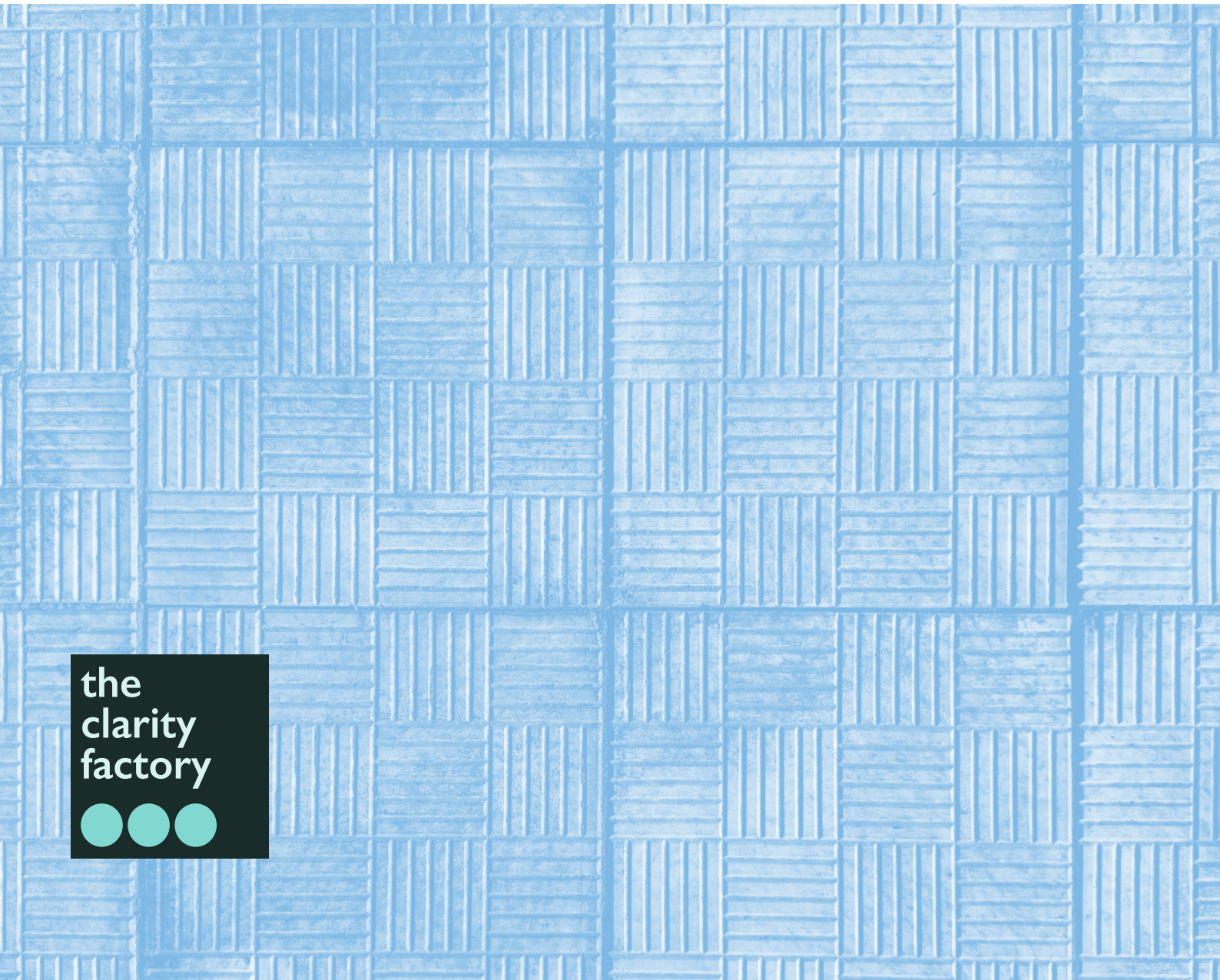
June 2025

Rachel Briggs OBE

Holistic Security

How physical and cyber security can join forces to strengthen operational resilience



the clarity factory

Partners
This research is kindly supported by partners, including Barclays, BP, Johnson Matthey and Scentre Group. The views experessed in this report are those of The Clarity Factory and do not necessarily reflect the views or positions of the companies who supported the work.

The following individuals 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: Alex Hawley, Derek Porter, Steve Brown, Matt Sinden and John Yates.

ISBN: 978-1-7384176-1-2

Contents

Clarity Up Front

A national museum suffers an IT outage after a terminated technology contractor gains access to an unauthorised area of the building and turns off the IT systems. Cyber defences are of limited value when the server-room door is left open.

A CEO travels to a high-risk country. The physical security team provides her with armed guards. Cyber security is not consulted, and the geolocation functionality on her laptop is left on. A criminal group targeting the company's IP tracks her movements and steals her laptop.

A telecoms company discovers an insider has been providing a nation-state actor with access to the company's systems. The employee went undetected for two years because the physical security team does not have access to cyber data on staff network activity. The tell-tale signs of unusual logins and declassification of sensitive documents were missed.

Major multinationals are operating in a global business environment characterised by elevated and interconnected security risks.

From cyber espionage and intellectual property theft to fraud, threats to senior executives and deep fakes, criminals, terrorists and nation states use the full spectrum of methods to target simultaneously across digital and physical domains.

A siloed approach in the face of joined-up security threats leaves companies exposed.

For twenty years, the proposed solution was convergence, whereby physical and cyber security merge into a single function. In theory, this makes sense. In practice, only 15% of companies have brought these teams together because it involves a huge organisational effort for an area of the business that is generally not a top board priority.

The imperative for partnership between physical and cyber security is greater today than it was two decades ago.

Companies need a way of achieving joined-up security that is nimble; organisation-model agnostic; flexible to organisational need, culture and risk appetite; and which can happen at pace and scale.

Our focus needs to shift from convergence and wholesale organisational redesign to partnership through holistic security, drawing together the knowledge, data, processes and resources of physical and cyber security.

Holistic security is an outcome, not an organisational structure. It describes a partnership between security functions that is engaged rather than transactional; a meeting of equals who bring different skills and experience and deliver holistic security outcomes through smart team working and the use of shared technology and resources.

Holistic security not only improves security outcomes; it also strengthens operational resilience because it improves risk management, creates strong and enduring enterprise-wide partnerships across risk functions, and integrates the three critical processes of operational resilience. As a result, holistic security enhances regulator and investor confidence, and is a signifier of a well-organised entity that can cope with whatever problems it encounters.

