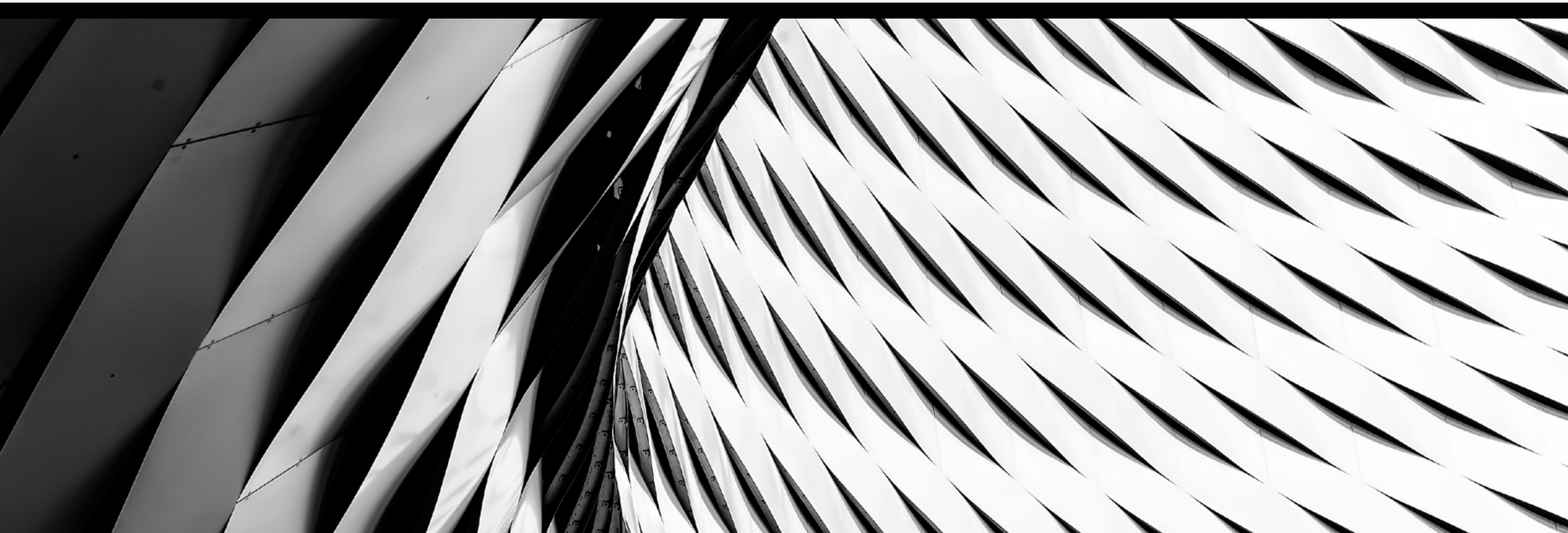
# Connected Corporate Security

HOW TO MANAGE THREATS AND RISKS WITH A UNIFIED MODEL



02 Introduction

04 Today's Global Business Operating Environment Calls for Connected Corporate Security

06 Effective Corporate Security Functions Connect **Within the Function**

08 Effective Corporate Security Functions Connect **Across the Business**

10 Effective Corporate Security Functions Connect **Between the Company and External Networks**

11 Connected Corporate Security in Practice

14 Achieving Connected Corporate Security

16 Conclusion

This report was written by Rachel Briggs OBE, Co-Founder and CEO of The Clarity Factory. It draws on thought leadership and latest data from the security industry, including two previous Clarity Factory reports, *The Business Value of Corporate Security* (kindly supported by AstraZeneca, Barclays, CRH, Holcim, ICF, Johnson Matthey, Proman AG, Shell, Sibylline and Sky) and *Empowering Diversity, Equity and Inclusion in Corporate Security* (kindly supported by the ASIS Foundation), as well as Rachel's previous co-authored report, *The Business of Resilience* (Demos). It also references a number of other seminal reports and surveys and links to the references used throughout.

*Drawing on industry thought leadership and the latest data, the views expressed are those of The Clarity Factory and do not necessarily reflect those of Ontic.*

# Today's global business operating environment is undoubtedly one of the most challenging companies have faced for several decades.

It is characterized by volatility, geopolitical divisions, heightened security risks, and economic fluctuations. Business leaders are asking functions across the business to do more with less, use technology to improve effectiveness and drive down costs, and come to terms with a range of medium- to long-term issues that will have a substantial impact on their business models, notably climate change and developments in AI.

The risk environment is changing. Risks are increasingly interconnected and often sit between or across several functions. Longer-term trends, such as climate change and AI, are not housed within any one function but pose significant challenges that companies must find smart ways to address.

## Against this backdrop, effective corporate security functions master connectivity on three levels: **within, across, and between.**

● **WITHIN THE CORPORATE SECURITY FUNCTION**
PAGE 6

Team members collaborate within the function, work on consolidated technology platforms, and seamlessly share data to generate better insights to manage complex and heightened security risks.

■ **ACROSS THE COMPANY**
PAGE 8

Corporate security functions partner with colleagues outside the security team, sharing data and fostering collaborative working arrangements to help the company deal with interconnected risks.

