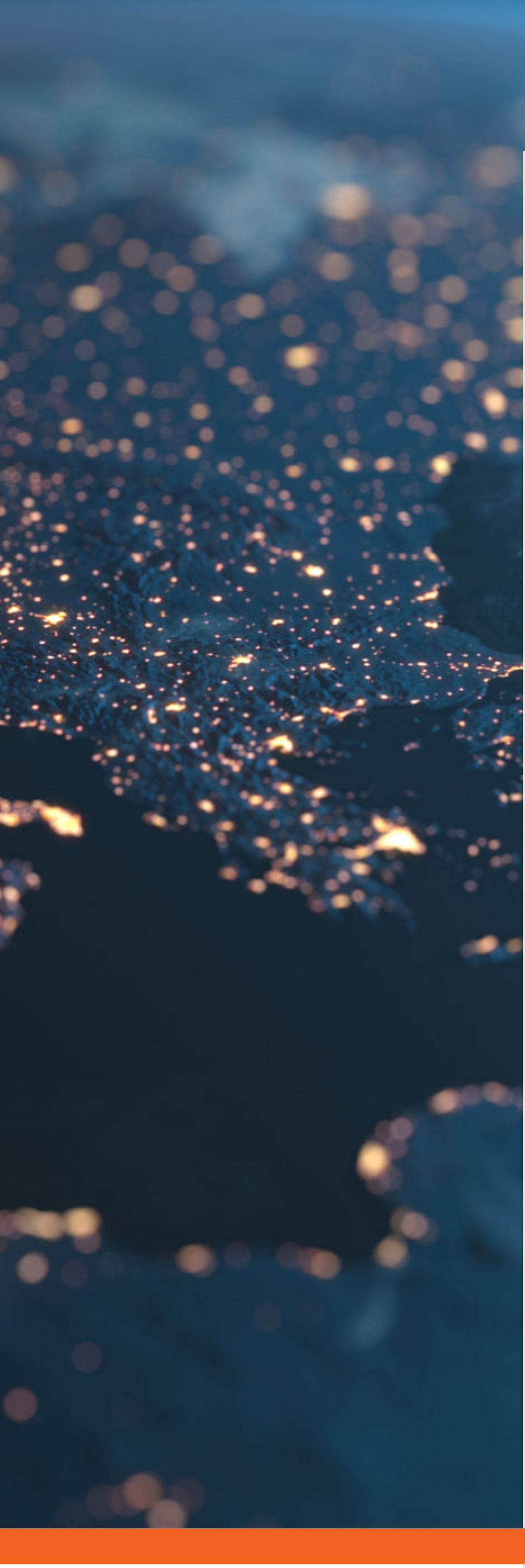
Allied Universal®

G4S
An Allied Universal® Company



World Security Report 2023

1,775 Chief Security Officers

30 Countries

Table of Contents

Introduction

We are pleased to present the first-ever World Security Report, which anonymously and independently surveyed 1,775 chief security officers (CSOs), or those in equivalent roles, at large global companies.

The respondents are from companies that have a combined annual revenue of $20 trillion in 2022. That's almost a quarter of the world's total annual gross domestic product (GDP).

The significance of the findings should not be underestimated. The world is an increasingly dangerous place and the hazards and threats that companies face are ever more complex and multidimensional.

In 2022 alone, more than USD $1 trillion in revenue was lost by companies as a consequence of internal and external physical security incidents. This is similar to the monetary impact caused by cyber incidents. One in four (25%) publicly-listed companies reported a drop in their corporate value in the last 12 months following an external or internal security incident.

Additionally, 200 global institutional investors were surveyed to understand the impact of security incidents on the value of publicly-listed companies.

The actual impact can be significant, with those investors estimating an average decrease in stock price of 29% in the wake of a significant internal or external security incident in the last 12 months.

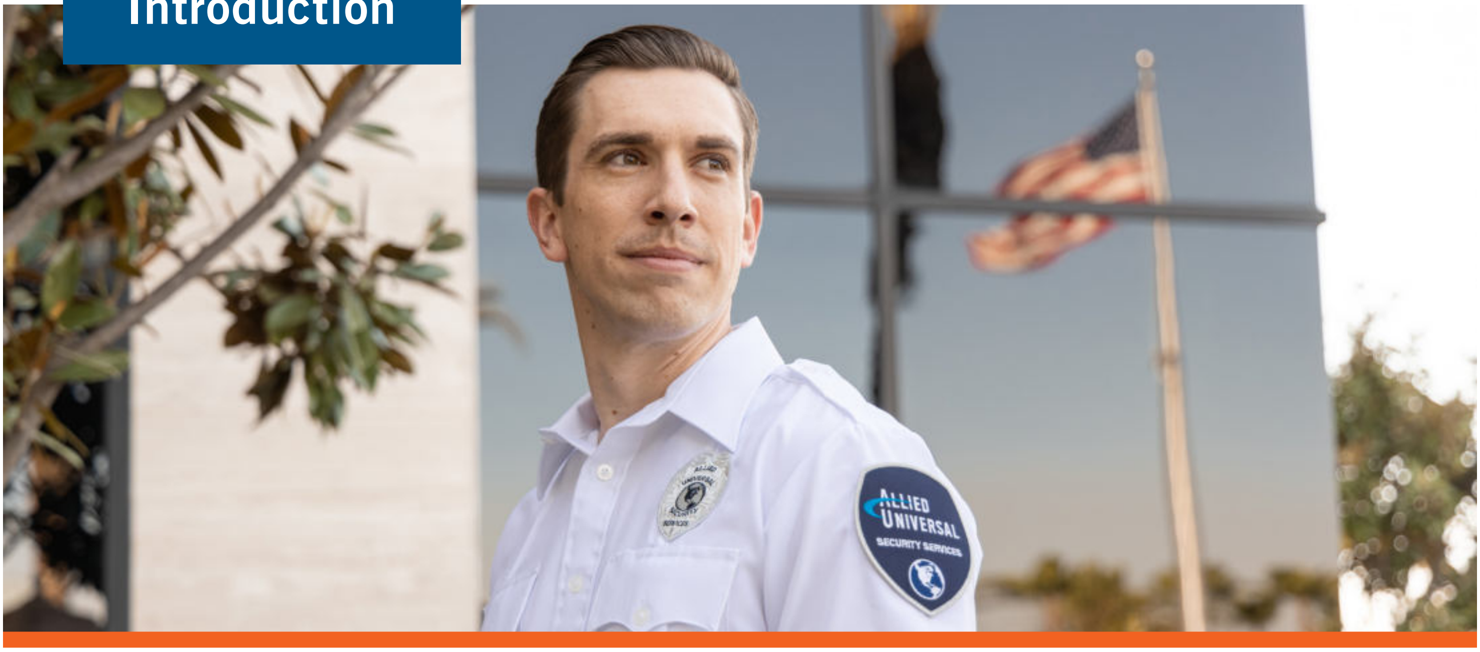
Nearly half of CSOs surveyed believe that economic unrest will be the biggest security-impacting hazard over the next 12 months.

Nations around the globe face multiple, significant economic pressures, including rising inflation and cost of living challenges, exacerbated by the first European war in a generation. These issues come on the heels of sizeable economic shocks following the COVID-19 pandemic.

The data confirms what we have already experienced – physical and cyber security are increasingly interlinked. The survey shows that nine out of 10 respondents said cyber threats, which threaten physical security systems, are challenging to their businesses.

Security budgets represent 3.3% of global revenue at respondent companies, which is around $660 billion annually. Almost half of CSOs said physical security budgets will increase significantly in the next 12 months, driven primarily by rising costs, economic instability and domestic security concerns.

Introduction



Interestingly, CSOs believe there is a disconnect between actual physical security incidents and the importance placed on them at their organization's board level. Nine in 10 CSOs said company leaders are more concerned with cyber than physical security.

Security is a people business and as the use of technology develops, the skills desired in a front-line security professional are rapidly evolving. At the same time, eight out of 10 respondents believe that over the next five years, the recruitment and retention of security professionals will be a major challenge.

It is clear that global companies expect security professionals to have a multitude of skills that they were not expected to have 10 years ago. For example, it is now much more important for a security professional to have technological capabilities and a high level of customer service training. People skills in front-line security professionals are more important than physical attributes of strength for nine out of 10 respondents. Global companies recognize the value of highly skilled and intelligent security professionals protecting their most important assets, with 94% saying the ability to speak multiple languages and 96% saying a higher education degree are important for a frontline security professional.

As the pace of technological advancement quickens, its importance as part of the best-designed security solution increases. The challenges of combining the right technology with the right people, are made evident in this report.

Encouragingly, it is also clear that when a company uses a single third-party security provider for more than 80% of its security requirements, not only does the number of incidents fall, but confidence in being able to effectively deal with security incidents increases dramatically. The data shows that a trusted partnership between a customer and their security provider transforms the effectiveness of the overall security program.

Steve Jones
Global Chairman and CEO
Allied Universal

Ashley Almanza
Executive Chairman
G4S, an Allied Universal company

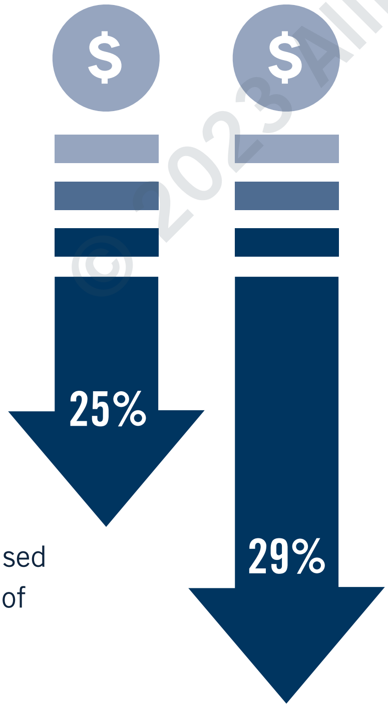
Research Results

1,775 chief security officers (CSOs) – or those in equivalent positions – were anonymously and independently surveyed to learn about the emerging and evolving threats they face, the technology they use and want to use, the people they employ, the skills they value, and the future of security globally. Respondents were from large **global companies in 30 countries with a combined revenue of USD $20 trillion in 2022.**

Impact of Security Incidents on Corporate Value

25% of **publicly-listed companies reported a drop in value** following an external or internal security incident over the last year.

A survey of 200 global institutional investors found an internal or external security incident caused an average decrease of 29%.



Impact of Security Incidents on Revenue

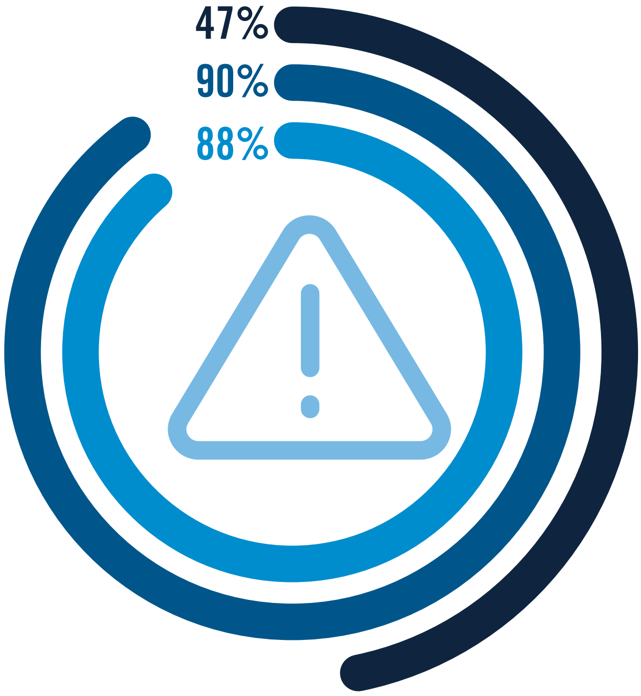
More than USD

$1 trillion

of revenue was lost because of internal and external physical security incidents in 2022.

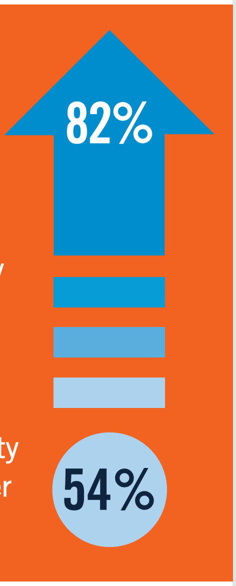
Introduction

Greatest Security-Impacting Hazards



- ● **47%** said **economic unrest** in the coming 12 months.
- ● **90%** said **cyber threats** that **threaten physical security systems** are challenging to operations.
- ● **88%** said **company leaders** are **more concerned with cyber security** than physical security threats.

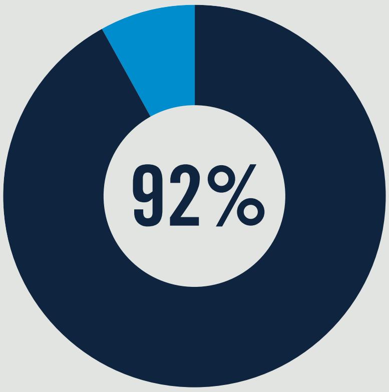
How to Increase Confidence in Security



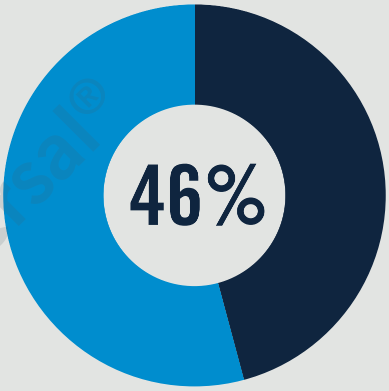
Higher levels of involvement with a security provider increases overall confidence **(from 54% to 82%)** in the ability to deal with security issues.

The greater a company's reliance on security providers to oversee their security, the lower the impact of threats.

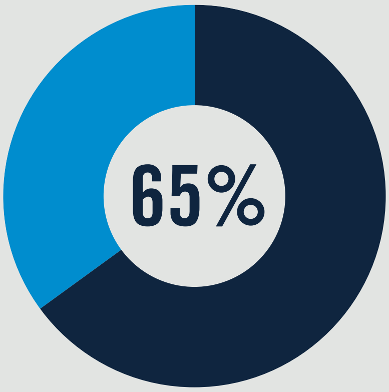
Strategies for Tackling Security Threats



Said that **people skills** in frontline officers are **more important** than physical attributes of strength.



Said **physical security budgets** are expected to **significantly** increase over the next 12 months.



Said their company currently uses **predictive technology to enhance security** and they intend to increase its use over the next 12 months.

Chapter One

Emerging and Evolving Threats

CSOs anticipate that **economic unrest** will be the greatest security-impacting hazard to affect their operations over the next 12 months, cited by 47% of respondents.

This will affect companies around the world and goes hand-in-hand with **social unrest**, where 35% anticipate a threat in the next year, up from 31% in the last 12 months. There is also an increase in threats expected from **disruption of energy supplies** where 33% expect this threat in the next 12 months, up from 30% in the last 12 months. The threat from **war and political instability** is also likely to increase, with 32% anticipating a threat, up from 25% in the last year.

Approximately one-third of CSOs anticipate all of these hazards will affect their physical security in the coming year as people are financially impacted by inflation and higher living costs or they are displaced from their homes by war or climate events.

Concerns about **economic unrest** increased markedly from the previous year when 39% of those surveyed said they experienced this hazard. **Economic unrest** has the strongest correlation with loss of revenue; meaning this was the hazard most likely to impact loss of revenue in the last 12 months.

The biggest security-impacting hazard last year was **pandemics** reported by 42% of those surveyed, a hazard that is expected to recede in the next year. It is the hazard that most correlates with **implementing more effective security** – meaning it was the hazard most likely to drive companies to improve their security.

-10%

Companies with **extensive third-party physical security** involvement are 10% less likely to have encountered external threats.

Chapter One

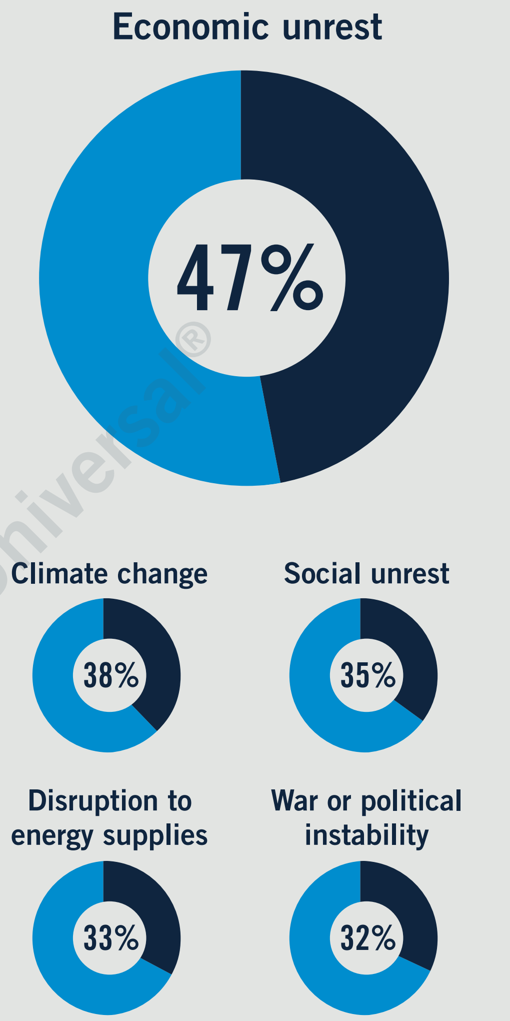
Climate change is expected to be the second most likely security-impacting hazard by 38% of participants in the next 12 months. More than one-third (34%) of CSOs confirmed their company has experienced a security hazard due to climate change.

This multitude of hazards impacting people is, in turn, driving both internal and external threats.

The two threat actor groups that caused the most security incidents over the previous 12 months were **subversives – hackers, protestors, or spies** and **economic criminals**, where 39% of respondents reported experiencing threats from both groups.

As the world continues to become more economically unstable, CSOs predict the threat from both **subversives** and **economic criminals** will increase considerably over the next 12 months with incidents committed by both groups expected to increase to 50% and 49%, respectively.

Greatest Security-Impacting Hazards



47% reported **economic unrest** as the greatest security-impacting hazard they will face over the next 12 months, followed by:
climate change (38%)
social unrest (35%)
disruption to energy supplies (33%)
war or political instability (32%)

89%

9 in 10 said their company experienced **some form of internal threat** in the last year and this is likely to increase to 92% in the year ahead.

⚠⚠⚠⚠⚠⚠⚠⚠⚠⚠

35%

Misuse of company resources or data was the most common internal incident with 35% of companies having experienced this.

36%

Leaking sensitive information is expected to be the biggest internal threat over the next 12 months, cited by 36% of respondents.

Internal Threats

Concerningly, internal threats are increasing. 89% of CSOs said their company experienced some form of internal threat in the last 12 months; this is expected to increase to 92% in the year ahead.

Misuse of company resources or data is the most common internal threat, with 35% having experienced this, followed closely by **leaking of sensitive information** at 34%. This threat is expected to become the biggest internal threat in the next 12 months.

Misuse of company resources or data has the strongest correlation with **implementing more effective security**. This was the internal incident most likely to drive companies to improve their security during the last 12 months.

Unauthorized access to company resources or data, **industrial espionage** and **intellectual property theft** are all expected to increase in the next year. Perceived financial gains may entice a company employee to share confidential information in exchange for payment.

Chapter One

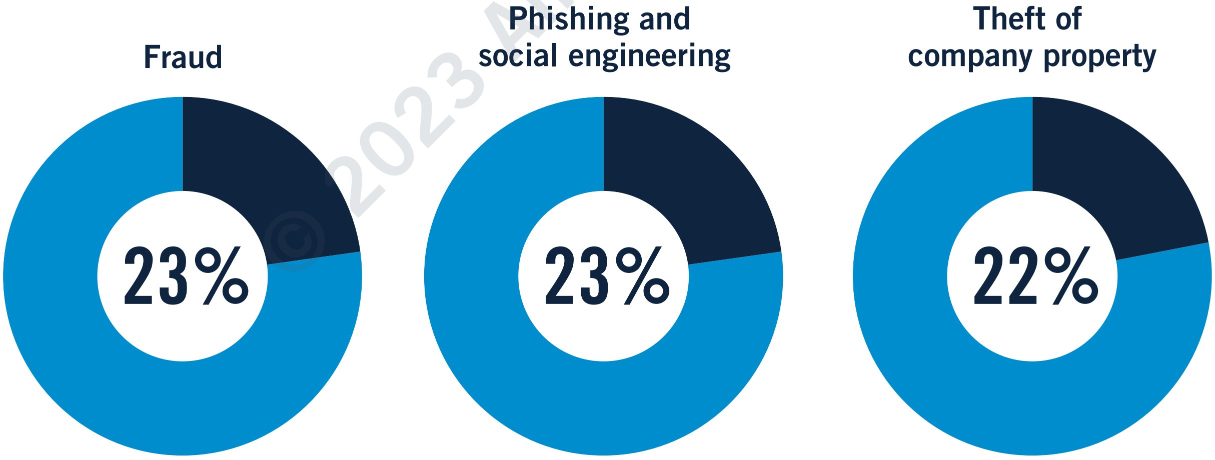
External Threats

Fraud is likely to be the biggest external threat in the next 12 months, predicted by 25% of CSOs. This is followed closely by **phishing and social engineering**[1] and **theft of company physical property** at 24% and 23%, respectively. All of these threats were the most experienced during the past year and are expected to remain the top threats next year.