The most mature companies practising holistic security:

- recruit security leaders who are enterprise risk leaders first, functional heads second;
- align and integrate their critical processes of operational resilience: business continuity, crisis management and disaster recovery;
- promote partnership working through robust governance and incentives frameworks;
- share technology, data and intelligence resources across security teams to get ahead of problems, reduce disruption and achieve productivity gains; and
- make partnership working easier and and siloed working harder through security operating models.

The journey towards holistic security has started, but most multinationals are at the less mature end of the spectrum.

The Clarity Factory Holistic Security Maturity Model (Table 1) is a simple and practical tool for multinational corporations. It offers a step-by-step process to achieve continual improvement and increased maturity.

Business executives can use the maturity model to start a conversation with their security leaders, asking:

- What is the value of holistic security for our organisation?
- What is our current level of maturity?
- What is the appropriate level of maturity given our risk profile and appetite and current business conditions?
- Which changes will give us the best return on investment?

Holistic security delivers a holistic response to today's holistic threat environment. Companies that achieve maturity, will also boost operational resilience.

Table 1
The Clarity Factory Holistic Security Maturity Model

	Level 1 >>>>>>>>>>>>	Level 2 >>>>>>>>>>>>	Level 3 >>>>>>>>>>>>	Level 4
Identity and culture	People identify with their own team and see partnership as a distraction Leaders celebrate their own wins, but don't acknowledge other security team success	People identify with their own team and see partnership as an ad hoc 'nice to have' Leaders celebrate their own wins and acknowledge other security team success	Partnership is part of how the team works Leaders celebrate wins by both security teams	Partnership is non-negotiable Leaders celebrate success through partnership
Leadership	Leaders strongly identify as functional heads; incurious about partnership Separate functional strategies; no areas of partnership identified	Leaders identify as functional heads; see limited value in partnership Separate functional strategies; disjointed approach to third parties and vendors	Leaders identify as risk leaders; value partnership across security functions Separate functional strategies; elements of partnership; disjointed approach to third parties and vendors	Leaders identify as enterprise risk leaders; partner across business with other functional risk leaders Joint cross-functional strategy; shared approaches to technology, third parties, government contacts and vendors
Incentives	Team members have outcome goals linked to their role	Team members have outcome goals linked to their role and functional objectives	Team members have outcome goals linked to their role, functional objectives and cross-functional work	Team members have behavioural goals as well as outcome goals, and objectives related to holistic risks
Clarity of roles	No discussion about respective areas of accountability	Ad hoc partnership; no clarity of accountability	Clear roles and areas of accountability	Clear and documented accountability of roles; regular reviews
Professional development	Learning focused on individual roles Focus on role-specific technical skills	Learning focused on individual roles; limited learning across functions Focus on role-specific technical skills; social skills 'nice to have'	Learning about other areas of security actively encouraged Social skills 'desirable'	Dedicated resources for cross-functional learning Social skills 'essential'
Reporting lines	Separate reporting lines, no supervisor expectation of collaboration	Separate reporting lines, some supervisor expectation of collaboration	Joint reporting lines, limited effort to realise opportunities of partnership	Joint reporting lines, opportunities for enhanced insight are embraced
Operational	No joint working groups Separate functional processes and resources	Ad hoc joint working groups in limited areas Separate processes and resources; ad hoc input from other function (e.g. intel, SOC, technology, data)	Working groups in critical areas and effort to co-work in same location Separate processes and resources; active input from other function (e.g. intel, SOC, technology, data)	Established working groups and co-location of teams Co-design of processes to benefit from diverse views and joint decision-making
Governance	Separate board reporting No governance structures to coordinate security No governance oversight to coordinate physical- and cyber-security roles in operational resilience processes (business continuity, crisis management, and disaster recovery)	Separate board reporting; joint discussions with board Nascent governance structures to coordinate security Operational resilience is aspirational; board and risk committee take ad hoc interest in operational resilience processes	Separate board reporting; proactive coordination of data Governance structures to coordinate security Expectation of joined up approach to operational resilience; limited governance structures to drive and incentivise partnership	Joint board reporting presenting holistic view of risk Mandated governance structures to coordinate security Established oversight of operational resilience processes; expectation of partnership across risk functions

Clarity Up Front

About The Clarity Factory

The Clarity Factory is an engine room generating knowledge, insights, and practical solutions for our increasingly complex world. We use our data to help clients benchmark against peers, stay on top of best practice, and strive for continual improvement and innovation. We run workshops and training to grow and develop the skills and competencies that security leaders and their teams need to deliver maximum value for their organisations.

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 advised many of the world's largest corporations on their corporate security, cyber security and operational resilience. Her work has influenced major corporations and governments at the highest levels.

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

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

Executive Summary

Multinational corporations face elevated and interconnected security risks, which demand a unified approach to risk management

Major corporations are operating in a global business environment characterised by elevated security risks. Business leaders surveyed by the World Economic Forum ranked security-related risks as some of the most severe they face, including cyber espionage and warfare, crime, illicit economic activity, and state-based armed conflict. Cyber security in particular has risen sharply up the board agenda.[1]

Threat actors use the full spectrum of methods to target simultaneously across digital and physical domains. Criminals, terrorists and nation states are not constrained by the silos that characterise multinational corporations. They work across the physical–digital divide to target IP, commit fraud, steal assets, or take down elements of the critical national infrastructure.

Business leaders also recognise that the risks faced by their organisations are increasingly interconnected and cannot be managed in silos. They place greater emphasis on a unified approach to risk management and expect risk leaders to work together to ensure the board receives a holistic view.

The risks managed by physical and cyber security teams increasingly sit in the middle of the Venn diagram between the two functions. A comprehensive and effective response requires partnership that draws together their knowledge, data, processes and resources. Some of the most critical touch points include IT

security, information security, access control, people security, insider risk, and fraud prevention.

The need for partnership between physical and cyber security has been clear for twenty years. 'Convergence' emerged as the 'best practice', whereby physical and cyber security are brought together into a single function. There is much to be commended about this model, but only 15% of companies have converged. This is because it involves a huge organisational effort by senior leaders, who do not understand the benefits for an area of the business that is not generally a top board priority.

We need a new approach to physical and cyber security partnership that is nimble; organisation-model agnostic; flexible to organisational need, culture, risk level and appetite; and is cognisant of the considerable difficulties of bringing together two very different groups of professionals.

We need to shift our focus from convergence and wholesale organisational redesign towards partnership through holistic security.

