December 2023

Rachel Briggs OBE

The Business Value of Corporate Security

Sustainable commercial success through resilience, insight, and crisis leadership in a volatile world

the clarity factory

Partners
This research is kindly supported by the following companies: AstraZeneca, Barclays, CRH, Holcim, ICF, Johnson Matthey, Proman AG, Shell, Sibylline and Sky. The views expressed in this report are those of The Clarity Factory and do not necessarily reflect the views or positions of the companies who supported this research.

The following individuals from the partner companies acted as members of the project's Advisory Council, informing and shaping the research, providing feedback on emerging findings, and offering invaluable input on the final report: Trevor Rees, Alex Hawley, Mark Wolsey, Cédrick Moriggi, Gerald Golding, Steve Brown, James Richardson, Duncan Manning, Justin Crump and Niall MacGinnis.


ISBN: 978-1-7384176-0-5

Contents

	Executive Summary	5
	Introduction	15
1	The Business Context for Corporate Security	17
2	Five Business Trends that Elevate the Business Value of Corporate Security	30
3	Circle of Control: Corporate security core tasks	35
4	Integration for a Unified View of Risk	40
5	Insight to Enhance Decision Making	49
6	External Networks: Insight, support and early warning system	54
7	Crisis Management and Crisis Leadership	57
8	Delivering the Vision: Success criteria for an effective CSO	62
	Conclusion	76
	Appendix 1: Methodology	78
	Appendix 2: Project Partners	78
	Appendix 3: Author Acknowledgements	79
	Endnotes	80

About The Clarity Factory

The Clarity Factory is an engine room generating knowledge, insights and practical solutions for our increasingly complex world. We conduct research, produce thought leadership, and consult with clients to help them solve knotty problems and support them as they strive for continual improvement and innovation. We specialise in corporate security, cyber security, and resilience. The Clarity Factory creates clarity from complexity – to enable our clients to thrive.

About the Author

Rachel Briggs OBE is a leading expert on security. She has worked with many of the world's largest corporations, advising them on corporate security and cyber security. She is co-author of *The Business of Resilience* and has written numerous reports, which have influenced government and private sector policy.

Rachel is Founder and CEO of The Clarity Factory. She was Founding Executive Director of Hostage US, the first Director of Hostage International, and held senior positions at RUSI, Demos and ISD. She was awarded an OBE in 2014 for her work with hostages.

Rachel is a regular keynote speaker and frequent commentator in print and broadcast media. She is an Associate Fellow of Chatham House and a board member of the Global Center on Cooperative Security and the Risk and Security Management Forum (RSMF).

Executive Summary

"Leaders can no longer assume that trouble may strike once every three or four years and be managed by outside crisis consultants. Instead, companies must prepare for a steady stream of upheavals—and hone their in-house skills for dealing with them... They should be ready."

– Nitin Nohria, former Dean, Harvard Business School

Purpose and audience

This report seeks to understand **what trends in the global business operating environment mean for the corporate security function**: its value proposition, narrative and positioning, leadership, talent strategy, areas of responsibility, relationship to the rest of the business, innovation, external stakeholders, and changing C-Suite needs.

It is intended as a guide for **senior business leaders** as they make decisions, such as who to hire as their Chief Security Officer (CSO)* and how to measure their performance, adequately resource the function, and benefit from corporate security's potential contribution across the value chain.

The report focuses on corporate security at multinational corporations. Although aspects might be relevant for other organisations, they are not the focus of this study.

* This report uses the job title 'Chief Security Officer (CSO)' to refer to the most senior person responsible for corporate security within a multinational company, but recognises that not all post holders hold this title.

In a global business environment characterised by volatility and increased security risks, effective corporate security is non-negotiable for commercial success.

> *More than half (57%) of board directors said they expected to increase their risk appetite.*

Business leaders predict that volatility will characterise their operating environment over the next decade. Four-fifths of leaders surveyed by the World Economic Forum think the next ten years will be characterised by volatility, and 20% see it in terms of 'progressive tipping points and persistent crises leading to catastrophic outcomes.'[1] As they grapple with heightened tensions in the Middle East, the Russian invasion of Ukraine, China's influence in its near neighbourhood as well as Africa and the Middle East, and the highest levels of political risk and unrest for five years,[2] business leaders face the effect of geopolitics on everything from supply chains and operational resilience to personnel security and new market entry or exit. The business leaders interviewed for this report cited geopolitics as the most important security risk facing their company, and a majority (51%) of CSOs surveyed ranked it as one of the three most important security risks for their organisation.

In a more difficult business environment, growth requires companies to be able to identify opportunities and lean into risk. More than half (57%) of board directors said they expected to increase their risk appetite (or had already done so).[3] Business leaders increasingly need more nuanced insight to calibrate the risks they take, trusted advisors willing to speak up when something is a risk too far, and highly effective crisis management capability, which becomes a source of organisational resilience, as a well as a standalone activity in response to crisis events. **Corporate security can contribute essential data on security risks, has a track record for being a trusted advisor on risk decisions, and is one of the company's centres of excellence on crisis management.**

As a result of these geopolitical shifts, along with technological innovation among threat actors, the free cross-border movement of people, and economic downturn, many multinational corporations continue to face sophisticated and persistent security risks. A majority of CSOs surveyed for this report said security risks have increased over the past 2–3 years and almost all (89%) said senior executives expect more from corporate security than they did 2–5 years ago. The risks range from crime and organised crime, insider risk, kidnapping, and terrorism, to intellectual property theft, ransomware attacks and state-sponsored espionage. Against this backdrop, **business leaders surveyed by PwC said they see corporate security as a business enabler that adds value.**[4]

The rise of interconnected and complex risks makes risk management more complex and places a premium on functions, like corporate security, that are effective integrators.

Multinational corporations increasingly manage risks that fall outside the remit of any individual function, and are dealing with multiple risks concurrently. Interconnected risks are not just harder to predict and manage; research shows they produce larger losses.[5] In this context, silos cause missed opportunities, obscure risks, and create blind spots.

This makes business leaders more focused on the connections between risks, as well as on the risks themselves, and they seek a more unified, functionally agnostic view of risk. They place a premium on functions staffed with people with reach and influence who are skilled collaborators and integrators. **Corporate security is one of the company's most connected functions;** it tends to be organised geographically, which produces a broad as well as deep view across the corporation, and it is delivered through delegation and influence, which requires the function to develop strong vertical and horizontal relationships. As a result, corporate security is seen by some executives as 'corporate glue.'

Multinational corporations are increasingly impacted by a range of social changes that affect their risk profile and require input from corporate security. There is growing pressure on companies to not just do their business fairly and ethically, but to take an active stance on political and social issues, whether directly linked to their business or not. This can make companies and their staff a target for attack; 11% of CSOs we surveyed said activism is one of the three biggest security risks for their organisation, and a majority (57%) said it was increasing. There is also growing expectation for CEOs to be the face of such public positions; 81% of investors globally say CEOs should be personally visible when discussing public policy with external stakeholders. This can increase the CEO's risk profile, and one-third (32%) of CSOs surveyed said threats to senior company executives have increased over the past 2–3 years.

In the age of 'polycrisis' – the simultaneous occurrence of several catastrophic events[6] – crisis management is a business-critical activity and a core leadership competency.

Many companies face a higher volume of crises that are more interconnected: extreme weather events, conflict, market volatility, reputational crises, geopolitical events and cyber-attacks, for example. For those used to operating in high-risk environments, this might not feel new, but for others, it requires a structural and cultural shift. **Corporate security functions are often at the heart of their company's crisis management capability;** three-quarters are responsible or accountable for crisis management and only 1% have no role at all. A majority led their company's pandemic response, and two-thirds of corporate security functions in companies impacted by the Ukraine war led those crisis management efforts.

'Crisis management' is a required skillset across the whole company.[7] Business leaders interviewed recognised that CSOs have exceptional crisis management skills and capabilities that can be of wider value.

Business leaders are adapting to these trends

Most of these trends are not novel, but the scale of change and profundity of impact require business leaders to adapt. They are responding in a number of ways:

- **Increasing their risk appetite.**
- **Shifting locations and supply chains.**
- **Increasing scenario planning.**
- **Bolstering crisis management capability.**
- **Seeking a different kind of leader with strong collaborative skills alongside administrative and financial competence.**

Corporate security is a critical function in a volatile world. It is a business enabler and contributes to commercial success.

This report – the culmination of a 12-month research project, involving surveys and interviews with business leaders, CSOs and security experts, and supported by ten multinational corporations – highlights **five critical ways in which corporate security is a business enabler that contributes to commercial success for today's multinational corporations.**

1. **Corporate security is non-negotiable for commercial success.** In a volatile, complex, high-risk operating environment, where security risks are rising, **effective corporate security is non-negotiable**, keeping the company safe and enabling business leaders to lean further into risk. Effective corporate security functions excel in 16 core tasks (Box 1) and enhance their value by additionally adopting responsibilities specific to their company, based on sector, geographical footprint, profile, products, and activities.

Box 1
Corporate security core tasks

Security audits	Executive protection	Investigations	Business continuity
Security assessment	Insider risk	Security technology	Training
Asset protection	Travel security	Threat intelligence	Crisis management
Identity and access management	Global meetings and events	Vetting and/or due diligence	Incident management

2. **Corporate security is an integrator that promotes a unified view of risk.**
Corporate security tends to be one of the company's most effective integrators. **CSOs are leading efforts to promote collaboration across risk functions to provide executives with a more unified view of risk.** Their function contributes across the value chain: as connected specialists, valued interlocutors on activities such as mergers and acquisitions (M&A) and new market entry or exit, and as the company's complex problem solver of first choice. Their ability to perform this integration role depends on vertical integration; CSOs usually sit at ex-comm minus 1 or above, and report into relevant governance bodies.

> *In a volatile, complex, high-risk operating environment, where security risks are rising, effective corporate security is non-negotiable.*

3. **Corporate security intelligence offers insight to enhance business decision-making.**
Companies that can harness data from across the value chain – including operations, the supply chain, corporate security, business intelligence, and cyber security – will tend to generate nuanced insights to drive better business decisions, allowing executives to lean into risk with greater confidence. Business leaders recognise the value of security intelligence,[8] and effective CSOs look for ways to use it to enhance outcomes across the business, including intelligence-driven decision making, supply-chain visibility, de-risking of product cycles, enhanced visibility of risks around M&A/divestment activities, and stakeholder insights to feed into environmental, social and governance (ESG) efforts. **Companies that fail to harness corporate security intelligence for broader business use leave valuable insight on the table.**

4. **Corporate security's external networks provide insight, support and an early-warning system.**
At a time when multinational corporations increasingly place a premium on external networks,[9] business leaders interviewed for this report acknowledged the **importance of corporate security's external network**. It not only delivers security outcomes, it helps leaders to understand what geopolitical trends mean for the company, offers insight, benchmarking and support, and acts as an early warning system. Effective corporate security functions invest in their networks, public–private partnerships, and membership organisations that support professional development, benchmarking and information sharing.

5. **Corporate security's crisis management expertise is business critical and can be used to enhance crisis leadership competency across the business.**
Corporate security functions are at the heart of their company's crisis management capability. As well as applying these skills in response to group-wide crises, CSOs can put them to wider use to enhance crisis leadership capability across the organisation; to **help leaders distinguish between an incident and a crisis, use crisis management procedures to help the business to make quicker decisions, and coach and mentor to develop executive crisis leadership talent.**

What business leaders need to know: success criteria for an effective CSO

Delivering the vision for effective corporate security outlined in this report relies on strong partnership between the executive committee and CSO and support from business leaders to promote the value of corporate security across the organisation, and ensure the function is well-placed and adequately resourced for success. It is dependent on five success criteria for an effective CSO, which should inform C-Suite efforts on CSO recruitment and succession planning, as well as their approaches to risk, resilience and security.

1. **A compelling narrative for corporate security**
Effective CSOs clearly articulate the value of the corporate security function. Their narrative is simple, high-level, emotionally engaging, and memorable, and chimes with the organisation's culture and style. It should be based as much on proactivity, prevention, insight and resilience as on reactivity and crisis response, as important as those things are.

2. **The right kind of corporate security leadership**
Effective CSOs lead with credibility, gravitas, innovation and personal resilience; and have business acumen; collaboration skills; exceptional stakeholder management capabilities; strong external networks; and demonstrable subject matter expertise.

3. **An innovation mindset**
Effective CSOs are always looking for ways to improve; they identify new ways of working – including the use of technology – to increase productivity, generate nuanced insights, share data across the business, reduce costs, and decrease company losses. CSOs require the support of the C-Suite in accessing resources, skills, and the help of technology colleagues.

4. **A fit-for-purpose talent strategy**
Effective CSOs recognise the need to assemble a team with the necessary skills, competencies and management experience:

- They bring in **new skills**, such as data scientists, Six Sigma practitioners, and software engineers, and emphasise business competencies, such as vendor and project management.
- They value **skills that boost collaboration** across the business, such as influencing, communication, and leadership.
- They attract candidates **with a wider range of backgrounds beyond government service** (i.e. military, law enforcement, diplomacy or intelligence).
- They understand the **'diversity dividend'**,[10] and strive for diversity, equity and inclusion to drive innovation, productivity and enhanced decision making.
- They recognise the importance of clear and structured **career pathways**.

5. **Adequate resourcing**
Effective CSOs secure the support of the C-Suite for adequate resource to provide excellence in core tasks and enable the function to contribute across the value chain. Budgets and headcounts vary considerably between companies, influenced by their respective risk profile, legacy, risk appetite, size, and overall financial position. Effective CSOs right-size their resourcing to the company's needs.

C-suite support for the business value of corporate security

As business leaders grapple with the challenges of doing business in a world characterised by volatility, increased security risks, shifting supply chains, and interconnected risk, the business value of corporate security is heightened. Effective business leaders reward CSOs who prioritise excellence in core security tasks – their circle of control – and recognise that security is critical for commercial success. In doing so, these CSOs generate opportunities to extend their circle of influence, allowing them to make a much wider contribution across the value chain.

There is no one-size-fits-all; companies will need to adapt the model presented in this report according to their sector, geographical footprint, products, activities, and risk appetite, and there are different levels of maturity among corporate security functions. The report focuses on corporate security at multinational corporations; companies with business operations and offices in two or more countries. Although aspects might be relevant for other organisations, they are not the focus of this study.

Senior leaders who support their CSOs in pursuing this vision will realise the business value of corporate security.

About this report

This report is the culmination of a 12-month research project supported by AstraZeneca, Barclays, CRH, Holcim, ICF, Johnson Matthey, Proman AG, Shell, Sibylline and Sky. It involved interviews with business executives (CEOs, COOs, CFOs, General Counsels, CMOs, CISOs, and other business leaders) and CSOs from multinational corporations; surveys of CSOs and young security professionals; expert interviews; and a thorough review of existing data.

The views expressed are those of The Clarity Factory and do not necessarily reflect the views or positions of the companies who supported the research.

Introduction

"The corporate security function is a really responsible function that is looking after the health and resilience of our business."