Theft of company physical property has the strongest correlation with implementing more effective security, meaning it was the external incident most likely to drive companies to improve their security in the last 12 months.

Fraud has the strongest correlation with loss of revenue, meaning it was the external incident most likely to lead to a loss of revenue in the last 12 months.

Universally, CSOs expect all external threats to increase in the next 12 months. Businesses in the financial services and consumer staples sectors predict the most significant increases in external threats, closely followed by those in the energy and real estate sectors.



Fraud and **phishing and social engineering** were the biggest external threats experienced in the last 12 months, both cited by 23% of respondents, followed by **theft of company property** at 22%.

Security Provider Involvement and Confidence

Companies can take measures to protect themselves from all threats. Those with extensive third-party physical security involvement – defined as more than 80% of security needs met by a security provider – are 10 percentage points less likely to have encountered external threats compared to those who have low involvement, with 83% and 93% experiencing a threat in the last year, respectively.

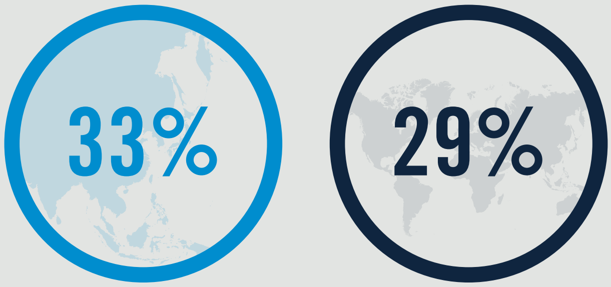
Having high levels of involvement from a security provider significantly increases confidence in being able to deal with incidents.

This shows that third-party providers should be a key part of a security strategy as their expertise brings significant benefits.

Dangerous Regions

Companies actively operating in dangerous regions are more likely to view these regions as risky when measuring threats and potential risks, compared to companies that do not have a footprint in those territories. Universally, there's a perception versus reality gap when it comes to security leaders' views of regions compared to companies that actually operate in them.

The most dangerous region is Northeastern Asia. Those that operate there consider it even more dangerous than those that don't. The same is true of Central America and Central and South Asia, which are, respectively, the second and third most dangerous regions in the world to operate.



Northeastern Asia is considered to be the **most dangerous geography** to operate in, both by those operating in the region (33%) and participants' global view of dangerous regions (29%).

[1] The use of deception to manipulate individuals into divulging confidential or personal information.

Chapter Two

People in Security

Despite rapid changes in technology over recent years, people remain a core part of the security programs of global companies. Rather than the basic need for frontline security professionals changing, data suggests it is the skills required in a security professional that have evolved. CSOs the world over increasingly want more from the security workforce they deploy.

Long gone are the days of the big, burly, often male, security guard, with a resounding 90% of CSOs saying **people skills** are more important than **physical attributes of strength**, and 95% citing **diversity of workforce** as an important credential when choosing a security provider.

More than nine in 10 CSOs agree that the following skills are highly desirable: **emotional intelligence** at 95%, a **higher education degree** at 96% and the ability to **speak multiple languages** at 94%.

Predictably, CSOs place great weight on having security professionals who have **integrity**, with 97% saying it is an important attribute and 74% saying it is extremely important.

Skills Required in Frontline Officers

67%

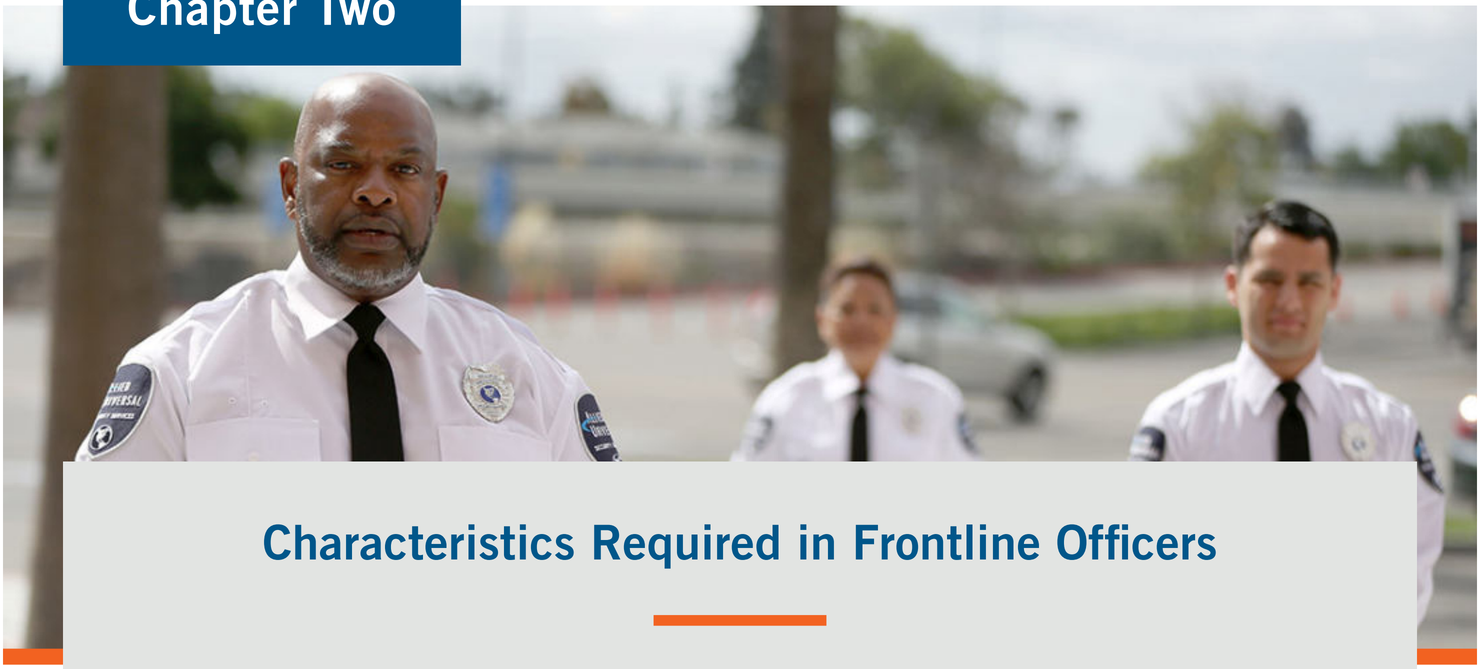
Think that **customer service skills** are extremely important.

63%

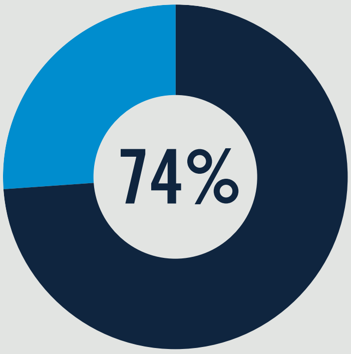
Said that a **higher education degree** is extremely important.

57%

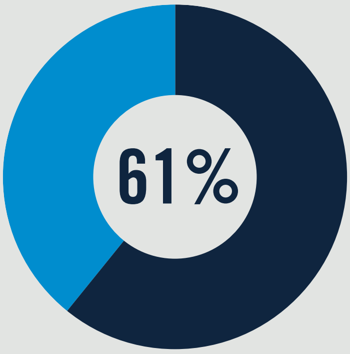
Believe that the ability to **speak multiple languages** is highly desirable.



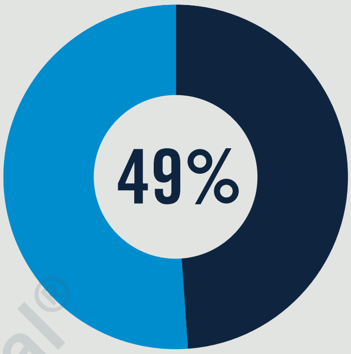
Characteristics Required in Frontline Officers



Believe that **integrity** and **honesty** are **extremely** important.

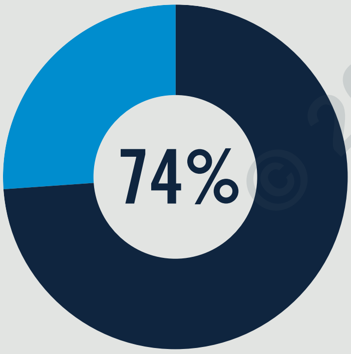


Think **emotional intelligence** is highly desirable.

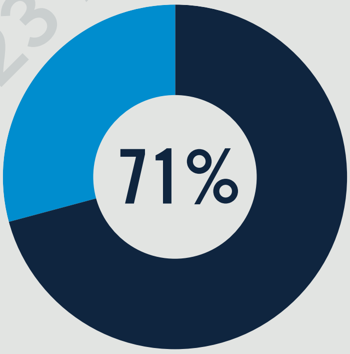


See a **military or law enforcement background** as extremely important.

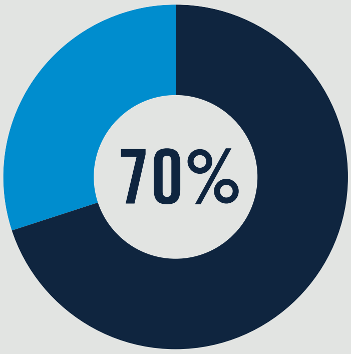
Characteristics Required in Security Leaders



Said **integrity** and **honesty** are extremely important.



Said the **ability to work collaboratively and effectively across an organization** are extremely important traits.



Said the following qualities are both extremely important in security leaders:
– Knowledge of **legal** and **regulatory** requirements.
– Strong understanding of **technology**.

People and Technology

There are broadly two types of security buyers and the less advanced tend to simply want guards on posts, without giving much consideration to skills and qualifications.

Technology development is the biggest disruptor in the workforce, but its impacts are likely to be positive overall. As technologies develop, CSOs want technology-savvy front-line security professionals. However, they are not easy to find.

Having a strong understanding of technology is high on the list of desired qualities and 85% of CSOs think this is going to become more important in the next five years.

One-third of respondents report that finding these security professionals is a challenge and can hamper the implementation of new technology. This is also true for a similar percentage of CSOs in relation to the skills of their own internal people.

88%

Said **technology** is changing the **skills required** for security professionals.

85%

Think a strong **understanding of technology** will be **very important** in the next five years.

Recruitment and Attributes

Recruitment and retention are anticipated to be the biggest problem areas for CSOs around the world over the next five years. Skills and experience are top of the list of challenges to recruitment, with 43% claiming the **unattractive role** of security as a career being **extremely challenging**.

90%

Believe **retention of qualified and experienced security staff** is a challenge.

The most important attributes in the ideal security leader are integrity and honesty, cited as **extremely** important by three-quarters of respondents. The ability to work collaboratively and effectively across an organization, knowledge of the legal and regulatory requirements and a strong understanding of technology are all **extremely** important qualities according to seven in 10 CSOs.

Industry Expert View

Antony Bailey

Global Asset Protection Manager

Security professionals are a vital component in the delivery of a holistic security solution – they are as fundamental in mitigating security risks and threats as fences, video surveillance and access control systems.

But there are many variables when it comes to finding the right people with the right skills, including availability and capability.

The latter has become even more important in today's security world where technology is an increasingly integral part of our defenses.

Security managers, then, should regularly be asking:
1. Do we understand the issues impacting staff skills – and what skills do our people need today to be effective and safe?
2. Given technology is so vital to their role, do we understand the balance of technical and practical skills needed in a modern security environment?

As the data in this report shows, while the general appearance of frontline security professionals is still very important – and by that I mean well-trained, disciplined, motivated individuals - capability does not end there.

We need thinking security professionals who can follow procedures yet still question at the right moment, remain adaptable and suggest improvements – who have a balance of practical knowledge, appearance, experience and academic ability. Soft skills such as emotional intelligence, intellect, de-escalation skills and, as mentioned already, the ability to use technology are also highly valuable attributes.

Having minimum standards across these skill sets, in addition to the existing standards on vetting, accreditation and training in different jurisdictions, could help to improve the professionalization of the security industry further.

Changing the way we assess security professionals could do the same. It's critical to review how they respond to an incident, but if acute awareness, observations and actions are in place, then the chance of an incident occurring is greatly reduced. I've found leading indicators of preparedness, training and internal test exercises to be more revealing than lagging indicators of assessing their reaction to events.

When it comes to the availability of security professionals, there's more work to do in making security a more attractive career, which is still viewed as a stopgap and, so, attracts transient workers such as students. Our industry needs to do a better job of demonstrating all the fantastic opportunities that are available, and that there is so much more to it than just standing outside a building.

Security officers with the right aptitude need to be invested in and have the chance to progress; they need to know that it's feasible for them to work their way up to become a cluster or regional manager, maybe even a global one.

Companies can also improve their approach to recognition of security professionals, an important part of retaining them. Too often, recognition is only shown after an incident occurs, when something has gone wrong; but we should be recognizing them when nothing happens, as clear a sign as any that they are doing their job effectively.

With demand for security services growing – and recruitment and retention issues persisting, not least because people are moving to less risky but equivalently paid jobs in other sectors and industries – security leaders need to double down on improving capability and availability of security professionals.

All views and opinions expressed in this article are Antony Bailey's own.

Biography

Antony Bailey currently manages the global security Enterprise Framework Agreement for a U.K. based international company and has extensive experience managing strategic and operational portfolios within public and private security in high-threat and permissive environments. Bailey applies a balance of academic knowledge and practical experience in managing and delivering security. Prior to moving into the commercial sector Bailey served 22 years in the U.K. military. He has an MSc in security and risk management from Leicester University.

Chapter Three

Technology and Security

The rapid evolution of technology is impacting physical security in multiple ways. Over the next five years, 98% of CSOs intend to invest in technology to improve overall security operations.

Cyber Advancements Threatening Physical Security

The survey data shows that physical and cyber security are increasingly interlinked. Nine in 10 respondents said cyber threats that threaten physical security systems are challenging to their business.

This highlights concerns among CSOs about the pace of technological change and the apparent disconnect between that rapid evolution and the ability to close the gap when new technology exposes potential vulnerabilities in either their physical or cyber security.

Bad actors typically choose the easiest route to expose a vulnerability and, therefore, a balance needs to be struck between physical and cyber security. A weakness in a physical security program could compromise a company's cyber security, but a weakness in cyber security can impact an organization's physical security, too.

The Challenges

87%

Said the shift from **staffed security** to **technology-enabled** is challenging.

41%

Stated concerns about the **cost to implement** technology followed closely by **cost to maintain** technology (40%).

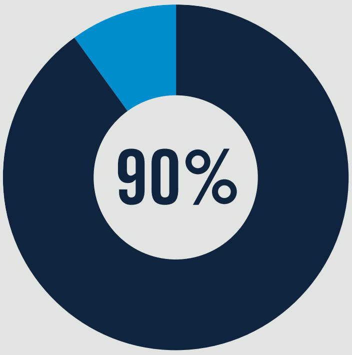
Future Technology Investment

CSOs want their physical security operations to react at speed and with an accurate read on the data that is available. In the next 12 months, nine out of 10 respondents will invest in remote response technology and more than half (51%) intend to invest in automated threat detection and response, as well as threat intelligence and analytics technology.

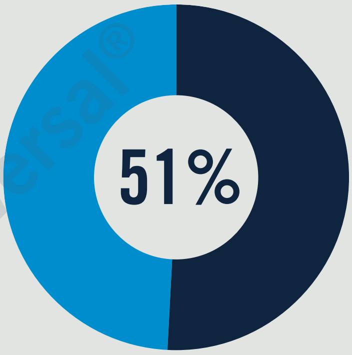
Top of the agenda for future investment is artificial intelligence (AI), with 42% intending to invest in AI and AI-powered surveillance in their physical security over the next five years. This is closely followed by biometrics and facial recognition technology at 40%. CSOs will expect security providers to mine their data and provide relevant insights to stop security incidents from occurring. And, increasingly, they will demand it.

Security providers who are integrators of physical security technology need to pay close attention to their cyber hygiene, and companies procuring the integrators' service must do the same. Every piece of physical security technology, once installed, is connected and becomes part of the company's digital footprint. Therefore, like any other technology, it is potentially vulnerable to attack and sufficient protections must be put in place to limit the risk.

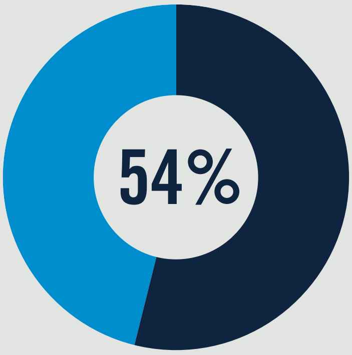
The Benefits



Said technology **improves** the overall **effectiveness** of security operations, enabling security staff to be more **productive** and **efficient**.



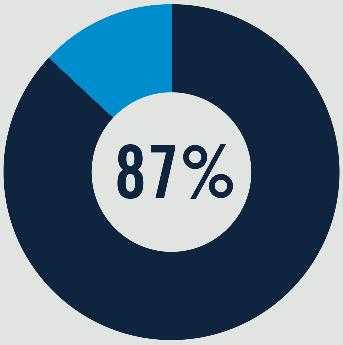
More than half said **threat detection and response** technology and **threat intelligence analytics** technology are important features to security operations.



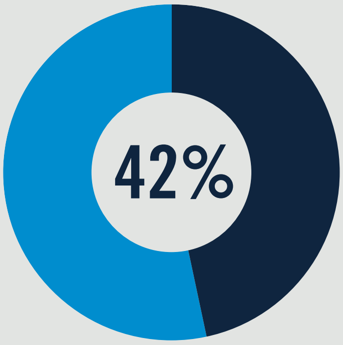
Real-time monitoring and alerting and **improved response speed to an incident** – both at 54% – are considered the most important features to security operations.

Chapter Three

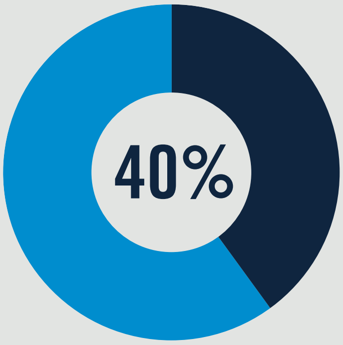
The Future



9 in 10 (87%) plan to invest in **remote response** in the next 12 months.



Over the next five years, 42% of respondents intend to invest in **AI and AI-powered surveillance** in their physical security operations.



This is closely followed by **biometrics and facial recognition** technology at 40%.

Security Technology Advancement

We asked CSOs to rate their technological advancement in terms of their physical security program, with a detailed set of criteria. These ranged from minimal tech use, to advanced and followed by cutting edge.

Companies that have already implemented cutting-edge technology are much more confident in their overall security operations. For those with basic technology use, the average confidence level is 63%, for advanced it is 69% and for cutting-edge it is 74%.

Where companies are struggling with the implementation of technology it is due to cost and lack of skills.

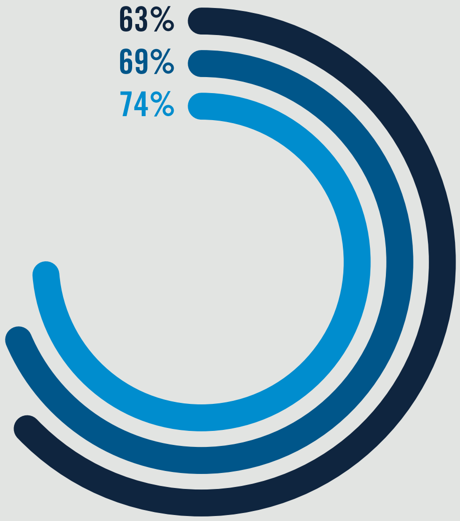
The shift from purely staffed security operations to technology-enabled is challenging according to nine in 10 CSOs. The top two barriers companies face when implementing technology are the costs, with 41% of CSOs concerned about implementation cost and 40% concerned about maintenance cost.

More than a third are concerned about the lack of skills in the security workforce (34%) and the lack of internal skills (32%) in their company to implement technology. This highlights a potential technology skills gap and shortage within the industry.