From convergence to holistic security – and operational resilience

Holistic security is an outcome, not an organisational structure. It describes a partnership between physical and cyber security that is engaged rather than transactional; a meeting of equals who bring together different skills and ways of working to provide a wraparound security service through smart team working and the use of shared technology and resources.

Companies that reach full maturity also boost operational resilience – because holistic security improves risk management, creates strong and enduring enterprise-wide partnerships across all risk functions, and integrates the three critical processes of operational resilience: business continuity, crisis management, and disaster recovery. As a result, holistic security enhances regulator and investor confidence, and is a signifier of a well-organised entity that can cope with whatever problems it encounters.

Holistic security requires significant behaviour change by physical and cyber security professionals, who have different backgrounds, skillsets, ways of working, priorities, and mindsets. Each group has very **low levels of awareness and understanding** of the other's areas of expertise, which creates fear of the unknown. The functions are also structured differently – physical security is usually geographically organised, cyber security vertically.

> *Successful change processes speak to our emotional needs first.*

Holistic security is underpinned by an understanding that successful change processes speak to our emotional needs first, and then build cultures, teams, habits and incentives that respond to our fear of uncertainty and failure, and the human instinct to default to old habits when things are stressful or unclear.

Achieving holistic security depends on:

- **creating an identity** where partnership is something that 'someone like me would do in a situation like this';
- **celebrating wins**;
- **building and incentivising new habits** through nudges, reminders or check lists to help teammates do the right thing, even when it doesn't feel natural;
- **making the right behaviour easier and the wrong behaviour harder** through team structures, working groups, and co-location;
- **being specific** about exactly how teammates should behave and work differently; and
- **breaking down the change into bite-sized chunks** to get started with early wins.

The journey towards holistic security has started, but maturity in most multinational corporations is low, and cyber security professionals are less convinced of the need to partner compared to their peers in physical security. The is frustrating for CSOs, but as business leaders, they must take the initiative to convince their CISO of the mutual benefits of partnership.

The success factors for holistic security

Our research identified eight success factors for holistic security:

1. **Identity and culture**: Teams understand the rationale for partnership and see it as 'something that people like us do' for the good of the organisation.

2. **Leadership**: CSOs and CISOs consider themselves risk leaders first and they are collaborators who model partnership.

3. **Incentives**: Teams have incentives for collaboration; they publicise and celebrate their partnership wins and acknowledge the essential role of failure in achieving change. They have behaviour goals as well as outcome goals.

4. **Clarity of roles**: Teams have clear roles and responsibilities and have broken down new ways of working into bite-sized chunks.

5. **Professional development**: Leaders encourage learning about one another's respective areas of security to build empathy, reduce fear of the unknown, and grow confidence in partnership.

6. **Shared reporting lines**: Where the CSO and CISO report into the same executive leader, solid relationships and empathy can be built from the top of the two functions. Leaders work together, spot opportunities for partnership, and build joint initiatives that move the relationship beyond transactional.

7. **Operational**: Teams establish structures and forums that reinforce partnership and build new habits, such as working groups and shared processes and resources.

8. **Governance**: Teams are part of common governance frameworks that promote partnership between security leaders and embed a unified approach to risk.

The Clarity Factory Holistic Security Maturity Model

The Clarity Factory Holistic Security Maturity Model is a simple and practical tool. It offers a step-by-step process to achieve continual improvement and increased maturity. Security leaders can use the model to start a conversation with one another, or with business leaders, asking questions such as:

- What is the value of holistic security for our organisation? What opportunities can holistic security offer us?
- How does our current model align or diverge from that of holistic security?
- Where are we currently on the holistic security maturity model?
- What is the appropriate level of maturity for us, given our risk profile and appetite and current business conditions?
- What changes will give us the best return on investment?

Not all factors on the holistic security maturity model are created equal. Companies should target the following as a matter of first-order priority: identity and culture; incentives; clarity of roles; operational structures (such as working groups); and low-hanging fruit where joint working will deliver fast wins.

One of the most promising success factors is **joint reporting lines for the CSO and CISO**. This is outside the gift of security leaders, but it should remain a north star as a company travels through the maturity levels. All the CSOs and CISOs we interviewed who had achieved joint reporting – whether their functions were converged or not – said it was a game changer.

Holistic security delivers a holistic response to today's holistic threat environment. Those companies that achieve maturity will also boost operational resilience.

About this report

This report is the culmination of a 12-month study supported by BP, Barclays, Johnson Matthey, and the Scentre Group. 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. It is based on a thorough research process, which included interviews with 27 CSOs and CISOs, a handful of C-Suite executives and several industry experts; a survey of 151 CSOs, 90 of whom were from multinational corporations; and a review of existing industry data.

This report seeks to offer practical guidance on how to enhance operational resilience and improve risk management by closing silos and reducing blind spots between physical and cyber security. It is intended as a guide for security and business leaders at multinational corporations. Although aspects might be relevant for other types of organisations, they are not the focus of this study.

While job titles vary, the report refers to Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs) as shorthand for the most senior physical or cyber security leader within the organisation.

The report refers throughout to physical security, which in many companies is known as corporate security.

