious Damage to Company Property	17% ↑	27%	15% ↑	23%	15% ↑	27%	16% ↑	39%	15% ↑	25%	17% ↑	20%
Industrial Espionage	16% ↑	28%	13% ↑	23%	16% ↑	29%	19% ↑	33%	9% ↑	16%	10% ↑	20%
Copyright Infringement	21% ↑	27%	15% ↑	21%	6% ↑	18%	22% ↑	38%	15% ↑	24%	14% ↑	25%

Q: What do you see as genuine external security threats for your company over the next 12 months?
Q: What types of external security incidents has your company experienced in the last 12 months?
Base: Chief security officers from medium and large companies (Global n=2352). APAC (n=464), Europe (n=464), LATAM (n=290), Middle East (n=232), North America (n=678), Sub-Saharan Africa (n=174)

External Threats Expected vs. Experienced
Global Average



CSO Survey 2025

Q: What do you see as genuine external security threats for your company over the next 12 months?
Q: What external security threats has your company experienced in the last 12 months?
Base: Chief security officers from large companies (Global n=2352)

CSO Survey 2023

Q: Which of the following do you see as genuine external security threats for your company over the next 12 months?
Base: Chief security officers from large companies (Global n=1775)

Internal Threats Expected vs. Experienced
Global Average

	2023 Expected	2024 Experienced	2025 Expected
Leaking Sensitive Information	36%	31%	32%
Policy Violations	29%	29%	27%
Misuse of Company Resources or Data	35%	29%	27%
Fraud	31%	27%	27%
Unauthorized Access to Company Data or Networks	34%	27%	28%
Theft of Company Physical Property	29%	26%	24%
Malicious Damage to Company Property	25%	23%	20%
Intellectual Property Theft	27%	20%	22%
Copyright Infringement	25%	19%	21%
Violence Against Other Employees	25%	19%	16%
Industrial Espionage	24%	18%	20%
Violence Against Customers or Contractors	NA	18%	17%
Sabotage	22%	16%	19%
None	8%	15%	13%
Other	1%	2%	1%

CSO Survey 2025
Q: What do you see as genuine internal security threats for your company over the next 12 months?
Q: What internal security threats has your company experienced in the last 12 months?
Base: Chief security officers from large companies (Global n=2352)

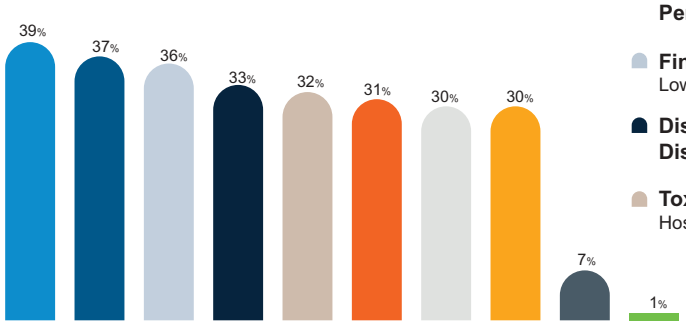
CSO Survey 2023
Q: Which of the following do you see as genuine internal security threats for your company over the next 12 months?
Base: Chief security officers from large companies (Global n=1775)

Top 5 Most Expected Internal Threats
2025 vs. Experienced in 2024 - Regional Comparison

	APAC		Europe		LATAM		Middle East		North America		Sub-Saharan Africa	
	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected	2024 Experienced	2025 Expected
Leaking Sensitive Information	34% –	34%	28% –	28%	29% ↑	31%	32% ↑	33%	26% ↑	30%	35% –	35%
Unauthorized Access to Company Data or Networks	32% ↓	31%	24% ↑	26%	24% –	24%	25% ↑	31%	27% ↓	26%	25% ↑	30%
Fraud	21% –	21%	28% ↓	24%	27% ↑	34%	27% ↓	26%	29% ↓	28%	42% ↓	39%
Policy Violations	33% ↓	31%	27% ↓	23%	22% –	22%	29% ↓	28%	29% ↓	23%	38% ↓	36%
Misuse of Company Resources or Data	33% ↓	32%	21% –	21%	26% –	26%	32% ↓	30%	26% ↑	28%	38% ↓	34%

Q: What do you see as genuine internal security threats for your company over the next 12 months?
Q: What internal security threats has your company experienced in the last 12 months?
Base: Chief security officers from medium and large companies (Global n=2352). APAC (n=464), Europe (n=464), LATAM (n=290), Middle East (n=232), North America (n=678), Sub-Saharan Africa (n=174)

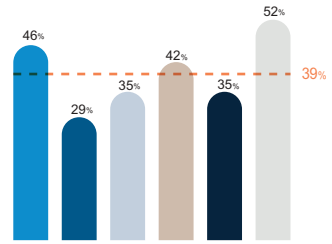
Factors that Contribute to Intentional Insider Threats
Global Average



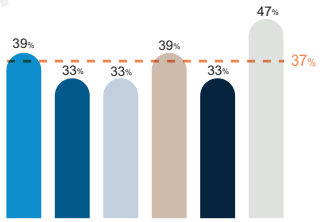
- **Influenced by Misinformation or External Radicalization**
- **Financial Stress or Personal Debt**
- **Financial Dissatisfaction**
  Low pay, lack of bonuses or incentives
- **Disengagement or Dissatisfaction with Work**
- **Toxic Workplace Culture**
  Hostility, lack of trust
- **Ideological or Political Motivations**
- **Poor Working Conditions or Lack of Career Growth**
- **Revenue Against Employer or Management**
- **None of the Above**
- **Other**

Q: Which of the following factors do you believe significantly contribute to intentional insider threats in their environment?
Base: Chief security officers from large companies (Global n=2352)