– C-Suite business leader*

The role and position of corporate security

Today's global business environment presents challenges to multinational corporations that impact the place and role of the corporate security function. Geopolitics is back on the agenda, ranked by business leaders interviewed as the most important security risk facing their respective companies. As they grapple with heightened tensions in the Middle East, the Russian invasion of Ukraine, China's influence in its near neighbourhood as well as Africa and the Middle East, and the highest levels of political risk and unrest for five years,[11] companies face the effect of geopolitics on everything from supply chains and operational resilience to personnel security and new market entry or exit. Eighty percent of business leaders think the next decade will be marked by varying degrees of **volatility**.[12]

Many companies face **sophisticated and persistent security threats** – ranging from crime, organised crime and insider risk to ransomware attacks and state-sponsored espionage – and CSOs interviewed reported diminishing support from law enforcement agencies. The **risks they face are increasingly interconnected**, which requires a more unified view of risk. Multinational companies are undergoing significant change, including efforts to use **technology, data and digitalisation** to drive innovation and efficiency. They are also often impacted by social and political trends that shift their risk profile; these make them greater targets for activism, insider risk and workplace violence.

* When quotes are attributed, they come directly from interviews carried out for this report. Quotes that are taken from secondary sources are referenced in the endnotes.

Most of these trends are not novel, but the scale of change and profundity of impact require business leaders to adapt. They are responding in a number of ways, including increasing their risk appetite, shifting locations and supply chains, increasing scenario planning, bolstering crisis management capability, and seeking a different kind of leader.

About this report

This report seeks to understand what these trends mean for the corporate security function: its value proposition, leadership, talent strategy, areas of responsibility, relationship to the rest of the business, innovation, external stakeholders, and changing C-Suite needs. It is intended as **a guide for senior business leaders** as they make decisions, such as who to hire as their CSO and how to measure their performance, adequately resource the function, and benefit from corporate security's potential contribution across the value chain.

"The measure of a powerful person is that their circle of influence is greater than their circle of control." [13]

The report is based on a 12-month independent research project, which was funded by ten companies: AstraZeneca, Barclays, CRH, Holcim, ICF, Johnson Matthey, Proman AG, Shell, Sibylline and Sky. A detailed methodology is included as an appendix. The views expressed in this report are those of The Clarity Factory, and do not necessarily reflect those of the partners.

There is no one-size-fits-all; companies will need to adapt the model presented in this report according to their sector, geographical footprint, products, activities and risk appetite, and there are different levels of maturity. The report focuses on corporate security at multinational corporations. Although aspects might be relevant for other organisations, they are not the focus of this study.

The business value of corporate security

Corporate security has always been essential for multinational corporations; maintaining the security of people, property and assets; enhancing resilience; and enabling the corporation to seize opportunities without undue risk.[14] As leaders grapple with the challenges outlined in this report, the importance of corporate security is heightened; its opportunity to influence made greater.

Senior leaders who support their CSOs in pursuing the vision outlined in this report will realise the business value of corporate security.

1 The Business Context for Corporate Security

"The geopolitical axis is forever twisting and turning... It can be all good today, and then up in arms tomorrow."

– Senior business leader

Summary

- **Geopolitics is back on the agenda and was ranked by business leaders interviewed for this report as the most important security risk facing their respective companies.** It is impacting everything from supply chains and operational resilience to personnel security and new market entry or exit. Executives predict that volatility will characterise their operating environment for the decade ahead.
- **Many multinational corporations face sophisticated, persistent and rising security risks**, ranging from crime and organised crime and insider risk to ransomware attacks and state-sponsored espionage. At the same time, **some CSOs reported diminishing support from law enforcement**, which cannot match the capability of threat actors, finds information sharing difficult due to regulation and shifting geopolitical alliances, and has increasingly stretched resources.
- **The risks faced by multinational corporations are often increasingly interconnected, which makes the losses potentially bigger and calls for greater collaboration between risk-related functions**, such as corporate security.
- **The long-term risks of climate change are driving some geopolitical trends, impacting operations and supply chains, and creating new security risks.** This requires corporate security to contribute to its company's growing ESG efforts.

- **Social and political trends are impacting a company's risk profile**; greater pressure to speak out increases the risk of activism; the demand for CEOs to be visible heightens their personal risks, and internal challenge from staff can result in unrest, workplace violence or insider risk. **This calls for a new style of leadership versed in crisis management and communications, and places a premium on external networks – such as those that the corporate security function has established – which offer insight, situational awareness and support.**

- **Technology is at the heart of most organisational change efforts**, and all functions are expected to seize the opportunities offered. Data mastery is key; a company's ability to harness and collate data from across its value chain – including corporate security – is directly proportionate to its ability to generate more nuanced insight to drive better decision-making, allowing it to lean into risk.

- **Corporate security is called upon to help the company anticipate and respond to technology-related risks and forge an ever-closer partnership with cyber security colleagues.**

- **In a post-truth world, disinformation can have tangible and significant impacts, including serious security risks**, such as reduced share prices, attacks on senior executives, protests, disruption to operations, and damage to important stakeholder relationships. This places a premium on **cross-functional collaboration** to improve anticipation of, response to, and recovery from such low-probability and -predictability – but high-impact – events.

Geopolitics, volatility and risk

Geopolitics is firmly back on the agenda and is causing disruption for many multinational corporations. For example, Russia's invasion of Ukraine has impacted everything from supply chains, operational resilience, and personnel security, to commodity prices, new market entry or exit, and the strength of international institutions. The rise of China continues to raise concerns about trade wars, critical supply chains, intellectual property theft, influence and instability in Africa, and the threat of aggression towards Taiwan and the wider South China Sea region. Both Russia and China are also active in the Middle East, causing that region

to look east as well as west, and the British Home Secretary sees the Iranian state as the biggest threat to the country's national security as it forges links with organised crime gangs.[15] Heightened tensions in the Middle East are likely to impact corporations operating across the region. As Sibylline CEO, Justin Crump, put it, 'Tensions between the US and China, as well as the shifting nature of once-established alliances and rivalries more broadly, are [also] increasing uncertainty and testing the operations of global businesses and institutions.'[16]

> *A majority of CSOs (51%) ranked geopolitics as one of the top three security risks facing their organisation.*

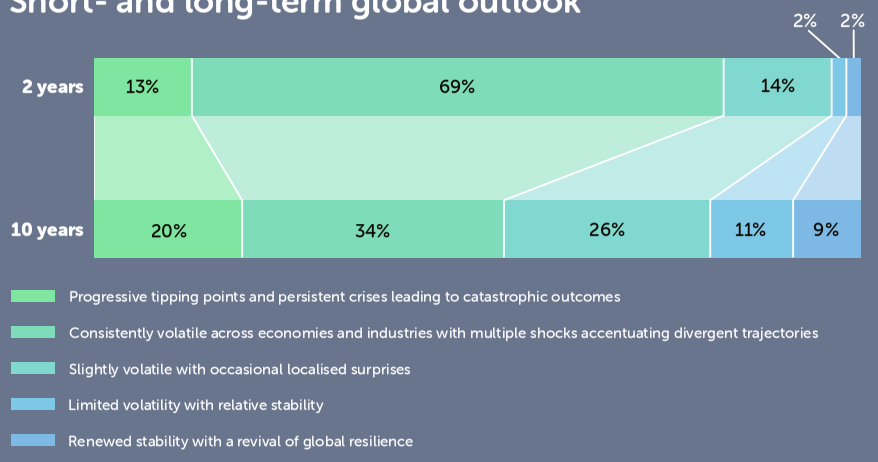
Political risk and unrest are at the highest level we have seen in the last five years, driven by a range of factors, including climate change, population movement, resource scarcity, and the new alliances of the multipolar world.[17] According to Freedom House, global freedom has declined for the 17th consecutive year, with new coups or attempts to undermine representative government taking place in Burkino Faso, Tunisia, Peru and Brazil, and the previous years' coups and ongoing repression continuing in Guinea, Turkey, Myanmar and Thailand, among others.[18]

Business leaders predict that volatility will characterise their operating environment over the next decade. According to the World Economic Forum, fewer than one in ten (9%) think the next decade will be characterised by 'renewed stability with a revival of global resilience', and twice as many (20%) see it in terms of 'progressive tipping points and persistent crises leading to catastrophic outcomes' as shown in Figure 1.

Most senior executives we interviewed ranked geopolitical risk as the most important security risk facing their organisation, mentioning issues such as unpredictable and unexpected conflicts, volatility in the Middle East, and global-south migration. As one said, 'The geopolitical axis is forever twisting and turning, which makes it somewhat unpredictable. It can be all good today, and then up in arms tomorrow.' A majority of CSOs (51%) ranked geopolitics as one of the top three security risks facing their organisation, as shown in Figure 2. **Business leaders view corporate security as a key contributor to the company's resilience in the face of geopolitical shifts**; geopolitics is a shared concern for both groups.

Figure 1

Short- and long-term global outlook



Source: Global Risks Perception Survey 2022–2023, World Economic Forum [19]

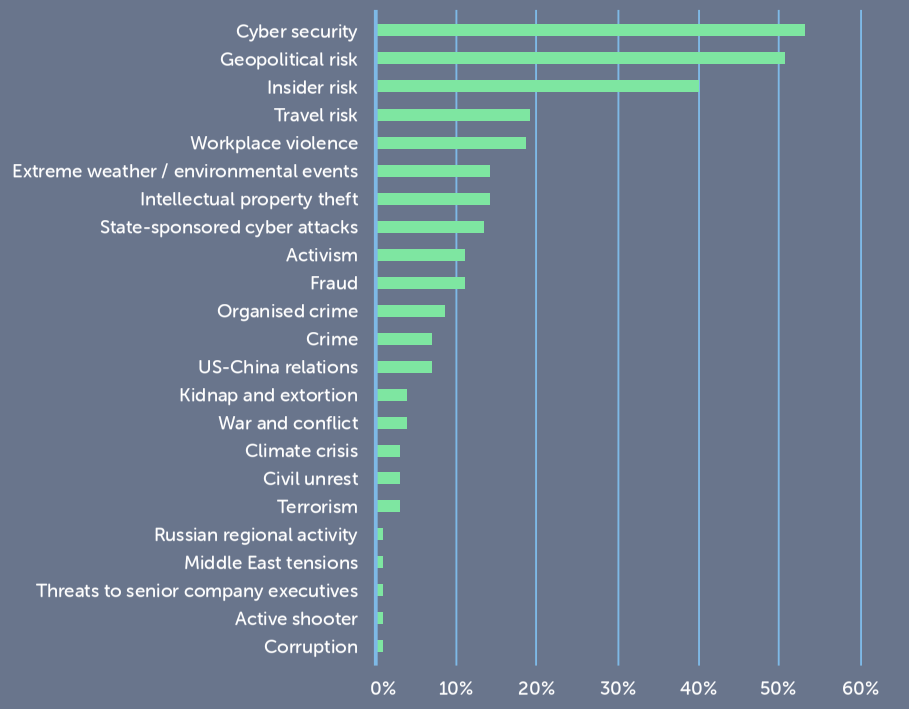
Sophisticated, persistent and rising security risks

Many multinational corporations continue to face sophisticated and persistent security risks, ranging from crime and organised crime, insider risk, kidnapping, and terrorism, to intellectual property theft, ransomware attacks and state-sponsored espionage. A majority of CSOs said security risks have increased over the past 2–3 years, as shown in Figure 3, as a result of geopolitical shifts, technological innovation among threat actors, the free cross-border movement of people, and economic downturn. Almost all CSOs (89%) said senior executives expect more from corporate security than they did 2–5 years ago.

CSOs also reported diminishing support from law enforcement: the sophisticated criminal threat is not matched by policing capabilities; shifting geopolitical alliances and stringent legal and regulatory frameworks make information sharing difficult; the free movement of people allows international criminal gangs to operate under the radar; and stretched public resources are prioritised for crimes primarily affecting citizens, rather than corporations.

Figure 2

What are the three biggest security risks faced by your organisation?



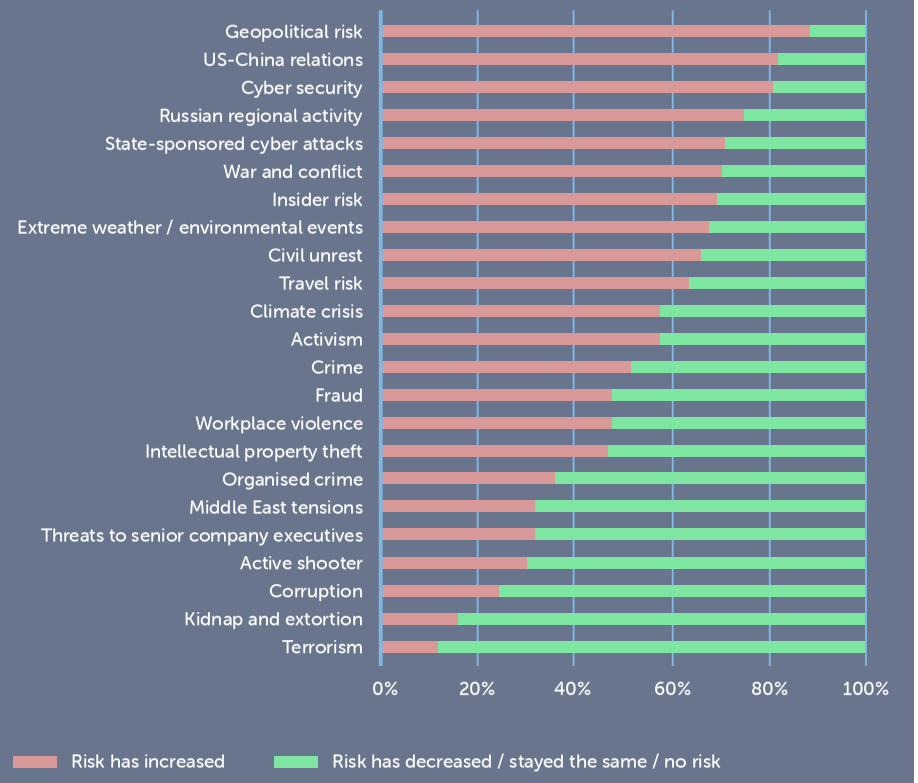
Source: The Clarity Factory CSO survey, 2023

Complex and interconnected risk landscape

The term 'polycrisis' – the simultaneous occurrence of several catastrophic events[20] – featured heavily in the World Economic Forum's 2023 Global Risks report. Figure 4, taken from that report, shows the interconnectedness of some of the biggest economic, environmental, geopolitical, social, and technological risks that multinational corporations face.[21]

Figure 3

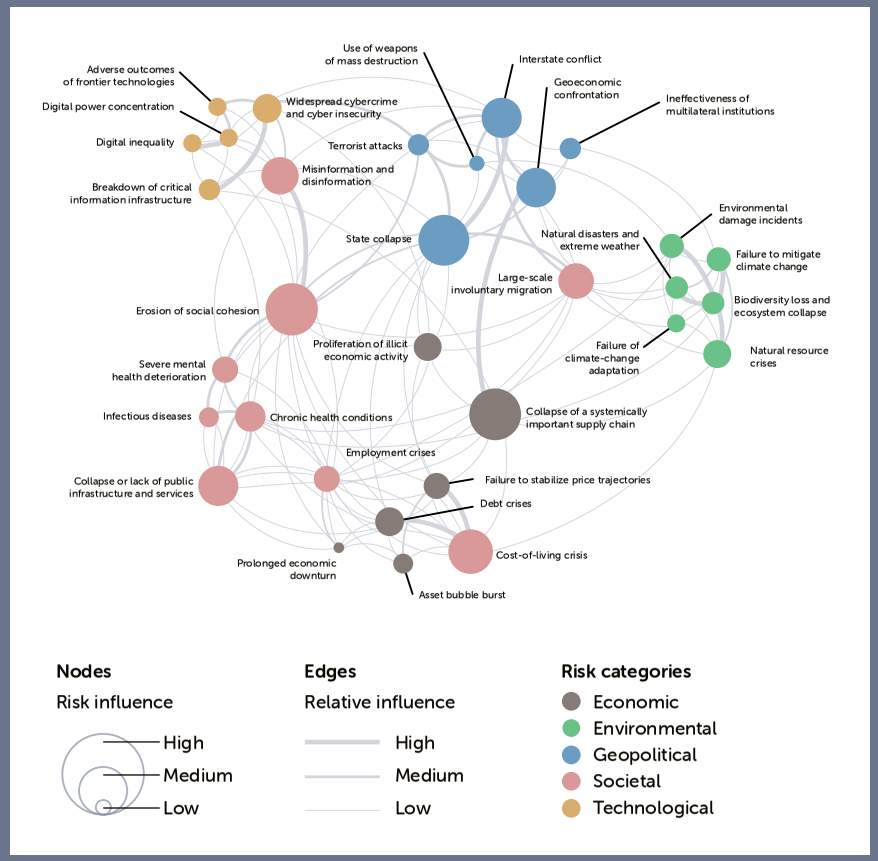
In your opinion, are the following security risks increasing, decreasing, staying the same or not a risk to your organisation?