1 Security Risks are Elevated and Interconnected

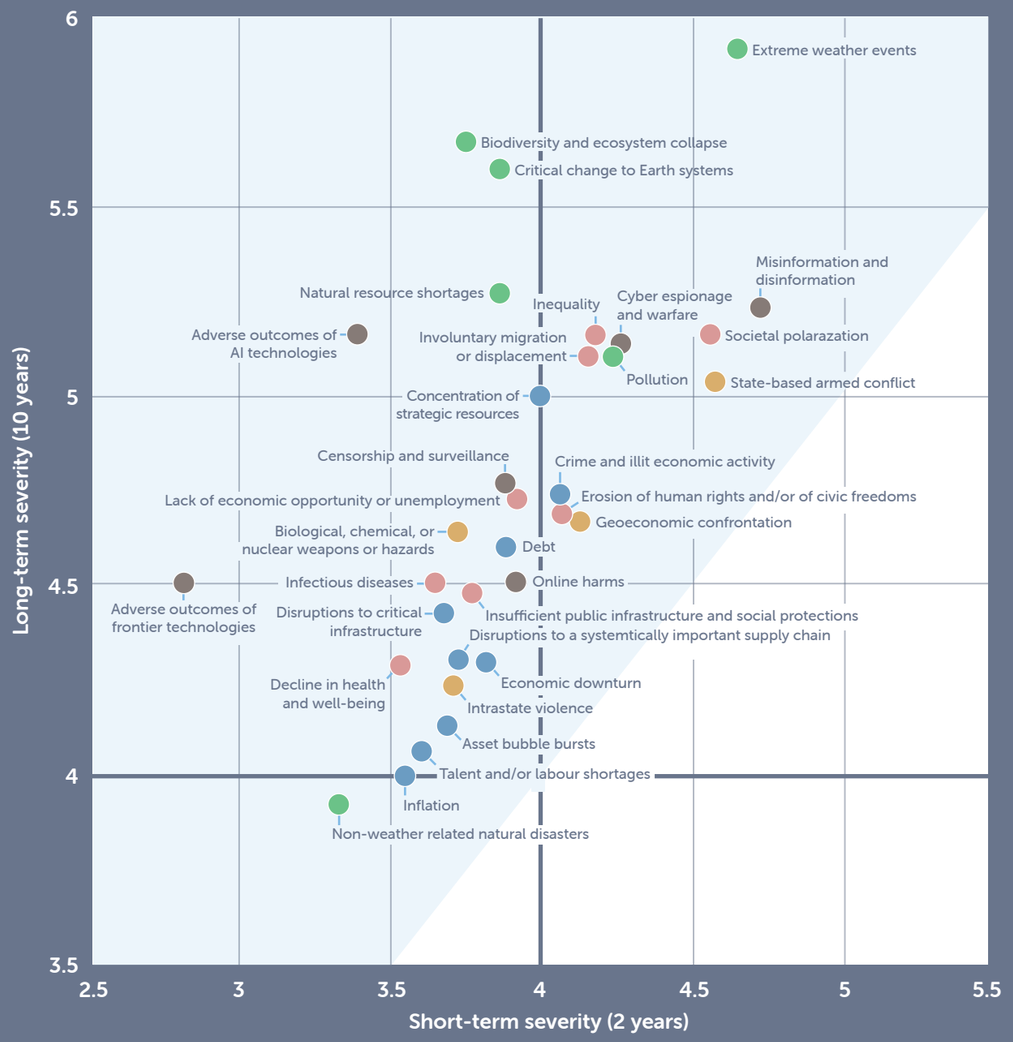
Summary

- Most multinational companies are operating in a global business environment characterised by elevated and interconnected security risks.
- Threat actors operate in a joined-up manner to target across a company's physical and digital assets, challenging the siloed structure of multinational corporations.
- Business leaders demand a holistic approach to risk management.
- Cyber security is a top board priority, and major multinationals are prioritising risk leadership capabilities over technical competencies when recruiting CISOs because they need someone who can lead upwards and across the business.
- Physical security leaders must also operate as risk leaders to be effective and equal partners within a holistic, enterprise-wide risk management framework.

Major corporations are operating in a global business environment characterised by elevated security risks. Business leaders surveyed by the World Economic Forum (WEF) ranked security-related risks as some of the most severe they face over both the short and long term (Chart 1); such risks include cyber espionage and warfare, crime, illicit economic activity, state-based armed conflict, and extreme weather events (the latter of which are often managed by the physical security function). A large majority of leaders think volatility will be prevalent over both two- and ten-year timeframes,[2] and therefore place greater emphasis on scenario planning. As McKinsey 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.'[3]

Chart 1

Risks ranked by severity over 2 and 10 years



Note: Severity was assessed on a 1–7 Likert scale (1 = Low severity, 7 = High severity.

Source: World Economic Forum Global Risks Perception Survey 2024–2025.

Cyber security is a top-three concern for most boards, as both threat and vulnerability have increased. According to a 2024 WEF survey, almost one-third of companies were materially impacted by a cyber event in the previous 12 months,[4] and four-fifths of leaders said they felt more or similarly exposed to cybercrime than they did the previous year.[5] There is widespread pessimism about the cyber threat. Almost all business and security leaders said they believed that global geopolitical instability would likely lead to a catastrophic cyber event in the next two years.[6]

Physical security has become a more significant concern for a wider variety of companies because of geopolitical turbulence. In recent years, businesses have been impacted by heightened tensions in the Middle East, the ongoing Russian invasion of Ukraine, China's influence in its own near neighbourhood as well as in Africa and the Middle East, and the highest level of political risk and unrest in five years. Closer to home, they are grappling with social and political fragmentation, employee disaffection, insider risk, workplace violence, and threats to senior executives.

Threat actors use the full spectrum of tools and tactics to target corporations simultaneously across digital and physical domains. This requires a coordinated response by physical and cyber security functions. Criminals, terrorists and nation states are not constrained by silos, and can work seamlessly across the physical–digital divide to target IP, commit fraud, steal assets, or take down elements of the critical national infrastructure.

The global risk picture is having a tangible impact on business operations. Almost half of all companies are shifting their supply chains or geographical footprint; investment in cyber security is at an all-time high; executives are ramping up protection for themselves and their families; business leaders use scenario planning for a wider range of disruptions; and regulators and investors are pressuring boards to demonstrate operational resilience.

Business leaders recognise that the risks they face cannot be managed in silos (Chart 2) – a view shared by executives we interviewed. They place greater emphasis on a unified approach to risk management and expect leaders of risk functions to work together to provide the board with a holistic view. A majority of multinationals have adopted an enterprise-wide risk-management

framework, incorporating functions such as physical security, cyber security, compliance, IT, supply chain, third party risk, and legal.[7] As risk-management expert Richard Chambers wrote, 'What is needed [instead] is a holistic, connected risk approach in which collaboration and data sharing are ingrained in the culture, and disparate teams work together to solve problems and meet the shared goal of mitigating risk.'[8]