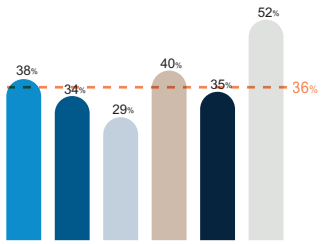
Top 5 Factors that Contribute to Intentional Insider Threats
Regional Comparison



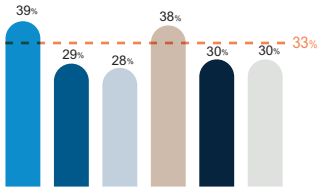
Influenced by Misinformation or External Radicalization



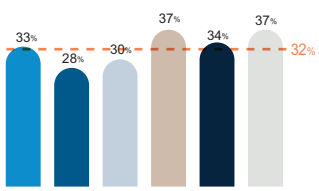
Financial Stress or Personal Debt



Financial Dissatisfaction
Low pay, lack of bonuses or incentives



Disengagement or Dissatisfaction with Work

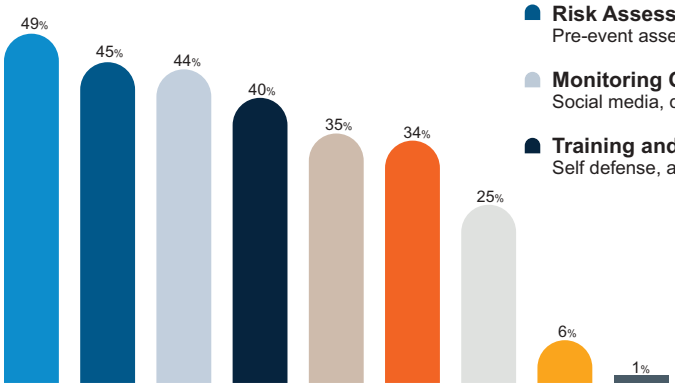


Toxic Workplace Culture
Hostility, lack of trust

APAC **Europe** **LATAM** **Middle East** **North America** **Sub-Saharan Africa** **Global Average**

Q: Which of the following factors do you believe significantly contribute to intentional insider threats in their environment?
Base: Chief security officers from medium and large companies (Global n=2352). APAC (n=464), Europe (n=464), LATAM (n=290), Middle East (n=232), North America (n=678), Sub-Saharan Africa (n=174)

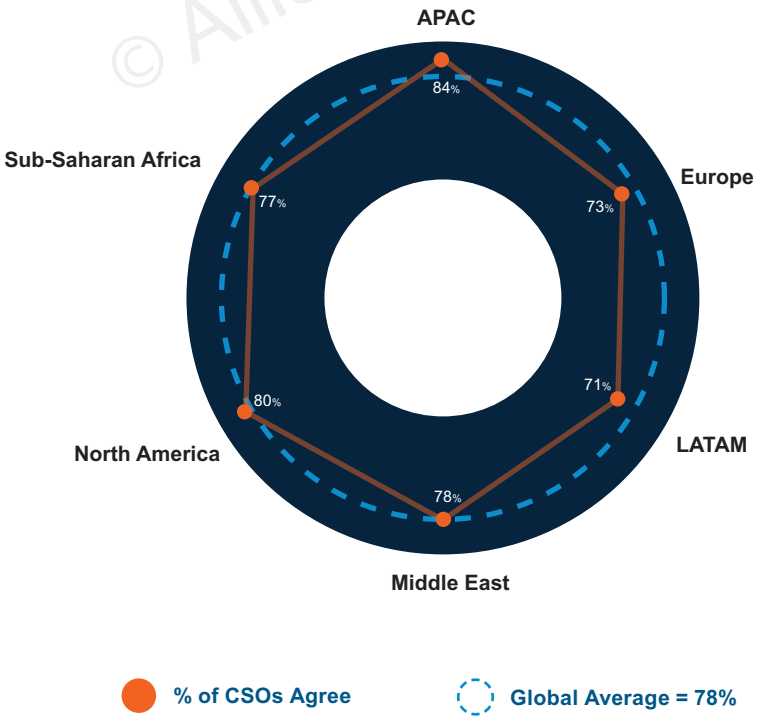
Measures to Mitigate the Threat of Violence to Leaders
Global Average



- **Enhanced Security Procedures**
  Enhanced background checks, on site firearms or explosives screening
- **Risk Assessment for Leaders**
  Pre-event assessments, travel risk management
- **Monitoring Online Threats**
  Social media, dark web, etc.
- **Training and Preparedness for Leaders**
  Self defense, awareness, or de-escalation
- **Providing Leaders Personal or Close Security Personnel**
- **Providing Leaders Personal Protective Equipment**
  Body armor, emergency escape masks
- **Family Protection For Leaders**
- **No Changes Planned**
- **Other**

Q: Which of the following measures are you taking to mitigate the threat of violence to your company's leaders?
Base: Chief security officers from large companies (Global n=2352)