◆ **BETWEEN THE COMPANY AND EXTERNAL NETWORKS**
PAGE 10

Corporate security professionals leverage their external network to benefit not just the corporate security team but the corporation at large. Connections with peers, stakeholders, local communities, and government agencies bring insight into processes like M&A and ESG and act as an early warning system in the face of fast-moving geopolitical events.

Some corporate security functions are well on their way to achieving the type of connectivity outlined in this report, but many are near the start of their journey. Within this report is a wealth of practical examples to help corporate security professionals at all levels of seniority enhance their own connectedness and that of their function. Corporate security is constituted in various ways, depending on the sector, risk profile, and legacy. This report focuses on the tasks widely considered to be core functional tasks.

In a world where threats are rising and becoming more complex, connected corporate security offers a model for managing and mitigating threats that is fit for purpose in today's global business environment. Together, we are stronger.

## KEY TAKEAWAYS

- Today's global business operating environment is characterized by instability, volatility, higher security risks, and risks that are increasingly interconnected.
- To avoid silos, companies are looking for a more unified view of risk and a way to manage hazards that fall across and between functions.
- The corporate security function's inherent structure and delivery mechanisms position it especially well to act as a connector within the organization.
- Effective corporate security functions connect on three levels:

  ● They connect **within the corporate security team**, ensuring systems, processes, tools, and technology are not siloed, which generates enhanced data insights where the whole is worth more than the sum of its parts.

  ■ They connect **across the business**, enabling the company to manage interconnected risks and those that don't fit neatly within one function.

  ◆ They connect **between the company and a wealth of external stakeholders** — including industry peers, government agencies, and local and regional contacts around the world — to help business leaders make sense of the more complex global business operating environment.

- Realizing connectivity on these three levels relies on the combined efforts of all members of the corporate security team in the following areas: talent, technology, business partnerships, and external networks.
- Corporate security leadership teams should foster collaborative and inclusive leadership, C-suite buy-in, and metrics that encourage and motivate connectedness.

# Today's Global Business Operating Environment Calls for Connected Corporate Security

The current operating environment for companies is one of the most challenging they have faced for several decades. Six key trends are critical to the corporate security function:

01 **Geopolitics** is impacting a range of things, such as supply chains, corporate locations, and executive travel. A majority of CSOs (51%) ranked geopolitics as one of the top three security risks facing their organization. Almost half of CEOs are considering adjusting their organization's locations and supply chains within the next 12 months to mitigate against exposure to geopolitical conflict, and in another study, three-quarters (73%) cited supply chain security as one of the main challenges facing corporate security in the next five years.

02 Business leaders recognize that **volatility** characterizes their operating environment.

03 **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, and resource scarcity.

04 A majority of CSOs said the **security risks** facing their companies had risen over the past 2–3 years, and another survey found that 83% of CSOs expect all types of physical security threats to increase over the next year As Dave Komendat, former Chief Security Officer for the Boeing Company, commented, "Security threats are more dynamic, convergent, and complicated than they have ever been."

05 Many of the **risks corporations face are increasingly interconnected**, such as cybersecurity and corporate security or the links between managing ESG and reputational risks, and require functions to work together to avoid blind spots and silos.

06 They are also grappling with a number of **medium- to long-term risks that don't fit neatly within one function**, such as AI and generative AI, climate risk, the growth of IP theft, including by state-sponsored actors, and disinformation. All functions need to play their part in helping the company understand these trends, manage the associated risks, and realize opportunities. For corporate security, that might include providing intelligence, identifying threat trends, and enabling security risk management. This requires corporate security functions to work at different speeds, juggling immediate firefighting and crisis response with longer-term, slower-burn imperatives.

As a result of these trends, business leaders are looking to all risk-related functions (including corporate security, cybersecurity, legal, compliance, external relations, and facilities management) to collaborate and share information to create a more unified view of risk.

**Corporate security is a function with higher-than-average levels of connectivity, described by some business leaders as "corporate glue."**

This is due to a number of reasons:

- Corporate security is often **organized geographically**, which means it has many more touch-points across the company than other functions.
- Corporate security is delivered through the everyday actions of employees across the company, **so strong relationships are baked into the work of the function.**
- Corporate security often plays a leading role in **crisis management**, which brings visibility, reach, and trust to the function.