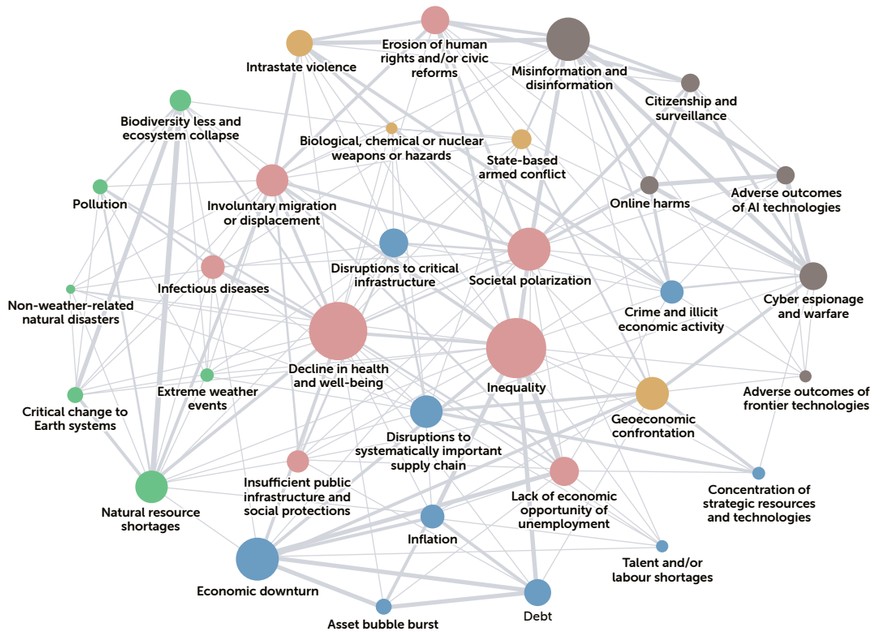
There is evidence that a holistic approach to risk management generates wider business benefits. For example, companies that integrate cyber security into their enterprise risk management programme and look at risk holistically outperform their peers on a range of business metrics, including revenue growth, market share, customer satisfaction and trust, and employee productivity.[10]

As part of their efforts to integrate cyber security into the risk-management framework, business executives are starting to prioritise risk leadership experience over technical capabilities when recruiting CISOs. They need cyber leaders who can communicate risk in a language the board understands, liaise with regulators and investors, and partner with other risk functions across the business. As one of the market's leading CISO recruiters put it, 'It used to be all about technology, but now they want someone who has experience influencing the board, with exceptional communication and relationship building skills, and who can embed the [cyber] security strategy into the business strategy.' Some companies are folding cyber, technology and operational risk into a combined role to create a holistic response across these business-critical areas.

This has implications for physical security leaders. They must also be risk leaders who work beyond their function within their company's enterprise-wide risk-management framework. Those that take a narrower, function-first approach will find themselves on the margins of their company's risk structure and lose influence as a result.

Chart 2

Global Risks Landscape: An interconnections map



Source: World Economic Forum Global Risks Report 2025.[9]

2 Physical and Cyber Security Risks are Increasingly Interconnected

Summary

- The risks managed by physical and cyber security teams are interconnected and the most effective security frameworks are underpinned by partnership.
- The most promising areas for partnership include access control, information security, people security (including executive protection, travel safety and special events), insider risk and fraud prevention.
- Physical and cyber security leaders must partner to clarify accountability for risks stemming from new technologies, such as vishing and deep fakes.
- Effective security relies on wider partnership with other functions, including HR, legal, technology, and compliance.

The risks managed by physical and cyber security teams are increasingly interconnected because threat actors work interchangeably across digital and physical tactics. An effective security framework draws together the knowledge, data, processes and resources from both functions.

> *We [CISO and CSO] realised that all the problems we face are somewhere in the middle of the Venn diagram.*
>
> — CSO

Security leaders understand the imperative for partnership; three-quarters of CSOs agree that the security risks their companies face need to be managed by more than one function. As one CSO said of his relationship with the CISO, 'We realised that all the problems we face are somewhere in the middle of the Venn diagram. The most effective way to manage those risks is by working in the space between our teams, getting beyond the org chart.'

Touchpoints between physical and cyber security

There are multiple touch points between physical and cyber security, including:

IT security, information security, and access control

Securing a company's network depends on cyber and physical security working together, with the former deploying digital controls and the latter monitoring and controlling access to physical locations to prevent unauthorised access to servers or devices. In January 2025, the British Museum suffered an IT outage after a terminated technology contractor was able to gain access to an unauthorised area of the building and turned off some of its IT systems.[11]

Companies contending with 'urban adventurers' – who break into physical sites and post videos online of their exploits – described the need for partnership between the two functions. A CSO we spoke to posed the question, 'Where would you place this risk? It's not really a cyber risk, but the videos expose the type and location of our cables. It's not really a physical security risk, but it exposes our locations. I bring the issue holistically to the board to give them the full picture and as a result we can manage it effectively without any friction.' IT security is always achieved through partnership between cyber and physical security.

You cannot deliver comprehensive information security unless physical and cyber security work together. Cyber teams secure the network and devices that house data and intellectual property, while physical security controls access to corporate locations housing paper-based information and digital assets.

People security, including executive protection, special events, and travel safety

Protecting a company's people – executives, travellers, event guests – rests within the domain of the physical security team, but increasingly requires input from cyber peers. For example:

- **Executive protection**: Most physical security teams are accountable for executive protection, covering office and home locations, as well as travel. Cyber security teams must advise executives on their digital footprint, secure devices and ensure

geolocation is disabled to prevent executives from being tracked, and monitor the dark web for threats. The cyber security operations centre monitors for unusual online behaviour, which can be a red flag for hacking, kidnap, or tracking.

- **Travel security**: A similar holistic approach is required for the company's travel security programme. If a device reveals a traveller's location, it can put them in physical danger.
- **Special event security, including for board meetings**: The 2024 murder of UnitedHealthcare's CEO is a reminder of the threat executives face at board meetings. Physical security teams are responsible for ensuring meetings and events are safe for attendees and free from violence, disturbance, and intimidation. The cyber security function oversees digital security, ensures secure access to sensitive board papers, and conducts dark web monitoring.

Insider risk

Insider risk is consistently ranked as a top-five security risk by CSOs (Chart 3), and covers a range of activities, such as information theft, espionage, sabotage, fraud, workplace violence, and unintended insider threat.[12] It is rising for several reasons, including increased organisational complexity, remote work, the cost of living, employee disillusionment about employers, and poor understanding of secure behaviours leading to unintended breaches.