Impact of Geopolitical Tensions on Supply Chain Security
Regional Comparison



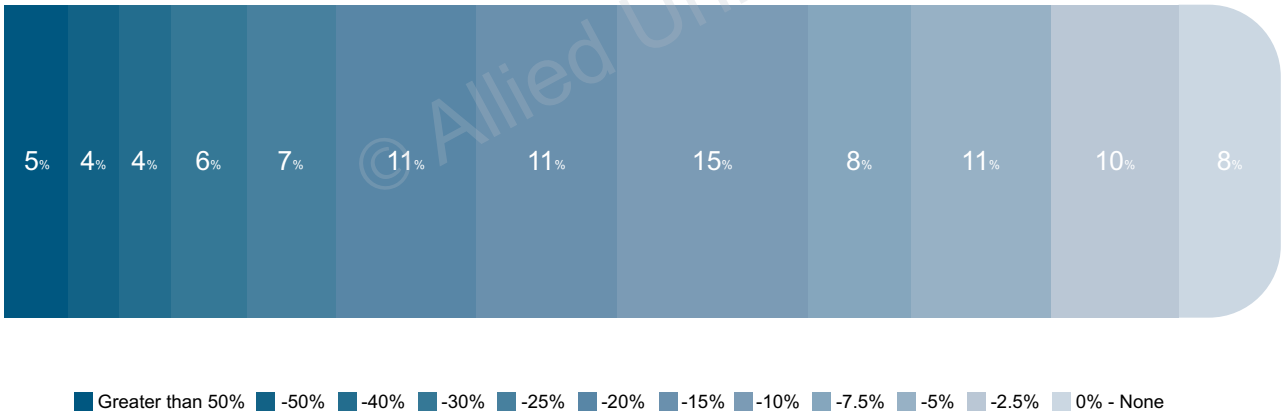
Q: Geopolitical tension will compromise the security of our supply chain over the next 12 months? (Respondents who agreed with this statement.)
Base: Chief security officers from medium and large companies (Global n=2352). APAC (n=464), Europe (n=464), LATAM (n=290), Middle East (n=232), North America (n=678), Sub-Saharan Africa (n=174)

Appendix

Charts
Chapter 2

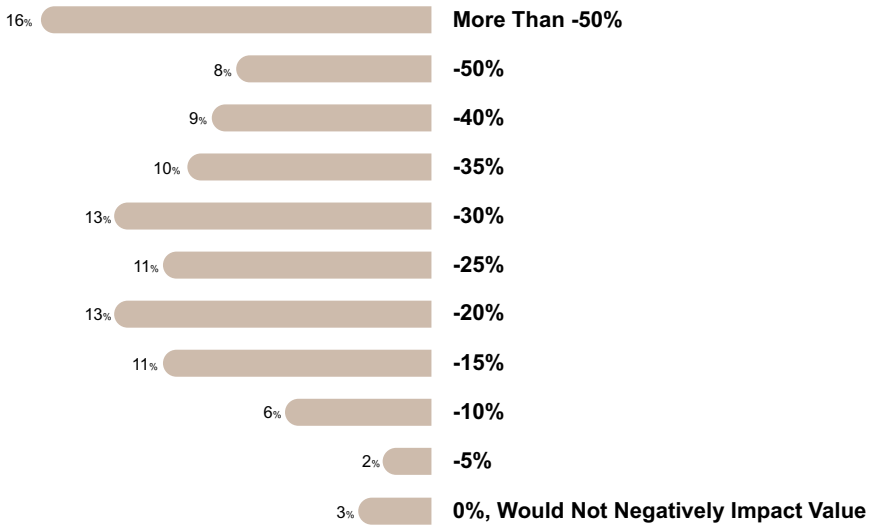
Physical Security:
A Strategic Imperative and Value Driver

Impact of Physical Security Incidents on Revenue
Global Average



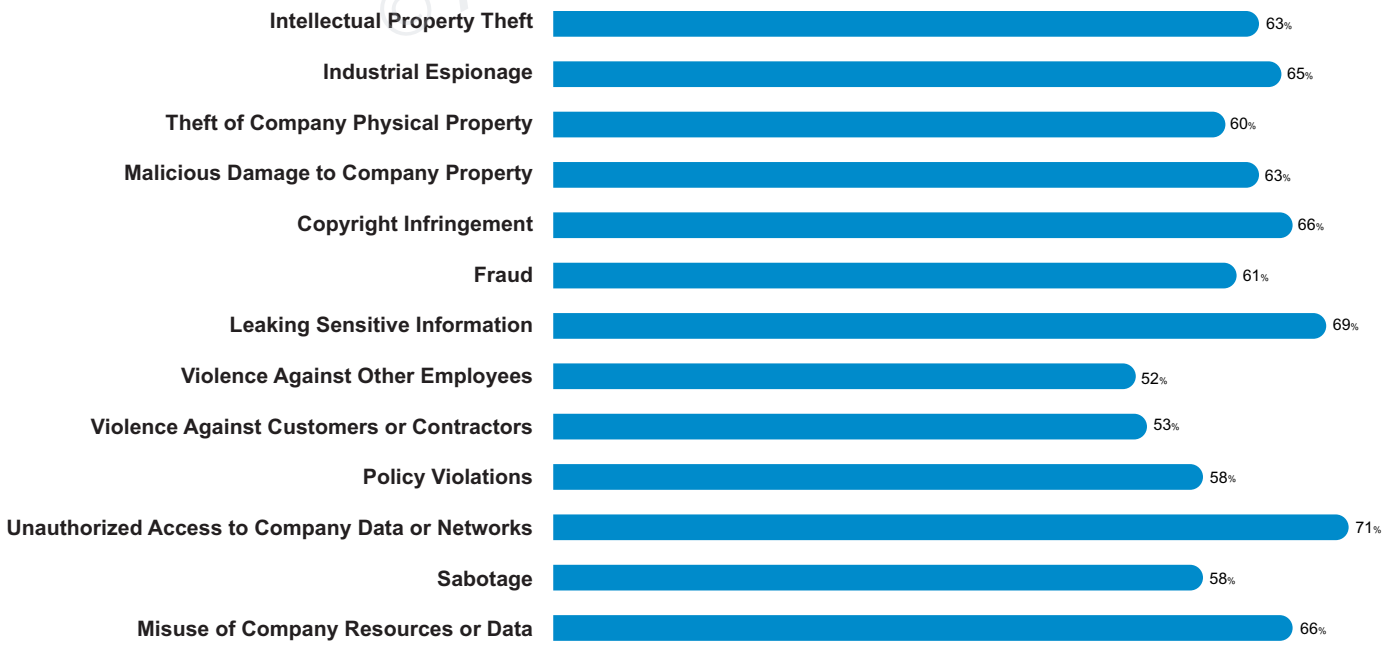
Q: What do you consider has been the negative impact of the following security incidents to revenue overall (cyber and physical)?
Base: Chief security officers from large companies (Global n=2352)