## CSOs ON SECURITY RISKS

51%

**ranked geopolitics** as one of **the top three security risks** facing their organization

*The Clarity Factory*

73%

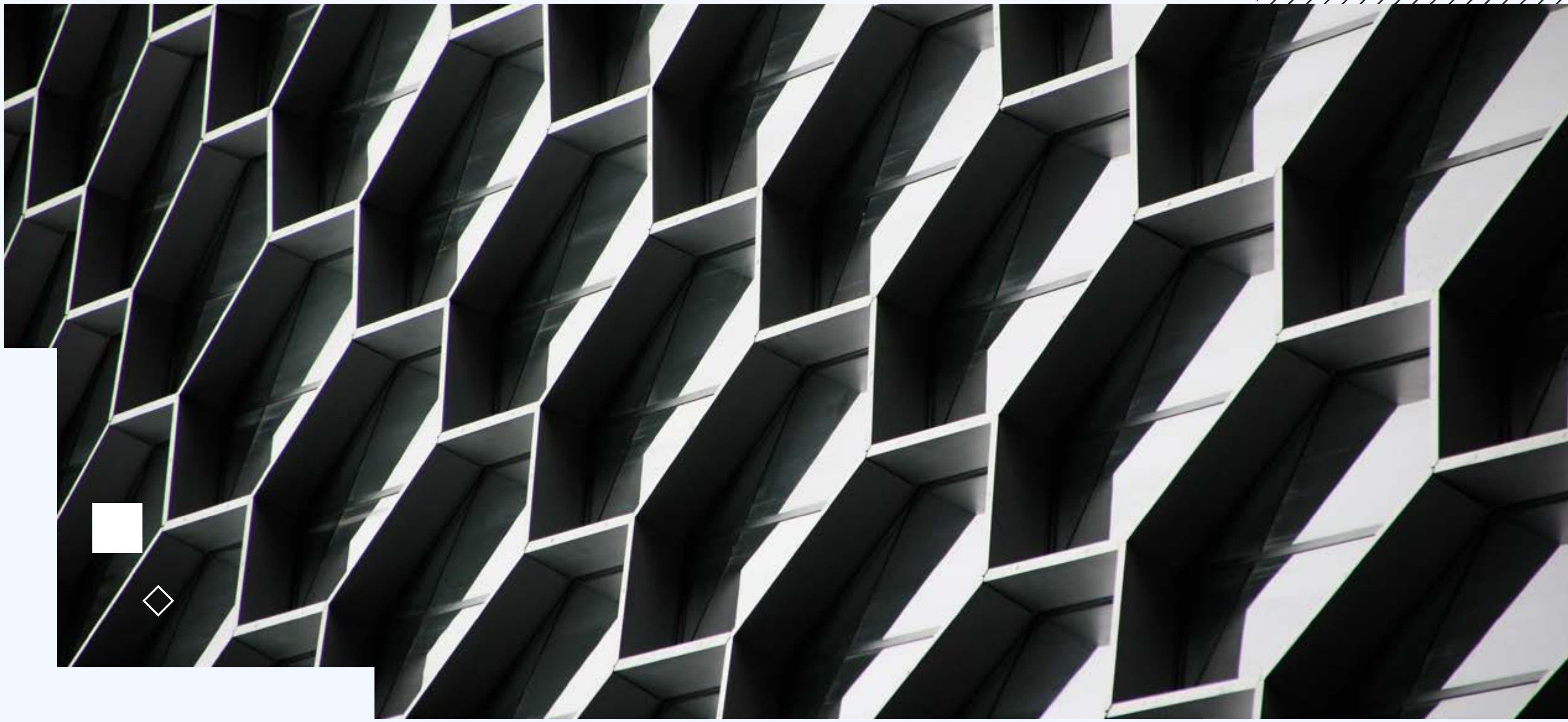
cited **supply chain security as one of the main challenges** facing corporate security