An effective insider risk programme must involve physical security, cyber security, and HR functions, whereby:

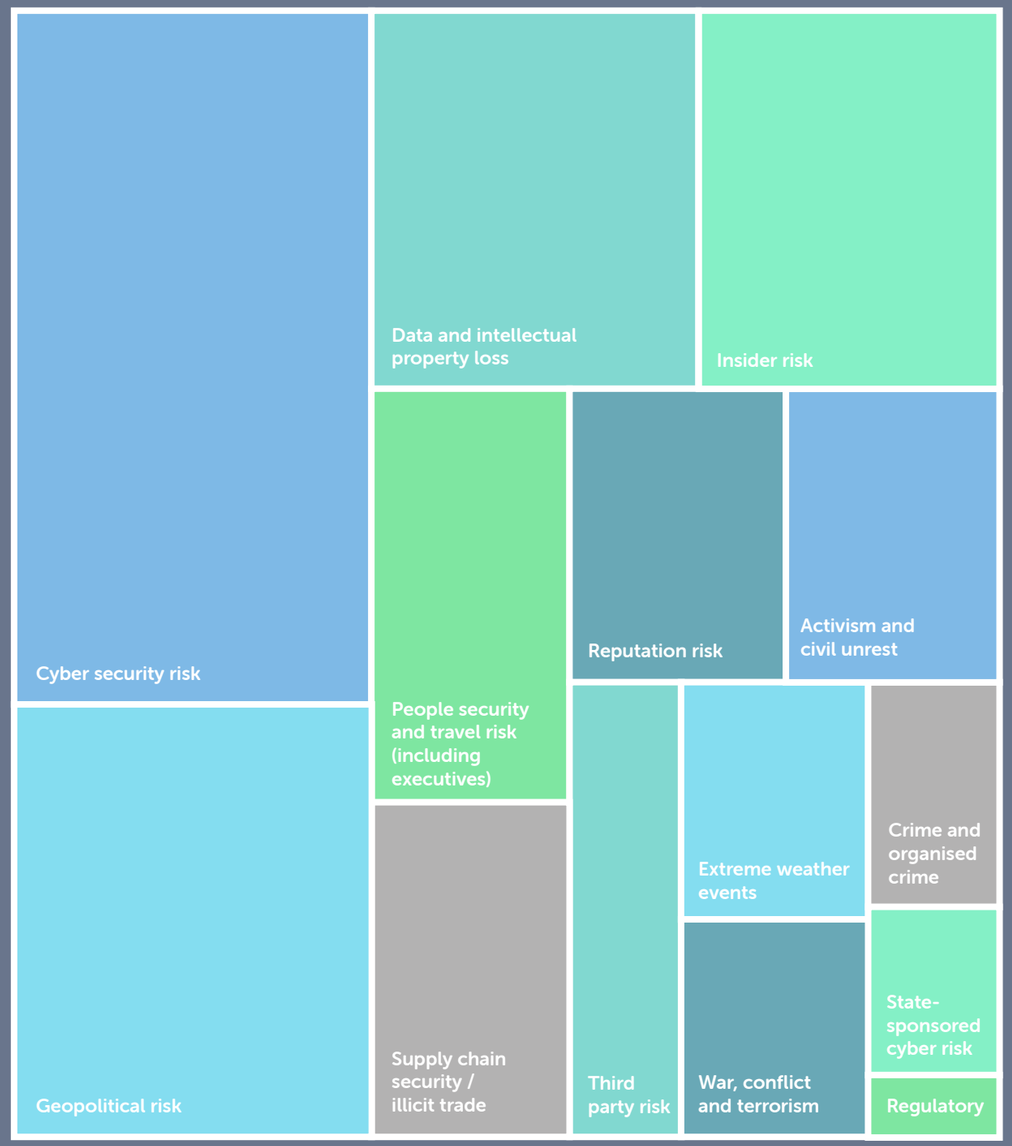
- **physical security** oversees access-management systems to track entry, exit and movement around premises;
- **cyber security** oversees network access and can spot unusual log ins; and
- **HR** handles employee disputes and disgruntled staff, and is responsible for offboarding processes that ensure dismissed employees' access rights stop.

Joining together cyber and physical access-control data can generate powerful insights to spot potential insider behaviour. If an employee badges into a building in London but logs into a workstation in New York, a holistic access-control system spots this 'impossible' travel and raises a flag for further investigation. Siloed systems miss this.

2 Physical and Cyber Security Risks are Increasingly Interconnected

Chart 3

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



Source: CSOs of non-converged security functions at MNCs, The Clarity Factory survey, 2024

Fraud prevention

Traditionally, physical security's role in fraud has focused on investigations after the loss has occurred. By partnering with cyber security and IT colleagues, physical security teams can build a virtuous cycle that shifts the focus towards prevention. In this scenario:

- **cyber security** provides intelligence to understand trends and behaviour patterns related to attempted and successful fraudulent transactions;
- **IT** revises the digital infrastructure, based on cyber security's trend analysis, to trigger interventions when fraud occurs; and
- **physical security** conducts investigations to recoup money and drive disincentives. Information from investigations feeds back into cyber security's intelligence operation to improve understanding of trends.

Risks from emerging technology

New technologies bring novel risks to multinational corporations, who are falling victim to scams such as:

- **Vishing**: Phone calls or voice messages purporting to be from reputable companies to induce individuals to reveal information, such as bank details and credit card numbers. Three-quarters of businesses have lost money to vishing, and vishing attacks in 2023 led to losses topping $10 billion in the United States.[13]
- **Deep fakes**: Videos generated by criminals using AI, to defraud organisations. For example, an employee from Arup transferred $25 million after taking a video call with what he thought was the CFO.[14] Just over half of CISOs say deep fakes pose a moderate-to-significant cyber threat to their organisation.[15]
- **Fake online profiles of company executives**: Often created on platforms like LinkedIn, for the purpose of deceiving people into sharing sensitive information, engaging in scams, or damaging the company's reputation by spreading false information.

Few companies have articulated clear accountability for these risks. They do not fall neatly within the purview of either physical or cyber security, because they do not normally cause physical harm and do not always take place on the company's network. It is important that CSOs and CISOs initiate a joined-up approach to risks like these, which are rising up the board agenda.

3 Beyond the Binary: From Convergence to Holistic Security

Summary

- The need for partnership between physical and cyber security has been clear for two decades – and 'convergence' emerged as 'best practice' for joined-up security.
- Convergence has only been adopted by a small minority of companies because it is difficult to achieve in practice.
- The need for partnership is greater today than it was twenty years ago, but we need an alternative to convergence that can adapt to risk profile and appetite, organisational structure, and culture.
- Holistic security offers a flexible model for joined-up security. It acknowledges the challenges of partnership, and that changing behaviour must address identity, culture and emotion before structures and systems.
- The journey towards holistic security has started, but maturity levels are low. Few CSOs and CISOs understand the full opportunities of partnership, which leads them to overestimate the maturity of their own partnership.