Financial Impact of a Security Incident on a Publicly Listed Company



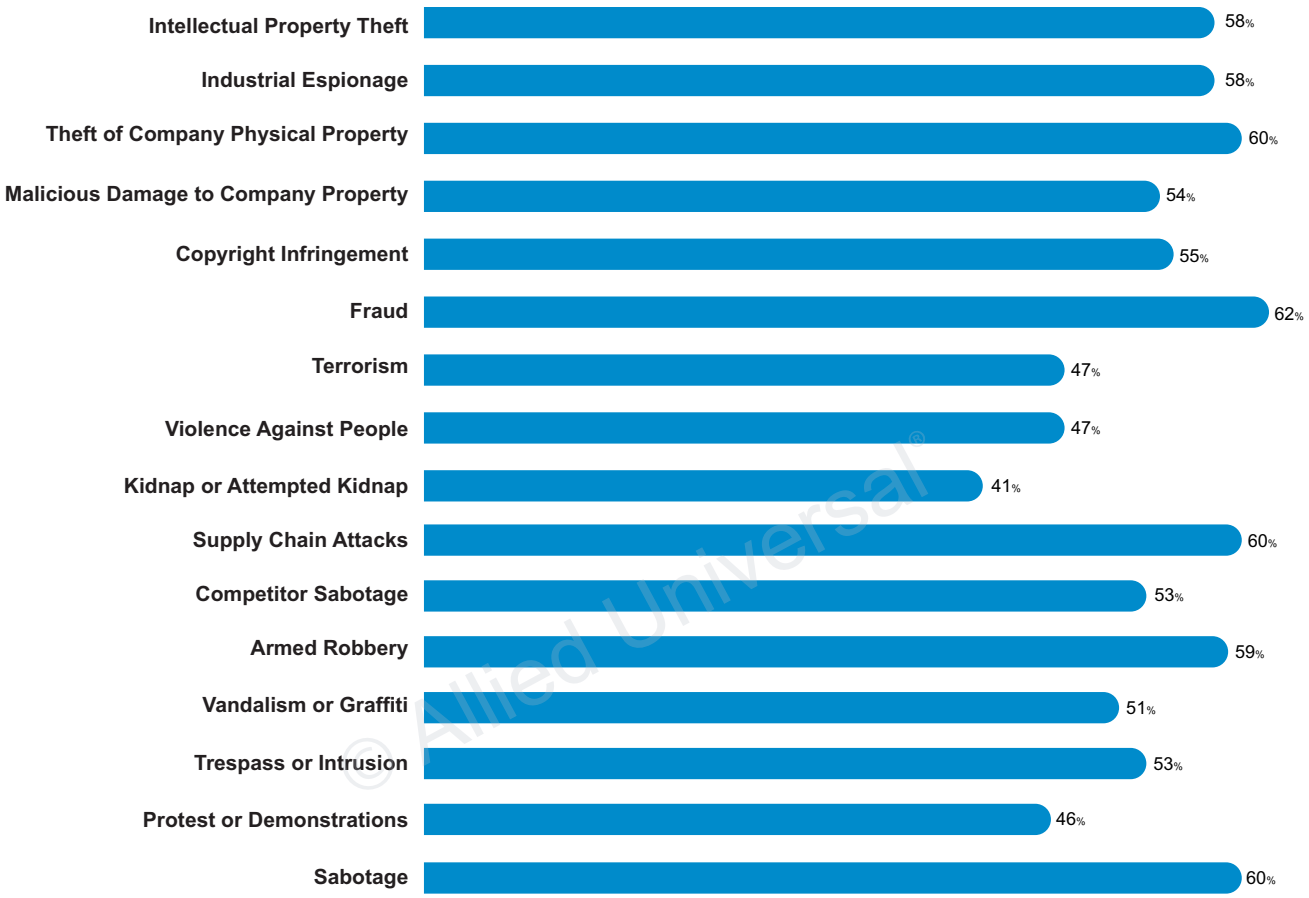
Q: What would you expect to happen to the value of a publicly listed company that experienced a significant internal or external security incident?
Base: Global institutional investors (n=200)

Influence of Internal Security Incidents Experienced on Budgets
Global Average



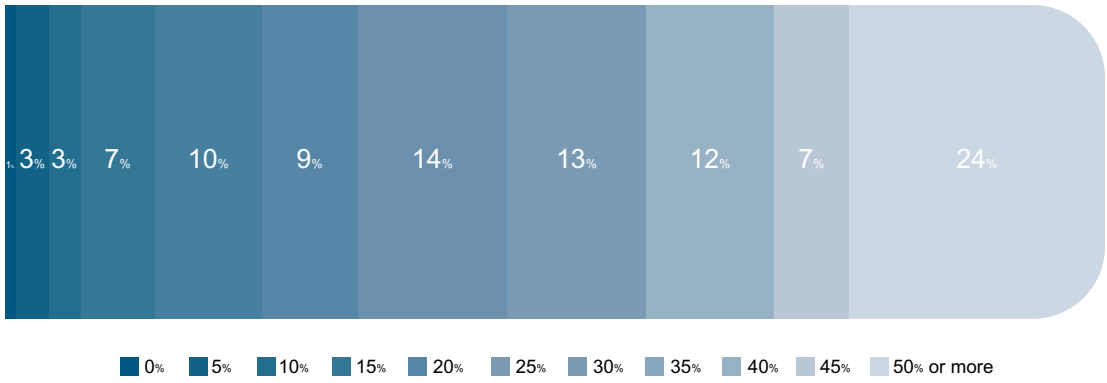
Q: Which of the following internal incidents most influenced the increase in budget?
Base: Chief security officers from large companies (Global n=2352). Percentages displayed in the graph are based on those who experienced these security incidents in the last year.