Companies are concerned that when technology is implemented, the skills are not there to manage any potential vulnerabilities that may arise in the overall security operations.

Despite these worries, CSOs agree that technology brings significant benefits. Technology improves the overall effectiveness of security operations, enabling security staff to be more productive and efficient according to nine in 10 respondents.

Confidence in Technology and Security



● **63%** basic technology
● **69%** advanced technology
● **74%** cutting-edge technology

Industry Expert View

Dave Komendat

President of DSKomendat Risk Management Services

The biggest opportunity for global companies in the use of new security technology is how it can advance the capabilities of organizations and reduce risk. As the world rapidly changes, its successful implementation is the key. Smart investment is required to do this and without a strategic commitment to enhance their security capabilities, a company puts themselves at growing risk each year.

Security threats are more dynamic, convergent and complicated than they have ever been. The biggest threat to security technology is the increased attack footprint by those who intend to disrupt or harm – there are more ways in than ever before and the impacts are magnified. Integrated security technology has become an Internet of Things, the more technology you install and connect, the higher the attack risk profile.

Technology has to be risk managed effectively. CSOs must ensure they work off a technology roadmap to ensure an effective ecosphere is created. Physical and cyber security are now inextricably interlinked – a weakness in one area could result in an incident in the other: it works both ways. CSOs need to have an understanding of cyber risk, even if it is not in their area of responsibility and chief information security officers (CISOs) need to understand the physical domain. Without this, cyber or physical could become a critical blindspot.

Investing in the right technology takes time and effort. Just because a technology appears to be exciting and sexy, without the proper due diligence into its return on investment – i.e. is it mature, is it reliable, does it do what we want and can it be implemented at scale – it may be a waste of time and energy.

There is considerable pressure on CSOs to look for cost efficiencies and increased productivity; with so much technology being used in other business functions and operations, the inevitable question is "what are we (CSOs) doing to implement new risk-reducing technology?".

AI is both an opportunity and a threat. The security benefits of AI are being explored now but it's very new, not fully understood and feared by some. There is good reason to be cautious. There is a critical need for guiding principles on what AI should and should not be used for within the security realm, such as advanced warning of threats, indicators of an insider threat and the ability to respond more quickly than traditional tools allow. AI can provide that advantage but it must be carefully used as the capability can be invasive and unnecessarily threaten a person's rights or privacy.

The backbone of a lot of security infrastructure still firmly sits in the 1980s, with technology such as turnstiles, proximity cards and basic video monitoring still in use. There are some attractive qualities in this, these work and they don't create a huge risk footprint as many are air-gapped away from company IT systems but, their capabilities are limited and they do not adequately address today's risks.

With few exceptions, the security community has been behind the curve in its use and implementation of new technologies. CSOs are now much more open to third-party security technology providers because they have greater focused expertise and they're effective in implementation at scale. CSOs need to do their research, but the benefits of third-party expertise are worth it.

Ultimately, the security community must seek out people with the right technical capabilities, otherwise it will never fully be able to use the best technology available. With huge recruitment pressures in industry globally, organizations are competing for a limited talent pool.

The big challenge in security is that the profession does not effectively market its technical and cyber career opportunities to young people. The profession needs to share its story with high school, technical college and university graduates that the security industry is a great place to work.

The security community has not targeted this group and it's critically important that it does now. The traditional pipeline of security talent is not diverse enough nor technically qualified. The real pool of talent is young adults who have grown up with technology, embraced it and know instinctively how to use it. We need that talent in the profession.

All views expressed in this article are Dave Komendat's own.

Biography

Dave Komendat has 36 years experience in the security industry, 14 as vice president and CSO of The Boeing Company. He is the founder and president of DSKomendat Risk Management Services, serves on several company advisory boards and holds board leadership roles with several non-profit organizations. In 2018, Komendat was awarded the Director's Award for Exceptional Public Service by FBI Director Christopher Wray.

Chapter Four

The Future of Security

The security industry is at a critical moment in its evolution. A challenging combination of increasing economic unrest and heightened tensions globally are converging at a time when technology capabilities are accelerating and the required skills for a security professional are transforming.

As physical and cyber security become increasingly symbiotic, the majority of security leaders are concerned and anticipate that cyber threats that threaten physical security systems will challenge their business.

There is concern about the pace of technological change and the apparent disconnect between that rapid evolution and the ability to close the gap when new technology exposes potential vulnerabilities.

Supply Chains

According to nearly nine in 10 CSOs (87%), geopolitical tensions are expected to compromise the security of supply chains and could result in disruptions to global trade in the next year.

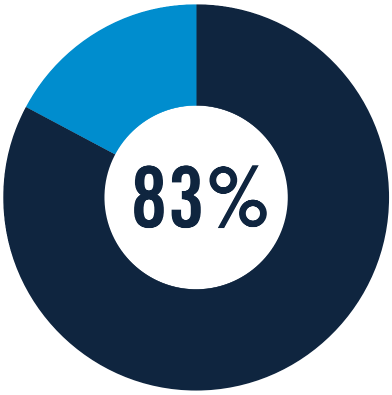
More than eight in 10 (83%) CSOs expect all types of physical security threats to increase over the same period.

In every area, CSOs are presented with challenges that ultimately create a gap in their preparedness that they are chasing to close.

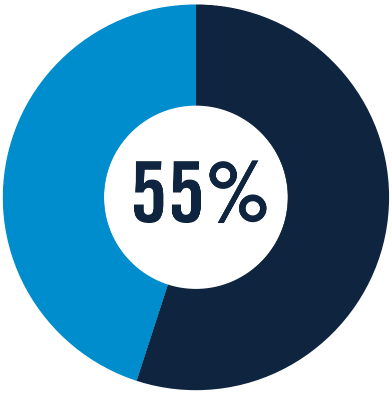
GEOPOLITICAL TENSION

87%

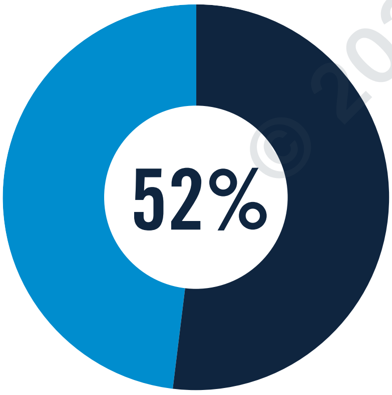
Think geopolitical tension will compromise the security of supply chains which could result in **disruptions to global trade.**



Said **physical security threats** will increase over the next 12 months.



Said **introducing new technology** will be their company’s priority over the next 12 months.

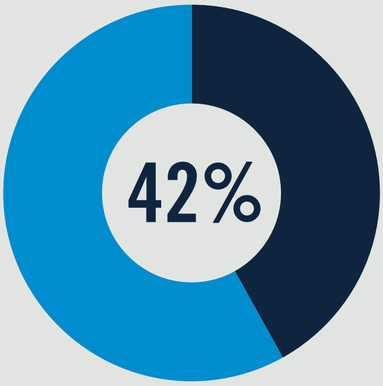


Said **training staff to use new technology** will be their company’s priority over the next 12 months.

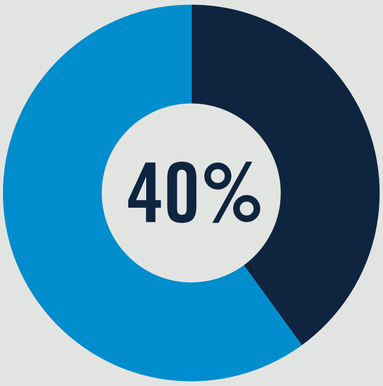
Physical Security Budgets

The majority of CSOs report that at their company’s board level leaders are more concerned with cyber than physical security. Despite this, nearly half of respondents believe that physical security budgets will increase significantly in the next 12 months. The top three drivers globally are expected to be **rising operational costs**, **international economic instability** and **domestic security concerns**.

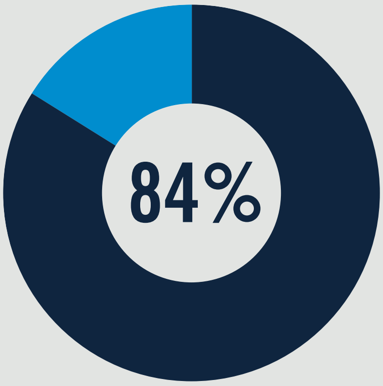
More than half of CSOs will prioritize their spending on the introduction of new technology and the training of staff in the next 12 months. More than one-third are concerned about the skills in their security workforce and a lack of skills in their own internal team to implement technology.



Consider **artificial intelligence and AI-powered surveillance** to be at the top of their future investments list for the next 5 years.



Will invest in **biometrics and facial recognition** in the next 5 years.



Said **recruitment of security professionals** will be challenging over the next 5 years.

Security Professional of the Future

The security professional of the future will be able to understand and interact with the technology required to do their job and keep safe the assets they are assigned to protect. That security professional is personable and helpful, with excellent de-escalation skills and the ability to read a situation. They are intelligent, educated and potentially bilingual.

Technology improves the overall effectiveness of security operations, enabling security staff to be more productive and efficient according to nine in 10 respondents. This suggests the time and cost of implementing technology is compelling.

Recruiting security officers will be a challenge for eight in 10 CSOs in the next five years, while the retention of qualified and experienced staff is even more so, according to nine in 10 respondents. This has not dampened the high standards and skill levels that CSOs increasingly demand.

Security providers can play a crucial role by offering relevant resources to help bridge the skills gap and enable their customers to better understand and use new technologies. In turn, security providers can help their customers stay ahead of emerging threats.

BARRIERS TO IMPLEMENTING TECHNOLOGY

35%

Stated a lack of internal skills **within their company.**

34%

Stated a lack of skills **in the security workforce in general.**

Industry Expert View

Mary Rose McCaffrey

The path ahead that CSOs will have to tread is one filled with a wide range of challenges, threats and geopolitical tensions – all of which have real-world implications.

Russia's attempted land grab of a neighboring democratic country in Europe sent shockwaves across the globe. It continues to engage in misinformation campaigns and cyber-attacks, and has revalidated the importance of NATO and the alliance upon which it was created following World War II.

China continues its strategic intent with aggression in the Pacific Rim. This continues to provide challenges to the countries and people of the region.

Nearly 40% of CSOs predict climate change will be a security concern for companies in the foreseeable future. Hurricanes, flooding, earthquakes and wildfires have put people and physical property at greater risk. CSOs will continually need to keep abreast of these threats to ensure their companies can prepare and protect against them.

At the time of writing inflation, not seen in decades, continues to be a factor. Governments are working to manage inflation, but it does have an impact on companies and people.

CSOs who are responsible for insider threats need to take into account inflation as a stressor on people and the potential risk to corporations; ranging from theft of intellectual property or in the worst case, potential workplace violence. Security is often the point of information for both internal and external threats to a company.

Even with the current challenges, technology can enable increased productivity. With appropriate investment, utility and maintenance, use of Robotic Process Automation (RPA), AI and other technologies can have an additive benefit to security.

Security can use technology to improve accuracy and reduce the manual labor involved in repetitive tasks.

In one example, an RPA was able to complete reviews of vetting paperwork in significantly less time with 99.6% accuracy, thereby allowing the security officers to focus on other strategic work. It took a human approximately 30 minutes to review and the RPA only three minutes.

This was a game-changer for personnel security and proves that technology is a critical enabler to the future of security.

It's really promising to see that just over 50% of respondents to this survey said that training staff will be a security budget priority over the next 12 months.

Employees leave companies for the inability to see career development and educational opportunities. The world is experiencing demographic challenges in the security space, containing five generations in the work environment. From increased retirements, hiring and retention demands in the current labor market, security leaders need to develop leaders rapidly.

I'm certain that CSOs reading this report are aware of the recruitment and retention challenges, so I won't argue this issue.

I am pleased to see the more human side of security officers were emphasized in the survey. There is often a mistaken perception that security is only focused on gates and guards, but this is only one of the countermeasures deployed within a robust security program.

Security officers are encouraged to demonstrate the full suite of skills to enable the business. I hope that recruiters of the future highlight these traits.

In addition, I am hopeful the profession will begin to reflect the population with both women and people of color moving up the career ladder.

The next few years will be challenging, but there are opportunities for CSOs to be leaders and to drive organizational change which protects people, data and assets and company brand, as without these things, there is no business.

All views expressed in this article are Mary Rose McCaffrey's own.

Biography

Mary Rose McCaffrey was vice president of Security at Northrop Grumman from 2016 to 2023. Her team enabled security performance, customer compliance, risk management and the protection of the company's personnel, facilities and programs globally.

Prior to Northrop Grumman, McCaffrey held leadership positions at the Central Intelligence Agency, the National Reconnaissance Agency, Office of Director of National Intelligence and the Department of Defense.

She is passionate about developing the next generation.

Asia Pacific

Companies in Asia Pacific were impacted by internal threats at a similar rate to the global average, with 90% experiencing an incident. The most common was **leaking sensitive information** at 39%, ahead of the world mean of 34%.

This was closely followed by **misuse of company resources or data** at 38%, which was also above the global average of 35%.

Similar to the global picture, 90% of respondents experienced an external security threat last year. **Phishing and social engineering** had the biggest impact in the past 12 months, cited by 29% of those surveyed, well above the world average.

Economic unrest is likely to be the biggest security-impacting hazard in the next year, cited by 52% and up from 44% in the previous 12 months. Asia Pacific will be impacted more than any other region by this hazard, on par with Sub-Saharan Africa. **Pandemics** was the most common hazard last year, reported by 49% of respondents, and higher than the world average of 42%.

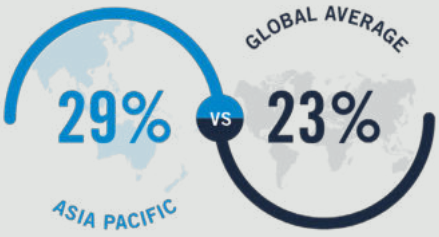
Climate change is expected to increase significantly to affect 40% of respondents in the next 12 months, up from 34% in the previous year, matching the global average.

Concerns about **war or political instability** are worsening, with 36% of respondents expecting it to be a security-impacting hazard next year, up from 27% in the previous year.

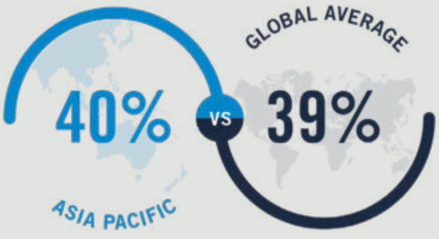
The threat actor group that most impacted the region is **subversives – hackers, protestors, or spies** according to 40% of companies, in line with the world mean. That's likely to be overtaken by a sharp rise in those affected by **economic criminals**, with 51% of those surveyed expected to be impacted in the coming 12 months.

Physical security budgets are anticipated to increase significantly by 42% in the next 12 months. This is being driven by **international economic instability** according to 54% and **rising operating costs** cited by 52%, both at levels above the global mean. Security budget priorities will be focused on **introducing new technologies** by 58% of respondents, followed by **optimizing security processes** by 57%, both above average.

Previously



Experienced **phishing and social engineering.**



Were impacted by **subversives – hackers, protestors, or spies.**

Regional

Asia Pacific is the second most advanced region in the world in its use of security technology, with 43% using **cutting edge** or **emerging** technology, beaten only by Latin America.

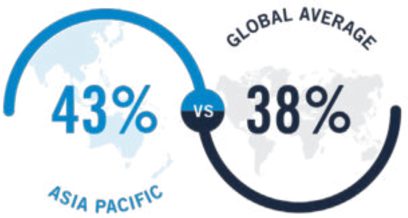
The biggest area of technology investment in the region will be in **artificial intelligence** (AI) technologies over the next five years, including **AI-powered surveillance and monitoring systems** at 48%, **AI and machine learning** at 47% and **AI-assisted threat intelligence** at 45%, all at levels above the global average.

The biggest barriers to using more technology is the **cost of implementation** and the **cost of maintenance** reported by 45% and 43%, respectively, of those surveyed, both above average.

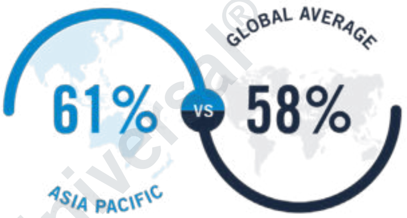
Hiring the right people in Asia Pacific is **extremely** or **very challenging** according to 61% of participants; North America and Latin America were the only regions where recruitment is more challenging. Accessing those with the right experience is the biggest challenge, according to 58% of respondents. This was followed by the retention of qualified and experienced staff at 57%.

The most important attributes in security professionals are **integrity and honesty**, a **strong understanding of technology** and **customer service skills**. The least important attribute cited was having a **military or law enforcement background**.

Currently

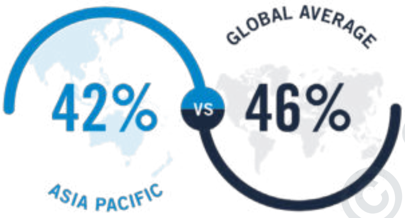


Use **cutting-edge** or **emerging** technology.

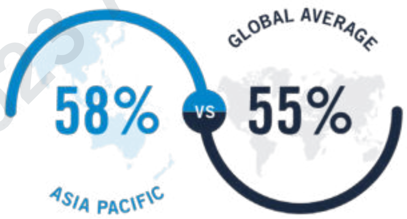


Of participants said it is **extremely** or **very** challenging to recruit.

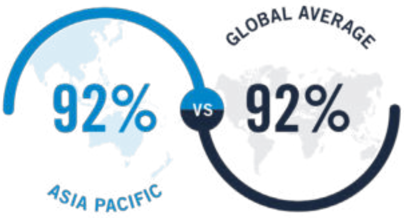
Looking Forward



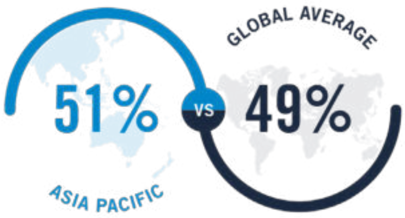
Expect physical security budgets to increase **significantly.**



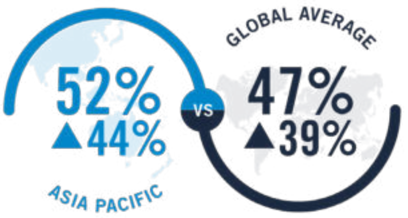
Said security budget priorities will be focused on **introducing new technology.**



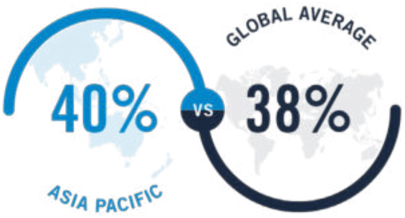
Expect to experience an **external security threat** in the next year.



Expect to be affected by **economic criminals** in the coming 12 months.



Said **economic unrest** is expected to rise in the coming year



In the next 12 months, **climate change** is expected to increase significantly as a hazard.

Europe

Fraud and **misuse of company resources or data** were the most common internal security threats experienced by European companies in the last 12 months, both at 30% and just below the global average of 32%.

Leaking sensitive information is expected to be the biggest internal threat in the coming year, according to 30% of respondents, below the global average of 36%.

The biggest external threat was **fraud**, impacting 21% of those surveyed in the last 12 months, below the world average of 23%.

Fraud will be overtaken by **phishing and social engineering**, anticipated by 22% of those surveyed in the coming year, below the global average of 24%.

Economic unrest at 33%, **pandemics** at 31% and **social unrest** at 30% were the most common security-impacting hazards during the last year. Economic unrest is expected to rise significantly to 42% in the coming year but will remain below the world view of 47%.

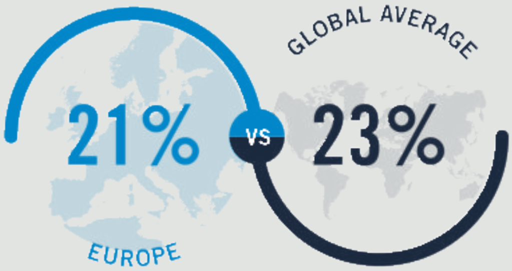
Disruption of energy supplies and **social unrest** will be the second highest hazards in the next 12 months, both cited by 31% of participants. However, both are expected at levels below the global averages of 33% and 35%, respectively.

Economic criminals are the threat actor group that most impacted companies in the region at 38%. That is expected to jump to 46% in the coming year, but will be slightly below the global mean of 49%.

Of the companies based in Europe, 41% expect to spend significantly more on physical security over the coming year. The drivers behind this are **rising operating costs** reported by 39% of respondents and **regulatory requirements** at 38%. Security budget priorities will be focused on **risk assessment and threat analysis** at 44%, followed by **training staff** and **introducing new technology**, both at 42%.