*PWC*

83%

expect all types of **physical security threats to increase** over the next year

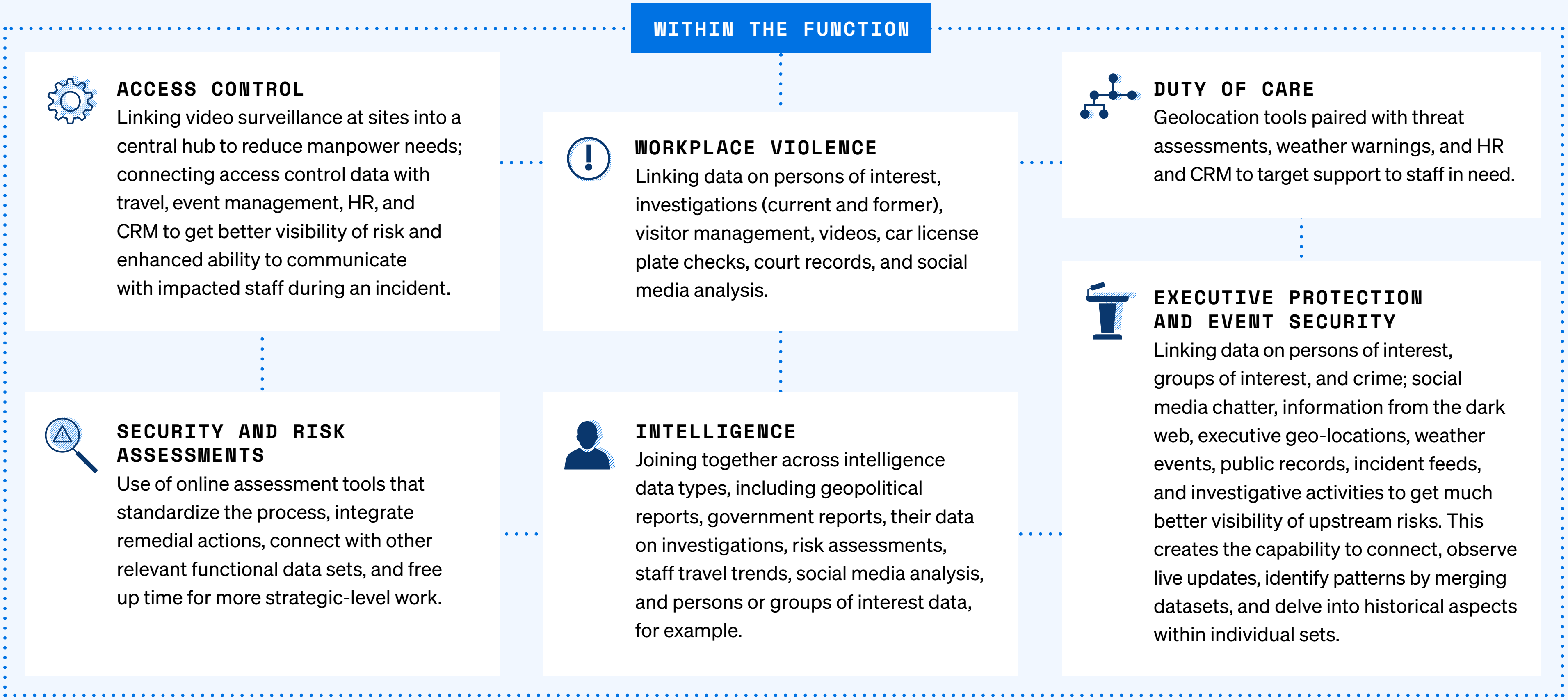
*G4S*



# Effective Corporate Security Functions Connect Within the Function

Research shows that a corporation's ability to harness its data dramatically improves performance: Organizations deemed to be 'data masters' have 70% higher revenue per employee, 245% higher fixed asset turnover, and 22% higher profitability.

Similarly, corporate security functions that connect and integrate their data derived from various security tasks — intelligence, investigations, security operations (including GSOC), and executive protection, for example — will likely improve productivity, effectiveness, decision-making, and lower costs. Corporate security functions can connect within in a number of ways:



WITHIN THE FUNCTION

**ACCESS CONTROL**
Linking video surveillance at sites into a central hub to reduce manpower needs; connecting access control data with travel, event management, HR, and CRM to get better visibility of risk and enhanced ability to communicate with impacted staff during an incident.

**WORKPLACE VIOLENCE**
Linking data on persons of interest, investigations (current and former), visitor management, videos, car license plate checks, court records, and social media analysis.

**DUTY OF CARE**
Geolocation tools paired with threat assessments, weather warnings, and HR and CRM to target support to staff in need.

**SECURITY AND RISK ASSESSMENTS**
Use of online assessment tools that standardize the process, integrate remedial actions, connect with other relevant functional data sets, and free up time for more strategic-level work.

**INTELLIGENCE**
Joining together across intelligence data types, including geopolitical reports, government reports, their data on investigations, risk assessments, staff travel trends, social media analysis, and persons or groups of interest data, for example.

**EXECUTIVE PROTECTION AND EVENT SECURITY**
Linking data on persons of interest, groups of interest, and crime; social media chatter, information from the dark web, executive geo-locations, weather events, public records, incident feeds, and investigative activities to get much better visibility of upstream risks. This creates the capability to connect, observe live updates, identify patterns by merging datasets, and delve into historical aspects within individual sets.

Achieving connectivity within the function at scale is best delivered through technology, and research shows that the use of technology can improve overall performance. Companies that have already implemented modern technology are much more confident in their overall security operations. For those with basic technology use, the average confidence level is 63%, compared to 69% for those who are advanced and 74% for those deemed cutting-edge. The vast majority of CSOs (90%) said technology improves the overall effectiveness of security operations, enabling security staff to be more productive and efficient, and around the same proportion (88%) recognize that technology is changing the skills required for security professionals.

Presently, many corporate security functions lack technology skills, budget, and know-how. As Dave Komendat put it, "With few exceptions, the security community has been behind the curve in its use and implementation of new technologies." Two-thirds of CSOs (66%) surveyed by The Clarity Factory had no technology-related skills within their teams. This is beginning to change; in another survey, 85% of CSOs said they think a strong understanding of technology will be very important in the next five years, and 55% said introducing new technology will be their priority over the next 12 months.

## CSOs ON TECHNOLOGY

90%

said **technology improves** the overall effectiveness of **security operations**

*G4S*

88%

recognize that **technology is changing the skills required** for security professionals

*G4S*

66%

had **no technology-related skills** within their teams

*The Clarity Factory*

85%

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

*G4S*

55%

said introducing **new technology will be their priority** over the next 12 months