Influence of External Security Incidents Experienced on Budgets
Global Average



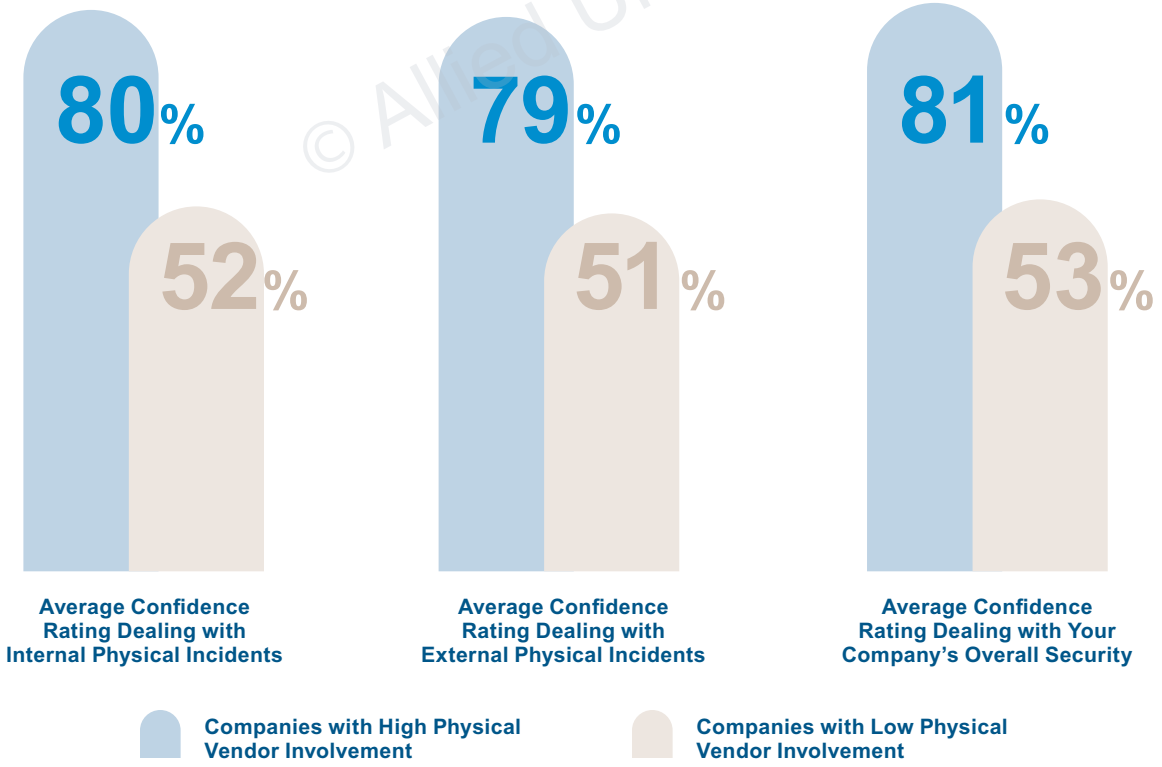
Q: Which of the following external incidents most influenced the increase in budget?
Base: Chief security officers from Large Companies (Global N=2352). Percentages displayed in the graph are based on those who experienced these security incidents in the last year.

Key Executives' Contributions Represent



Q: Thinking of an executive's contributions to strategic decisions, leadership, and innovation, how much of a company's overall value do you think its key executives (e.g., CEO, CFO, etc) represent?
Base: Global institutional investors (n=200)

Confidence in Dealing with Threats vs. Level of Vendor Involvement
Global Average



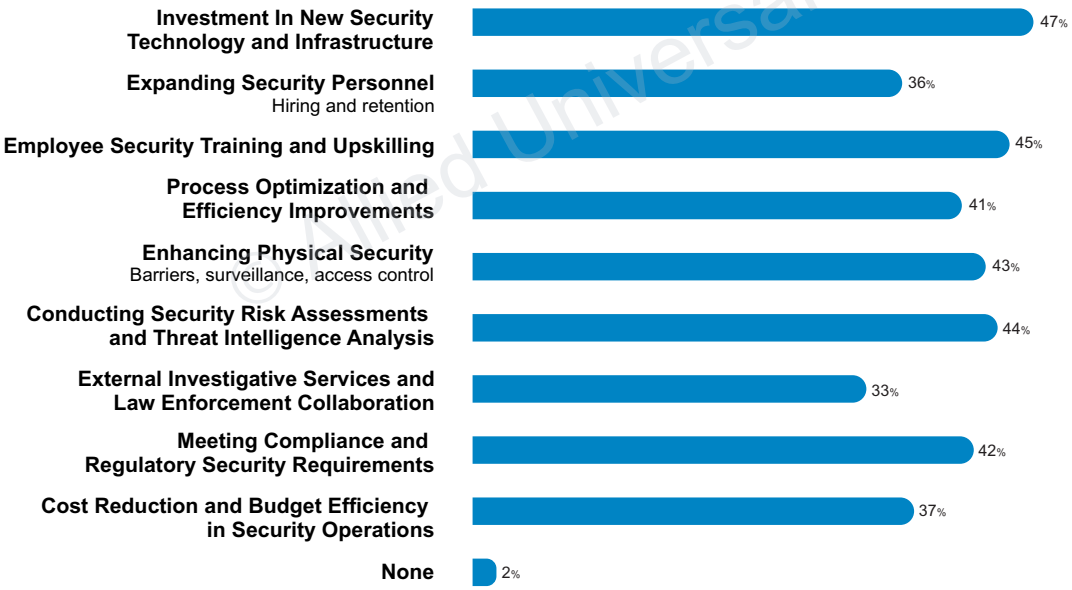
Q: Approximately what percentage of your overall security is provided by third-party vendors?
Q: Using the dropdown scale below, please rate how confident you are with your company being able to adequately deal with the following security issues/risks?
Base: Chief security officers from Large Companies (Global N=2352)