Beyond convergence

The need for partnership between physical and cyber security is not new; it has been a topic of conversation within the industry for more than twenty years. 'Convergence' quickly emerged as the 'best practice' for achieving a joined-up security capability, whereby physical and cyber security are brought together into a single function. There is much to be commended about this model, and many of the leaders we interviewed who run converged functions spoke of its benefits. In practice, however, only 15% of multinational corporations have brought their security functions together.[16]

There are five reasons why adoption of the convergence model has been limited:

- Merging two functions is a **huge organisational effort** requiring senior-level buy-in.
- It involves one **senior budget holder losing** and another winning, which creates poor incentives to change.
- **Security has not been a big enough business priority** to warrant the effort.
- The decision to converge is **not within the gift of its main advocates**, CSOs and CISOs.
- **Business leaders do not generally appreciate the benefits of greater partnership until they see it working in practice**.

> *There are no signs that convergence will emerge as a widely adopted solution.*

The imperative for partnership is greater today than it was two decades ago, but there are no signs that convergence will emerge as a widely adopted solution. An ASIS Foundation study found that two-thirds of those that had not converged said they had no plans to do so.[17] We need a new way of achieving joined-up security that overcomes the challenges convergence has faced.

We need an approach to partnership that is nimble; organisation-model agnostic; can be started within security teams without senior-level sign-off; is flexible to organisational need, culture, and risk level and appetite; and is cognisant of the considerable difficulties of bringing together two different groups of professionals. We need to shift our focus from convergence and wholesale organisational redesign towards partnership through holistic security.

A CSO told us, 'The key question we must keep asking ourselves is how does this decision ensure our desired outcome is delivered? Where things sit on an org chart rarely materially impacts that. Instead, we need to stay laser focused on our mission, our intent, our desired outcomes – and structures and processes are secondary to those imperatives.'

3 Beyond the Binary: From Convergence to Holistic Security

Holistic security

Holistic security is an outcome, not an organisational structure. It describes a partnership between physical and cyber security that is engaged rather than transactional and a meeting of equals who bring together different skills, knowledge and ways of working. Regardless of whether the functions merge, sit in the same part of the business, have a common C-Suite leader, or are entirely separate, security professionals come together to deliver holistic security outcomes through smart team working and the use of shared technology and resources.

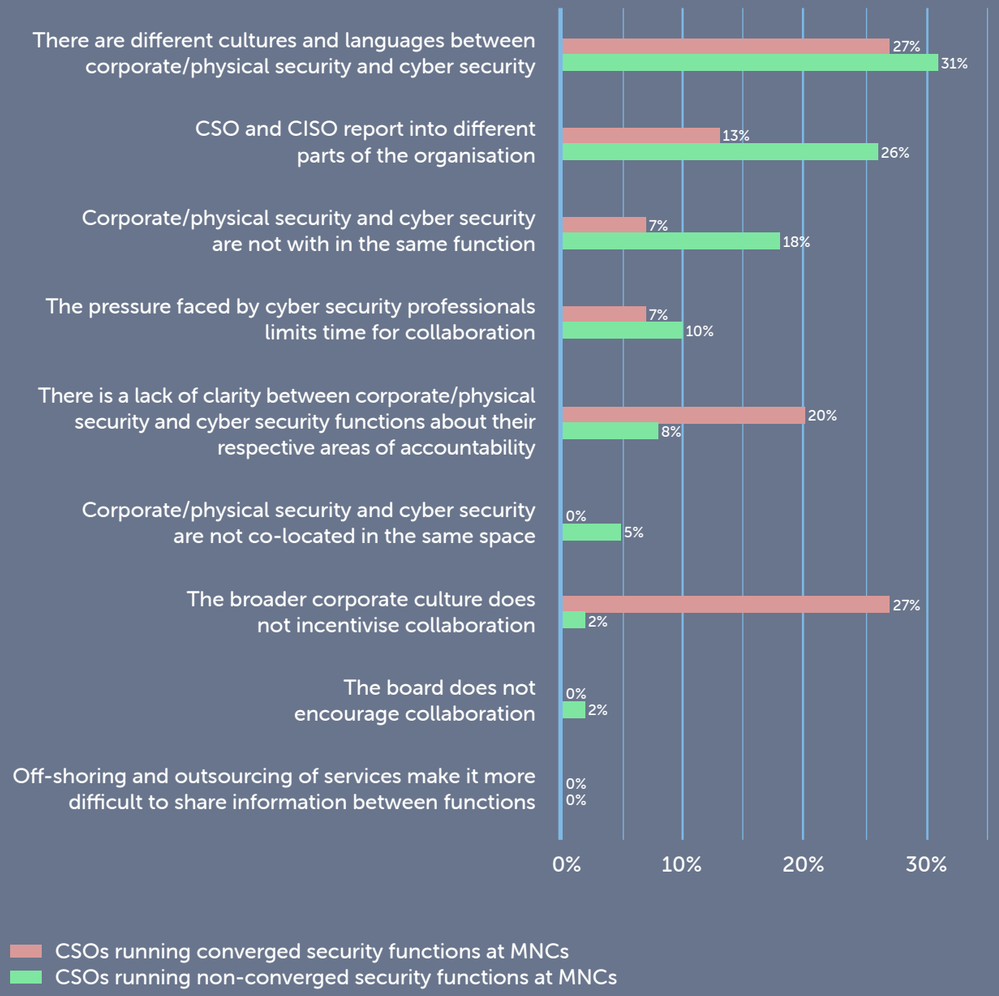
Holistic security recognises that partnership is difficult because it requires significant behavioural change by physical and cyber security professionals. CSOs from both converged and non-converged functions ranked cultural and language differences as the most important challenge to partnership working (Fig 1.), and a C-Suite executive who manages the CSO and CISO told us, 'It's like two different DNAs coming together and trying to figure out how to work together.'

The challenges of such partnerships are manifold:

- There are **significant differences** between the groups – educational and professional backgrounds, skillsets, cultures and ways of working, assumptions about roles and priorities, and perspectives on problems and solutions.
- Each group has very **low levels of awareness and understanding** of the other's areas of expertise, which creates fear of the unknown.
- The functions have **different organising logics** – physical security is normally geographically structured while cyber is an increasingly vertical and centralised function as boards seek visibility and assurance.
- The **cyber-security function is under intense pressure** due to fast-moving threats, growing vulnerabilities, and a limited talent pool. CSOs rated cyber workload as a key challenge for partnership (Fig. 1), and a CSO told us, 'Cyber are trying to implement so many programmes at the same time so for understandable reasons they suffer from tunnel vision.'

Figure 1

What is the most important obstacle to collaboration between corporate/physical security and cyber security?