European companies have the second highest use of **basic** or **minimal** technology, with 36% of respondents saying this is their level of advancement. Only the Middle East has a higher percentage of companies using only basic technology. Europe is the least advanced region in the use of **cutting edge** and **emerging** technologies at 31%.

Previously



Were impacted by the external threat of **fraud.**

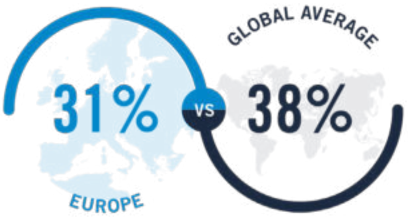
Regional

Over the next five years, and in-line with global trends, AI will be the biggest area of investment, according to 35% of respondents, albeit below the global average of 42%. The greatest barrier to technology implementation is the **cost to implement**, cited by 36%, followed by the **cost of maintenance** at 34%.

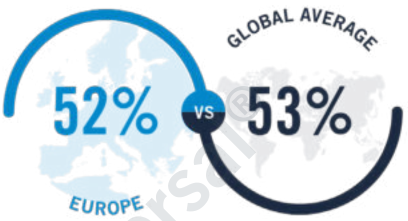
Hiring the right staff is expected to be a challenge, with 58% reporting it is **extremely** or **very challenging** to find the right people, albeit it is more challenging according to 71% of participants in North America, 66% in Latin America and 61% in Asia Pacific. The biggest barriers were **retaining qualified staff** reported by 52%, **experience** was cited by 49%, and 47% said it was hard to find people with the **appropriate skills**.

Qualities in security professionals most sought after in the region are **integrity and honesty** and **industry-specific experience**. The least important attributes were the **ability to speak multiple languages** and having a **military or law enforcement background**.

Currently

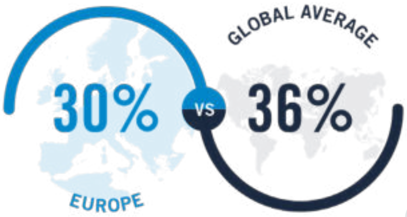


Use **cutting-edge** and **emerging** technologies.

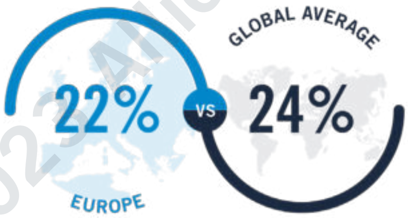


Reported it is **extremely** challenging to retain qualified staff.

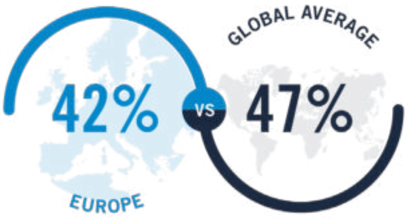
Looking Forward



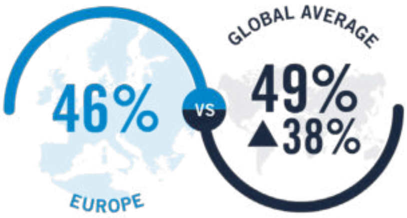
Expect **leaking sensitive information** to be the biggest internal threat in the coming year.



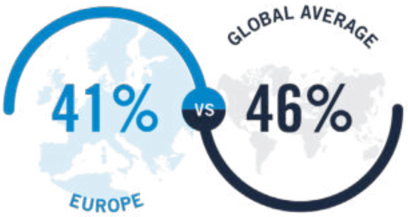
Anticipate **phishing and social engineering** will be the biggest external threat in the next 12 months.



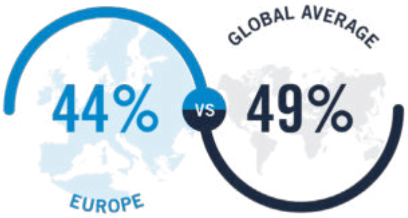
Expect to be impacted by **economic unrest** in the coming year.



Will be impacted by **economic criminals** in the coming year.



Expect to spend **significantly** more on physical security budgets in the next 12 months.



Will prioritize **risk assessment and threat analysis.**

Latin America

Latin America experienced more internal security threats, according to 92% of respondents, than the world average of 89% over the last year. **Theft of company physical property** was the most common, experienced by 37% of respondents and above the world average of 32%, but lower than Sub-Saharan Africa at 43% and North America at 39%.

The biggest internal threat in the next 12 months is anticipated to be **leaking sensitive information** by 34% of participants, while **theft of company physical property** is likely to decline markedly by six percentage points. Latin America will remain slightly above the world mean of 92% for anticipated internal threats over the next 12 months, at 94%.

The most prevalent external threats were **theft of company physical property** and **vandalism**, both reported by 26% of those surveyed and above the world averages of 22% and 20%, respectively. **Theft of company physical property** is likely to decline in the next year by two percentage points. **Fraud** is anticipated to be the biggest external threat for 29% of respondents in the coming 12 months. Only Sub-Saharan Africa is expected to exceed this according to 34% of participants.

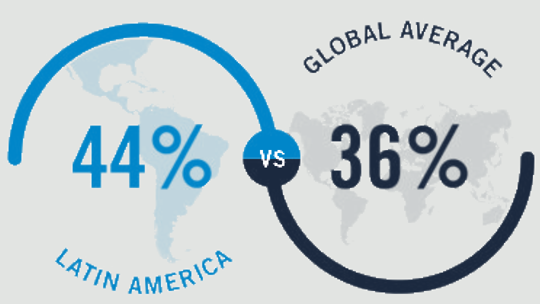
The threat actor group that most affected participants in the last year was **petty criminals** and, at 44%, was significantly above the world average of 36%. **Subversives – hackers, protestors, or spies** are anticipated to impact 50% of respondents in the next 12 months, a significant 18 percentage point increase from the previous year.

Economic unrest is expected to be the biggest hazard in the next 12 months by 43% of those surveyed. Last year, **pandemics** was reported by 51% as the most experienced hazard. Concern about **pandemics** is likely to drop by 10 percentage points this year.

Physical security budgets will increase significantly for 49% of participants, above the global mean of 46%. The drivers behind this are **rising operational costs** cited by 50% and **international economic instability** reported by 47% of those surveyed. Security budget priorities will be focused on **training staff** at 59% and above the world average of 52%, and **introducing new technology**.

Latin America-based companies are the most advanced in the world in their use of **cutting-edge** and **emerging** technology, with 45% of participants at this level of innovation and well above the world average of 38%. Those surveyed have aspirations of becoming even more advanced, with 65% seeking to reach this level of advancement within 12 months, well ahead of the average aspiration of 52%.

Previously



Were impacted by **petty criminals** in the last year.

Regional

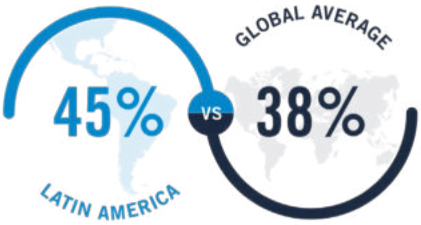
Over the next five years, companies in the region will invest the most in **AI-powered surveillance and monitoring systems** and **biometrics and facial recognition** technology at 49% and 44%, respectively, above the global averages of 42% and 40%, respectively.

Participants in the region reported that the main barriers to using new technology were the **cost of implementation** reported by 43% and the **cost of maintenance** reported by 38%.

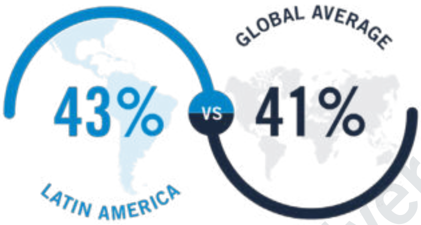
Hiring the right people is very challenging in Latin America, with 66% of respondents reporting it is **extremely** or **very challenging** to recruit – second only to North America at 71%. The biggest barriers to hiring are finding people with the **appropriate skills** at 61%, followed by the right **experience** at 59%.

The qualities most sought after in security officers in the region are **integrity and honesty**, a **strong understanding of technology**, **industry-specific experience** and **emotional intelligence**. The least important attributes were having a **military or law enforcement background** and the **ability to speak multiple languages**.

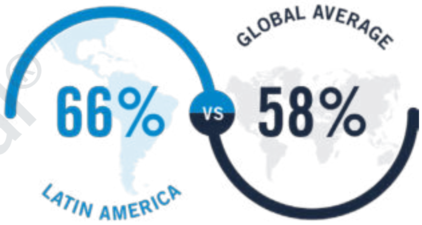
Currently



Use **cutting-edge** and **emerging** technology.

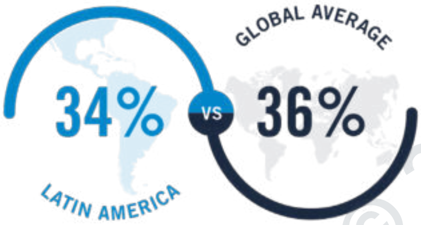


Said the main barriers to using new technology were the **costs of implementation**.

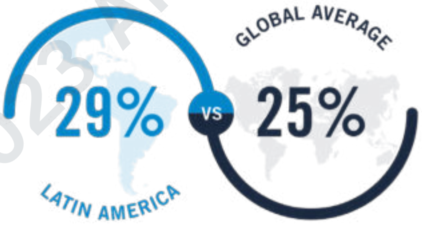


Said **hiring the right people** is very challenging.

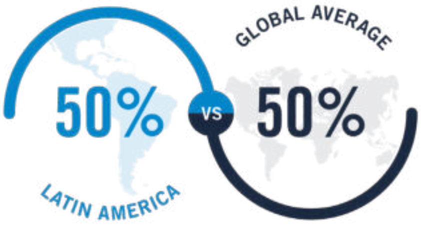
Looking Forward



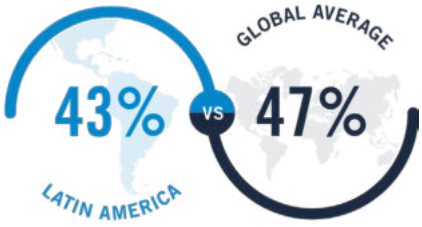
Expect to be impacted by internal **leaking sensitive information** in the next 12 months.



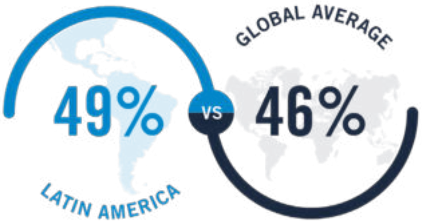
Anticipate **fraud** will be the biggest external threat in the next year.



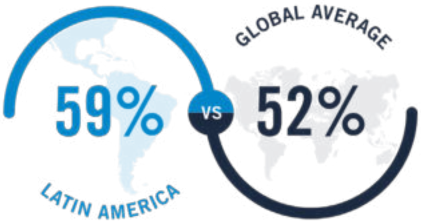
Expect to be impacted by **subversives** in the next 12 months.



Expect to be impacted by **economic unrest** in the next year.



Said their physical security budget will increase **significantly** in the next year.



Will prioritize spending on **training staff**.

Middle East

Companies in the Middle East suffered fewer internal threats than the global average. The most common internal incident was **misuse of company resources or data**, noted by 35% of respondents over the last 12 months, closely followed by **leaking sensitive information** at 34%.

Leaking sensitive information is expected to be the biggest internal threat at 35%, while **misuse of company resources or data** is expected to decline in the next year.

External threats were lower than the world average with 78% having experienced an incident. The most common was **fraud**, experienced by 22% of respondents, followed by **phishing and social engineering**, impacting 20% of those surveyed.

External threats are expected to jump in the next year, with 87% of respondents anticipating they will experience one, with **fraud** noted by 25% of respondents as the biggest potential threat. The second biggest is **malicious damage to company property**, expected by 24% of those surveyed.

Security-impacting hazards were experienced by 75% of companies over the last year, below the world average. The most experienced was **economic unrest**, reported by 38% of respondents, in line with the world average. This was closely followed by **climate change**, the impact of which was reported by 36%, slightly above the global mean.

The impact of hazards is expected to increase significantly in the coming year, anticipated by 91% of companies. **Economic unrest** is expected to jump to 44% and **climate change** hazards are also likely to rise, according to 41% of those surveyed.

Threat actor groups impacted 69% of companies in the Middle East over the last year, below the global average of 76%. This is expected to jump in the next 12 months to 84% of those surveyed.

Economic criminals were the threat actor group that most affected the Middle East, reported by 41% of respondents and above the global average, while 36% said they were affected by **subversives – hackers, protestors, or spies**. The threat from **subversives** is expected to soar with 50% expecting to be impacted, while the threat from **economic criminals** will also increase, according to 48% of companies.

Investment in physical security will increase, with 52% expecting to spend significantly more in the next year, above the global average and beaten only by North America. **Domestic security concerns** and **rising operating costs** are driving this. Security budget priorities will be focused on **introducing new technology** and **training staff**, reported by 59% and 52% of respondents, respectively.

Cutting-edge or **emerging** security technologies were used by 32% of companies in the region, below the global average of 38% at this level of innovation.

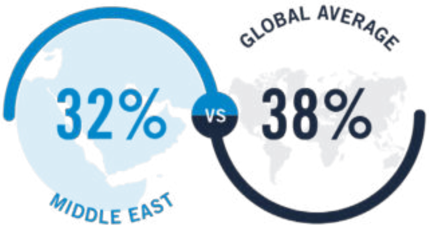
Basic or **minimal** technology is used by 42% of companies, the highest of any region suggesting the Middle East is behind the curve in technology uptake. Companies expect to invest in technology with 47% reporting they want to be using **emerging** or **cutting-edge** technology in a year's time. This lags the global ambition of 52%.

The biggest barrier to using technology was a **lack of internal expertise** reported by 44% of companies, higher than the global average of 35%. Over the next five years **artificial intelligence (AI)** and **biometrics** will be the biggest areas of investment, in line with global trends.

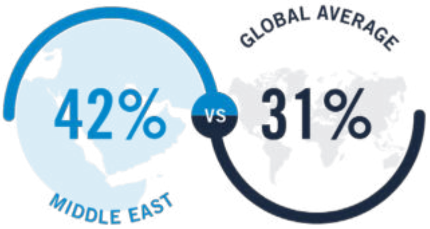
Hiring the right people in the Middle East was less challenging than every other region apart from Sub-Saharan Africa, with 47% of participants finding it **extremely** or **very challenging** to find the right people. Finding people with the **appropriate skills** was the most challenging according to 49% of respondents.

The three most important qualities in security professionals are: **integrity and honesty**, **a strong understanding of technology** and **industry specific experience**.

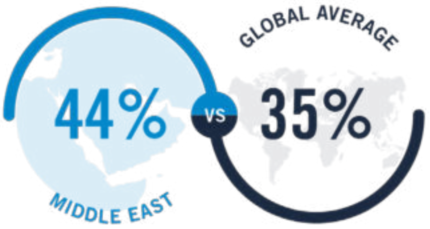
Currently



Use **cutting-edge** or **emerging security** technology.

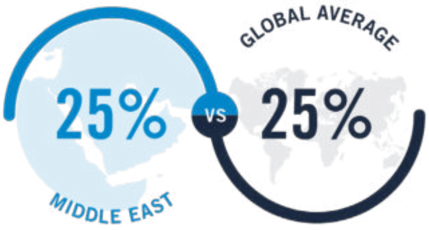


Of companies use only **basic** or **minimal** security technology.

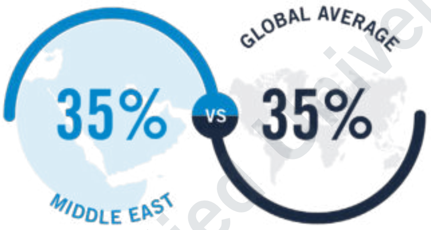


Said the biggest barrier to using technology is a **lack of internal expertise.**

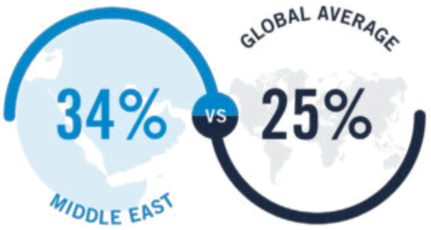
Looking Forward



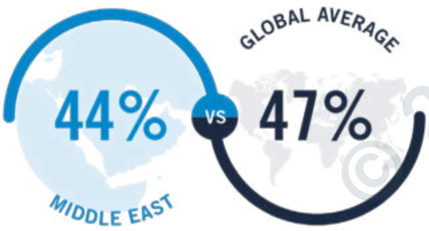
Anticipate they will be impacted by external **fraud.**



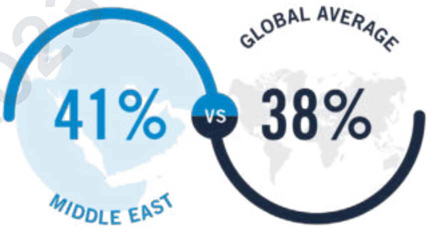
Said **leaking sensitive information** will be the biggest internal threat.



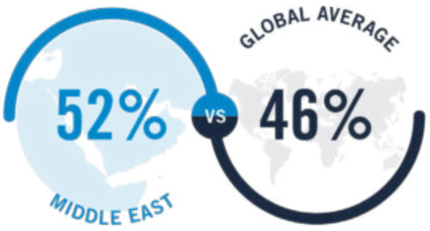
Predict that **copyright infringement** will be the second biggest internal threat next year.



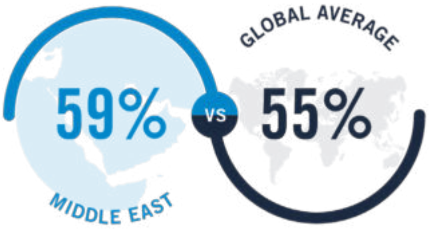
Expect to be impacted by **economic unrest.**



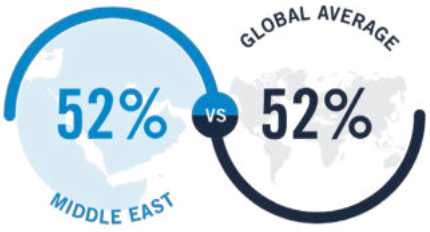
Expect to experience **climate change.**



Expect to spend **significantly** more on physical security in the next year.



Will spend on **introducing new technology.**



Will invest in **training staff.**

North America

North American companies have faced significant internal and external threats and security-impacting hazards over the last 12 months, all significantly above the global average. This is expected to ease slightly over the next year, but security-impacting hazards are a concern.

The most experienced internal threat was **copyright infringement** at 41%. This was closely followed by **theft of company physical property**, **misuse of company resources or data**, **leaking of sensitive information** and **policy violations**, all reported by 39% of respondents and well above the world mean. **Theft of physical property** is expected to remain at that level over the next year, while the rest are predicted to decline.

Top of the list of external threats experienced was **theft of company physical property**, with 32% of respondents reporting they had experienced this, 10 percentage points above the global average. This was followed by **malicious damage to company property**, experienced by 28% of companies, versus a world average of 21%.

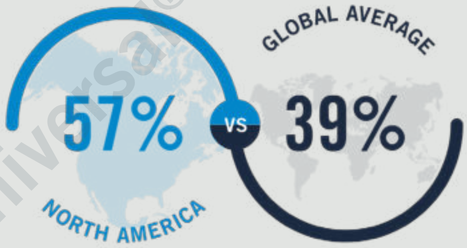
Phishing and social engineering and **vandalism** are predicted to increase, while all other external threats will decline slightly over the next 12 months.

Economic criminals were responsible for the greatest number of security incidents in the last year, with 57% of respondents citing this threat actor group as affecting them. This was markedly above the global mean of 39% and is expected to increase further over the next year.

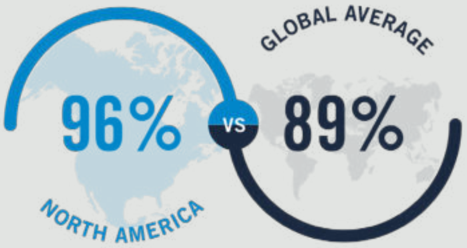
Economic unrest was a serious security-impacting hazard, experienced by 47% of North American respondents in the last 12 months. This compares to a global average of 39%, the biggest hazard experienced globally.

Climate change was the second biggest hazard reported by 42% of respondents, this is substantially higher than the world mean of 34%. Both of these hazards are likely to worsen for companies over the next year, with the impact of **climate change** rising to 48% of respondents and **economic unrest** to 49%.