*G4S*

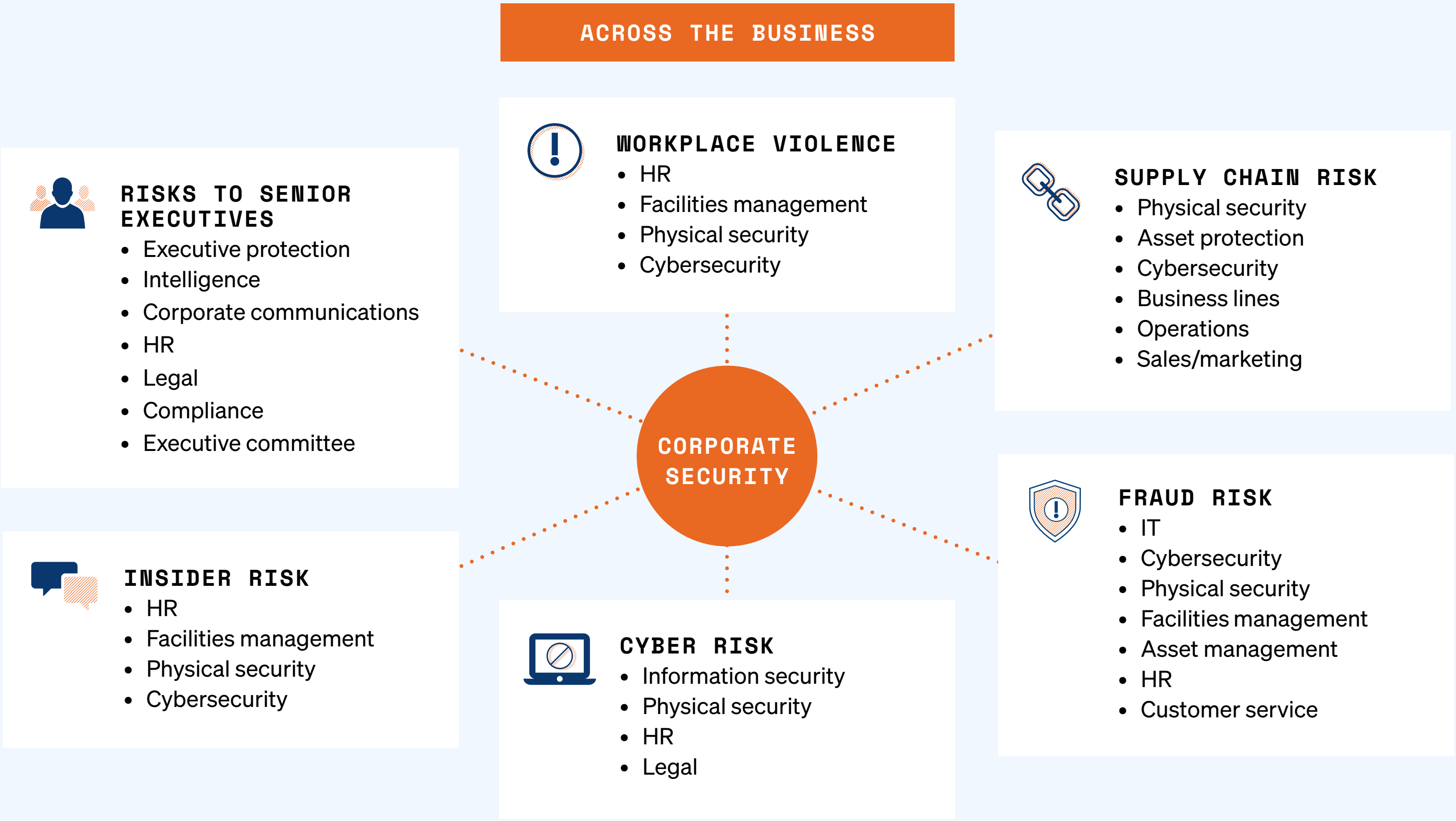
> "With few exceptions, the security community has been behind the curve in its use and implementation of new technologies."

**DAVE KOMENDAT**
Former Chief Security Officer for the Boeing Company

# Effective Corporate Security Functions Connect Across the Business

In managing and mitigating interconnected risks, corporate security is required to collaborate with risk functions across the business to avoid silos and blind spots.

The examples below highlight the functions that corporate security needs to collaborate with across the business in relation to a range of different risks:



ACROSS THE BUSINESS

CORPORATE SECURITY

### RISKS TO SENIOR EXECUTIVES

- Executive protection
- Intelligence
- Corporate communications
- HR
- Legal
- Compliance
- Executive committee

### WORKPLACE VIOLENCE

- HR
- Facilities management
- Physical security
- Cybersecurity

### SUPPLY CHAIN RISK

- Physical security
- Asset protection
- Cybersecurity
- Business lines
- Operations
- Sales/marketing

### INSIDER RISK

- HR
- Facilities management
- Physical security
- Cybersecurity

### CYBER RISK

- Information security
- Physical security
- HR
- Legal

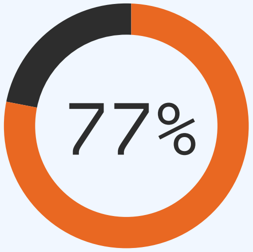
### FRAUD RISK

- IT
- Cybersecurity
- Physical security
- Facilities management
- Asset management
- HR
- Customer service

While informal collaboration can be beneficial, formal partnerships are critical to corporate security's connectivity across the business and can take a number of forms:

### INTEGRATION INTO THE ENTERPRISE RISK MANAGEMENT (ERM) FRAMEWORK

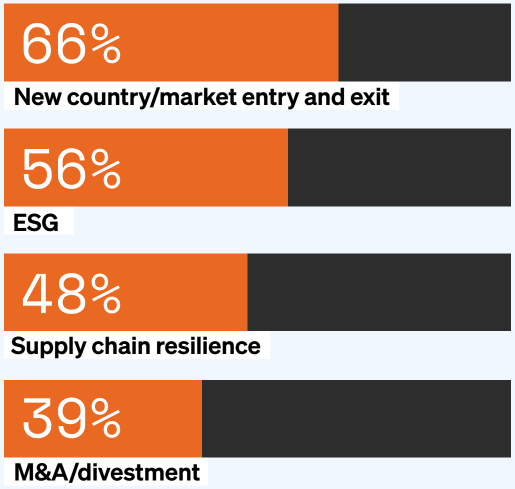
Some corporate security functions own a larger part of operational risk, sit on risk or resilience boards, are part of their company's ERM framework, report to the board's risk-audit committee (77% of CSOs), or have other risk leaders serve on the corporate security leadership team. There are different levels of maturity across corporate security functions in terms of their influence within the risk management sphere.



of CSOs report to **the board's risk-audit committee**

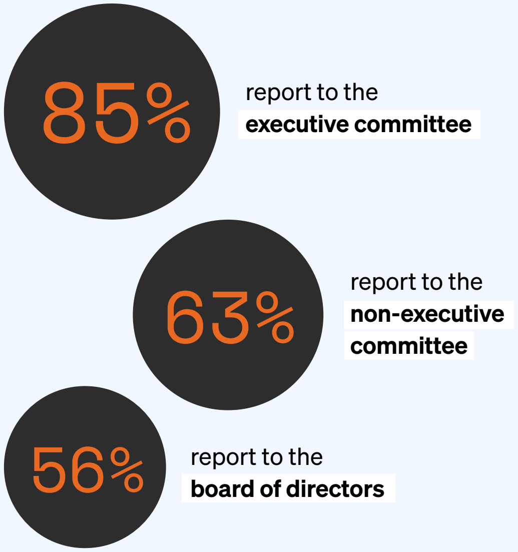
### CONTRIBUTIONS ALONG THE VALUE CHAIN

Corporate security functions contribute to a range of activities along the value chain: new country/market entry and exit (66% are involved), ESG (56%), supply chain resilience (48%), and M&A/divestment (39%).



### GOVERNANCE

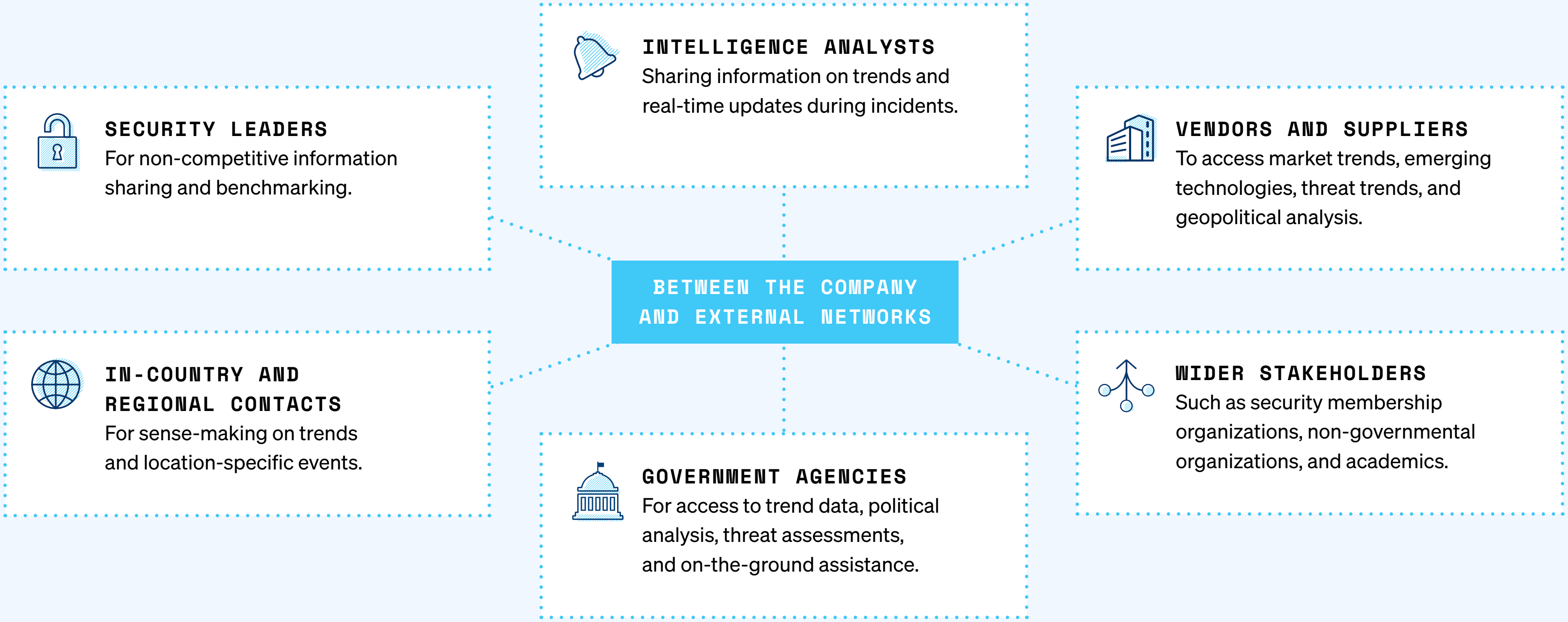
CSOs report into key governance forums: 85% report to the executive committee, 63% to non-executive directors, and 56% report to the board of directors.