Appendix

Charts
Chapter 3

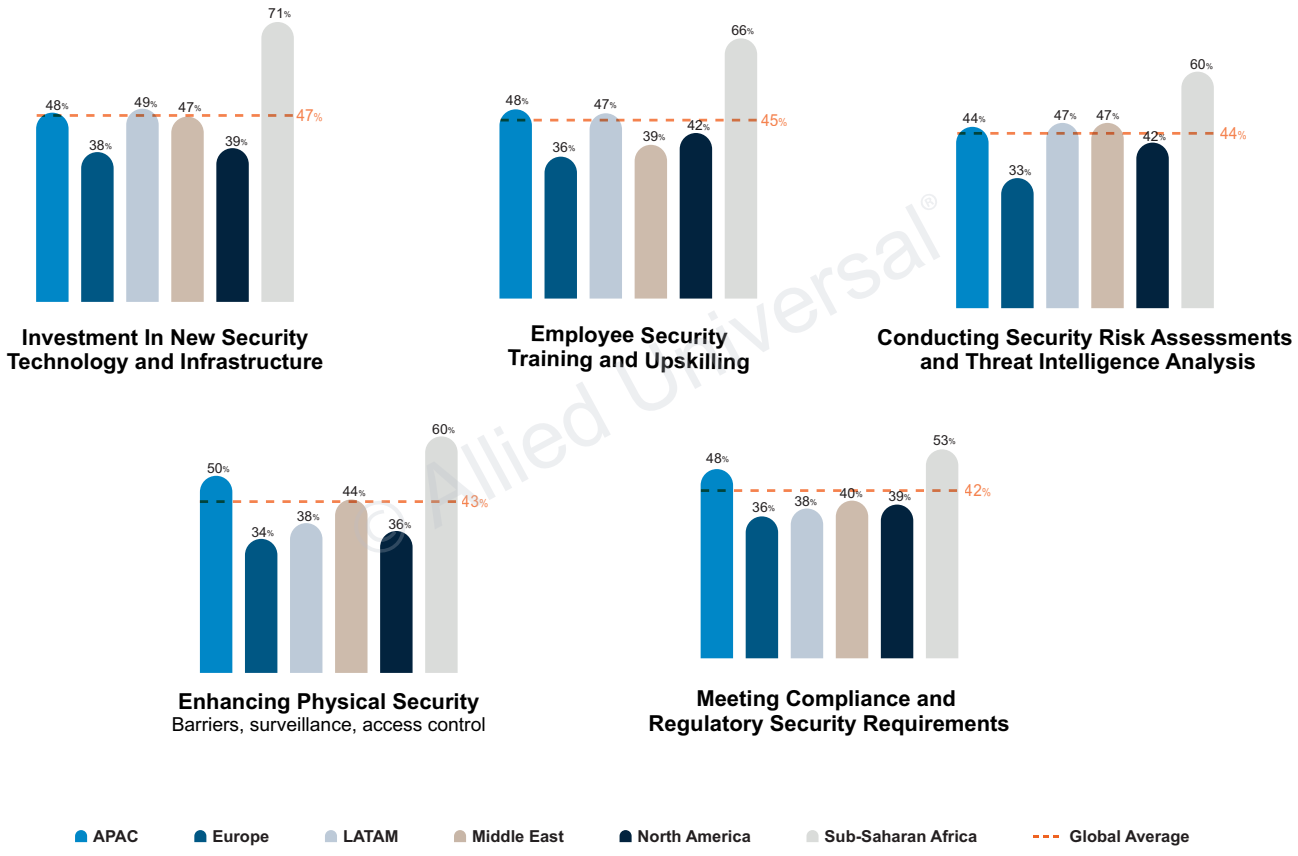
The Changing Security Workforce: Culture, Competence and Capacity

Security Budget Priorities
Global Average



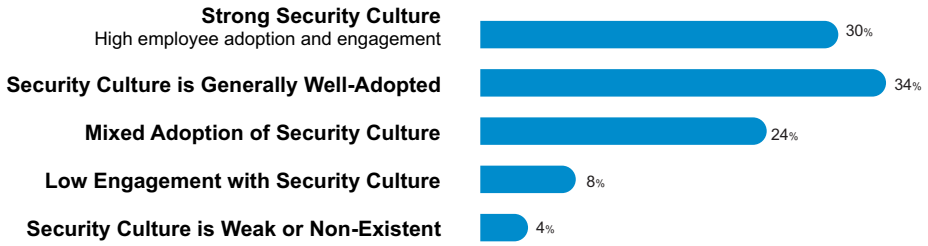
Q: What are your company's top security budget priorities for the next 12 months?
Base: Chief security officers from large companies (Global n=2352)