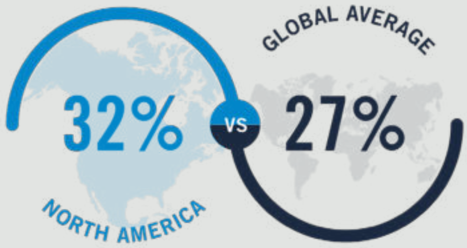
Previously



Were impacted by **economic criminals.**



Of companies experienced an **external threat** in the last 12 months.



Of respondents experienced **theft of company physical property.**

Regional

Companies plan to invest significantly more in physical security in the next year with 59% confirming this and well above the global average. This is driven by **rising operational costs** at 56%, **domestic security concerns** and **duty of care to employees**, both at 53% – all significantly above the world view.

Security budget priorities will be focused on **introducing new technology** at 58% and spending on **compliance and regulatory requirements** at 54%, both above the world average.

Companies intend to implement more effective security as the main impact of all threats, with 39% making this choice in North America, well above the global average of 32%.

North America is the third most advanced region in the use of **cutting edge** and **emerging** technology at 40% of those surveyed. Latin America and Asia Pacific had a higher concentration of companies using this level of innovation.

However, North America also has the second highest percentage of companies using only **basic** or **minimal** technology at 36%, suggesting that there is a big gap between the most and least advanced.

Over the next five years and in line with global trends, **artificial intelligence (AI)** and **biometrics and facial recognition** will be the biggest areas of investment by 44% and 42% of respondents, respectively. Companies will also invest in robotics, drones and autonomous vehicles at a rate well above the global average.

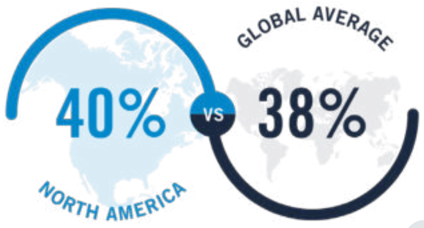
The biggest barrier to using more technology cited by 45% of companies was **cost of maintenance** and **lack of skills in the security workforce** at 42%, both above the average.

Hiring the right people is more challenging in North America than anywhere else, with 71% saying it is **extremely** or **very** challenging to recruit.

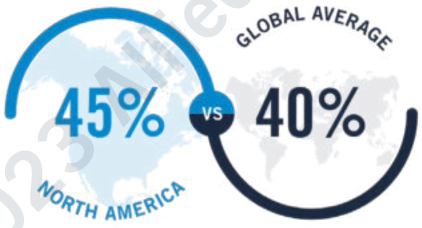
The biggest barriers to finding the right people are **experience** at 60%, the **appropriate skills** at 58% and **workforce diversity** at 57%, all more challenging in North America against the world average.

Integrity and honesty, the **ability to speak multiple languages**, a **military or law enforcement background** and customer service skills were the most sought-after qualities in security professionals in North America. The least important attributes were **a strong understanding of technology** and **emotional intelligence**.

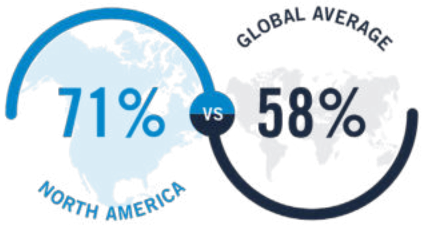
Currently



Of companies use **cutting-edge** or **emerging** security technology.

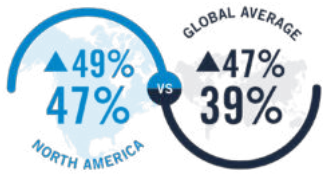


Said **cost of maintenance** was the biggest barrier to using more technology.

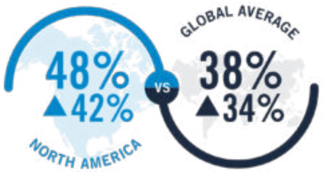


Said **hiring the right people** is extremely or very challenging.

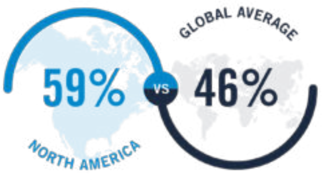
Looking Forward



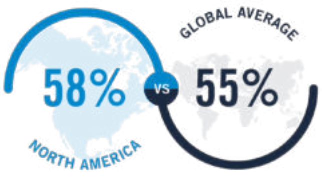
Said **economic unrest** was the biggest security-impacting hazard. This is expected to rise next year.



Climate change is anticipated to impact respondents in the next 12 months, up from the previous year.



Will invest **significantly** more in physical security in the next 12 months.



Expect to spend on **introducing new technology.**

Sub-Saharan Africa

Companies in Sub-Saharan Africa faced the most significant internal threats of all regions in the last 12 months: 96% reported an internal threat compared with the global average of 89%.

The two greatest internal threats, reported by 49% of respondents, were **fraud** and **misuse of company resources or data**.

Internal incidents are expected to remain at the same level next year, with Sub-Saharan Africa still the most impacted region in the world. **Misuse of company resources or data** is expected to be the highest threat for 54% of respondents, significantly higher than the global average of 35%.

Companies in Sub-Saharan Africa are also battling external threats at a higher rate than the global average. The two most experienced external threats in the last year were **fraud** at 33%, and **vandalism** at 27%. **Fraud** is expected to increase to 34% next year, the highest level of any region in the world.

The biggest jump in external threats next year is likely to be in **theft of company physical property**, expected by 28%, compared to 19% who experienced it in the previous year.

The threat actor group that most affected the region was **subversives – hackers, protestors or spies** – with 52% of respondents reporting they were impacted over the last year, well above the world average. This is likely to worsen, with 58% anticipating they will be affected in the coming year.

The threat from **economic criminals** represented the biggest jump, with 53% expecting to be affected in the next year. That is a 10-percentage point increase, making it the second-biggest group likely to affect the region.

Economic unrest was the biggest security-impacting hazard, reported by 49% in the last year; and it is expected to increase to 52% in the upcoming year, ahead of the global mean. **Climate change** was the second greatest hazard reported by 44% of respondents, this will stay the same over the next 12 months. **Disruption of energy supplies** at 48% will be the second biggest impact in the next year, up 10 percentage points compared with the previous year and significantly above the world average.

Companies plan to invest in physical security with 43% of respondents reporting they will significantly increase spending next year, albeit this is below the global mean. The two biggest drivers are **rising operating costs** and **international economic instability**. Security budget top priorities are **training staff** at 72%, **introducing new technology** at 67% and **risk assessment/threat analysis** at 60%. Companies in the region will spend on these priorities at levels well above the global average.

Companies in the region are the third most advanced in the world after Latin America and North America in their use of **cutting-edge** or **emerging** technology, with 39% of companies at the highest level of innovation. The region also has the second lowest level of companies using **basic** or **minimal** technology at 25%, behind only Latin America which is the most advanced region in the world for security technology use.

Biometrics and facial recognition will be the biggest area of technology investment in the next five years according to 59% of those surveyed in Sub-Saharan Africa, followed by **internet of things and connected devices** at 46%. This is significantly above the global average for investment in these areas.

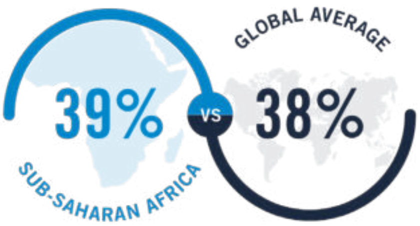
Regional

The biggest barrier to using more technology cited by 52% of companies in the region was the **cost of maintenance**, much higher than the global average of 40%.

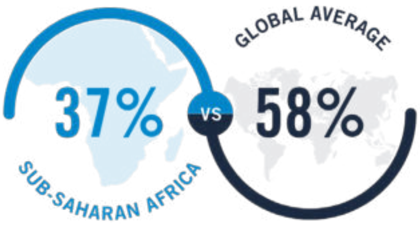
Hiring the right people in Sub-Saharan Africa was less challenging than in any other region, with only 38% of respondents reporting it is **extremely** or **very** challenging to recruit.

The biggest barrier to hiring is the **perception of low career progression**, followed by finding people with the **appropriate skills** and **experience.** The qualities in security professionals that are most attractive in Sub-Saharan Africa are **integrity and honesty** and **industry-specific experience**, both well above the global average. The least important attribute was having a **military or law enforcement background**.

Currently

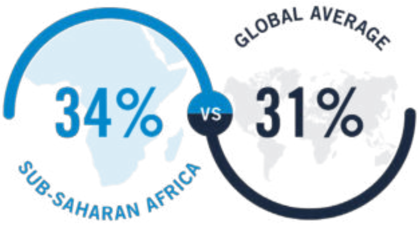


Of companies use **cutting-edge** or **emerging** technology.

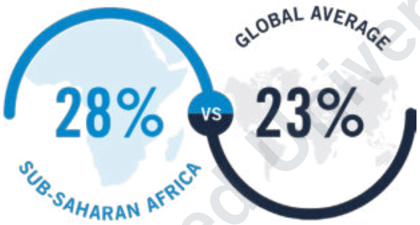


Reported it is **extremely** challenging to recruit.

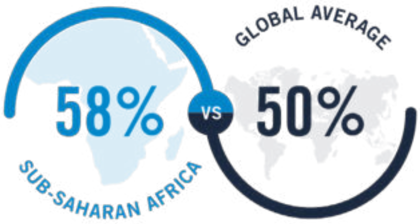
Looking Forward



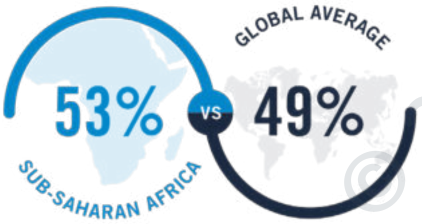
Are likely to experience external **fraud** in the next 12 months.



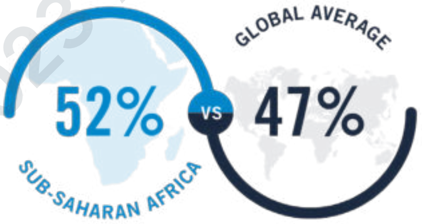
Are likely to be impacted by external **theft of company physical property.**



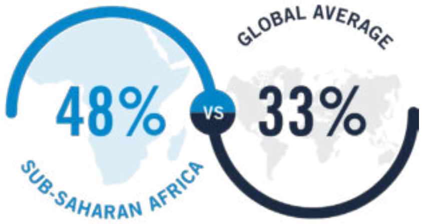
Anticipate they will be affected by **subversives** in the next year.



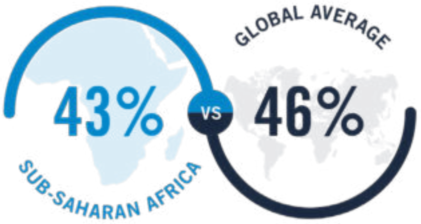
Expect to be affected by **economic criminals** in the coming 12 months.



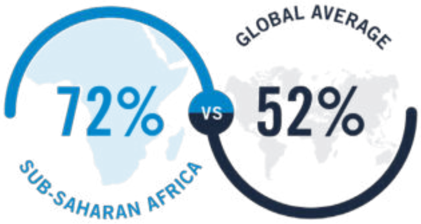
Predict they will experience **economic unrest** in the upcoming year.



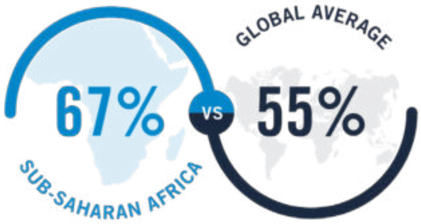
Expect to be affected by **disruption of energy supplies.**



Will **significantly** increase spending on physical security.



Will invest in **training staff.**



Will invest in **introducing new technology.**

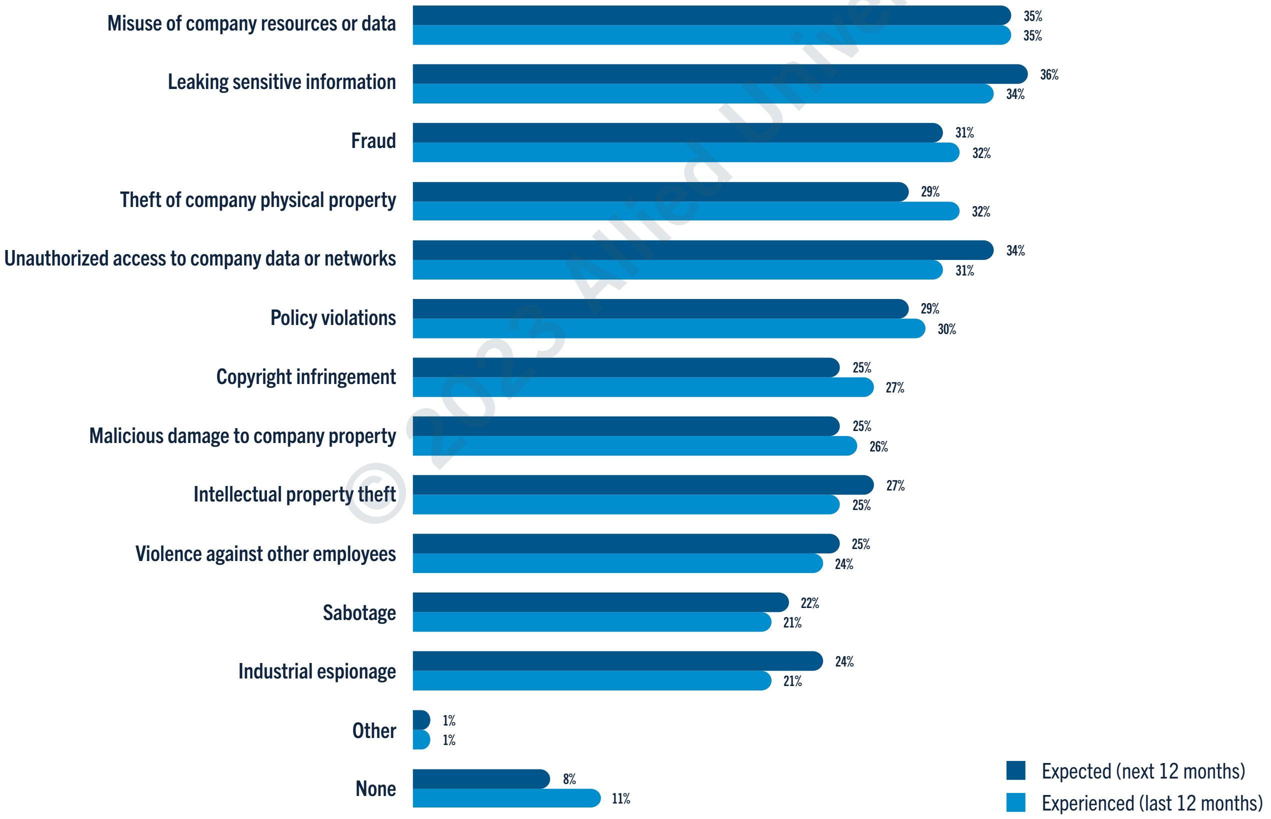
Appendix

Charts

Chapter One: Emerging and Evolving Threats

Internal Threats

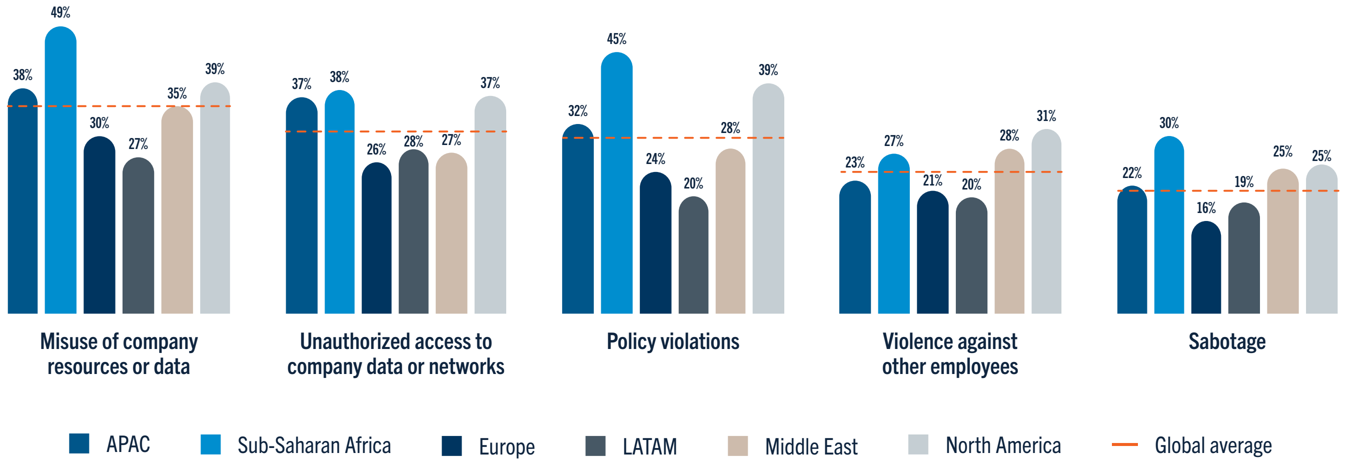
Experienced vs Expected Threats - Global Average



Q: What internal security threats has your company experienced incidents of in the last 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 companies (Global n=1775)

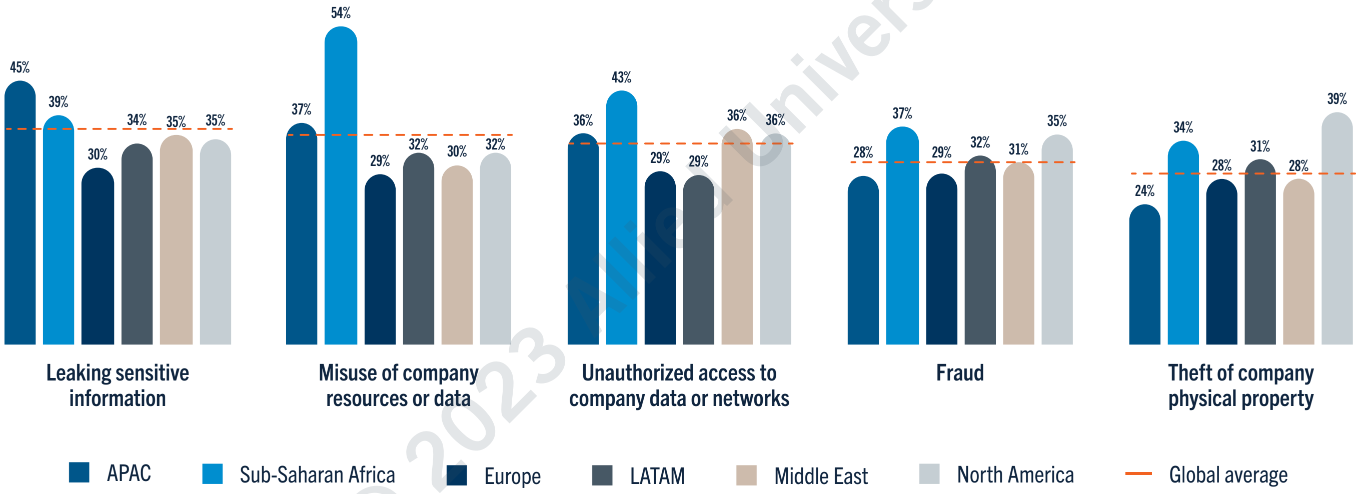
Appendix

Top 5 Most Experienced Internal Threats
Regional Comparison



Q: What internal security threats has your company experienced incidents of in the last 12 months?
Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