Cross-company collaboration is enhanced by the smart use of shared technology platforms and professionals with the qualities, skills, and attributes like communication and soft skills to be effective partners and collaborators across the business.

# Effective Corporate Security Functions Connect Between the Company and External Networks

In a volatile world, where corporations are expected to take a stance on social and political issues and are held accountable for what happens beyond the boundaries of their business, and where mis- and disinformation are rife, a corporate security professional's external network is not only essential in helping them to do their own job, it can also add tremendous value to the business as a whole. These networks are especially helpful in relation to ESG, climate risks, regulation, M&A, community relations, political risk, and new market entry and exit. Corporate security functions offer the business access to a range of external networks:



**INTELLIGENCE ANALYSTS**
Sharing information on trends and real-time updates during incidents.

**SECURITY LEADERS**
For non-competitive information sharing and benchmarking.

**VENDORS AND SUPPLIERS**
To access market trends, emerging technologies, threat trends, and geopolitical analysis.

**BETWEEN THE COMPANY AND EXTERNAL NETWORKS**

**IN-COUNTRY AND REGIONAL CONTACTS**
For sense-making on trends and location-specific events.

**WIDER STAKEHOLDERS**
Such as security membership organizations, non-governmental organizations, and academics.

**GOVERNMENT AGENCIES**
For access to trend data, political analysis, threat assessments, and on-the-ground assistance.

# Connected Corporate Security in Practice

Effective corporate security functions connect on all three levels — within, across, and between — to provide comprehensive security coverage to their companies and significant contributions that help to create a unified view of risk. This can be seen in the three examples below, drawn from Clarity Factory interviews with CSOs.

## Intelligence

### SITUATION

- 52% of C-suite executives surveyed by PwC said they would like more security intelligence skills within their corporate security function.
- Corporate security accounts for 23% of all corporate intelligence (the remainder is generated by other parts of the business), but only 49% of corporate security functions collaborate with business intelligence analysts elsewhere within their organization.
- In the current global business operating environment, insight is critical for effective and timely decision-making, meaning there is an imperative to join up intelligence across the business.

### SOLUTION

- A large multinational company has consolidated all business intelligence within the corporate security function, incorporating traditional security intelligence alongside that normally generated by other parts of the business. It is now the central repository and engine room for all business intelligence.
- The CSO saw an opportunity to use security intelligence for commercial benefit. As the business saw the value-add of this intelligence, demand grew, and the entire business intelligence process was brought into the corporate security function over several years.
- As a result of its ownership of business intelligence, the corporate security function's involvement is formally mandated as part of various business processes, such as M&A, new business, and new country/market entry and exit.

### OUTCOME

- Tailored insight on business partners and reputational risk.
- Higher quality products.
- Cost savings on external vendors.
- Efficiency gains by centralizing.
- The corporate security function is involved in activities along the value chain much earlier, including business development and M&A.

CFO (NOT THE CASE STUDY COMPANY)

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

## Investigations and Supply Chain

### SITUATION

- 58% of corporate security functions are accountable or responsible for investigations.
- A minority (37%) of corporate security functions are accountable or responsible for supply chain security, and 48% are involved in supply chain resilience, but a sizeable majority (73%) of CEOs cited supply chain security as one of the main challenges facing corporate security in the next five years and 46% have changed or expect to change supply chains as a result of geopolitics.

### SOLUTION

- A multinational corporation uses a data-driven software platform to improve its investigations and enhance the security of supply chains.
- The platform integrates a wide range of data: loss cases for specific locations, historical data from investigations, known entities and persons of interest, raw material data, supply chain information, customs information, and sales and marketing data regarding anticipated and actual delivery of goods.
- New insights generated enable the function to de-risk the product at each step in the chain, meaning they are more able to anticipate problems rather than wait for something to go wrong at the end of the supply chain.

### OUTCOME

- The company anticipates problems further up the supply chain.
- There is a seamless integration of intelligence and investigations data to enable risk decision-making.
- Investigators connect a wider range of data sources.
- It is easier to spot emerging trends.
- Due to its success, the function seeks to expand the platform's use to physical and personnel security.

### CORPORATE SECURITY FUNCTIONS

58%

are accountable or **responsible for investigations**

37%

are accountable or **responsible for supply chain security**

48%

are **involved in supply chain resilience**

## Extreme Weather Events

### SITUATION

- Extreme weather events are an increased risk for many companies, and climate risks dominate the top-ranked risks for CEOs over 2-year and 10-year time horizons.
- 14% of CSOs ranked extreme weather/ environmental events as one of the top three security risks impacting their company, and two-thirds (67%) said the risk to their company has increased in the last 2–3 years.

### SOLUTION

- A large multinational corporation used a geo-intelligence platform to dramatically change its response to a hurricane event.
- The platform brought together multiple data sources: evacuation areas, staff home locations, company building locations, supply chain, and changing weather patterns.
- The data indicated the hurricane's impact would be on staff homes rather than company locations and supply chain.
- As a result of this insight, the CSO suggested a strategy to push support to staff rather than wait for them to log incoming requests for help. The company surged resources to designated locations: HR colleagues who could cut checks for staff in need, truckloads of merchandise and emergency supplies, fuel vendors, and mobile shower units.
- The CSO described it as 'a pivotal moment', saying, "If we hadn't built out a platform and pulled all our assets into one pane of glass, we would not have had the same response. We would have been so far behind the game."