Source: The Clarity Factory CSO survey, 2023

Figure 4

Global risks landscape: an interconnections map



Source: Global Risks Perception Survey 2022–2023, World Economic Forum

Interconnected risks are not just harder to predict and manage; they also produce larger losses. In the decade leading up to 2012, over one-third (38%) of the thousand largest global public companies suffered a 'value killer loss'.[22] Although the most notable trigger for high-value killer risks over that period was a high-impact, low-frequency event, such as the credit crisis or the eurozone crisis, the magnitude of loss was amplified by interdependencies among risks within an organisation.[23] In other words, the higher the interdependency between risks, the higher the losses. **This makes business leaders more focused on the connections between risks, as well as on the risks themselves, and means risk-related functions, such corporate security, are increasingly called upon to collaborate across the business.**

Long-term risks: Climate

According to the World Economic Forum, business leaders are firmly focused on climate risk, which accounts for four of the top-five risks in the short-term, and six of the top-ten over the long-term (see Figure 5). According to a 2023 PwC survey of 4,410 global CEOs across 105 countries, a majority expect some degree of impact from climate change within the next 12 months, primarily in their cost profiles and supply chains.[24]

Many large corporations manage their climate efforts through their ESG agenda, which has moved from being a marginal corporate activity to a mainstream board concern. Two-thirds of directors (65%) say that ESG is part of the board's enterprise risk management discussions, is regularly part of the board's agenda (55%), and is linked to company strategy (57%).[25]

As corporations deal with the consequences of climate change and adjust their business model, corporate security is increasingly involved – whether through providing security for new supply routes, understanding and advising on the impacts of migration or resource conflicts, or playing a leading role in responding to climate-related crises impacting the company, such as extreme weather events, which 14% of CSOs in our survey cited as a top-three security risk for their company. The corporate security function does not own or lead ESG, but should be a contributor.

Figure 5

Global risks ranked by severity

	Short term	Long term
1.	Cost-of-living crisis	Failure to mitigate climate change
2.	Natural disasters and extreme weather events	Failure of climate-change adaption
3.	Geoeconomic confrontation	Natural disasters and extreme weather events
4.	Failure to mitigate climate change	Biodiversity loss and ecosystem collapse
5.	Erosion of social cohesion and societal polarization	Large-scale involuntary migration
6.	Large-scale environmental damage incidents	Natural resource crises
7.	Failure of climate-change adaption	Erosion of social cohesion and societal polarization
8.	Widespread cybercrime and cyber insecurity	Widespread cybercrime and cyber insecurity
9.	Natural resource crises	Geoeconomic confrontation
10.	Large-scale involuntary migration	Large-scale environmental damage incidents
11.	Debt crises	Misinformation and disinformation
12.	Failure to stabilize price trajectories	Ineffectiveness of multilateral institutions and international cooperation
13.	Prolonged economic downturn	Interstate conflict
14.	Interstate conflict	Debt crises
15.	Ineffectiveness of multilateral institutions and international cooperation	Cost-of-living crisis
16.	Misinformation and disinformation	Breakdown of critical information infrastructure
17.	Collapse of a systemically important industry or supply chain	Digital power concentration
18.	Biodiversity loss and ecosystem collapse	Adverse outcomes of frontier technologies
19.	Employment crises	Failure to stabilize price trajectories
20.	Infectious diseases	Chronic diseases and health conditions
21.	Use of weapons of mass destruction	Prolonged economic downturn
22.	Asset bubble bursts	State collapse or severe instability
23.	Severe mental health deterioration	Employment crises
24.	Breakdown of critical information infrastructure	Collapse of a systemically important industry or supply chain
25.	State collapse or severe instability	Severe mental health deterioration
26.	Chronic diseases and health conditions	Collapse or lack of public infrastructure and services
27.	Collapse or lack of public infrastructure and services	Infectious diseases
28.	Proliferation of illicit economic activity	Use of weapons of mass destruction
29.	Digital power concentration	Proliferation of illicit economic activity
30.	Terrorist attacks	Digital inequality and lack of access to digital services
31.	Digital inequality and lack of access to digital services	Asset bubble bursts
32.	Adverse outcomes of frontier technologies	Terrorist attacks

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."
Source: Global Risks Perception Survey 2022–2023, World Economic Forum

Risk categories
- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Social changes

Multinational corporations are increasingly impacted by a range of social changes that affect their risk profile and require input from corporate security. There is growing pressure on companies to not just do their business fairly and ethically, but to take an active stance on political and social issues, whether directly linked to their business or not. As Lucien Alziari, Chief Human Resources Officer at Prudential, commented, 'There was a time when a CEO could say, "But what does this have to do with my company? Isn't this a matter in the personal or political sphere?" Such a perspective is unlikely to serve any executive well in the times ahead.'[26] Taking a public stance on such issues can make companies and their staff a target for attack; 11% of CSOs we surveyed said activism is one of the three biggest security risks for their organisation, and a majority (57%) said it was increasing.

There is growing expectation for CEOs to be the face of such public positions; 81% of investors globally say CEOs should be personally visible when discussing public policy with external stakeholders and two-thirds (60%) of people agreed with the statement 'when considering a job, I expect the CEO to speak publicly about controversial social and political issues that I care about.'[27] **This can increase the CEO's risk profile**, and one-third (32%) of CSOs surveyed said threats to senior company executives have increased over the past 2–3 years. This underlines the importance of effective executive protection and security at company events.

Social and political positions can also generate internal risks, which touch upon the work of a number of functions, including corporate security, cyber security, human resources (HR), and external relations. Staff are increasingly likely to make their views known; in 2020, Facebook employees staged a virtual walkout in opposition to the company's decision not to remove inflammatory posts by President Trump following the murder of George Floyd.[28] Workplace violence was ranked as a top-three risk by two-fifths (18%) of CSOs and half (47%) said it is increasing; in an effort to tackle this problem, the Society for Human Resource Management is launching a 'workforce civility' initiative, which frames political differences as a diversity issue.[29]

Insider risk, one of the causes of which is worker disillusionment or disengagement,[30] is also growing: 40% of CSOs ranked it as a top-three risk, and 69% said it is increasing. Almost all (90%) cyber-security professionals, who are often centrally involved in detecting insider risks, believe their organisation is vulnerable to insider threats, which cost a median of USD 4.45 million to recover from and take 314 days to identify and contain.[31]

> *"40% of CSOs ranked insider risk as a top three risk, and 69% said it is increasing."*

These social changes require a new style of corporate leadership and enhanced competence in crisis management and communication, to ensure incidents do not spiral into crises; as Glenn Kelman, CEO of Redfin, put it, 'I wasn't trained to do this.' They also place a premium on external networks, as companies increasingly look to partners, suppliers, local communities, stakeholders and influencers to share data and insights, act as an early warning system, and offer support when things escalate. As PwC's annual global CEO survey put it, 'The diversity and complexity of today's business challenges are placing a premium on the ability to collaborate across the boundaries of the corporation.'[32]

Technological changes

Technology is transforming almost every aspect of how multinational corporations operate; 60% of senior executives say digital transformation is the most important driver of growth,[33] and digital capability is at the heart of effective execution, from supply chain resilience and new product development to consumer services and ESG reporting.[34] **Corporate security, like all functions, is expected to embrace the opportunities offered by technology, in terms of productivity, interoperability, and cost savings**.

A company's ability to master its data dramatically improves its performance; organisations deemed to be 'data masters' have 70% higher revenue per employee, 245% higher fixed asset turnover, 22% higher profitability, and enjoy a performance advantage of 30–90% in various metrics across customer engagement, top-line benefits, operational efficiency, and cost savings.[35] **Companies that can harness and collate data from across the value chain** – operations, the supply chain, corporate security, business intelligence, cyber security, for example – **will tend to generate much more nuanced insights to drive business decisions, allowing them to lean into risk with greater confidence**.

The opportunities of technology are balanced by the risks; in a PwC poll, 85% of C-Suite executives ranked cybercrime as the top challenge facing their company,[36] and over half (51%) of board members cited cyber security as a serious risk.[37] One of the business executives interviewed commented, 'Cyber has come up fast in the outside lane and has now taken over from physical security threats in many places.' **Most corporate security functions do not have responsibility or accountability for cyber security, but ever-closer involvement is essential given the interdependencies between the two.**

In recent months, considerable attention has been devoted to the rapid advancements in AI, particularly following the launch of generative AI products. The opportunities for businesses are considerable; as Paolo Bonomo, a non-executive director, put it, 'If you're not interested in artificial intelligence, if you don't have a strategy for that . . . you are falling behind.'[38] For all its promise, concerns remain – and **executives look in part to corporate security for advice on the challenges to the business from AI.**

Post-truth

"If you're not interested in artificial intelligence, if you don't have a strategy for that... you are falling behind."

Perhaps the most insidious risk of all is the emergence of the so-called 'post-truth' era,[39] where falsehoods spread significantly faster than the truth.[40] **Misinformation and disinformation have eroded trust in experts precisely at the moment we most need insight-driven decision-making to prevent, manage, and bounce back from incidents and crises.** The consequences of disinformation – such as the examples in Box 2 – can be serious, including decreased share prices, attacks on senior executives, protests, disruption to operations, and damage to important stakeholder relationships. **Preparing for and responding to such incidents requires a cross-functional approach, and corporate security is at the heart of many such scenarios.**

Box 2

Disinformation campaigns impacting multinational corporations

- In 2016, ahead of the US presidential election, fake rumours spread online that Pepsi's CEO, Indra Nooyi, had told Trump supporters to 'take their business elsewhere.' Pepsi's stock fell nearly 4%.[41]
- In early 2020, India's Ministry of Tourism issued an order stating that hotels across the country would be closed until mid-October. It was false.[42]
- In 2020, conspiracies circulated online – originating from an anonymous QAnon conspiracist – that a furniture retailer, Wayfair, was involved in a child trafficking operation. It triggered a crisis communications cycle, CEO Niraj Shah was personally targeted with hateful messages, and there were attempts to short the company's stock.[43]
- In 2020, a fake press release was issued, purportedly by the Grand Hyatt hotel in Seattle, saying it would offer its hotel to shelter the homeless from the dense smoke pervading the area from nearby wildfires. The Hyatt faced two waves of protest: first from those who gathered around the hotel to protest their housing the homeless, and later from those who scolded the hotel for not protecting the homeless when the deception was cleared up.[44]
- A 2021 press release from Portuguese oil company, Galp, committed to withdrawing from northern Mozambique on environmental grounds and paying compensation to local communities. It was fake.[45]

2 Five Business Trends that Elevate the Business Value of Corporate Security

"During the pandemic, Boards of Directors recognised that they needed to become comfortable operating in an environment of significant risk, as standing still was not an option. This drove them to embrace the "try fast, fail fast approach" ... and [they] will continue taking risks."

– Gartner [46]

Summary

- **In a more difficult and volatile business environment, a majority of executives are increasing their risk appetite in order to identify opportunities.** Corporate security can offer more nuanced insight, trusted advice, and a highly effective crisis management capability as a source of organisational resilience.
- **As multinational companies manage risks that span functions – falling outside the remit of any individual function – and deal with multiple risks concurrently,** corporate security is particularly well placed to play a central role in a unified risk management framework because it is one of the most connected functions.
- **Multinational companies are shifting locations and adjusting supply chains, thereby creating new security risks. This makes corporate security's core role non-negotiable for commercial success.** Corporate security can also offer valuable intelligence insights; normally responsible for some of the company's critical asset registers, their input can also help to increase visibility of supply chain vulnerabilities.

- **Business leaders are increasing scenario-planning activity to achieve resilience in the face of volatility.** They place a premium on cross-organisational crisis management structures that enable the company to move fast, withstand shocks, and pivot to opportunities. **Corporate security functions are one of the centres of excellence for crisis management, bring insight to scenario planning, and hold a rich network of external contacts that can offer support, early warning, and assistance.**
- **Businesses are looking for a new type of leader, capable of navigating the current complex and volatile global business environment.** CSOs, like all leaders, need to demonstrate these skills and competencies.

The current nature of the global context for multinational companies is driving five business trends that elevate the contribution of corporate security to the value chain.

Increased risk appetite

In a more difficult business environment, growth requires companies to be able to identify opportunities and lean into risk. More than half (57%) of board directors said they expected to **increase their risk appetite** (or had already done so).[47] Partha Iyengar from Gartner explained, 'During the pandemic, Boards of Directors recognised that they needed to become comfortable operating in an environment of significant risk, as standing still was not an option. This drove them to embrace the "try fast, fail fast approach" . . . and [they] will continue taking risks.'[48]

Business leaders increasingly need more nuanced insight to calibrate the risks they take, trusted advisors willing to speak up when something is a risk too far, and highly effective crisis management capability, which becomes a source of organisational resilience, as a well as a standalone activity in response to crisis events. Corporate security can contribute essential data on security risks, has a track record for being a trusted advisor on risk decisions, and is one of the company's centres of excellence on crisis management.

Unified view of risk

Multinational corporations increasingly manage risks that span functions – falling outside the remit of any individual function – and are dealing with multiple risks concurrently. In this context, silos cause missed opportunities, obscure risks, and create blind spots.