Top 5 Security Budget Priorities
Regional Comparison



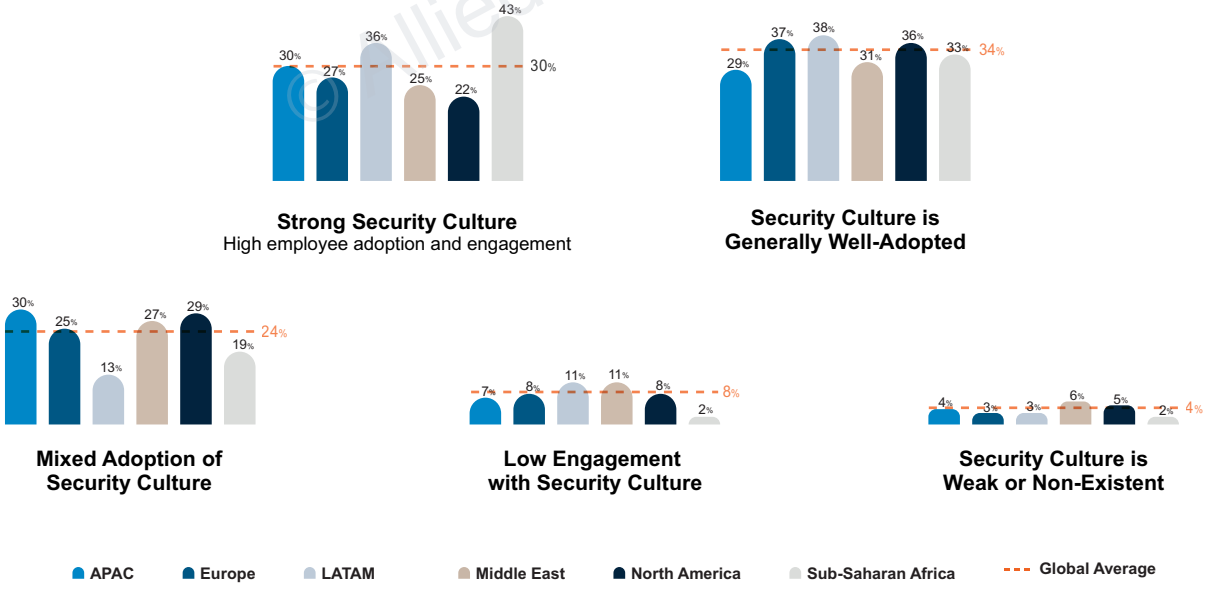
Q: What are your company's top security budget priorities for the next 12 months?
Base: Chief security officers from medium and large companies (Global n=2352). APAC (n=464), Europe (n=464), LATAM (n=290), Middle East (n=232), North America (n=678), Sub-Saharan Africa (n=174)

Adoption of Security Policies
Global Average



Q: How would you rate employee adoption of security policies and best practices in your company?
Base: Chief security officers from large companies (Global n=2352)

Adoption of Security Policies
Regional Comparison



Q: How would you rate employee adoption of security policies and best practices in your company?
Base: Chief security officers from medium and large companies (Global n=2352). APAC (n=464), Europe (n=464), LATAM (n=290), Middle East (n=232), North America (n=678), Sub-Saharan Africa (n=174)

Driving Factors of New Security Technology
Global Average

Q: What factors are driving your company's adoption of new security technology?
Base: Chief Security Officers from Large Companies (Global N=2352)

Security Culture
Regional Comparison

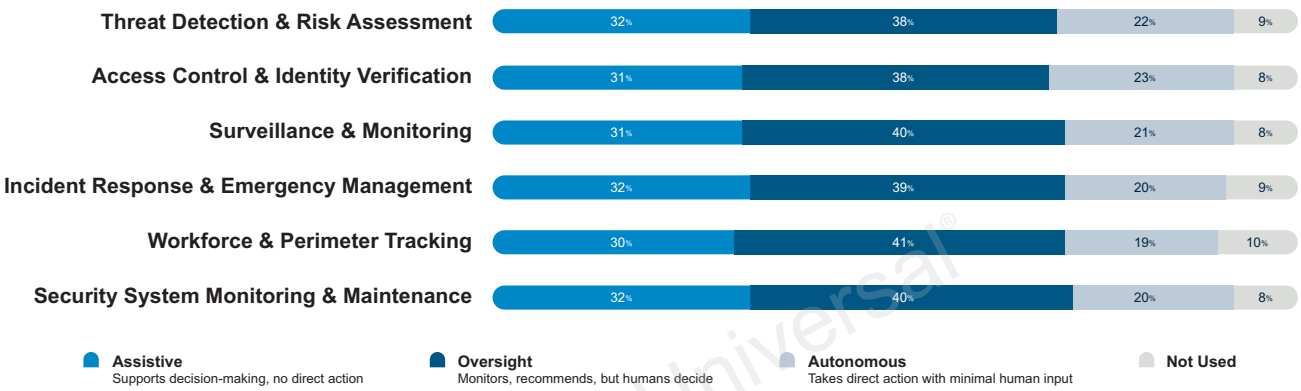
Q: How would you rate employee adoption of security policies and best practices in your company?
Base: Chief security officers from medium and large companies (Global n=2352). APAC (n=464), Europe (n=464), LATAM (n=290), Middle East (n=232), North America (n=678), Sub-Saharan Africa (n=174)

Appendix

Charts
Chapter 4

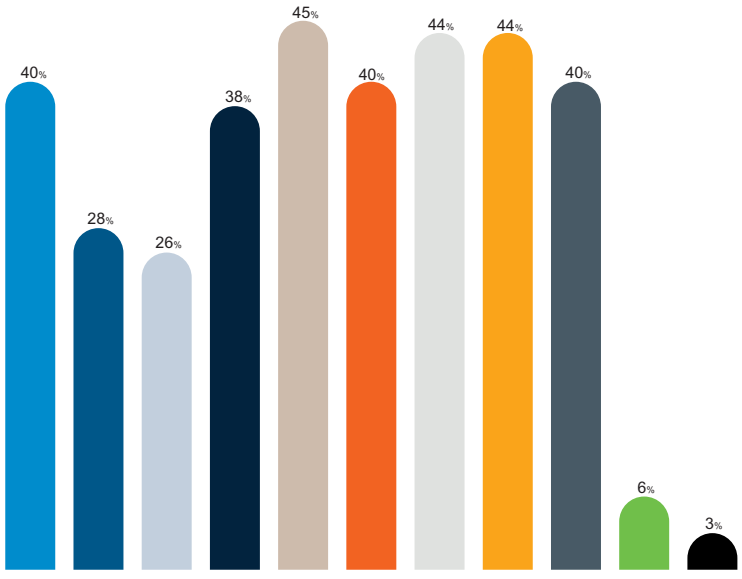
AI and Tech: A Reality Check

Current Use of AI
Global Average



Q: How is AI currently being used in your company to help with the following?
Base: Chief security officers from large companies (Global n=2352)