Top 5 Most Expected Internal Threats
Regional Comparison

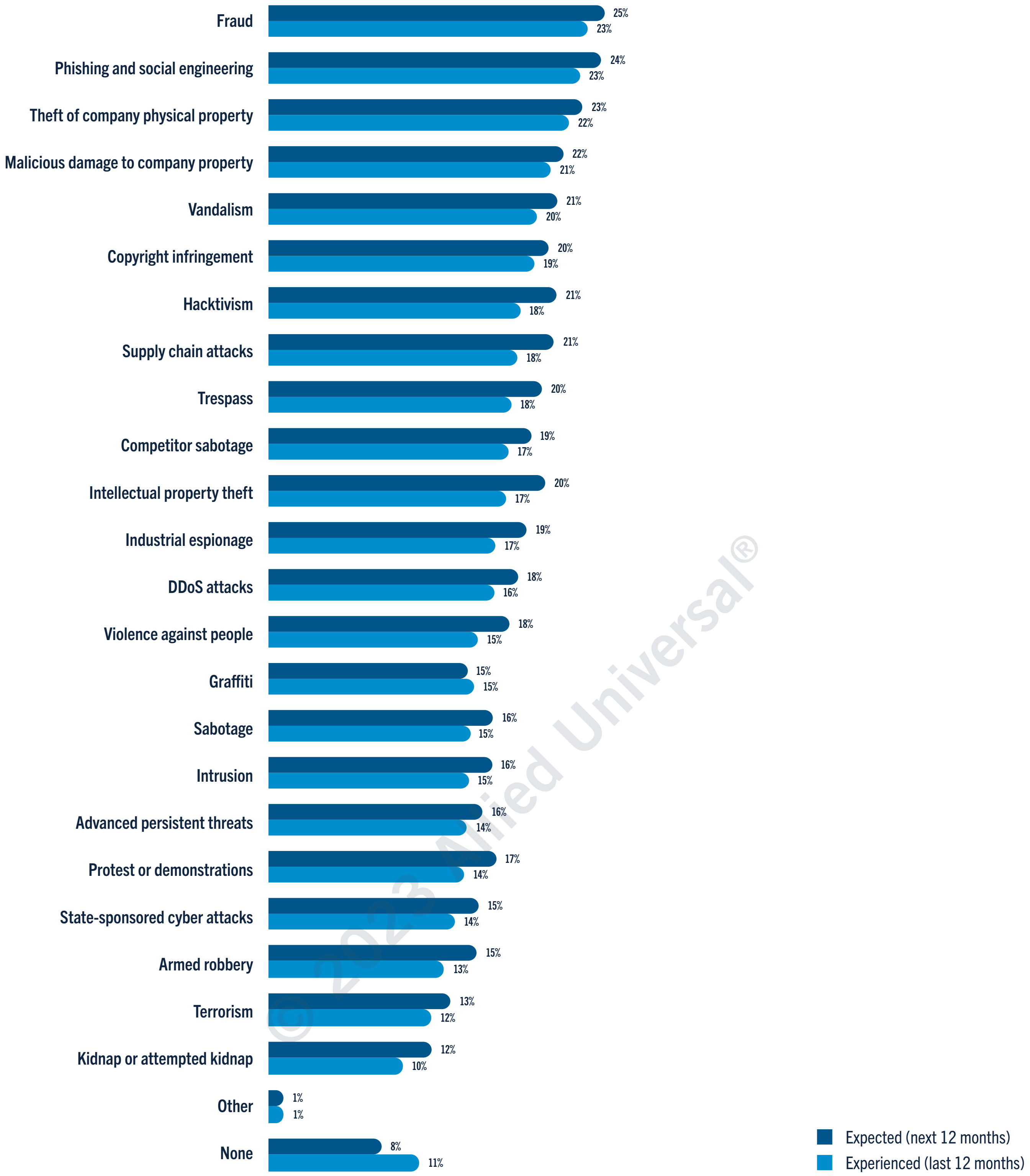


Q: What do you see as genuine internal security threats for your company over the next 12 months?
Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

Appendix

External Threats

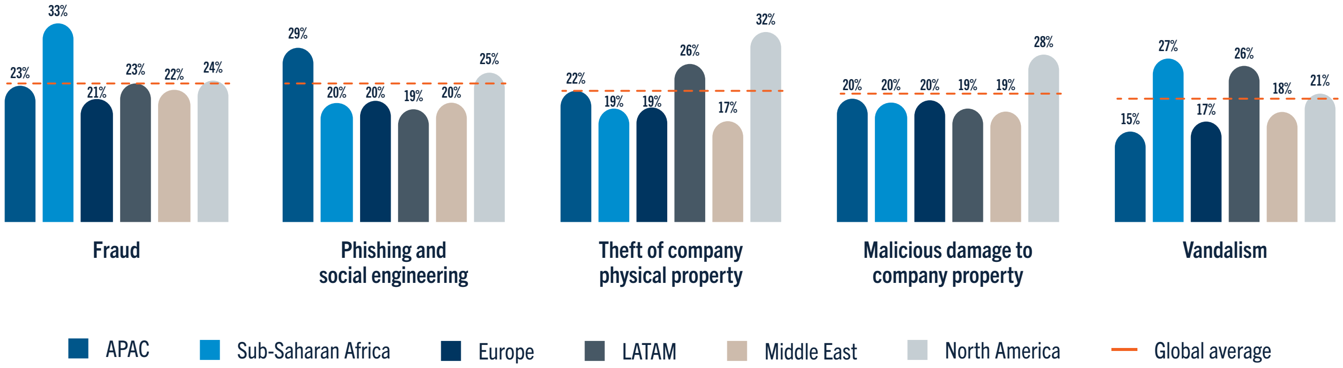
Experienced vs Expected Threats - Global Average



Q: What external security threats has your company experienced incidents of in the last 12 months?
Q: What 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)

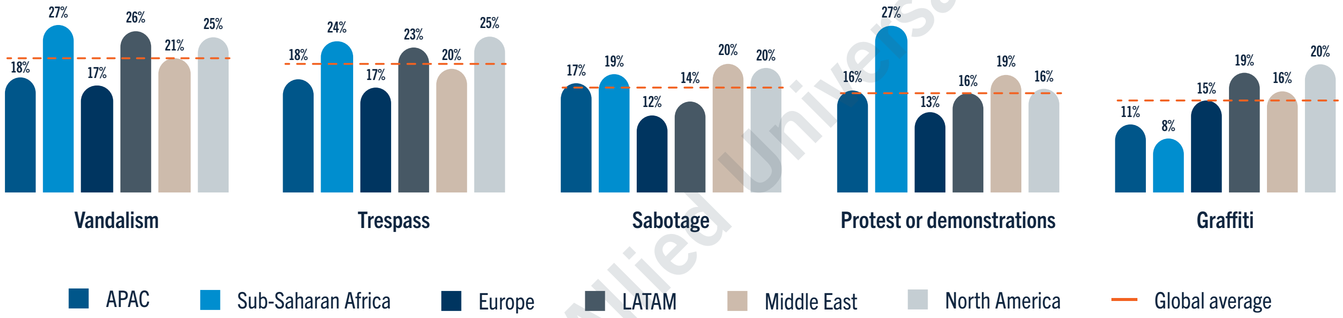
Appendix

Top 5 Most Experienced External Threats
Regional Comparison



Q: What external security threats has your company experienced incidents of in the last 12 months?
Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

Top 5 Most Expected External Threats
Regional Comparison

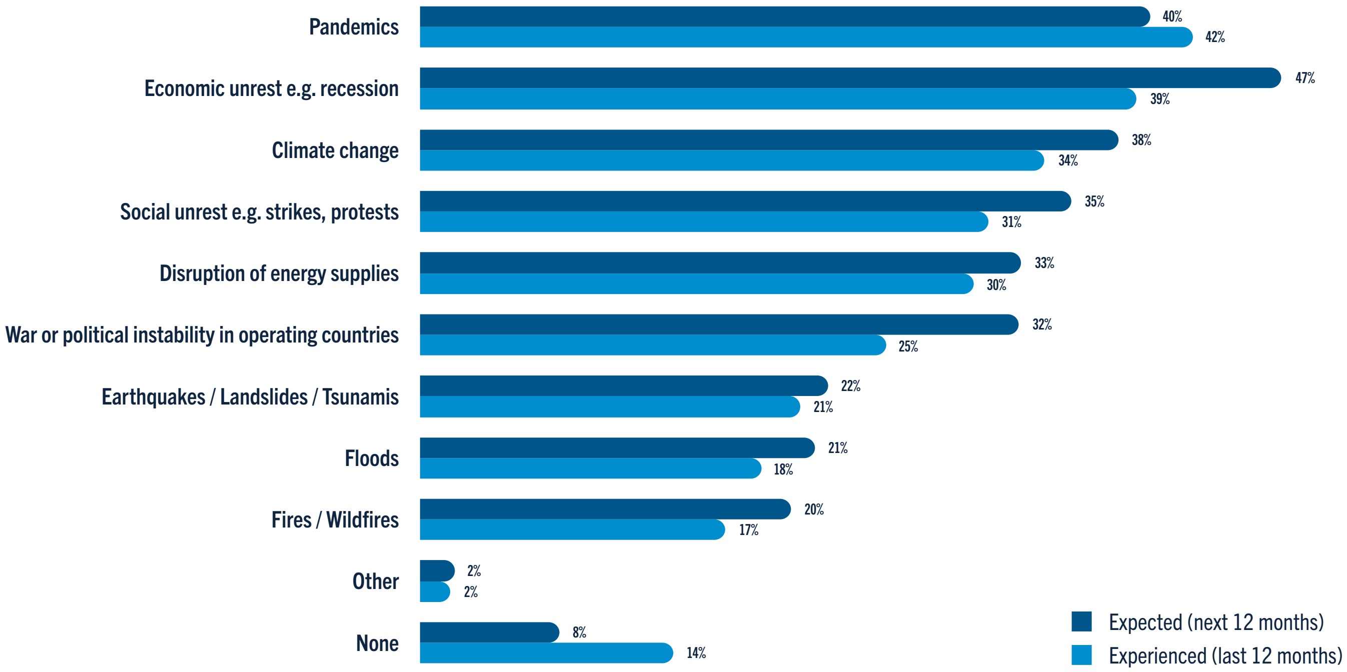


Q: What do you see as genuine external security threats for your company over the next 12 months?
Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

Appendix

Security-impacting Hazards

Experienced vs Expected Hazards - Global Average



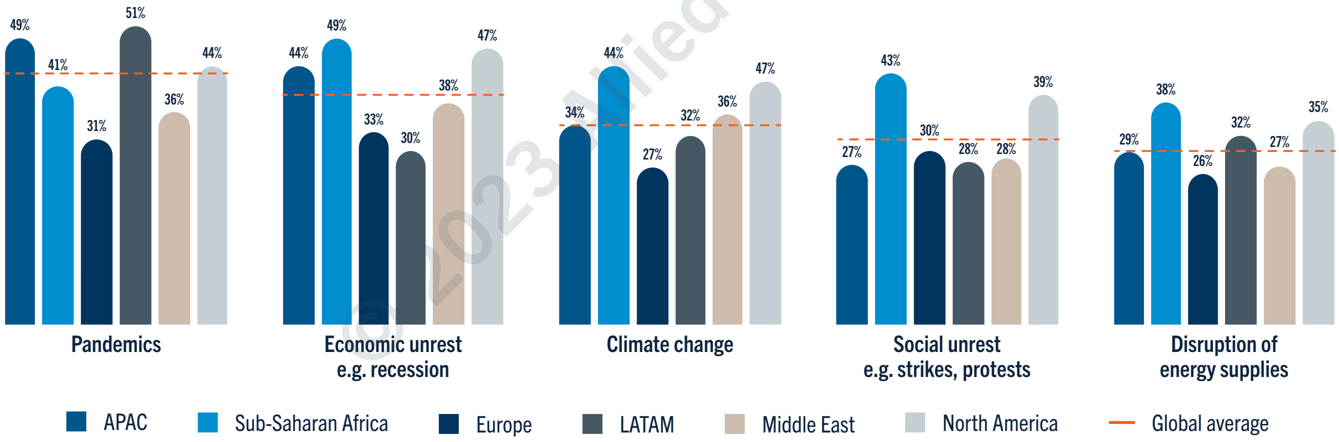
Q: Has your company experienced any incidents of the following security impacting-hazards in the last 12 months?

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

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

Top 5 Most Experienced Security-impacting Hazards

Regional Comparison



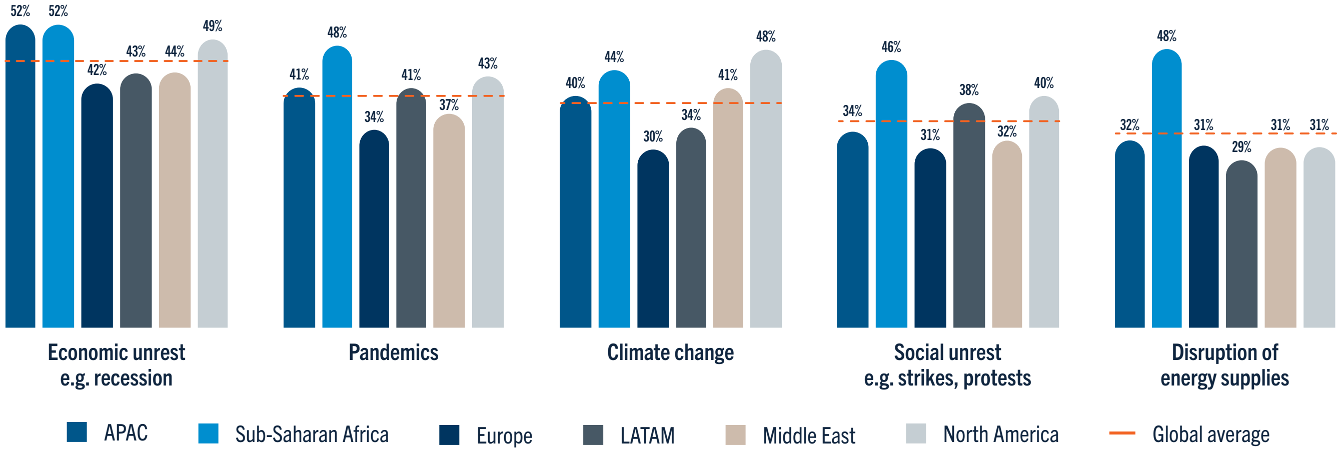
Q: Has your company experienced any incidents of the following security impacting-hazards in the last 12 months?

Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

Appendix

Top 5 Most Expected Security-impacting Hazards

Regional Comparison

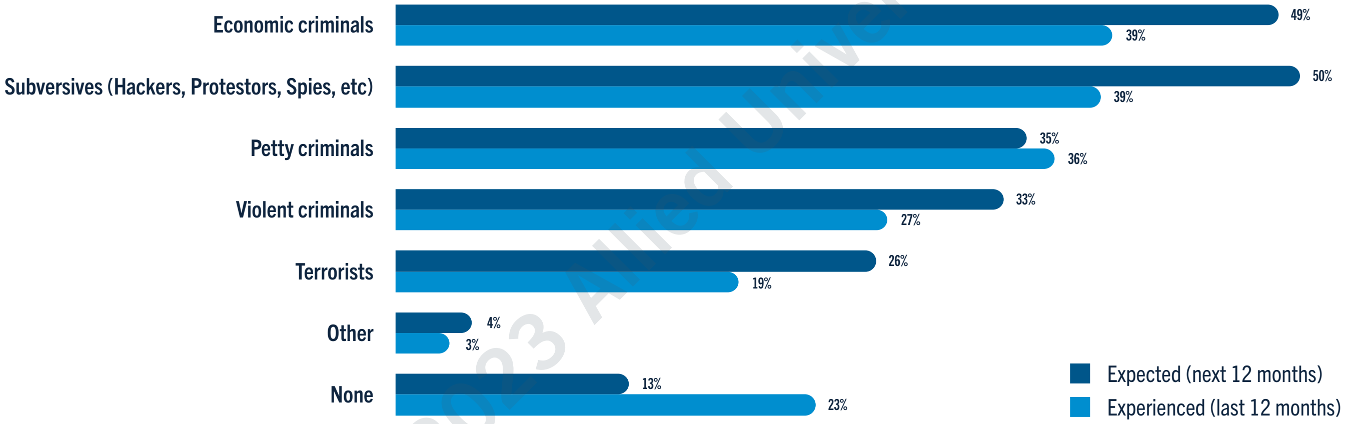


Q: What do you see as genuine security-impacting hazards for your company over the next 12 months?

Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

Threats By Groups

Experienced vs Expected Threats - Global Average



Q: Has your company experienced any security incidents involving any of the following groups in the last 12 months?

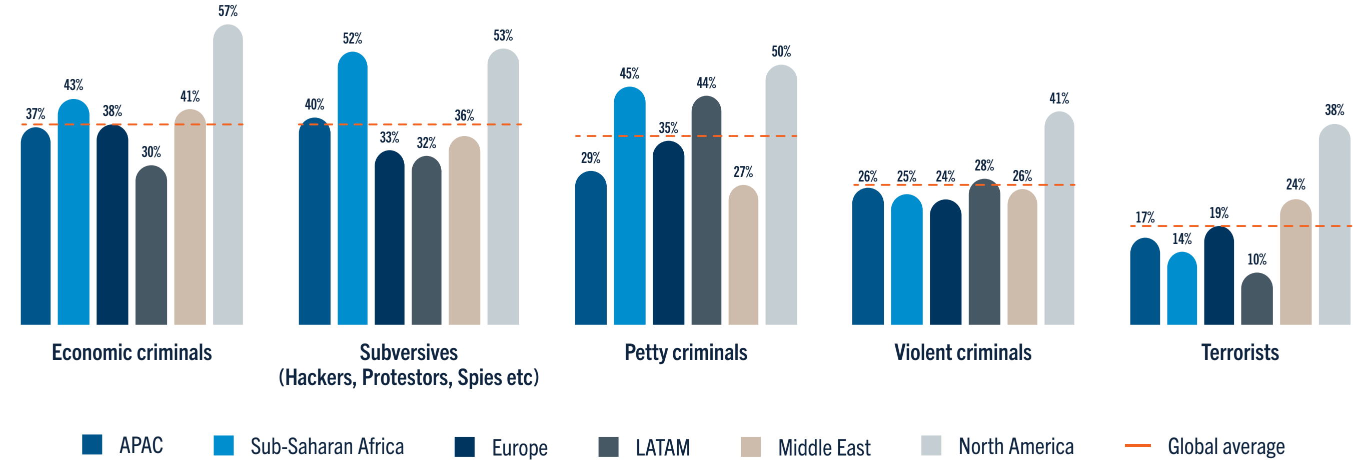
Q: What groups do you see as genuine security threats to your organisation over the next 12 months?

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

Appendix

Most Experienced Threats By Threat Actor Groups

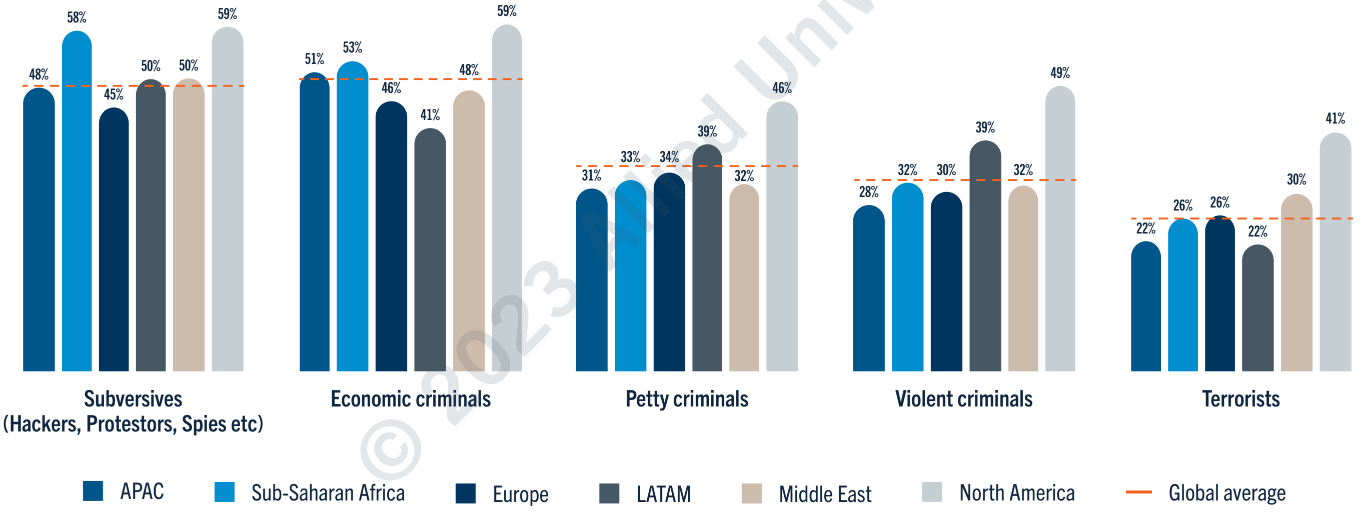
Regional Comparison



Q: Has your company experienced any security incidents involving any of the following groups in the last 12 months?
Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