Business leaders need a more unified, functionally agnostic view of risk and place a premium on functions staffed with people with reach and influence who are skilled collaborators and integrators. A growing majority of companies (83%) have an enterprise risk management (ERM) programme,[49] which should include corporate security alongside a range of risks, including cyber security, information security, reputational, social and political, environmental, and technology risks. **Corporate security is one of the company's most connected functions – seen by some executives as 'corporate glue'.**

Shifting locations and supply chains

> *46% of CEOs are considering adjusting their presence in their current markets within the next 12 months to mitigate against exposure to geopolitical conflict.*

As a result of shifting geopolitics and the after-effects of the global pandemic, many multinationals are reconsidering their geographical footprint and pulling out of some countries entirely. Almost half (46%) of CEOs surveyed by PwC said they are considering adjusting their organisation's presence in their current markets and/or expanding into new markets within the next 12 months in order to mitigate against exposure to geopolitical conflict.[50] Market entry and exit are not new, but the intensity of change and the significance of some of the geopolitical trends are making shifts faster and more consequential than in most previous periods. Some companies are exploring ways to deglobalise, allowing them to isolate problems locally to limit the impact and increase resilience.[51]

Business leaders recognise that shifting their operational footprint can throw up new security risks, and rely on excellence of delivery from their corporate security team to allow the executive to focus on opportunities and growth. They also require more nuanced insights to drive higher risk decisions, often at pace. **Corporate security's core tasks are non-negotiable for commercial success in today's global business environment**, and the function has vital intelligence and data that can improve insight.

The same trends are leading many multinational corporations to adjust their supply chains; almost half (46%) of CEOs in a PwC poll said they were considering adjusting supply chains,[52] including through on- and near-shoring. In another study, three-quarters (73%) cited supply chain security as one of the main challenges facing corporate security in the next five years.[53]

Business leaders need greater visibility and up-to-date data on assets, full supply chain verticals, and the changing threat picture on the ground. Some are creating AI-enabled supply chain control towers; connected dashboards of data, key business metrics, and events to allow the business to understand, prioritise and resolve critical issues in real time.[54] Corporate security is well placed to contribute; it often plays a key role in managing corporate asset registers, can contribute situational threat assessment data, is well used to working across the business, and often has teams geographically located to provide a comprehensive risk picture. **Corporate security input to supply chain risk management and resilience is important.**

Increased scenario planning and adaptation

Business leaders are increasing scenario planning for a wider range of disruptions,[55] including 'black swan' (unpredictable, high-impact), and 'grey rhino' (probable, high-impact) events, and understand that being prepared makes them agile.[56] As a McKinsey report put it, 'Even as boards and CEOs work to build capabilities in managing such [geopolitical] risks and developing geopolitical resilience, the imperative to lift one's gaze and look around the corner has become key to strategy and performance. Scenario planning is squarely back.'[57]

Business leaders interviewed said they place a premium on cross-organisational crisis management structures that enable their companies to move fast, withstand and limit negative impacts, and pivot to opportunities as soon as possible. Structures that might once have been seen as superfluous in medium- to low-risk enterprises are now recognised as a source of resilience and a contributor to growth. As economist, W Brian Arthur, put it, 'Adaptation lies in having at the ready a repertoire

of available responses . . . Adaptation means having a tool kit of backup preparedness: people, plans, responses, ideas, possibilities, attitudes, and equipment that allow you to construct solutions quickly.[58] **Corporate security functions are one of the centres of excellence for crisis management, can bring invaluable insight to the scenario-planning process, and have an extensive external network that can offer support, community, and practical assistance in crisis situations.**

Different kinds of leadership

Where previously firms hiring C-Suite executives were looking primarily for technical expertise, administrative skills, and a track record of managing finances, an analysis of 5,000 executive role job descriptions from a 20-year period found that companies now emphasise one qualification above all others: strong social skills.[59] **They look for leaders whose skills match the challenges of the volatile and complex global business context**; individuals who are able to navigate complex stakeholder relationships, are adept at public relations, can handle complexity and ambiguity with a calm and measured response, and are able to motivate a diverse and increasingly technologically savvy workforce. Business leaders are looking for executives, including CSOs, who demonstrate competence in these skills and qualities.

3 Circle Of Control

Corporate security core tasks

"I look to them for absolute guidance, counsel, reassurance, and a view. I take what they say as expert input and am guided by it as to what we are looking to do. I have a lot of confidence in our CSO and his team. It would be very, very rare that I would actually go against what they say."

– Senior business executive

Summary

- **The C-Suite sees corporate security as a business enabler that provides a baseline of protection from which the company can operate with confidence. Corporate security is non-negotiable for commercial success.**
- **There are 16 core tasks for corporate security:** security audits, security assessment, asset protection, identity and access management, executive protection, global meetings and events, travel security, insider risk, investigations, vetting and/or due diligence, threat intelligence, security technology, business continuity, incident management, crisis management, and training.
- **Corporate security functions enhance their value by adopting additional responsibilities specific to the unique risk profile of their company**, which is based on sector, geographical footprint, profile, products, and activities.
- **Effective corporate security functions recognise that competence in their circle of control – their core tasks – earns them the trust needed to extend their circle of influence and make enhanced contributions along the value chain.**

Corporate security contributes to commercial success

In a global business context characterised by fast-changing dynamics, volatility, and complex and interconnected risks, the C-Suite sees corporate security as a business enabler that adds value. [60] At a time when many multinational companies are facing higher and new security risks, effective **corporate security functions provide a solid baseline of protection that enables the company to operate safely, be resilient in the face of shocks, and manage through crises with confidence.** As the quote from a senior executive at the start of this chapter demonstrates, many look to the corporate security team for guidance and reassurance during the decision-making process. **Effective corporate security is non-negotiable for commercial success and a source of business advantage.**

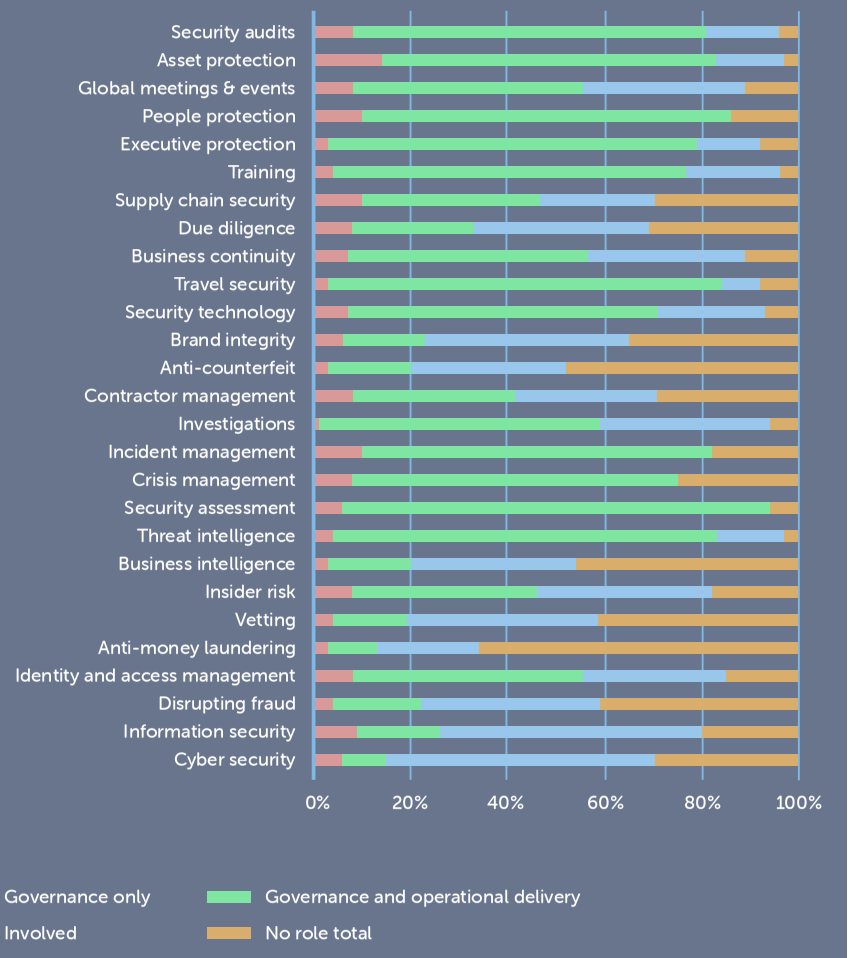
Excellence in core tasks

Our research suggests there are 16 core tasks for corporate security, as shown in Box 3. The majority of CSOs surveyed confirmed they have accountability or responsibility for these tasks, with the exception of insider risk and vetting and/or due diligence. These three areas are included within the core list because of their increased importance to the company and the relevant expertise corporate security has in these areas: investigations, highly developed internal and external networks, security intelligence, and oversight of data relating to access and facilities. Figure 6 shows the breakdown of corporate security responsibilities for all tasks (including a number that are not considered part of the 'core' list).

Box 3
Corporate security core tasks

- Security audits
- Executive protection
- Investigations
- Business continuity
- Security assessment
- Insider risk
- Security technology
- Training
- Asset protection
- Travel security
- Threat intelligence
- Crisis management
- Identity and access management
- Global meetings and events
- Vetting and/or due diligence
- Incident management

Figure 6
Corporate security tasks: nature of role



Source: The Clarity Factory CSO survey, 2023

Company-specific responsibilities

Effective corporate security functions enhance their value by additionally adopting responsibilities specific to their company, based on sector, geographical footprint, profile, products, and activities. These are described in more detail in Box 4.

Core tasks: competency, trust, and a license to operate

"Corporate security functions spend an average of 75% of their time on their core tasks."

Effective corporate security functions dedicate the majority of their time to exceptional execution of their core tasks or company-specific responsibilities; the CSOs interviewed said that their teams spend an average of three-quarters (75%) of their time on this work. This is vital because excellent corporate security is non-negotiable in the current business environment. **Effective CSOs recognise that competence within their circle of control earns them the trust needed to extend their circle of influence,[61] which in turn allows them to make an enhanced contribution along the value chain.[62]**

Box 4
Factors impacting a multinational corporation's security risk profile

Sector

- **Intellectual property** tends to be higher risk for pharmaceutical companies.
- **Brand integrity** is especially important in the luxury goods sector.
- **Fraud** will usually be high on the risk register for banks and retailers.
- **Information security** is especially critical for legal firms and those holding sensitive client or customer data, such as healthcare providers.
- Companies handling highly valuable goods, such as precious metals, are likely to have **organised crime** at or near the top of their security risk register.

Geography

- Some risks are geographically specific, such as **kidnap**, **piracy**, or **civil war**, so firms tied to those locations, such as extractives, are more likely to be impacted.
- Some organisations, such as the media, run towards danger, taking them into the path of **wars and conflicts** that others would avoid.

Profile

- Some sectors are more prone to **political activism**, such as banking and energy companies, and the pharmaceutical industry, which was subject to conspiracy theories and attacks during the pandemic.
- **Social and investor pressure** for companies to take a stand on social and political issues will likely make a wider range of companies and sectors a target for activism in the years ahead.

Products

- Companies with high-value products, such as precious metals or luxury brands, will require much higher security around their transport and **supply chains**.

Activities

- Certain risks are time-limited, such as those associated with mergers and acquisitions or divestment activities, when **insider risk** or **espionage** might be more likely to occur.
- New market entry can spike an organisation's **travel risks** due to new travel patterns.

4 Integration for a Unified View of Risk

"Security is unique in their ability to reach right across our business."

– Senior business executive

Summary

- **Business leaders increasingly seek a more unified view of risk and place a premium on functions that can connect across the corporation.**
- **Effective corporate security functions are uncompromising in their pursuit of excellence in their core tasks; this unlocks opportunities for them to expand their circle of influence and contribute along the value chain.**
- **Corporate security is one of the company's most effective integrators**, due to the fact it is often geographically organised, delivers through a delegated model, relies on influence to bring about change, and usually plays a central role in the all-critical area of crisis management.
- **Corporate security is one of the functions at the heart of a company's unified view of risk**, and has developed a range of models to fulfil this role.
- **Effective corporate security functions that have mastered excellence in their core tasks are able to make wider contributions along the value chain**: as connected specialists, valued contributors to activities such as M&A and new market entry or exit, and the company's complex-problem solver of first choice.
- **Corporate security's ability to act as a strategic integrator rests on vertical integration**: effective CSOs usually sit at ex-comm minus 1 or above, and report into relevant governance bodies.

Circle of control, circle of influence

Business leaders increasingly seek a more unified view of risk, which places a premium on functions that can connect across the company; integration and collaboration are business enablers. According to management research, there are two types of executives: those with a specific, focused specialisation or technical expertise, who have a siloed sphere of influence, and those who have a broader, cross-functional purpose across the organisation, who have a wider sphere of influence because they are required to work across multiple organisational silos.[63] Successful CSOs bridge these two categories; they are uncompromising in their pursuit of excellence in their core tasks, which in turn unlocks opportunities for wider influence. As the CEO of Procter and Gamble put it, 'the measure of a powerful person is that their circle of influence is greater than their circle of control.'[64] **Corporate security is one of the company's most effective integrators**, and CSOs we interviewed described how partners across the business proactively seek their input. The word cloud in Figure 7 shows how CSOs describe their closest professional relationships across the organisation.

Figure 7

Corporate security's closest professional relationships across the business

What are your closest professional relationships across the business?
Source: The Clarity Factory interviews with CSOs, 2023

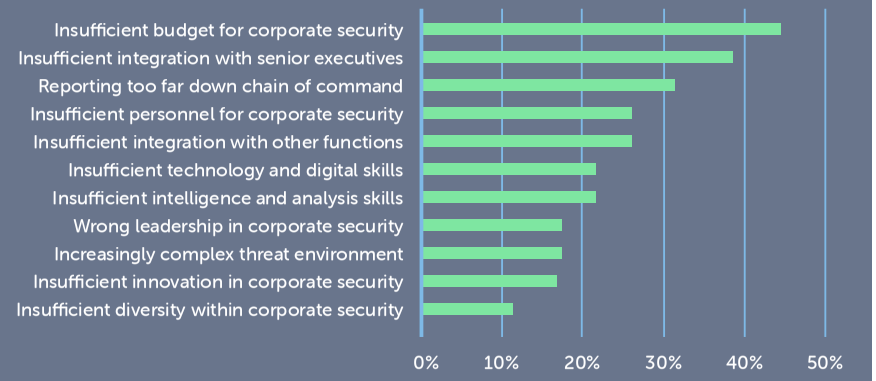
Corporate security is a natural integrator

There are also a number of structural factors that make corporate security one of the company's most effective integrators:

- **Organising logic: corporate security is often one of the few functions organised geographically rather than by business units, which means it touches multiple business lines and has a broad as well as deep view across the organisation.** One senior executive told us, 'Security is unique in their ability to reach right across our business.'
- **Delegated delivery: effective corporate security is delivered through the everyday actions of employees across the company,[65] which requires the function to develop strong vertical and horizontal relationships.** One-quarter (26%) of CSOs said insufficient integration with other functions is one of the biggest obstacles to their success, as shown in Figure 8.
- **Change through influence: the success of a corporate security function is proportionate to its ability to influence.** Business leaders recognise this; one commented, 'The biggest asset that our security team has is that relationship with the rest of the business. They are accepted and known. We always recruit for people's ability to build those relationships, as much as their expertise. Everyone is so busy, we need to be sure that when the security team ask for their time, people are willing to stop what they are doing. We can't have them telling the security team to come back another day; it's too important.'
- **Crisis management: corporate security's role in crisis management brings visibility, reach, and trust to the function, as well as an extensive network across the business**, especially in recent years due to a succession of large-scale crises. One CSO commented, 'The value proposition for corporate security is at an all-time high. What that's produced is more of those moments where someone doing M&A work will say, "Hey, why don't we loop in corporate security to get their perspective on it."' Another said, 'As a result of Covid, there were people who didn't have anything to do with us, who suddenly had sight of security and realised how we can support them, where previously they would have been dismissive.'