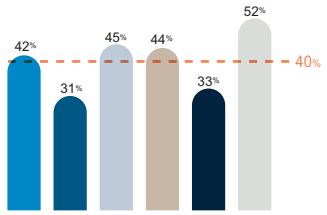
Crucial Cutting-Edge Technologies Over the Next Two Years
Global Average



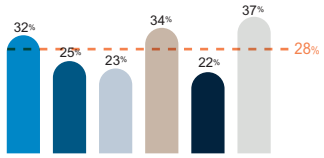
- **Biometric Access Control** Including facial recognition
- **Robotics and Autonomous Security Patrols**
- **Drones and Unmanned Aerial Systems (UAS)**
- **Smart Security Infrastructure for Buildings and Public Spaces**
- **AI-Powered Intrusion Detection and Perimeter Security**
- **Internet Of Things (IOT) - Enabled Security Devices and Sensors**
- **AI-Driven Threat Detection and Risk Assessment**
- **AI-Powered Video Surveillance and Analytics**
- **AI-Assisted Threat Intelligence and Automated Incident Response**
- **Other Technological Advancements**
- **None**

Q: Which of the following cutting-edge technologies would you classify as crucial for your operations over the next 2 years?
Base: Chief security officers from large companies (Global n=2352)

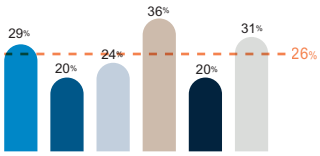
Crucial Cutting-Edge Technologies Over the Next Two Years
Regional Comparison



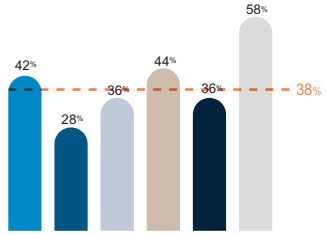
Biometric Access Control
Including facial recognition



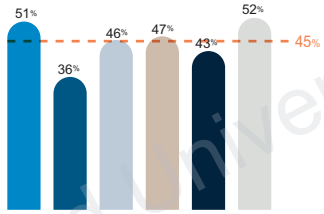
Robotics and Autonomous Security Patrols



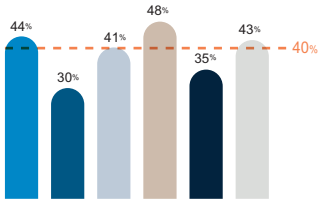
Drones and Unmanned Aerial Systems (UAS)



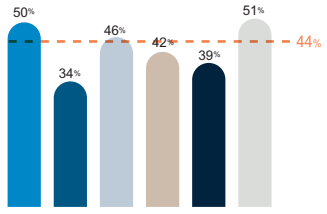
Smart Security Infrastructure for Buildings and Public Spaces



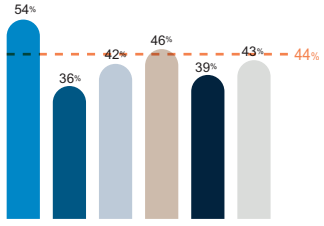
AI-Powered Video Surveillance and Analytics



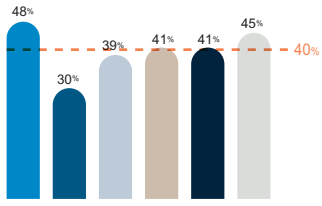
Internet Of Things (IOT) - Enabled Security Devices and Sensors



AI-Driven Threat Detection and Risk Assessment



AI-Powered Intrusion Detection and Perimeter Security



AI-Assisted Threat Intelligence and Automated Incident Response

APAC | Europe | LATAM | Middle East | North America | Sub-Saharan Africa | Global Average

Q: Which of the following cutting-edge technologies would you classify as crucial for your operations over the next 2 years?
Base: Chief security officers from medium and large companies (Global n=2352). APAC (n=464), Europe (n=464), LATAM (n=290), Middle East (n=232), North America (n=678), Sub-Saharan Africa (n=174)

World Security Report

Methodology

This report includes insights from two key audiences. Both audiences completed a quantitative online survey.

Audience 1: Security Decision Makers

Profile: Physical security decision makers for large and medium companies across 31 markets

Number of Respondents: n=2,352 (2023: n=1,775)

Date of Research: March 21 - April 16, 2025

Weighting: The data was weighted to ensure comparability with the 2023 results. Each country was weighted to have the same representation in the aggregated total, with the exception of the U.S. which was double.

Audience 2: Global Institutional Investors

Profile: Global institutional investors managing $1 trillion in assets

Number of Respondents: n=200 (2023: n=200)

Date of Research: April 8 - 14, 2025

Global Survey Conducted by

FTI CONSULTING

ALLIED UNIVERSAL®
There for you.

G4S
An ALLIED UNIVERSAL Company

About World Security Report

This landmark research is an independent, anonymous survey of 2,352 chief security officers (CSOs) from 31 countries representing companies with combined revenue of more than $25 trillion. Additionally, the report gathers views from 200 global institutional investors who manage over $1 trillion in assets.

About Allied Universal

Allied Universal® is the world's leading security and facility services provider, trusted by over 400 *Fortune* 500 companies. With operations in more than 100 countries, we deliver robust security services, cutting-edge AI-powered technology, and tailored solutions that give our clients the confidence to focus on their core business. Our commitment to innovation, value, and customer relationships drives our mission of helping to protect people, businesses, and communities. Our excellence begins with strong local leadership and presence, as we deliver on the promise of our integrated security solutions. At Allied Universal, we are dedicated to security and safety, enabling our clients to thrive. For more information, visit aus.com.

World Security Report.com