Most Expected Threats By Threat Actor Groups

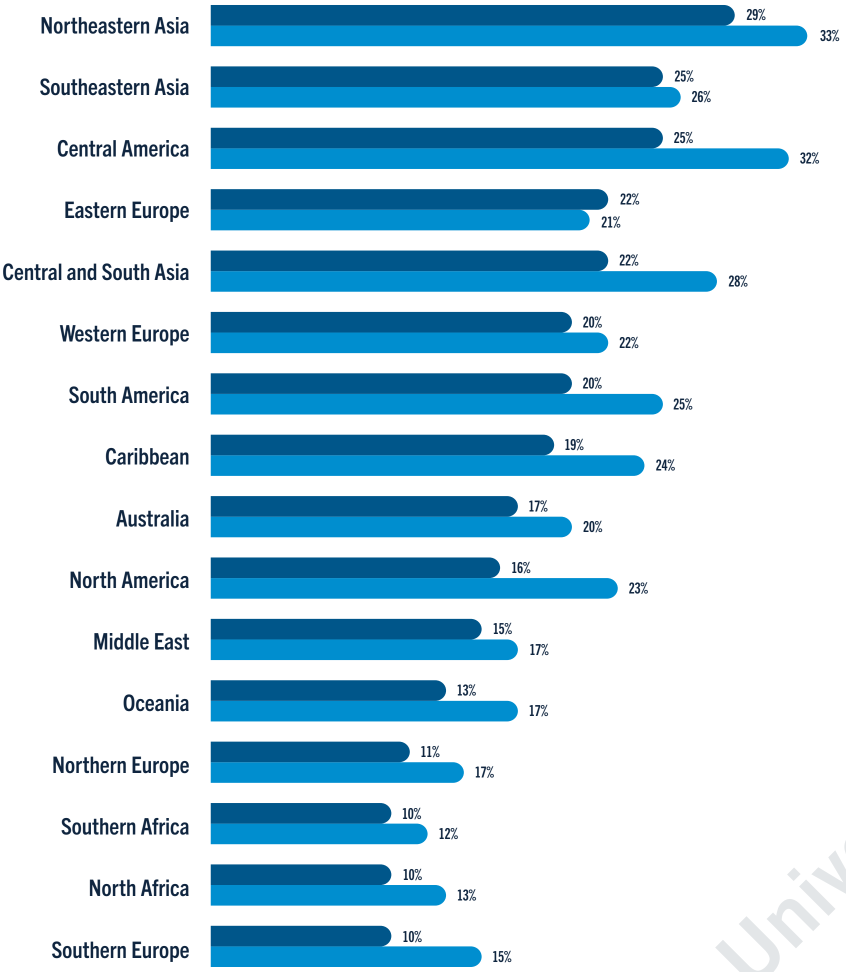
Regional Comparison



Q: What groups do you see as genuine security threats to your organisation over the next 12 months?
Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

Appendix

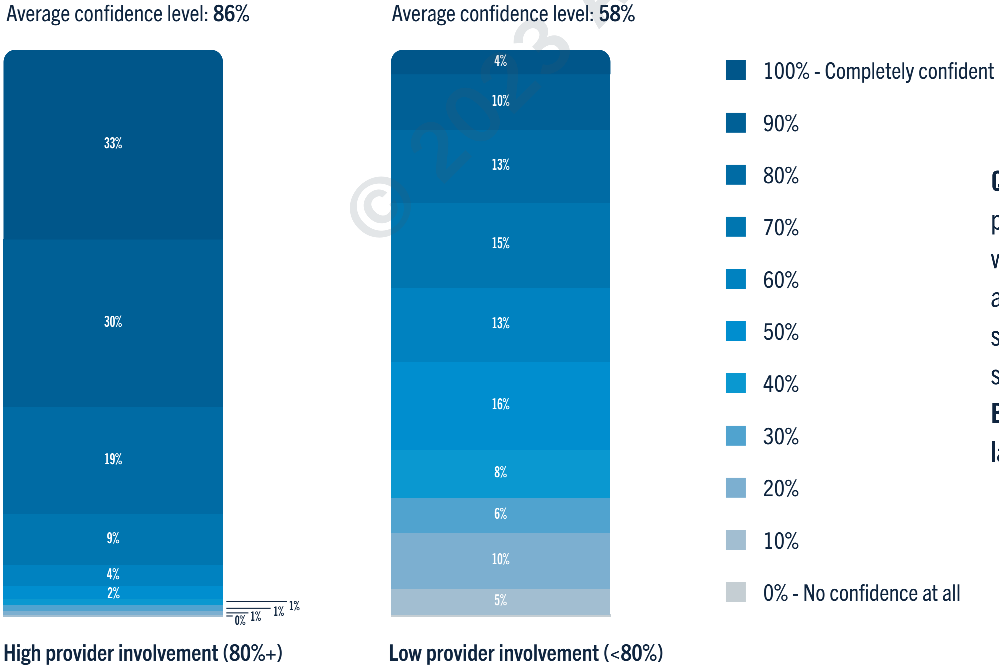
Considered Dangerous Geographies For Companies To Operate In
Global View vs View From Those Operating In That Region



Q: Which do you consider to be dangerous geographies to operate in when measuring the threats and potential risks?
Base: Chief security officers from large companies (Global n=1775)

- Global view of dangerous regions
- View from those operating in that region

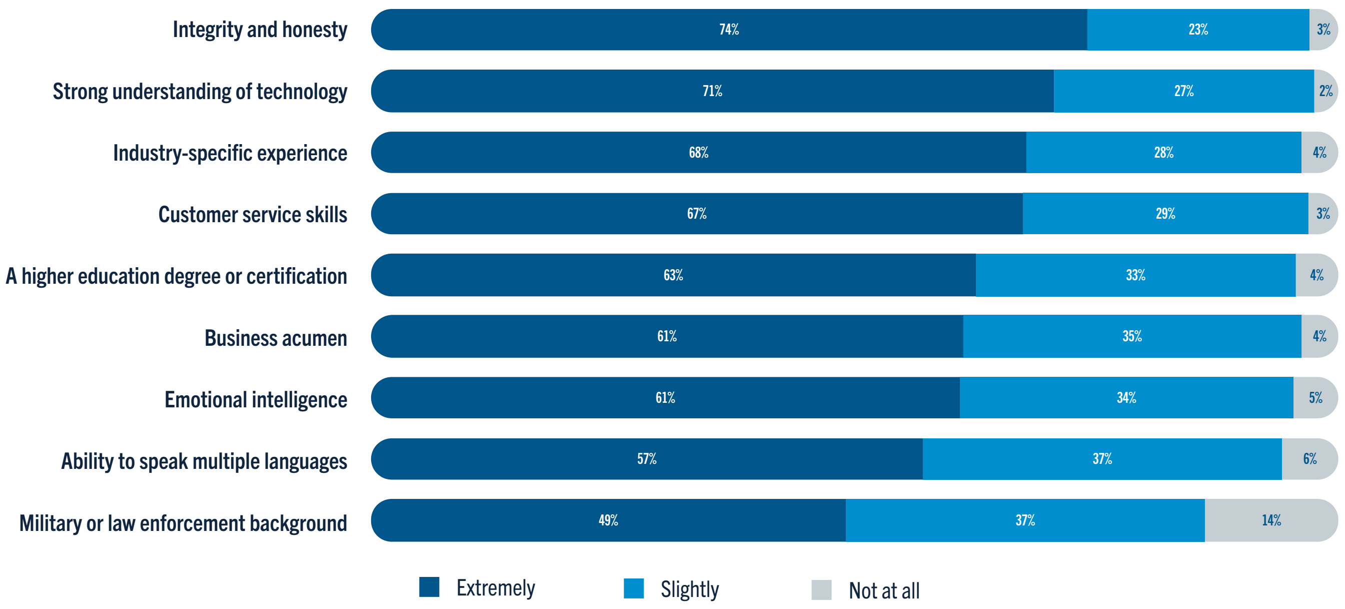
Percentage Of Security Provided By Supplier Confidence To Deal With Overall Security Issues
Global Average



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? (Your company's security overall)
Base: Chief security officers from large companies (Global n=1775)

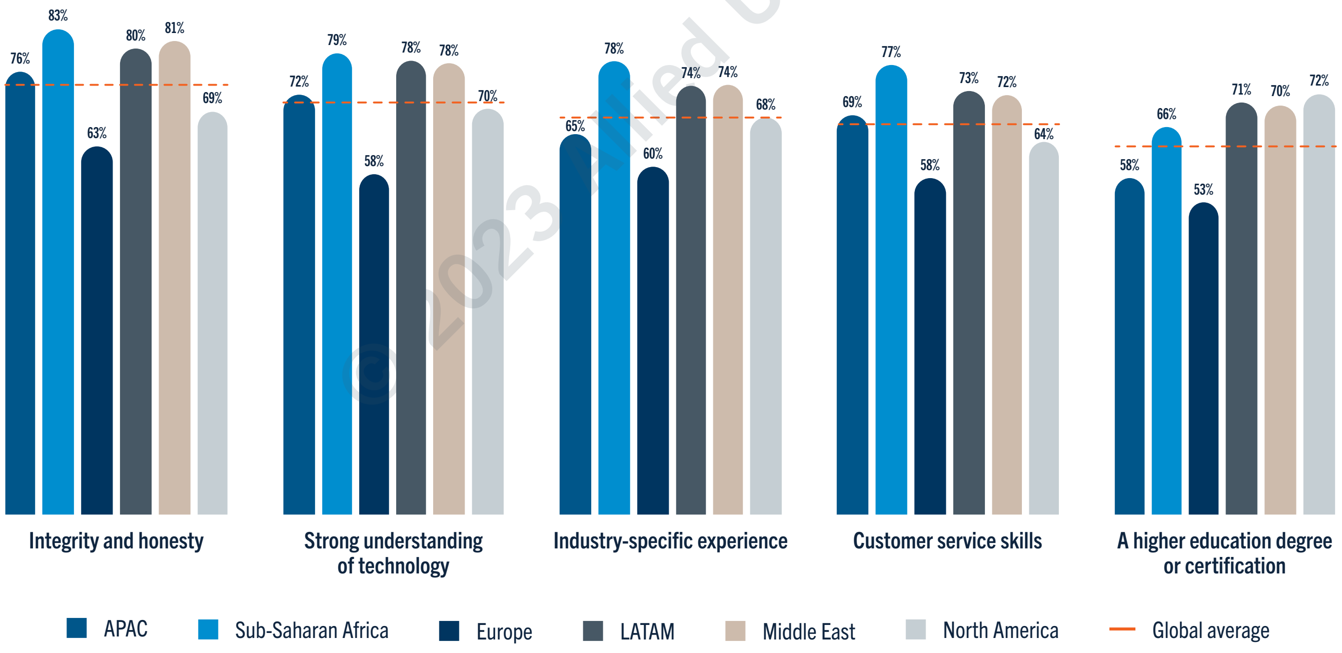
Chapter Two: People in Security

Importance Of Frontline Officer Skills
Global Average



Q: How important are the following for people working in security as a front-line officer or similar?
Base: Chief security officers from large companies (Global n=1775)

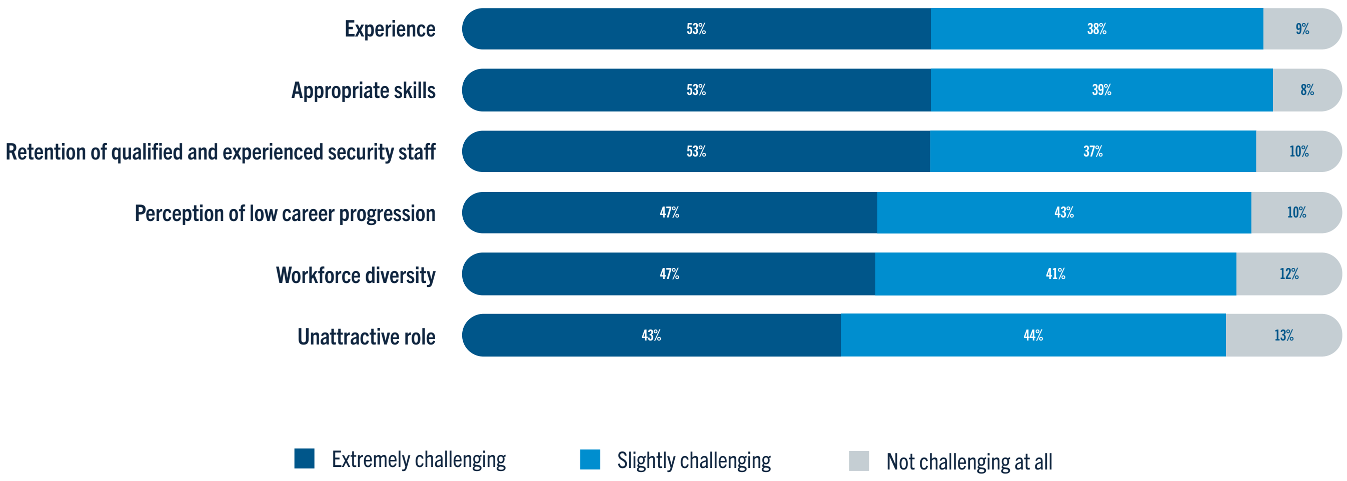
Top 5 Most Important Frontline Officer Skills
Regional Comparison



Q: How important are the following for people working in security as a front-line officer or similar?
Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

Appendix

Challenges To Recruitment Of Security Staff
Global Average

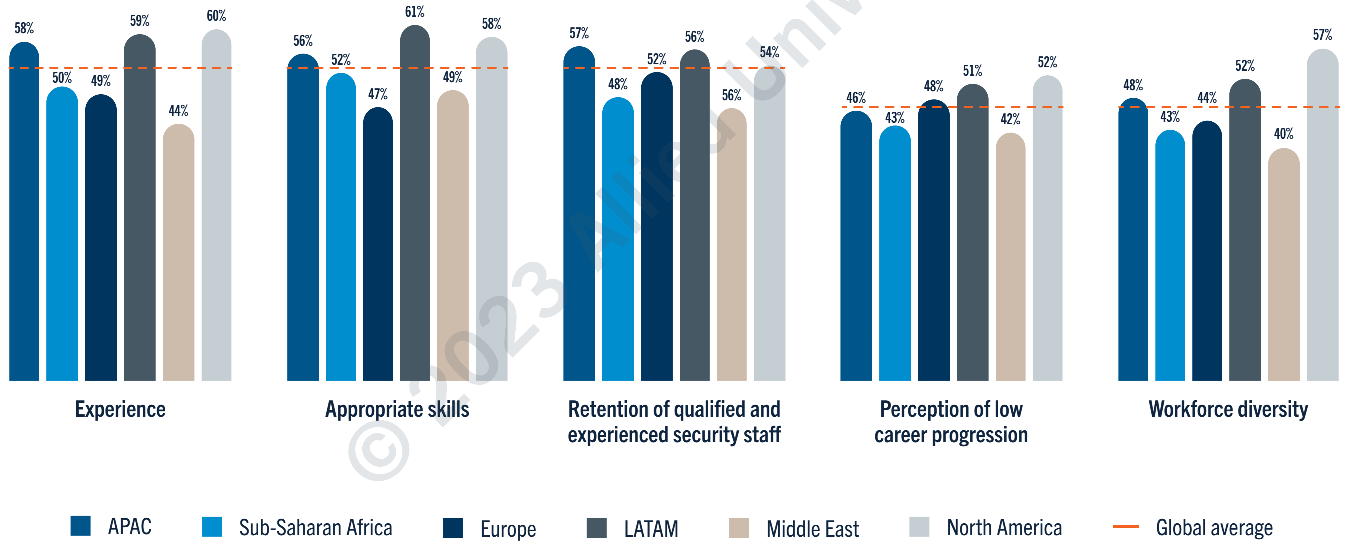


Q: How challenging are the following areas to the recruitment of security staff?

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

Top 5 Biggest Challenges To Recruitment
Regional Comparison

% show **'extremely challenging'** score



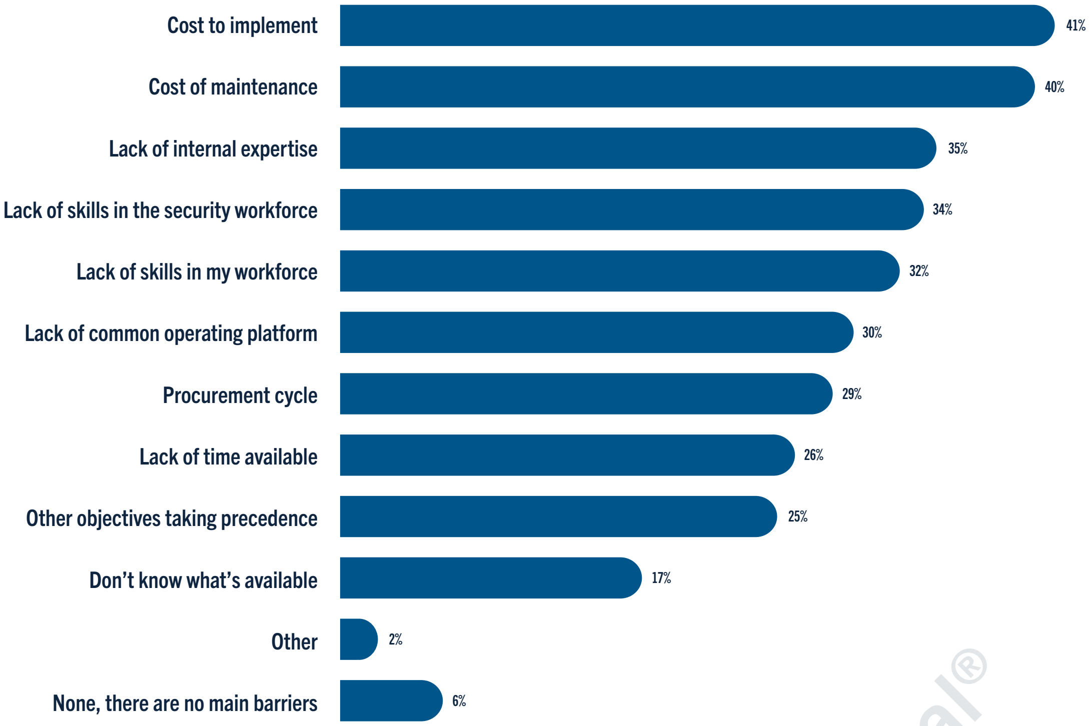
Q: How challenging are the following areas to the recruitment of security staff?

Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

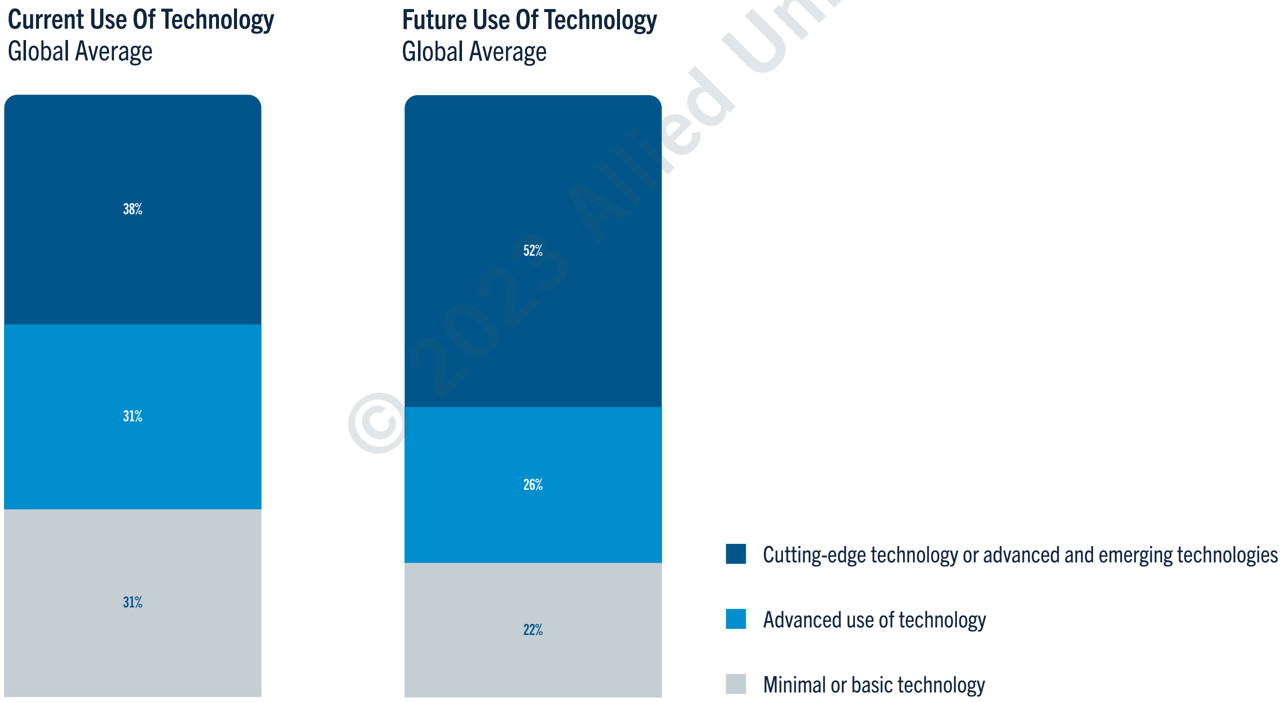
Chapter Three: Technology and Security

Barriers To Implementing Security Technology

Global Average



Q: What are the main barriers to implementing technology within your security operations?
Base: Chief security officers from large companies (Global n=1775)