Figure 8

Biggest obstacles to the effectiveness of corporate security



What do you consider to be the biggest obstacles to the effectiveness of corporate security?
Source: The Clarity Factory CSO survey, 2023

Corporate security at the heart of a unified view of risk

The extent of corporate security's integration makes it ideally suited to play a key role in bringing about a unified view of risk, which business leaders increasingly demand. One CFO interviewee commented on the connections among risk, resilience, and security, 'I think it's odd if they are not joined together.' Corporate security, cyber security, information assurance, IT, legal, compliance, sustainability, government and external relations, health and safety, and HR functions are more often coming together to create a more joined up approach to risk. As one CSO put it, 'Risk owners are coming out of their silos. Risk itself isn't siloed, it's completely blended. Given that reality, we have to think about how we get stuff done and that leads us to collaborating more.' Although there is no one-size-fits-all approach to this, Box 5 outlines various ways that CSOs described their role within risk management, a number of which have cross-functional dimensions that serve to unify and integrate views of risk across the organisation.

Box 5
Corporate security's growing role within risk management

- **Responsibility for risk**: one CSO interviewee recently assumed responsibility for all operational risk excluding financial and another is in discussions about doing so; another has the role of Director of Risk and is working with colleagues to integrate security into risk management processes.
- **Risk frameworks**: one CSO interviewee created a security enterprise risk-management framework, which was subsequently adopted by the company as its ERM framework.
- **Risk boards and forums**: a number of CSOs are involved in enterprise-wide risk or resilience boards or forums.
- **Board risk-audit committee**: most CSOs (77%) provide reports into their board risk and audit committee, or equivalent.
- **Leadership team**: several CSOs have extended leadership teams, which include members from other functions.

Corporate security's contributions across the value chain

Effective corporate security functions that have mastered excellence in their core tasks are able to make wider contributions along the value chain.[66]

Connected specialists

Effective corporate security functions lend their specialist knowledge and expertise to colleagues accountable or responsible for activities that are closely linked to the security brief, as shown in Figure 6 in the previous chapter. For those tasks where fewer than half of the surveyed CSOs were accountable or responsible, a majority said that they are still involved in some way. They are not in control, but they make it their business to influence and input.

Valued contributors

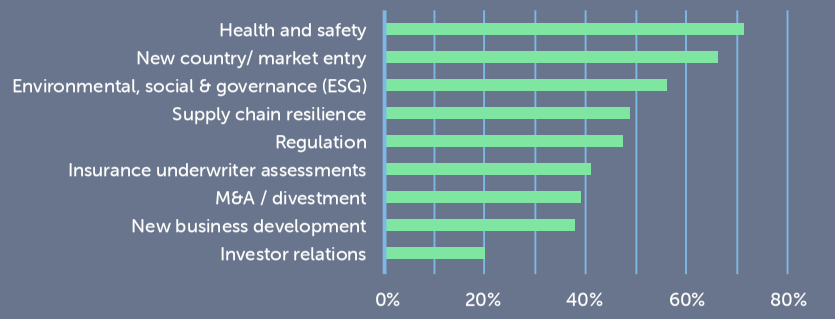
Effective corporate security functions are valued contributors, where relevant, to a broader range of business activities across the value chain, such as health and safety, new country/market entry, ESG, supply chain resilience, regulation, and M&A/divestment, as shown in Figure 9. Box 6 provides further details of the function's involvement in these areas.

Box 6
Corporate security's contribution to activities across the value chain

- **New country/market entry and exit**: especially for companies operating in moderate- to high-risk countries, the corporate security function is often formally incorporated into new country/market entry and exit, or there is at least an expectation that it will be consulted. Among the CSOs we surveyed, two-thirds said their functions are actively involved in this area, and a further 25% said they believe they should be. Fewer than one in ten (9%) said they do not see any role for corporate security in new country/market entry.
- **ESG**: over half (56%) of CSOs said their functions are involved in ESG, with input mostly informal. Given the increased importance of ESG; corporate security's oversight of key issues, such as investigations, due diligence, and vetting; and the growing value of the function's insight, there is scope for greater and more formal involvement for corporate security in ESG.
- **Supply chain resilience**: multinational corporations are shifting supply chains, which creates risks as well as opportunities. Although fewer than half (48%) of corporate security functions contribute at present according to our survey, a further third (32%) of CSOs said they think they could add value in this area, given that many maintain critical asset registers, hold data that could enhance visibility of supply chain risks, or oversee due diligence processes that could be extended to suppliers.
- **M&A/divestment**: two-fifths (39%) of corporate security functions are involved in M&A and divestment activities, usually informally, and the same proportion of CSOs said that they think the function should have a role. Only one corporate security function whose CSO was interviewed is formally written into the M&A process, largely as a result of the fact it is responsible for business intelligence. This CSO commented, 'We proved ourselves, made significant cost savings on external consultants, and raised the standard because we could be laser focused on implications for our business. Corporate security's intelligence is institutionalised within the M&A process; you have to come to us if you want to engage in M&A. As a result, we are drawn into the conversation far earlier around a new business opportunity. The days of finding out about a contract about to be signed or contract having been signed and then having to retrofit, is almost gone.'

Figure 9

Corporate security's contribution along the value chain



Please indicate whether corporate security currently plays a role in each of the areas listed.
Source: The Clarity Factory CSO survey, 2023

Complex-problem solver of first choice

Many corporate security functions have become the complex-problem solver of first choice for senior executives, thanks to their networks and crisis management skills. One CSO commented, 'I think we're seen as people who get things done. You can give us a problem and we will see it through, bring the relevant business parts together and make sure that something is actioned and actually happens. I think we are seen as helping the business . . . experts in different fields who . . . come to this with a pragmatic business-orientated mindset.'

Vertical integration

Corporate security's ability to perform as an integrator rests on vertical integration, which brings upwards influence and support. Achieving vertical integration depends upon two factors:

1. Length of reporting

   Effective CSOs usually sit at ex-comm minus 1 (EC-1) or above, as confirmed by the majority of CSOs (55%) surveyed. Sitting below this level presents a significant challenge; 38% of CSOs said insufficient integration between corporate security and senior executives was one of the biggest obstacles to the effectiveness of their function, and one-third (31%) cited reporting too far down the corporate chain of command (see Figure 8). There is a diversity of accountability for corporate security at executive committee level, with the most common being the General Counsel (33%) and Chief Operating Officer (COO) (18%). Almost one in ten CSOs said there is no one on their executive committee with responsibility for corporate security.

> *A majority of CSOs (55%) sit at ex-comm minus 1 or above.*

2. Governance

   Effective CSOs routinely report into the relevant governance bodies of their organisation, notably the board of directors, the executive committee, and the risk and audit committee or equivalent. This demonstrates appropriate executive and board attention, with frequency of interactions depending upon the organisation's risk profile. A majority of CSOs surveyed have established appropriate reporting procedures:

   - A large majority (85%) provide reports to their executive committee.
   - Three-quarters (77%) provide reports to their risk and audit committee, or equivalent.
   - Two-thirds (63%) provide reports to non-executive directors.
   - Just over half (56%) provide reports to their board of directors.

Corporate security and cyber security

Debates about the convergence of physical and cyber security have raged for well over a decade, and C-Suite leaders are looking for ways to breakdown silos. Nevertheless, only 15% of CSOs surveyed reported having accountability or responsibility for cyber security, and some CSOs commented that cost and complexity were factors in preventing convergence. Just over half (58%) agreed that effective security risk management relies on corporate/physical security and cyber security converging into a single function, and support for this among security professionals under the age of 35 was considerably

higher (79%). Another study found that almost all (92%) C-Suite executives feel corporate security should be accountable or responsible for cyber security.[67]

Whether or not convergence becomes the norm, the scale of the cyber threat and the importance of a joined-up approach make imperfect cooperation preferable to delayed convergence. **Effective corporate security functions are implementing corporate–cyber fusion models.** As one CSO put it, 'If you're not doing the fused approach, you're missing an opportunity to provide a genuinely optimised security capability or service.'

CSOs described a number of fusion models:

- A 'converged lite' model.
- CSO and Chief Information Security Officer (CISO) sitting on one another's leadership teams.
- Joint working groups.
- Joint reporting to the risk and audit committee by the CSO and CISO.
- A security leads forum comprising heads of business continuity, cyber security, corporate security, and product security, which meets monthly to improve joined-up problem analysis and solutions.

5 Insight To Enhance Decision Making

"I think intelligence is critical, because it's the foundation from which we can do everything else."

– Senior business executive

Summary

- **Business leaders recognise the value of security intelligence, driven in large part by C-Suite concerns about geopolitical trends.**
- **Effective corporate security functions have intelligence capability.** They are continually innovating the tools and methods used and looking for ways to join up their own data to generate better insights.
- **Corporate security intelligence can generate useful insights for the rest of the business**, such as supply chain security, assets, business continuity, and operational resilience.
- **Effective corporate security functions are looking at ways to bring together the different strands of intelligence from across the business into a fusion model. This would serve to generate insights across the value chain**, including intelligence-driven decision-making, supply chain visibility, de-risking of product cycles, and enhanced visibility of risks related to new market/country entry and M&A/divestment activities. These insights could also feed into ESG efforts.

Decision-making in complex risk environments requires more nuanced insight

In a complex global business environment, multinational companies require more nuanced insight to drive better decision-making. C-Suite executives recognise the value of corporate security intelligence; a majority (52%) of those surveyed by PwC said they would like more security intelligence skills within their corporate security function,[68] and a CFO interviewee commented, 'I think intelligence is critical, because it's the foundation from which we can do everything else.' CSOs reported an uptick in demand, with one commenting, 'It's now only in this new geopolitical light that the business is starting to ask for more analysis.'

Effective corporate security functions have increased their intelligence capability over the past decade. Three-quarters (75%) have professionally trained intelligence analysts in their teams; almost two-thirds (61%) plan to increase their capacity over the next 1–2 years; and roughly the same proportion (64%) have a 24/7 Global Security Operations Centre (GSOC). Developments in data mining, open-source intelligence, and analytics are accelerating this trend, increasing the potential range, depth, and quality of insight. Some teams are experimenting with AI and generative AI tools.

Many CSOs are looking for ways to join up their own data across the function to dramatically enhance the insights they can derive. Manish Mehta, Chief Product Officer at Ontic, drew an analogy with the development of the US interstate highway system, 'In the 1950s, the US government faced a choice as they were building interstate highways; should it be an open system that connected the interstate with local and regional roads, creating a road network that allowed you to travel anywhere across the country. Or, instead, should it be a closed system with tolls between roads. Lucky for us, they went for the former. We need to do the same in corporate security; rather than multiple separate disconnected datasets, we need to join together all our data so the whole is worth more than the sum of its parts and we are able to generate really powerful insights.'

> *52% of C-Suite executives want more security intelligence skills within their corporate security function.*

Corporate security intelligence can benefit the rest of the business

Corporate security intelligence and data is being used to enhance outcomes across the business, as outlined in Box 7. As one CSO put it, 'The company is totally data driven. If you're not aligned with data, you're not going to make your business case. I think it's a massive opportunity for functions, including ourselves, to really demonstrate business value in a way we've never done before.'

A number of companies have elevated the position of intelligence within their organisations, which underlines its importance to senior leaders. For example, Standard Industries' intelligence function was moved out of security in 2021, and their Head of Global Insights now sits on the Executive Leadership Team; meanwhile, Finserv has elevated its Geopolitical Analysis team out of the corporate security function to sit alongside it, with the two now reporting as peers into the Head of Global Services.[69]

Box7

Examples of corporate security's use of data

- **Supply chain security and resilience**: a pharmaceutical company is tracking product data (raw material production, supply, delivery to pharmacy) to understand how to protect every aspect of the supply chain. To do this, they are bringing together data from commercial, business, insurance and supply chain sources to understand how to de-risk the product at each step in the chain.
- **Assets, supply chain, and business continuity**: in the wake of the Russian invasion of Ukraine, some companies realised they did not have a full picture of how their assets, supply chains, and business operations would be impacted. Many corporate security functions are involved in various aspects of managing asset registers, so have vital information to input. Some are extending their definition of 'assets' to include suppliers, contractors, partners, and investors, helping the business to take a more holistic view of risk.
- **Operational resilience**: some corporate security functions are combining their information with that on supply chain, critical path, contractors, and new market entry into a shared data bank to provide enhanced visibility for the business on its exposure and vulnerabilities.

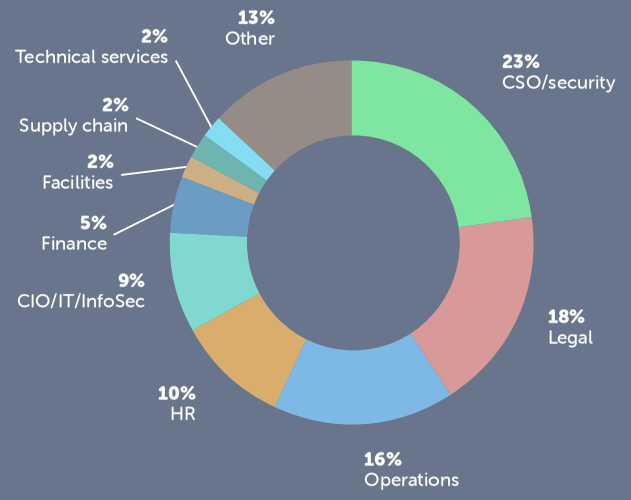
The Clarity Factory interviews with CSOs, 2023

Joined-up cross-organisational intelligence

Corporate security accounts for around one-quarter (23%) of all corporate intelligence, the remainder coming from a range of functions, as shown in Figure 10.[70] Wherever it sits, there are producers and consumers across the business, and **there are benefits to bringing the different strands of intelligence together in a fusion intelligence model**; for instance, this would enable intelligence-driven decision-making, supply chain visibility, de-risking of product cycles, enhanced visibility of risks related to new market/country entry and M&A/divestment activities, and insights around stakeholders. These insights could also feed into ESG efforts.

Figure 10

Location of corporate intelligence



Location of corporate intelligence within multinational corporations
Source: How Corporate Intelligence Teams Help Businesses Manage Risk, Paul R Kolbe and Maria Robson Morrow, 2022 [71]

> *We need to join together all our data so the whole is worth more than the sum of its parts and we are able to generate really powerful insights.*

There is potential to create much more nuanced insight through closer collaboration between intelligence functions across the business. Currently, according to our survey, just half (49%) of corporate security functions collaborate with business intelligence analysts elsewhere within the organisation. Only one CSO interviewee said they are accountable and responsible for their organisation's entire business intelligence process, although there were examples given of increased cooperation, such as products shared between corporate security and business intelligence functions, special reports selectively shared with colleagues based on need and interest, and functions refocusing intelligence reporting away from security analysis to business insights. As Manish Mehta of Ontic commented, 'If you are going to be proactive, you have to know history, which provides context and helps to make patterns more visible. This can only happen if your data is stored together in a database, enabling you to collect and connect the dots.'