### OUTCOME

- Of the 10,000 impacted people messaged via the platform, 99.7% responded within 72 hours.
- The company was able to resume operations faster than its competitors.
- It achieved timely and targeted delivery of assistance for staff and their families.
- It spent less because it was ahead of the problem rather than responding after the event.
- Their approach generated a positive impact on staff morale and turnover.

**THE CSO OF THE GEO-INTELLIGENCE PLATFORM:**

"It makes visible something that otherwise is invisible. It doesn't matter how many people you have, the human brain simply cannot pull all of that data together before things have changed and it's not relevant anymore… It's eye-opening what it's done for us in terms of efficiency and decision-making. Our ability to analyze the impact to our company of specific events — it now happens within minutes, not hours."

# Achieving Connected Corporate Security

Connected corporate security functions deliver greater value for their company, both in terms of enhanced team performance and increased contribution across the business. Achieving connected corporate security rests on a strategy delivered by wall team members that is underpinned by:

## Talent

All team members involved in recruitment, training, and talent development should prioritize skills that are critical for connection: collaboration, communication, social skills, stakeholder management, project and vendor management, technology, and data analysis.

Corporate security functions must recruit not just for technical specialisms, such as investigations or intelligence, but also select candidates with the right competencies to connect within, across, and between.

Diversity of thought, perspective, and experience is especially important in achieving connectedness across the business, so team members should ensure talent strategies include diversity, equity, and inclusion. Teams that lean into diversity, equity, and inclusion also innately harness critical thinking with diverse thought processes — avoiding bias or group think.

Corporate security functions need the technology skills that can amplify connectivity, such as data scientists, software engineers, agile professionals, experts in human factors, and machine learning engineers. Presently, only one-third of functions have team members with these types of skills.

Corporate security team members can help to raise awareness and comfort levels in using technology among colleagues to drive an innovation mindset within the function.

## Technology

The effectiveness of connected corporate security is amplified by technology-driven data-sharing systems that enable data sharing and collaboration. The use of SaaS tools has proliferated across corporations as CIOs rationalize and consolidate these tools. Corporate security functions also need to be part of this change process.

Corporate security team members should look for smart ways to use technology to drive improvements in their own work and create better and more systematic opportunities for collaboration at scale.

Given the technology skills gap in most corporate security functions, the technology strategy must align closely with the talent plan.

## Partnerships

While the formation of formal partnerships normally rests with the function's leadership, there are opportunities for all team members to foster and promote collaboration through how they interact with colleagues across the business.

A culture of connectedness starts within the function, and corporate security team members should look for ways to collaborate with one another, including across task areas and geographical regions.

## External networks

Professional networks not only help security professionals get the job done, they also offer insight to colleagues across the business.

Corporate security team members should actively seek opportunities to leverage their networks for the advantage of colleagues beyond their function by providing valuable insights, intelligence, and established connections.

Corporate security team members should invest in their own network development, including through membership organizations, online forums, and location-based networks.

Members of the corporate security function leadership team have added responsibilities in building a culture of connected security. They can contribute in the following ways:

## Leadership

Connected corporate security is led by Heads of Security and their deputies who are comfortable with collaboration, delegation, and an open leadership style. In dynamic and evolving settings, adaptability is crucial, and a strict team hierarchy can hinder the flow of valuable ideas and critical information to decision-makers, leading to innovation roadblocks. Leaders who embrace openness and inclusivity encourage collaboration, empowering team members to forge productive connections with external partners.

Corporate security leaders should engage in their professional development to enhance their ability to act as open leaders and effectively delegate throughout the function.

Corporate security leaders should ensure team members are evaluated on their collaboration and partnership performance alongside other metrics.

Corporate security leaders should build a talent strategy that can deliver connected corporate security by bringing in new technology skills, upskilling existing team members, recruiting with collaboration in mind, and investing in appropriate professional development.

## C-Suite Buy-In

Corporate security functions can only execute the strategy detailed in this report if they secure support from decision-makers, including an endorsement for their place in crucial processes and forums within the organization's space.

Corporate security leaders should develop a clear and compelling narrative about the value the function can add and ensure it aligns with how their company articulates risk in its 10-K or annual report.

## Metrics That Matter

Corporate security leaders should incorporate metrics that measure collaboration and its benefits and work with partners across the business to develop and measure them. What is measured is managed.

# Conclusion

In today's global business operating environment, connectivity is essential for the success of any function. Corporate security professionals have always been natural connectors outside the company, but those who can master connectivity within the function and across the business will have heightened influence and impact across their companies.

Connected corporate security relies on intentional strategies incorporating technology, talent, and partnerships that involve all members of the function, along with strong and inclusive leadership and C-suite buy-in.

Today's operating environment is challenging. Corporate security functions are called upon not just to deliver effective security but to connect within, across, and between to deliver value across the whole company.

**Connected security is not only desirable — it is essential to the future success of the function and the business.**