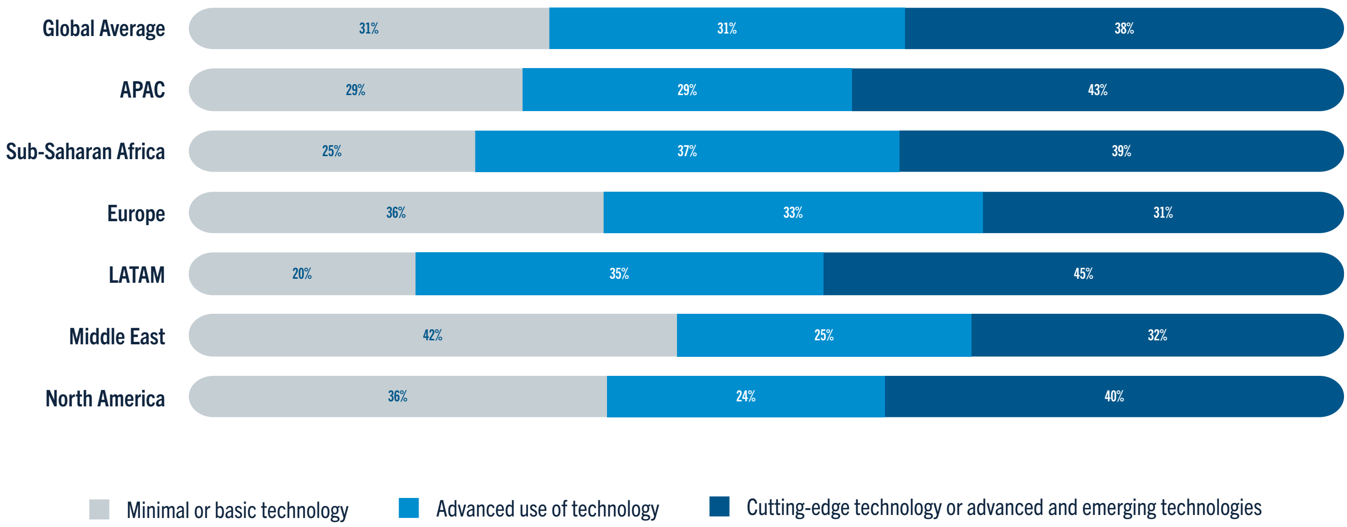


Q: How would you describe your company's current typical use of technology in your security operations?
Base: Chief security officers from large companies (Global n=1775)
Q: Where would you like your company to be in the next 12 months with regards to security related technology?
Base: Chief security officers from large companies (Global n=1775)

Appendix

Current Use Of Technology

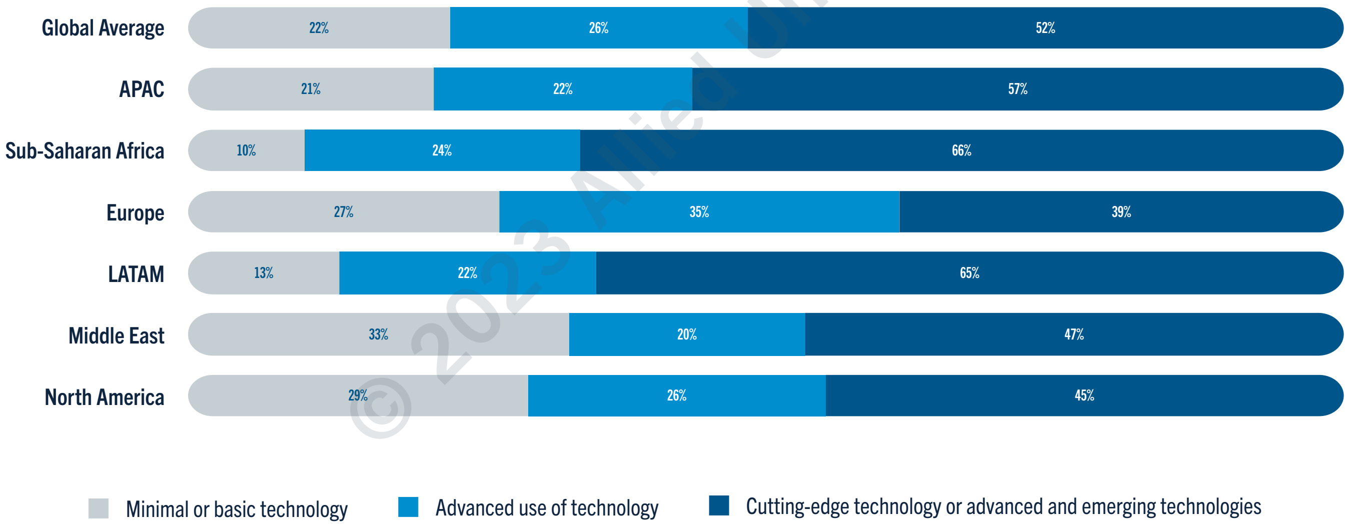
Regional Comparison



Q: How would you describe your company’s current typical use of technology in your security operations?
Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

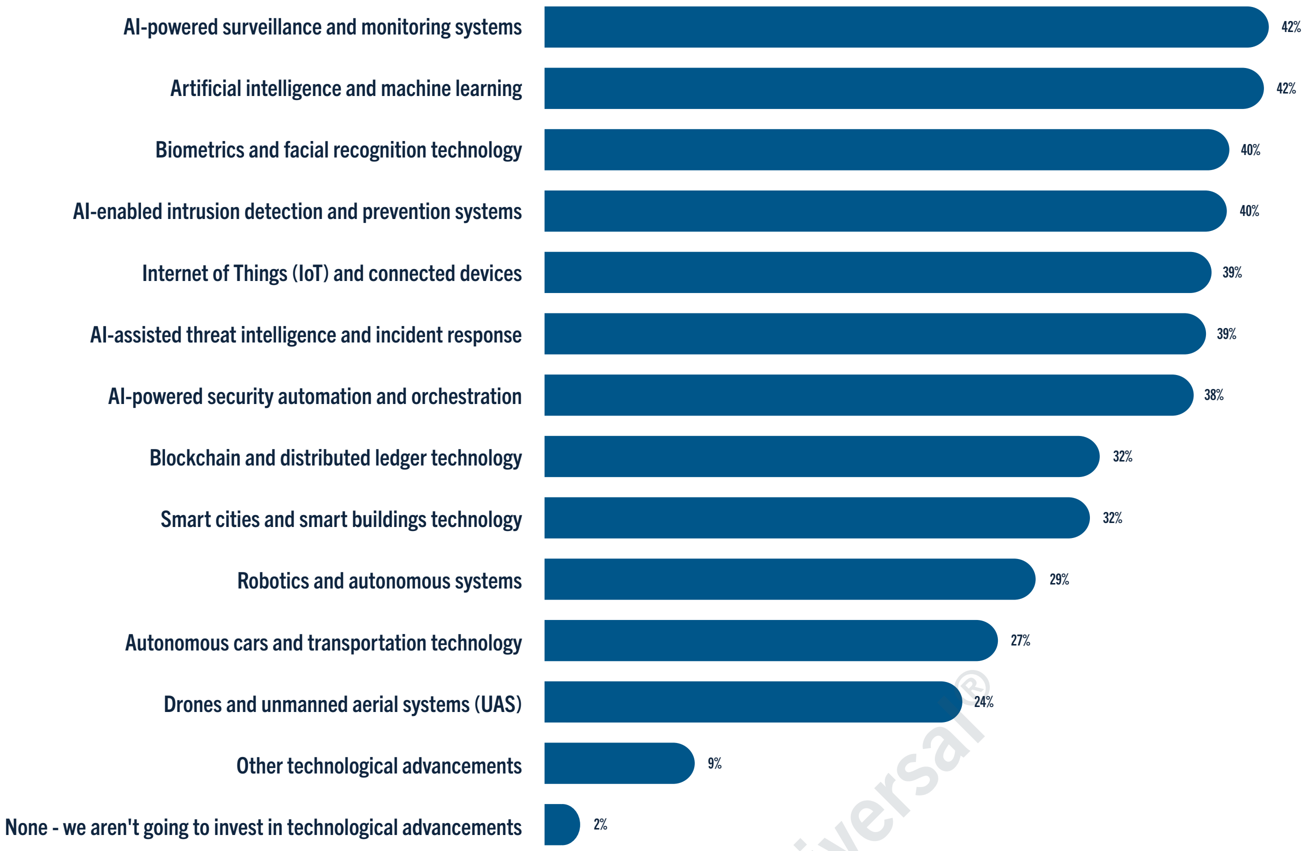
Future Use Of Technology

Regional Comparison



Q: Where would you like your company to be in the next 12 months with regards to security related technology?
Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

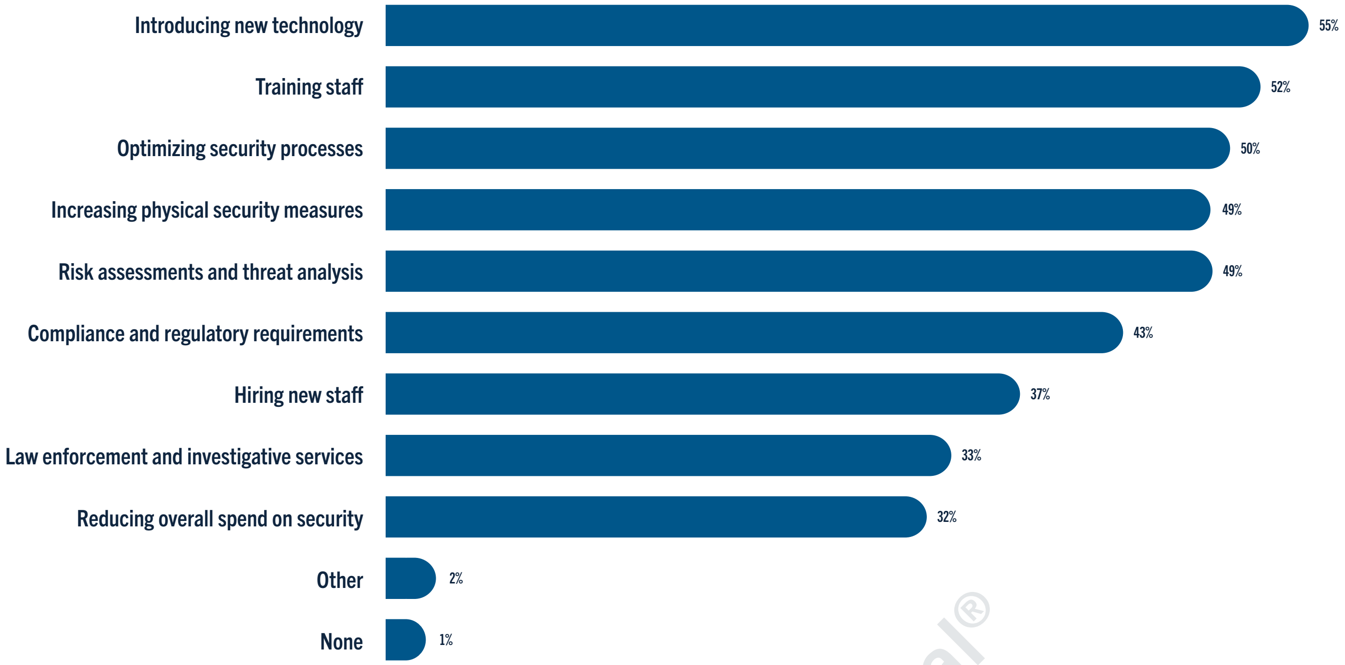
Planned Technology Advancements In The Next 5 Years
Global Average



Q: What technological advancements will your company be utilising (either investing internally or outsourcing to a security vendor) over the next five years to improve its physical and cyber security operations?
Base: Chief security officers from large companies (Global n=1775)

Chapter Four: The Future of Security

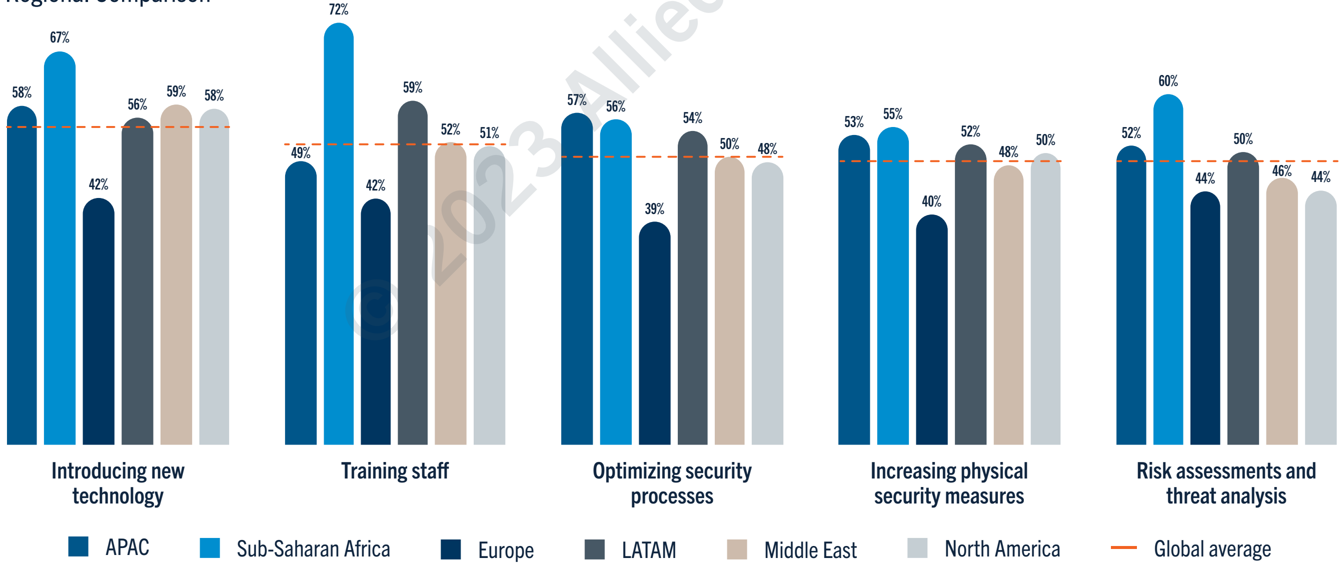
Security Budget Priorities In The Next 12 Months
Global Average



Q: What are your company's security budget priorities over the next 12 months?

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

Top 5 Security Budget Priorities In The Next 12 Months
Regional Comparison

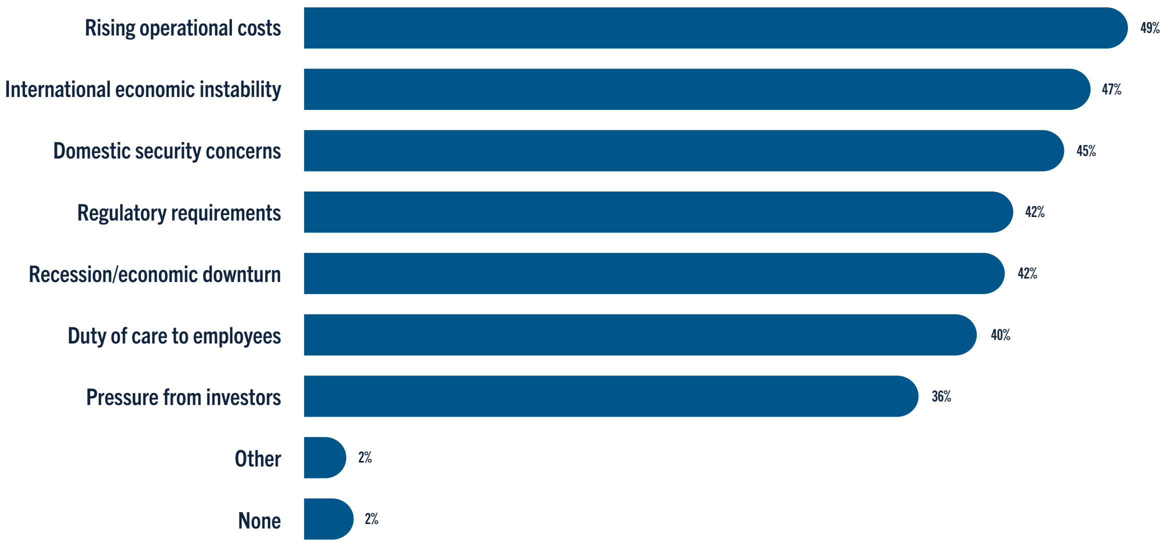


Q: What are your company's security budget priorities over the next 12 months?

Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Europe (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

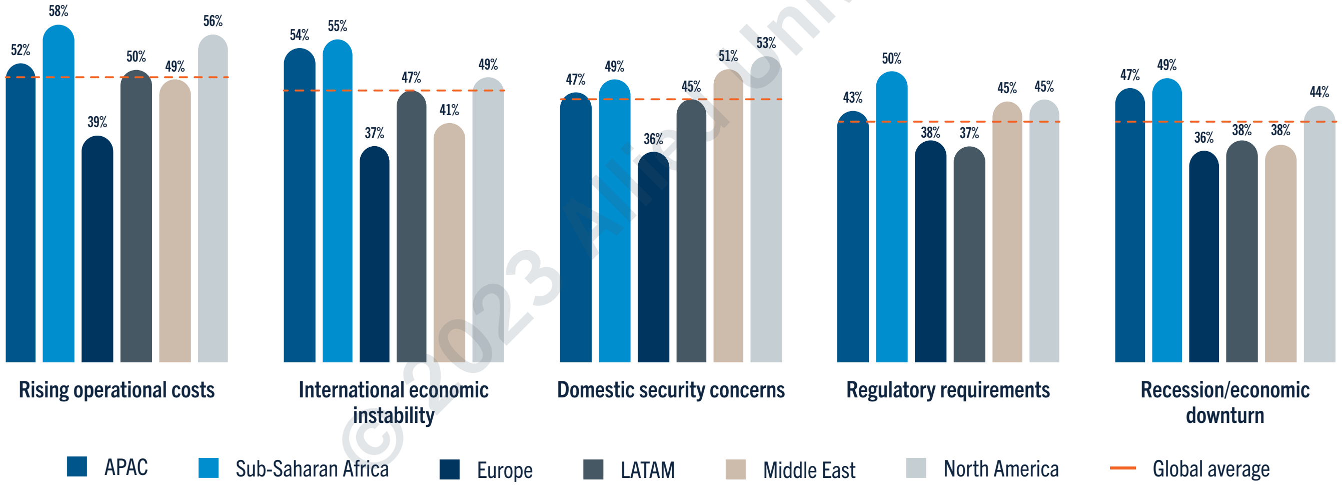
Appendix

Areas Likely To Increase Security Budgets In The Next 12 Months
Global Average



Q: Which of the following are likely to increase security budgets over the next 12 months?
Base: Chief security officers from large companies (Global n=1775)

Top 5 Areas Likely To Increase Security Budgets In The Next 12 Months
Regional Comparison



Q: Which of the following are likely to increase security budgets over the next 12 months?
Base: Chief security officers from large companies (Global n=1775), APAC (n=458), Sub-Saharan Africa (n=166), Euope (n=446), LATAM (n=309), Middle East (n=235), North America (n=160).

Methodology

Audience One: Global Company Security Managers

Research was carried out via an online survey, between March 20 and 31, 2023, with a total of n=1,775 physical security respondents in large companies across 30 countries and 13 languages. A quota-based random selection process was used within each country by industry and each country's data was weighted to have an equal proportion in the global results (with the exception of the U.S. to reflect their larger economy). Respondents collectively boasted a combined global revenue exceeding USD $20 trillion.

Audience Two: Global Institutional Investors

Online research on April 17, 2023, with a total of n=200 global institutional investors. A quota-based random selection process was used to select them by type and geography. Respondents have a sum of over USD $1 trillion in AUM (assets under management).

For more information on the methodology,

contact dan.healy@fticonsulting.com

Provided by FTI Consulting LLP

The research was conducted with two audiences.

About World Security Report 2023

This landmark research is an independent, anonymous survey of 1,775 chief security officers (CSOs), or those in equivalent roles, from large, global companies in 30 countries, with a combined annual revenue of $20 trillion in 2022, representing a quarter of the world's total gross domestic product (GDP).

About Allied Universal

The world's leading security and facility services provider and trusted partner to more than 400 of the *FORTUNE* 500, Allied Universal® delivers unparalleled customer relationships, innovative solutions, cutting-edge smart technologies and tailored services that enable clients to focus on their core businesses. With operations in over 100 countries, Allied Universal is the third-largest private employer in North America and seventh in the world. Annual revenue is more than $20 billion. There is no greater purpose and responsibility than serving and safeguarding customers, communities and people.

For more information, visit aus.com.

WorldSecurityReport.com

An ALLIED UNIVERSAL® Company