6 External Networks

Insight, support, and early warning system

"The diversity and complexity of today's business challenges are placing a premium on the ability to collaborate across the boundaries of the corporation." [72]

— PwC

Summary

- **Business leaders place a premium on external networks**, as they navigate a complex business environment, are under pressure to take a stand on social and political issues, and where reputation management is harder.
- **Business leaders value the external networks of CSOs** that offer insight and situational awareness to drive better business decisions.
- **Effective corporate security functions carefully develop their external networks** and invest in public–private partnerships and membership organisations that support networking, professional development, benchmarking, and information sharing.

The growing importance of external networks

Multinational corporations that are operating in a global business environment with fragmented information, rapidly changing circumstances, and interconnected risks, and are increasingly required to take a stand on political and social issues in a time of declining trust, increasingly place a premium on external networks. As a recent annual CEO survey conducted by PwC put it, 'The diversity and complexity of today's business challenges are placing a premium on the ability to collaborate across the boundaries of the corporation.'[73]

Corporate security's external networks add value to business decision-making

> *An effective CSO prides him or herself on never being more than a phone call away from the information they need.*

Corporate security professionals are not unique in developing a network of contacts; but while most professional networks focus on getting the next job, theirs are mostly about getting the current job done. Information sharing on trends, real-time updates on incidents impacting peer companies, informal benchmarking, and sharing recommendations on reliable vendors are all daily fare for corporate security practitioners. Many of these relationships go back decades; they are long, based on deep trust, and CSOs regularly go above and beyond to help another CSO in need. An effective CSO prides him or herself on never being more than a phone call away from the information they need.

A number of private sector security membership organisations have developed over the past four decades that support networking, professional development, benchmarking, and information sharing – these include the International Security Management Association (ISMA), the Risk and Security Management Forum (RSMF), and ASIS International, to name a few.

Business leaders acknowledged the importance of corporate security's external network; it was one of the most cited points when interviewees were asked to describe the value proposition of the CSO. It not only delivers for corporate security, but increasingly for business executives seeking to understand geopolitical trends and what they mean for the company. **Corporate security's external network adds value to core business decisions.**

Business leaders and CSOs said they value four aspects of the corporate security external network:

- **Non-competitive information sharing: CSOs within the same sector regularly share sensitive information because security is deemed to be non-competitive.** One former CSO recalled, 'When I joined the company, I had my first meeting with the Chairman. He asked me if I shared security information with other companies. I immediately responded that I did, at the same time thinking I might be leaving my job very soon. I was ready to defend myself, but he responded, "Excellent, please continue to do so." He became my best supporter thereafter.'

- **Cross-sector benchmarking: CSOs often compare notes with peers in other sectors to get a holistic view.** As one CSO reflected, 'My boss will regularly ask me what our competitors are doing on any given security issue, but one of the things he says he appreciates most is the fact I can also tell him what my peers in other sectors are doing, which offers a broader perspective on our decision-making and guards against sectoral group think.'
- **Access to government agencies: CSOs have trusted relationships with government agencies**, as a result of the fact that many have former government backgrounds, and the existence of public–private partnerships. Business leaders said they prize these relationships. One commented, 'Our security is intelligence-led and threat-based. We place emphasis on assessing the threat, and a key part of that is intelligence and getting access . . . the kind of person who understands intelligence and what to do with it, what's a proportionate response. At the top, I look for security professionals who understand that . . . and have access.'
- **Broader use for the business: corporate security's external networks complement the intelligence capability within the team in offering insight to business decision-making.** One CSO described an annual industry gathering that senior leaders from the company attend: 'Our CEO tells me that it's the security meetings he finds most useful during that week; he gets real value from them due to the quality of information that's shared.'

7 Crisis Management and Crisis Leadership

"Security professionals have a facility in crisis management that I find very useful. They are naturally better at that stuff than the majority of our employees, including in crises that have nothing to do with security, but where you want a calm, organised head who thinks in terms of risk."

– Senior business executive

Summary

- **Crisis management is a business-critical activity** for multinational companies faced with a succession of crises.
- **Business leaders recognise the critical skills corporate security professionals have in crisis management**, the majority of whom are part of their company's centre of excellence and are accountable or responsible for both security and non-security crises.
- **Effective corporate security functions have realised a number of positive side-effects of their role in crisis management**, including greater functional visibility, enhanced understanding and appreciation among the business of the value of crisis management, shifting perceptions of the function from being rigid to highly adaptable, and greater trust.
- **Business leaders increasingly recognise that 'crisis management' is a required skillset across the whole business.** Effective corporate security functions are helping to build crisis management capacity in a number of ways, including better decision-making in fast-paced, information-poor situations, and coaching, mentoring, and executive talent development.

Crisis management is a business-critical activity for multinational companies

Whether or not you subscribe to the concept of 'permacrisis', companies are facing a higher volume of crises that are more interconnected, including the global pandemic, Russia's invasion of Ukraine, the resulting energy crisis, increasingly extreme weather events, mass shootings, and ransomware attacks in recent years. For companies used to operating in high-risk environments – oil and gas, and media, for example – this might not feel new. For many others newly navigating complex and interconnected risks, it requires a structural and cultural shift.

Corporate security: a critical part of the crisis management centre of excellence

Business leaders said they recognise the critical skills corporate security professionals bring to crisis management. One commented, 'Security professionals have a facility in crisis management that I find very useful. They are naturally better at that stuff than the majority of our employees, including in crises that have nothing to do with security, but where you want a calm, organised head who thinks in terms of risk.'

> *"Our value is derived primarily from responding to operational disruptions when people are really concerned that it's going to throw off our revenue streams."*

Corporate security functions are usually one of the functions at the heart of their company's crisis management capability; three-quarters (75%) of CSOs surveyed said they are responsible or accountable for crisis management within their organisation, and only 1% reported having no role at all. A majority (60%) led their company's pandemic response, and two-thirds (67%) of corporate security functions in companies impacted by the Ukraine war led those crisis management efforts. As a result, most CSOs (71%) confirmed that they have discretion within their budget to respond to unanticipated, fast-moving events.

The exact nature of the role that corporate security functions play in crisis management varies. Insights from our research include:

- **Type of role**: a small minority of CSOs (8%) are accountable for crisis management and own the process, standards, and training; two-thirds (67%) are accountable and also have responsibility for delivering crisis management.
- **Type of crisis**: a majority (56%) of the CSOs surveyed are responsible for all types of crises, both security and non-security.

- **Crisis management structure**: multinational corporations tend to have permanent or ad-hoc crisis management committees or taskforces, with CSOs often playing a central role, such as chief of staff, subject matter expert, or mentor to the committee chairperson.
- **Time-limited structures**: some multinational corporations convene time-limited taskforces to respond to crises, where the CSO's role will vary depending on the nature of the crisis.

Crisis management brings corporate security to the heart of the business

As a result of their role in crisis management, effective corporate security functions have realised a number of positive side-effects, which were described in our research:

- **Visibility**: almost all CSOs (89%) said the visibility and profile of corporate security has risen as a result of their role in crisis management.
- **Enhanced understanding of crisis management structures**: business leaders better understand and appreciate the value of the structure and discipline that CSOs and their teams bring to crisis management. One CSO told us, 'The CEO was really grateful that we had a process to follow. A few times early on, the COO, who has a habit of jumping in with solutions, had to be rowed back. Eventually, he realised the importance of having the process.'
- **Shifting perceptions of corporate security**: seeing the team in action has shifted perceptions and dispelled stereotypes of the corporate security function among the rest of the business. One CSO said, 'We showed people through how we responded to that crisis that we could be agile, whereas I think some people think of security as rigid. We were the ones who stepped up to the plate and really morphed in order to meet the demands of the pandemic.'
- **Trust**: crises create conditions conducive to trust building for effective corporate security functions. One CSO commented, 'I think it's incident after incident. Our value is derived primarily from responding to operational disruptions when people are really concerned that it's going to throw off our revenue streams. We provide clarity and navigate the company through those difficult moments. It's non-stop. You show up for those events, and then the trust just grows.'

According to Sandra Sucher and Shalene Gupta, there are four types of trust: competence, motives, means, and impact (see Box 8).[74] The unique feature of a crisis situation is that it brings all these factors together simultaneously, enabling rapid and substantive trust-building. Competence is the foundational element; only corporate security functions that are effective gain the trust dividend offered by crisis situations.

Box 8
Four ingredients of trust

- **Competence**: your ability to create and deliver products and/or services through a combination of process excellence, technological know-how, and managerial smarts.
- **Motives**: your good intentions for doing what would be best for all the people and groups you interact with. And when confronted with the necessity to make painful decisions, thinking through how to balance the needs of different groups to cause the least amount of harm.
- **Means**: the fairness of your processes and treatment of people when distributing rewards and pain points. Ensuring that your processes allow for open and transparent communication so that people affected by a decision can weigh in.
- **Impact**: the overall effect, both intended and unintended, of your actions on other people. And when the consequences are unintended, do you stand up and take responsibility?

Source: The Power of Trust: How Companies Build it, Lose it, Regain it, Sandra J Sucher and Shalene Gupta, 2021, p. 8

Crisis management: a business-critical leadership capability

'Crisis management' is more than a discrete task of the corporate security function or the central crisis management team; increasingly, it is a required skillset across the whole business. Nitin Nohria, former Dean of the Harvard Business School, summarised its centrality in the current global business environment, 'The new zeitgeist will [also] require a greater emphasis on crisis management skills. Leaders

can no longer assume that trouble may strike once every three or four years and be managed by outside crisis consultants. Instead, companies must prepare for a steady stream of upheavals – and hone their in-house skills for dealing with them. They can't afford to merely react; they should anticipate, plan, and organize for potential challenges.'[75] Business leaders we interviewed echoed this; one senior executive said, 'Every element of the business needs to be able to do crisis management.'

Business leaders recognise that CSOs have exceptional crisis management skills and capabilities that can be of wider value to the company; one interviewee commented, 'I think corporate security has a unique set of assets when it comes to crises. They help us to be clear about the difference between a crisis and noise, they are good at standing back and assessing. There are a lot of great techniques that come with crisis management that can be applied in business situations.'

Effective corporate security functions can put their crisis management expertise to use for the wider business in a number of ways:

- **Incident versus crisis: there is a premium on senior leaders who can distinguish between an incident and a crisis**; unnecessary activation of a crisis management team can be costly, distracting, and has the potential to become a self-fulfilling prophesy.
- **Better decision-making: in an environment characterised by decision-making at pace with limited information, crisis management experience can be instructive.** One CSO said, 'We use the same crisis management procedures when we've had major business issues, and we've been using that as a model for how to make quicker decisions in business units generally.'
- **Crisis management capacity-building: some CSOs coach and mentor and others are using their crisis management expertise to develop executive talent.** Referring to those CSOs with prior government experience, one commented, 'Because companies are going to be in a permacrisis, they need to have a level of competence in leadership, crisis leadership, and nobody in the business has got that level of competence because they haven't done it. If you're making decisions where lives are at stake rather than the loss of a deal for USD 50 million, it's a very different ballgame. This is an area where CSOs can add significant value.'

8 Delivering the Vision

Success criteria for an effective CSO

"You can only challenge from a position of respect, not authority. Telling people to do things isn't sustainable. So we look for people with relationship skills, communications skills, who are collaborative."

– Senior business executive

Summary

- **Business leaders consider corporate security to be a critical function** and need to lend their support in realising the core supporting elements of an effective corporate security function.
- **In order to unlock opportunities to contribute along the value chain, CSOs need to develop a compelling narrative** that draws colleagues towards collaboration and ensures the perception of the function is based as much on proactivity, prevention, insight and resilience as it is on reactivity and crisis response.
- **Business leaders need to select CSOs** that lead with credibility, gravitas, innovation and personal resilience; and that have business acumen; collaboration skills; exceptional stakeholder management; strong external networks; and demonstrable subject matter expertise.
- **Effective CSOs have an innovation mindset**, always striving for better ways to work.
- **Effective CSOs have a fit-for-purpose talent strategy,** to attract the best professionals, from a diverse range of backgrounds and possessing a variety of skills.
- **Business leaders should support CSOs with adequate budget and headcount**, without which the vision outlined in this report will not be achievable.

Delivering the vision

In today's complex and volatile global business environment, C-Suite executives consider corporate security to be a critical function. Delivering the vision for effective corporate security outlined in this report relies on strong partnership between the executive committee and CSO, as well as support from business leaders to promote the value of corporate security across the organisation, and ensure the function is well-placed and adequately resourced for success.

Executives and the CSO should work together to achieve the following supporting elements of an effective corporate security function:

- A compelling corporate security narrative.
- The right kind of corporate security leadership.
- An innovation mindset.
- A fit-for-purpose talent strategy.
- Sufficient resourcing.

A compelling corporate security narrative

Effective CSOs clearly articulate the value of the corporate security function. Their narrative is simple, high-level, emotionally engaging; memorable; and it chimes with the organisation's culture and style. An effective narrative is not a list of deliverables and KPIs – these are important management tools, but hard for busy executives to remember or share. Good narratives focus on the why rather than the what, which is what makes them engaging and relatable.

Developing a corporate security narrative is important for two reasons. First, security is not front and centre for business executives most of the time, but CSOs need to convince them to dedicate attention and resource outside of crisis moments. As one business leader put it, 'The majority of the time, they are engaging the business on topics that are not currently critical so you need to be able to get them engaged and thinking about things that might happen in the future. That requires really strong relationship building skills and an ability to be an engaging storyteller.'

Second, while crisis response is increasingly important for multinationals, it is important to ensure that perceptions of the corporate security function reflect the totality of its role. It would be easy for a narrative to emerge about corporate security as a fixer, problem solver and fire fighter. The narrative should be based as much on proactivity, prevention, insight, and resilience as it is on reactivity and crisis response, as important as those things are. The business value of corporate security can only be fully realised if the business has a full and nuanced perception of the function.

Effective CSOs continually reinforce the narrative. A May 2022 survey at the height of the pandemic – when corporate security was highly visible – found disparity between C-Suite and CSO understandings of the scope of corporate security.[76] Figure 11 shows the key words that non-security business leaders gave in this research to describe the function; most fit with the picture painted in this report, but overall it shows room for continued work on a shared understanding.

Figure 11

What five words would you use to describe your corporate security function?

Source: The Clarity Factory interviews with non-security business executives, 2023

The right kind of corporate security leadership

"When you think about how the world is changing, the scale of the challenges we face – from climate change to AI – companies are being taken into places that are high risk but potentially high reward. It will take some really savvy leaders thinking about risk in this brave new world to steer companies forward effectively. The CSO of the future needs to be both a big thinker and a true globalist."

— Kathy Lavinder, Founder and Executive Director, SI Placement

To meet the challenges outlined in this report, effective CSOs need to lead with credibility, gravitas, innovation and personal resilience; and to have business acumen; collaboration skills; exceptional stakeholder management; strong external networks; and demonstrable subject matter expertise.

CSO leadership attributes

- **Credibility**: effective corporate security is non-negotiable; the function's ability to contribute along the value chain is contingent on excellence in core tasks. The CSO must have credibility with colleagues up, across and down the organisation in order to build trust and partnerships.
- **Gravitas**: effective CSOs influence the C-Suite, lead during a crisis, and are willing to challenge senior decisions. They are business enablers who are not afraid to say 'no' when they think it is a risk too far. One senior executive told us, 'At times, when you speak to security, they are so keen to partner and enable that there's a tendency to say, "well, if that's what you want to do, we can enable you to do it." That's great, but we also want them to say "no, that it's not the right thing to do."'
- **Innovation**: effective CSOs never stop asking themselves whether they can do things better, and they have an inclusive leadership style that empowers all team members to contribute fully. Dominant hierarchies are less successful in complex and fast-moving environments; a study that examined the safety outcomes of thousands of Himalayan expeditions found that teams with more dominant hierarchies are significantly more likely to die. As

the author put it, 'When the environment can change dramatically and suddenly, people have to adapt and come up with a new plan. In these cases, we need everyone's perspective brought to bear and hierarchy can hurt by suppressing these insights.'[77]

- **Personal resilience**: effective CSOs are highly resilient individuals – calm under pressure, able to make tough and timely decisions in high-stakes situations, willing to take personal risks in speaking up, competent at handling sensitive issues, and can contend with unpredictable hours and significant travel.

> *They need to bring people and business together, understand the business priorities and how they relate to security. Business acumen would be my number one priority.*

Business acumen

With corporate security engaging more parts of the value chain, effective CSOs take an active interest in the business. This attribute was valued by the senior executives interviewed; one commented, 'What I would be looking for in that role is people that understand the business end to end. They need to be functional experts, of course, but they need to bring people and business together, understand the business priorities and how they relate to security. Business acumen would be my number one priority.'

Collaboration skills

Like all business leaders, effective CSOs also need skills that boost collaboration, such as self-awareness, the ability to listen and communicate, a facility for working with different types of people and groups, and high emotional intelligence. Although business acumen is highly important, Figure 12 shows the dominance of these other skills among those listed by CSOs as being most important to them in their role. Soft skills were also highly valued by senior executives. As one commented, 'You can only challenge from a position of respect, not authority. Telling people to do things isn't sustainable. So we look for people with relationship skills, communications skills, who are collaborative.'

Figure 12

What are the most important qualities, competencies and experiences for a senior corporate security leader?

Source: The Clarity Factory, CSO survey, 2023

Exceptional stakeholder management skills

Effective CSOs have exceptional stakeholder management skills, which are critical in collaborating with other risk-related functions. To demonstrate the importance of this, CSOs interviewed for this report said that they spend an average of one-third of their time engaging with stakeholders inside or outside the business. As one put it, 'If I was hunkering down in the security realm, I'd be isolating myself rather than integrating myself.' Senior executives said they value this, 'The role has to touch many layers of the organisation, from the top of house to boots on the ground, so being able to communicate in an influencing way is really important. You need to command the respect of everyone from the CEO to the field staff.'

Strong external networks

Senior business executives emphasised the importance of strong external networks, which offer access to privileged information, benchmarking, and relationships and influence of broader benefit to the business.

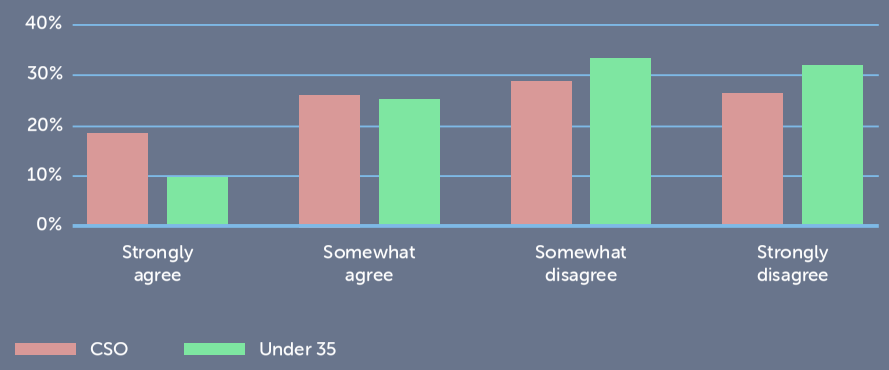
Subject matter expertise

Excellence in core tasks is critical and unlocks further opportunities to contribute across the value chain. It is important that CSOs have relevant subject matter expertise. For many years, government experience was considered a shorthand for relevant prior experience; data from Security Management Resources (SMR), a recruitment consultancy, showed that 70% of their candidates for security, risk and resilience positions globally had this background.[78] Data for this report suggests this trend is reversing; only one-quarter of CSOs surveyed said their teams were made up of a similar proportion with government backgrounds, and only one-third of surveyed security professionals under the age of 35 have prior government experience. A majority of both CSOs and security professionals under the age of 35 disagree with the notion that prior government experience (military, diplomacy, police or intelligence) is essential to being an effective CSO, as shown in Figure 13.

Senior executives were evenly divided on whether this kind of government experience is relevant for a CSO. Some perceived a rigidity among those from a non-business background, and spoke of this and other disadvantages, while others appreciated the skills it brings: 'The reason a military background can be helpful is because it tends to give people a good ability to plan and see several steps ahead . . . it brings a huge network of other like-minded individuals that they all know and trust and exchange ideas with, and I think that's incredibly valuable.' Ultimately, the trend is towards recognising the value offered by a background in military, diplomacy, police or intelligence, while appreciating other valid experience.

Figure 13

Prior military, diplomacy, police or intelligence experience is essential to being an effective Chief Security Officer



Source: The Clarity Factory CSO and Next Generation surveys, 2023

An innovation mindset

Effective corporate security functions challenge themselves to improve and are open to new ways of working. A majority of CSOs (65%) and security professionals under the age of 35 (55%) think their function is keeping pace with innovation across the business. Effective CSOs are identifying ways to use new technologies and ways of working to increase productivity, generate more nuanced insights, share data across the business, reduce costs, and decrease company losses (see Box 9).

Box 9
Examples of corporate security's use of technology

- **Access control**: linking video surveillance at sites into a central hub to reduce manpower needs; using data on use of space to help the business make decisions about utilisation.
- **Security assessments**: use of online assessment tools that standardise the process, enable wider input beyond the security team, and free up time for more strategic level work; integration of real-time access-control data to produce dynamic security assessments.
- **Perimeter security**: use of drones to increase visibility around the perimeter and decrease manpower needs.
- **Investigations**: use of a tool that tags people, places, locations and incidents, which are cross-referenced with sales and marketing information about where products should be located. This helps to spot problems before they emerge, allowing remedial action.
- **Tools for the business**: a business continuity tool, accessible to anyone in the business, that helps them to understand what business continuity is, how to think about it, and how to develop and test a business continuity plan. 'It means we can focus as a central team on the big things that really matter or the most important parts of the business.'
- **Intelligence**: GSOCs, open-source intelligence, generative AI products, use of AI-powered threat-intelligence tools to get ahead of unfolding events; use of an enterprise intelligence platform to log all intelligence and provide a cross-business view of risk.
- **Fraud**: use of an AI-powered card verification platform to reduce fraud and generate fewer false flags, thereby improving customer experience and generating a higher volume of sales; pooling data to spot precursor behaviours to get ahead of fraud before money is taken from customer accounts.
- **Duty of care**: use of geolocation tools to target support to staff in need; virtual travel platforms to facilitate targeted communications in the event of an incident.
- **Insider threat**: use of machine learning and natural language processing to reduce false positives when spotting suspicious precursor behaviour.

The Clarity Factory interviews with CSOs, 2023

In order to enhance their use of relevant new technologies, corporate security functions require support from the C-Suite to overcome four key challenges:

- **Legacy systems**: some corporate security functions have old legacy IT systems and technology budgets are quickly absorbed by updates.
- **Prioritisation**: some CSOs find their ambitions hampered because they are a lower priority for limited IT and product team resources. One CSO commented, 'We have such ambitious plans, but being able to access the resources internally has proven much more challenging than it should be. We tend not to be the priority because we're not revenue generating. We have mapped out 40 different internal and external data sources that we want to go into a data lake, but we can't get anyone to actually flood the lake with that data.'
- **Expertise**: some corporate security functions could progress further if they had technology, data and digital skills within the team; this could help them to better understand technology opportunities, get the most from suppliers, and build and test prototype systems to attract internal investment. Two-thirds (66%) of CSOs said that they don't have specialist technology skills, such as machine learning engineers, data scientists or product managers, within their teams.
- **Budget**: only one-fifth (22%) of corporate security functions have an innovation/R&D line item within their budget; the majority (68%) are required to submit a request for any innovation or R&D spend, which likely slows efforts.

A fit-for-purpose talent strategy

Effective CSOs recognise the need to assemble a team with the necessary skills, competencies and management experience:

- **New hard skills**: effective CSOs are beginning to invest in new skills and roles. Of the CSOs surveyed, 16% have data scientists on their team; 16% have software engineers, developers, or coders; 15% have agile coaches, technology product managers, or scrum masters; 7% have human factors, user experience, or user interface

designers; and 4% have machine learning engineers. They are also increasing emphasis on business skills, such as vendor and project management.

- **Skills that boost collaboration**: like the CSO, corporate security team members need skills that boost collaboration within the team and across the business, such as influencing, communication, and leadership.
- **Diversity of professional background**: effective CSOs recognise the benefits of government experience alongside the need for a more diverse range of backgrounds.
- **Diversity in the security leadership team**: effective CSOs recognise the 'diversity dividend': the contribution of diversity – especially within leadership – to innovation, productivity, better decision-making, and closer alignment with the business.[79] They track diversity data and use it as a management tool to support and challenge practices around recruitment, evaluation, pay reviews, and promotions. A majority of CSOs have leadership comprising fewer than 25% either women or ethnic minorities.
- **Career pathways**: a majority (69%) of security professionals under the age of 35 see corporate security as an attractive career option for young people, and effective CSOs recognise the importance of a clear and structured career pathway for their team. Younger professionals are looking for leadership development, new skills, training in products and tools, and business-related professional development.

> *69% of security professionals under the age of 35 see corporate security as an attractive career option for young people.*

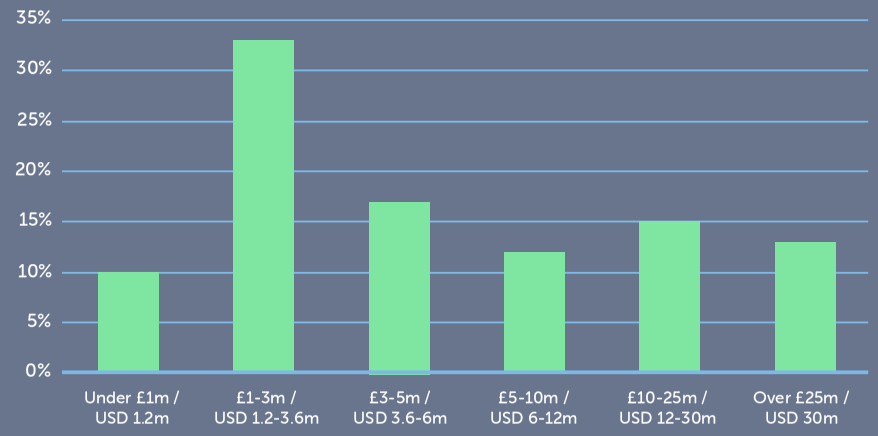
Adequate resourcing: budget and personnel

Effective CSOs secure the support of the C-Suite for adequate resource to provide excellence in core tasks and enable the function to contribute along the value chain. Budgets and headcounts vary considerably between companies, influenced by their respective risk profile, legacy, risk appetite, size, and overall financial position. The following data on budget and personnel is included for purely illustrative purposes.

Budget

Two-thirds (65%) of CSOs consider they have sufficient financial resource to deliver effective corporate security, and two-fifths (39%) expect their budget to grow over the next 2–3 years. Budget is considered the most important potential obstacle to the success of their function, cited by 44% of those surveyed (Figure 8). There was a wide range of corporate security budgets disclosed in our survey, from under £1 million to over £25 million, with the median corporate security budget (excluding guarding) coming in at £3–5 million (see Figure 14).

Figure 14
Corporate security budget, excluding guarding



Source: The Clarity Factory CSO survey, 2023

The framework outlined in this report will require additional funding for some companies. CSOs shared examples of successful advocacy to secure resourcing, which are outlined in Box 10.

Box 10
Examples of CSO advocacy for increased resources

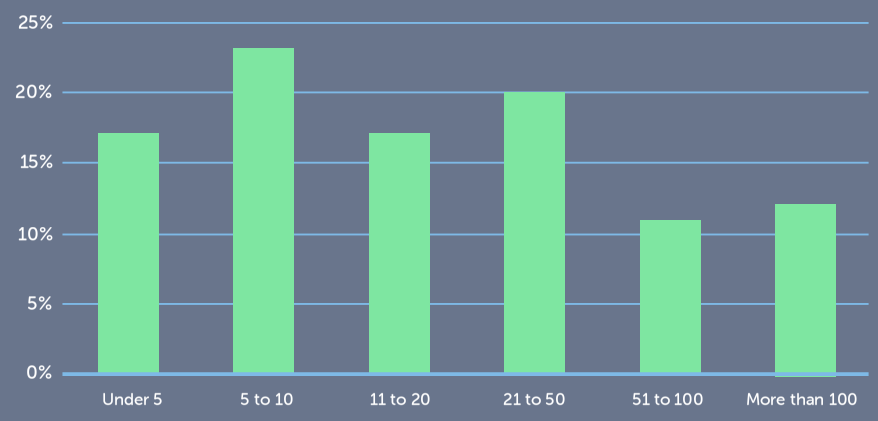
- **Pilot initiative**: a CSO demonstrated the value of due diligence by running a time limited exercise for a senior appointment, which uncovered information that would have been damaging had the appointment gone ahead. This created a proof of concept and the company has now invested in a full-scale due diligence programme.
- **Smart use of data and analytics**: in the face of staffing cuts across the business, one CSO used data and analytics to demonstrate under-staffing in some of his key roles. As a result, corporate security was the only function to not only avoid cuts, but receive additional head count: 'Feedback was extremely positive, that we'd applied data and objectivity as opposed to stating my judgement. Using data made it far more compelling and difficult to argue against.'
- **Self-financing to create proof of concept**: one corporate security function used its discretionary R&D budget to pilot an anti-fraud initiative, which demonstrated a reduction in losses. On the strength of these results, the function was granted 30 additional headcount and an investment of £1 million in technology to scale up.
- **Value-add beyond security**: one CSO demonstrated the value-add of a new investigations case management system for other functions: 'We made the business case, which stressed the benefits data privacy and regulatory support, as well as security. If I had just said we need it because it makes it easy for us, we wouldn't have got anywhere with it.'
- **Business-relevant ask**: one CSO within the pharmaceutical industry requested additional budget for anti-counterfeit measures and couched the ask in terms of patient safety, which is the most important issue for any company in this sector.
- **Culturally appropriate ask**: one CSO told us about a successful request to move the location of one of their country HQ offices within a medium-risk country: 'I played within the culture of the organisation rather than against it. We are a matrix organisation; if you follow the process, it takes forever and a day. If you go straight in at executive level and say, I need 15 minutes of your time, here is an issue, here is a solution, here's the decision I need you to make, it's done. What I learned was in issues of significance, do not allow process to constrain risk management. We had data to back it up, but my executives are not interested in walking through data, they want to know what insights I derive from the data and what decision I need them to make. Data is important, but understanding how to engage at board level for impact is more important.'

The Clarity Factory interviews with CSOs, 2023

Personnel

The number of full-time employees (FTE) or equivalent within corporate security functions varies considerably within our research data, from under 5 (17%) to more than 100 (12%), as shown in Figure 15. The median FTE headcount among CSOs surveyed was 11–20, and a majority (55%) said they anticipate headcount remaining static over the next 2–3 years. Personnel is considered to be one of the most important potential obstacles to the success of corporate security teams, cited by one-quarter (26%) of CSOs (Figure 8).

Figure 15
Full-time (FTE) headcount for corporate security, excluding guarding personnel



Source: The Clarity Factory CSO survey, 2023

Conclusion

"The measure of a powerful person is that their circle of influence is greater than their circle of control."

– AG Lafley, former CEO, Procter and Gamble

This report has demonstrated **corporate security's elevated contribution to business success** at a time when senior executives are increasingly required to lean into risk and opportunity to deliver growth.

Effective CSOs dedicate the majority of their function's time to achieving excellence within their core activities and enhance their value by additionally adopting responsibilities specific to their company's needs. By focusing on their circle of control they earn the trust and credibility to extend their circle of influence, enabling them to **contribute across the value chain** as well. They offer integration, insight, external networks, and crisis competency, among other things, which help to build operational resilience.

The vision for corporate security outlined in this report rests on five factors:

- A compelling narrative.
- The right kind of CSO.
- An innovation mindset across the function.
- A fit-for-purpose talent strategy.
- Adequate resourcing.

This report offers a practical guide for executives seeking best practice from corporate security. The model outlined will feel familiar to some companies and aspirational for others; there are different levels of maturity across the corporate security functions of multinational corporations.

Business leaders must decide how best to adapt the model to their company's specific needs, and resourcing will be influenced by risk profile and overall financial position.

Effective corporate security is a partnership between the C-Suite and the CSO, who must work together to ensure the function is well led and resourced, sits at the right level to influence, and, as a result, is able to realise the opportunities to contribute value beyond the boundaries of the function.

This is the business value of corporate security.

Appendices

Appendix 1: Methodology

The research for this report was conducted by Rachel Briggs OBE of The Clarity Factory, and included the following elements:

- **Literature review**: an extensive review of literature and data relating to the themes covered within the research.
- **Interviews with business leaders**: structured interviews with 16 business leaders from the following roles: CEO, COO, CFO, HR, marketing, business and country leaders, General Counsel, and CISO.
- **Interviews with CSOs**: structured interviews with 19 CSOs from the following sectors: banking, consulting, defence, energy, extractives, fast-moving consumer goods, manufacturing, media, pharmaceuticals, precious metals, and retail.
- **Expert interviews with a range of relevant professionals**: informal interviews with 20 experts across a range of relevant fields.
- **Survey of CSOs**: an anonymous survey was conducted, for which we received 102 responses, of which 72 were from respondents who self-identified as CSOs at multinational corporations. The CSO survey data quoted in this report refers to this sample of 72 CSO respondents.
- **Survey of security professionals under the age of 35**: an anonymous survey was conducted, for which we received 187 responses, of which 172 were from respondents who self-identified as professionals under the age of 35. The survey data presented relates only to responses from those self-identifying as being under the age of 35.

Appendix 2: Project Partners

This research is kindly supported by the following companies: AstraZeneca, Barclays, CRH, Holcim, ICF, Johnson Matthey, Proman AG, Shell, Sibylline, and Sky. The views expressed in this report are those of The Clarity Factory and do not necessarily reflect the views or positions of the companies who supported this research.

The following individuals from the partner companies acted as the project's Advisory Council, informing and shaping the research, providing feedback on emerging findings, and offering invaluable input on the final report: Trevor Rees, Alex Hawley, Mark Wolsey, Cédrick Moriggi, Gerald Golding, Steve Brown, James Richardson, Duncan Manning, Justin Crump, and Niall MacGinnis.

Appendix 3: Author Acknowledgements

I would like to express my sincere thanks to the companies who supported the research underpinning this report. They recognised the importance of independent research and provided help without any desire to influence the findings. They are: AstraZeneca, Barclays, CRH, Holcim, ICF, Johnson Matthey, Proman AG, Shell, Sibylline, and Sky.

A huge thank you to the representatives from those companies who formed the project's Advisory Council. They shared their knowledge, experience, and contacts, and dedicated significant amounts of time to review survey data and draft findings. The report is much improved for their input. They are: Trevor Rees, Alex Hawley, Mark Wolsey, Cédrick Moriggi, Gerald Golding, Steve Brown, James Richardson, Duncan Manning, Justin Crump, and Niall MacGinnis. In particular, I would like to highlight Mark Wolsey, who was the driving force behind making the project happen.

Most of the people I interviewed for this report did so on condition of anonymity, so I am unable to thank them individually. Needless to say, this research would not have been possible without their willingness to share their experience and time. Yet again, I was reminded that the security community is full of individuals of the highest calibre who collaborate for the collective good.

I would like to thank a number of individuals who contributed, whether through sharing ideas, reviewing my work, or assisting with logistics: Arian Avila, Jerry Brennan, Richard Brinson, Amy Buckley, Riccardo Cociani, Leo Collins, Eduardo Damm Bragan, Laura Davey, Kathy Lavinder, Edie Lipton, Tim McNulty, Manish Mehta, Carl Miller, Peter O'Neil, Chuck Randolph, Amy Reynolds, Jim Rudden, Catriona Scholes, Valeria Scuto, Liana Semchuk, and John Smith.

I would like to thank those people who have helped with the production and dissemination of this report: Tom Hampson (Reforma), Sophie Gillespie (Inkwell Communications & Design Studio), and Ayo Awokoya, Rob Blackhurst and David Hands (Apollo Strategic Communications).

Finally, I would like to thank three security industry membership organisations, which create space for benchmarking, thought leadership and connection. Their meetings help me to advance my thinking, and their members are a regular source of support and inspiration: The Risk and Security Management Forum (RSMF), ASIS International, and The International Security Management Association (ISMA).

All errors are, of course, my own.

Rachel Briggs OBE, 25 October 2023

Endnotes

1. Global Risks Perception Survey 2022–2023, World Economic Forum
2. 'The Trendline: Global political risk at highest level in five years', Jess Middleton, Maplecroft, 2 February 2023
3. Gartner says 57% of boards of directors are increasing their risk appetite into 2022', 2021
4. *Corporate Security*, PwC, 2022
5. *The Value Killer Revisited: A Risk Management Study*, Deloitte, 2014
6. 'We're in a polycrisis, and this is what it means', Carsten Brzeski, *ING*, 12 May 2023
7. 'As the world shifts, so should leaders', Nohria, 2022
8. *Corporate Security*, PwC, 2022
9. *Winning Today's Race While Running Tomorrow's*, PwC, 2023
10. *Empowering Diversity, Equity and Inclusion in Corporate Security*, Rachel Briggs OBE and Paul Sizemore, ASIS International, 2023
11. 'The Trendline: Global political risk at highest level in five years', Jess Middleton, Maplecroft, 2 February 2023
12. *Global Risks Perception Survey 2022–2023*, World Economic Forum
13. 'Designing high-performance jobs', Simons, 2005
14. *The Business of Resilience: Corporate Security for the 21st Century*, Rachel Briggs and Charlie Edwards, Demos, 2006
15. 'Iranian state "now biggest threat to UK": Home secretary's fears over spying links to gangs', Caroline Wheeler and Gabriel Pogrund, *The Times*, 6 August 2023
16. *Sibylline World Risk Register: Mid-Year Forecast 2023*, Sibylline, 2023
17. *The Trendline: Global political risk at highest level in five years*, Middleton, 2023
18. *Freedom in the World 2023: Marking 50 years in the Struggle for Democracy*, Freedom House, 2023
19. Global Risks Perception Survey 2022–2023, World Economic Forum
20. 'We're in a polycrisis, and this is what it means', Carsten Brzeski, *ING*, 12 May 2023
21. *The Global Risks Report 2023, 18th Edition, Insight Report*, World Economic Forum, 2023
22. A 'value killer loss' is defined as a share price decline of more than 20% in a one-month period relative to the MSCI Global 1000 Index in the same period.
23. *The Value Killer Revisited: A Risk Management Study*, Deloitte, 2014
24. *Winning Today's Race While Running Tomorrow's*, PwC, 2023
25. *Charting the Course through a Changing Governance Landscape: PwC's 2022 Annual Corporate Directors Survey*, PwC, 2022
26. 'As the world shifts, so should leaders', Nohria, 2022
27. *2022 Edelman Trust Barometer*, Edelman, 2022
28. 'Leadership in a politically charged age', Kteily and Finkel, 2022
29. 'There's a rumbling now': CEOs get into the business of tackling extremism', Andrew Edgecliffe-Johnson, *Financial Times*, 15 September 2023

30. 'Insider risk', Gates, 2021
31. 'Insider risk', Gates, 2021
32. *Winning Today's Race While Running Tomorrow's*, PwC, 2023
33. 'Funding digital transformation growth in 2022', Tomoko Yokoi, *Forbes*, 4 February 2022
34. 'The essential components of digital transformation', Tomas Chamorro-Premuzic, *Harvard Business Review*, 23 November 2021
35. *The data-powered enterprise: why organisations must strengthen their data mastery*, Cap Gemini, 2020
36. *Charting the Course through a Changing Governance Landscape*, PwC, 2022
37. *PwC Pulse Survey: Managing Business Risks*, PwC, 2022
38. *Strategic Transformation: Mastering Strategy Implementation in Transformative Times*, Brightline Project, Management Institute, 2020
39. *Post Truth: The New War on Truth and How to Fight Back*, Matthew D'Ancona, Ebury Press, 2017
40. *Weaponized Social Media: The New Brand Reputation Challenge*, Graphika, 2021
41. *Weaponized Social Media*, Graphika, 2021
42. Examples taken from: 'The rise of disinformation and corporate risk', Michael Gipps, *International Security Journal*, 14 July 2021
43. *Weaponized Social Media*, Graphika, 2021
44. Examples taken from: 'The rise of disinformation and corporate risk', Gipps, 2021
45. Examples taken from: 'The rise of disinformation and corporate risk', Gipps, 2021
46. 'Gartner says 57% of boards of directors are increasing their risk appetite into 2022', 2021
47. Gartner says 57% of boards of directors are increasing their risk appetite into 2022', 2021
48. Gartner says 57% of boards of directors are increasing their risk appetite into 2022', 2021
49. *Strengthening Enterprise Risk Management: A Key to Success in a Volatile Environment*, Auditboard, 19 May 2020
50. *Winning Today's Race While Running Tomorrow's*, PwC, 2023
51. 'As the world shifts, so should leaders', Nohria, 2022
52. *Winning Today's Race While Running Tomorrow's*, PwC, 2023
53. *Corporate Security*, PwC, 2022
54. *Winning Today's Race While Running Tomorrow's*, PwC, 2023
55. *Black swans, gray rhinos, and silver linings: Anticipating geopolitics risks (and openings)*, Grant, Haider, and Raufuss, 2023
56. *Winning Today's Race While Running Tomorrow's*, PwC, 2023
57. *Black swans, gray rhinos, and silver linings: Anticipating geopolitics risks (and openings)*, Grant, Haider, and Raufuss, 2023
58. 'Crossing the river by feeling the stones', interview with W. Brian Arthur, *McKinsey Quarterly*, 1 August 2023
59. 'The C-Suite skills that matter most', Raffaella Sadun, Joseph Fuller, Stephen Hansen, and PJ Neal, *Harvard Business Review*, July–August 2022
60. *Corporate Security*, PwC, 2022
61. Drawing on *the 7 Habits of Highly Effective People*, Covey, 2020
62. *The Power of Trust*, Sucher and Gupta, 2021
63. *The Influence of Security Risk Management: Understanding Security's Corporate Sphere of Risk Influence*, ASIS Foundation, 2023
64. 'Designing high-performance jobs', Simons, 2005
65. *The Business of Resilience*, Briggs and Edwards, 2006

66. The 'value chain' refers to the chain of activities that together result in the creation of value for an organisation. It comprises primary activities: logistics, operations, marketing and sales, and services; and support activities: infrastructure (accounting, legal, finance, control, public relations, quality assurance and general management), technical development, human resources and procurement.
67. *Corporate Security*, PwC, 2022
68. *Corporate Security*, PwC, 2022
69. 'How corporate intelligence teams help businesses manage risk', Paul R Kolbe and Maria Robson Morrow, *Harvard Business Review*, 4 January 2022
70. 'How corporate intelligence teams help businesses manage risk', Kolbe and Robson Morrow, 2022
71. 'How corporate intelligence teams help businesses manage risk', Kolbe and Robson Morrow, 2022
72. *Winning Today's Race While Running Tomorrow's*, PwC, 2023
73. *Winning Today's Race While Running Tomorrow's*, PwC, 2023
74. *The Power of Trust*, Sucher and Gupta, 2021, p. 8
75. 'As the world shifts, so should leaders', Nohria, 2022
76. *Corporate Security*, PwC, 2022
77. *Rebel Ideas: The Power of Thinking Differently*, Matthew Syed, John Murray Publishers, 2021
78. *Empowering Diversity, Equity and Inclusion in Corporate Security*, Briggs and Sizemore, 2023
79. *Empowering Diversity, Equity and Inclusion in Corporate Security*, Briggs and Sizemore, 2023

About The Clarity Factory

The Clarity Factory is an engine room generating knowledge, insights and practical solutions for our increasingly complex world. We conduct research, produce thought leadership, and consult with clients to help them solve knotty problems and support them as they strive for continual improvement and innovation. We specialise in corporate security, cyber security, and resilience. The Clarity Factory creates clarity from complexity – to enable our clients to thrive.

Ways you can work with The Clarity Factory

- Sponsor research to drive insight and innovation in your industry.
- Commission thought leadership to promote new ideas and position your brand.
- Commission a benchmarking study to understand how you compare with your peers.
- Book Rachel Briggs to deliver a keynote at your event.
- Ask us to deliver training and capacity building.

Sign up to our monthly newsletter

https://www.clarityfactory.com/subscribe

Get in touch

info@clarityfactory.com

Other reports by Rachel Briggs

- *Empowering Diversity, Equity and Inclusion in Corporate Security*, with Paul Sizemore, ASIS International, 2023
- *Cyber Security Leadership is Broken: Here's how to fix it*, with Richard Brinson, Savanti, 2022
- *Effective Board Governance of Cyber Security: A source of competitive advantage*, with Richard Brinson, Savanti, 2023
- *The Business of Resilience*, with Charlie Edwards, Demos, 2006

the clarity factory

Today's global business environment presents challenges to multinational corporations: geopolitics, volatility, sophisticated and persistent security risks, pressure to respond to social and political issues, and risks that are increasingly interconnected. Companies are responding by increasing their risk appetite, shifting locations and supply chains, increasing scenario planning, bolstering crisis management capability, and seeking a different kind of leader.

This report seeks to understand what these trends mean for the corporate security function: its value proposition, leadership, talent, areas of responsibility, business alignment, and changing C-Suite needs.

As leaders grapple with the challenges outlined in this report, the importance of corporate security is heightened; its opportunity to influence made greater.

Senior leaders who support their CSOs in pursuing the vision outlined in this report will realise the business value of corporate security.

AstraZeneca BARCLAYS CRH HOLCIM ICF

JM Johnson Matthey Inspiring science, enhancing life PROMAN SIBYLLINE sky

ISBN 978-1-7384176-0-5

www.clarityfactory.com