Source: The Clarity Factory survey, 2024

Converged security models are not immune from these challenges. One CSO with a converged function told us, 'You can bring people together in a single function, but it's not converged unless you have a converged mindset.' Others described encouraging colleagues from different verticals to work together, and finding they tend to revert to siloed working by default.

Holistic security is a change management challenge

Delivering holistic security is a change management challenge. Most major change efforts fail because they focus on strategy, structure and systems at the expense of culture, identity and emotion. As John Kotter and Dan Cohen say in *The Heart of Change*, '... the core of the matter is always about changing the behaviour of people, and behaviour change happens in highly successful situations by speaking to people's feelings.'[18]

Successful change efforts focus on emotional needs first, and then build cultures, teams, habits and incentives that respond to our fear of uncertainty, concerns about failure, and the human instinct to default to our comfort zone. Structures matter, but only to the extent that they reassure, build new habits, change behaviour, and create a shared identity.

Achieving holistic security depends on:

- **Creating an identity** where partnership is something that 'someone like me would do in a situation like this'. Effective leaders project a team identity that is proud of change and acknowledges that failure will happen because change is difficult. As Rosabeth Moss Kanter said, 'Everything can look like a failure in the middle.'[19]
- **Celebrating partnership wins** – because success is contagious.
- **Building and incentivising new habits** through nudges, reminders or checklists to help teammates remember to do the right thing, as it won't feel natural to them.
- **Making the right behaviour easier and the wrong behaviour harder** through team structures, working groups and co-location.
- **Being specific about exactly how teammates should behave differently**. It won't be obvious or intuitive, and when they

inevitably lose their way, they will default to old ways of working unless they have guidance.

- **Breaking down change into bite-sized chunks to help deliver early wins**. As Chip and Dan Heath say in *Switch*, 'When you engineer early successes, what you're really doing is engineering hope. Hope is precious to a change effort.'[20]

The journey towards holistic security has started, but most companies with non-converged security functions are at the less-mature end of the spectrum. Among the CSOs and CISOs we interviewed, most described their relationship as non-existent or transactional. A CSO said, 'We have regular touch points, but there is not much depth to the relationship.' Few were able to give concrete examples of how they work with colleagues, and some described their relationship as strained or confrontational. Most CSOs struggle to get started because they don't understand the opportunities and benefits of partnership.

Physical security functions are beginning to contribute to areas of cyber security. We asked CSO survey respondents to categorise their function's involvement in a range of areas as 'primary accountability', 'consistent contribution', 'ad hoc contribution', or 'no involvement' (Chart 4). Responses show that they are beginning to play a role in cyber-security governance, data loss and information protection, disaster recovery, identity threat detection and response, IT risk, security architecture and security engineering.

Cyber-security leaders are less convinced of the value of working together. According to an ASIS Foundation study, one-third of CISOs felt their function would be greatly strengthened by convergence with physical security, compared to 43% of CSOs. One-quarter of CISOs did not think it would make any difference.[21] A CSO described the relationship this way, 'We think about cyber more than cyber think about us. I think we are very much an afterthought to them.' Physical security leaders can be forgiven for being frustrated by this imbalance, but as business leaders they have an obligation to seize the initiative and convince their CISO of the mutual benefits of working together.

3 Beyond the Binary: From Convergence to Holistic Security

Chart 4

Levels of accountability or involvement by non-converged corporate/physical security teams

Primary Accountability	Asset protection Business continuity Crisis management Executive protection Global meetings & event security Incident management/ response Insider risk	Investigations People protection Security assessment Security audits Security culture, awareness & training	Security operations (threat analysis & monitoring) Security technology Threat intelligence Travel security
Consistent Contribution	Anti-money laundering Brand integrity Business intelligence Cyber security Data loss & info protection	Disaster recovery Disrupting fraud Identity & access management Identity threat detection & response	Privacy Supply chain security Third party risk Vetting
Ad Hoc Contribution	Anti-counterfeit Cyber security governance Due diligence	Investigations, forensics & e-discovery IT risk	Regulatory compliance Security architecture Security engineering
No Involvement	Application security & testing Configuration & vulnerability management	Line 2 assurance Network security Software development	

Note: This chart shows the typical level of accountability on average for non-converged corporate/physical security teams at MNCs

Source: The Clarity Factory survey, 2024

4 The Business Benefits of Holistic Security

Summary

- A company's ability to respond to, and recover from, shocks is business critical, and boards use operational resilience as a framework to achieve this.
- Holistic security can strengthen operational resilience, and in doing so, it protects shareholder value and promotes competitive advantage.
- Holistic security enhances operational resilience by improving risk management, strengthening key processes (business continuity, crisis management and disaster recovery) and building confidence among investors and regulators.
- Holistic security also drives efficiency and productivity gains.

A company's ability to respond to, and recover from, shocks is critical in today's volatile business environment. Operational resilience has become the organising principle many boards use to deal with multiple concurrent disruptions and to reassure regulators and investors. The appearance of being joined up generates confidence because it is a signifier of a well-organised entity that can cope with whatever problems it encounters.

Holistic security not only improves security outcomes, it also strengthens operational resilience, improves risk management, enhances investor and regulator confidence, and drives efficiency and productivity gains. In doing so, it protects shareholder value and promotes competitive advantage by reducing operational downtime, disruption, and regulatory scrutiny. As one CSO put it, 'A robust and integrated security approach instils confidence in our partners and investors that their investments, collaborations, and data are well protected. This translates into improved business relationships and reputation.'

Holistic security improves risk management

Business leaders increasingly demand a unified approach to risk management, and recognise the risk-management dividend of partnership between physical and cyber security when they see it in action. A C-Suite member from one of the world's largest companies told us, 'I am a better risk owner as a result of having them both report into me. I went through a set of risk reviews recently, and having them both in those conversations made it very easy, straightforward and seamless for me. I also had greater confidence the agreed actions would be implemented because they are both part of the same organisation. We can have integrated conversations about risk without it being a major event.'

Executives who have not witnessed holistic security do not normally comprehend its importance and are therefore unlikely to create the impetus for change. A leading CISO recruiter told us, 'People underestimate how important the relationship is between corporate and cyber security. I'm shocked at how many of my clients don't bring it up as much as I would expect them to. They still see them in silos. Nine times out of ten they don't mention it.' Similarly, a CSO commented, 'Board members are the last to realise the importance of integration. They don't understand that technology is not the realm of the CISO and protection is not solely in the realm of the CSO. They just don't have that expertise.' This partly explains why convergence has not taken off, and means that CSOs and CISOs must make a compelling business case for partnership.

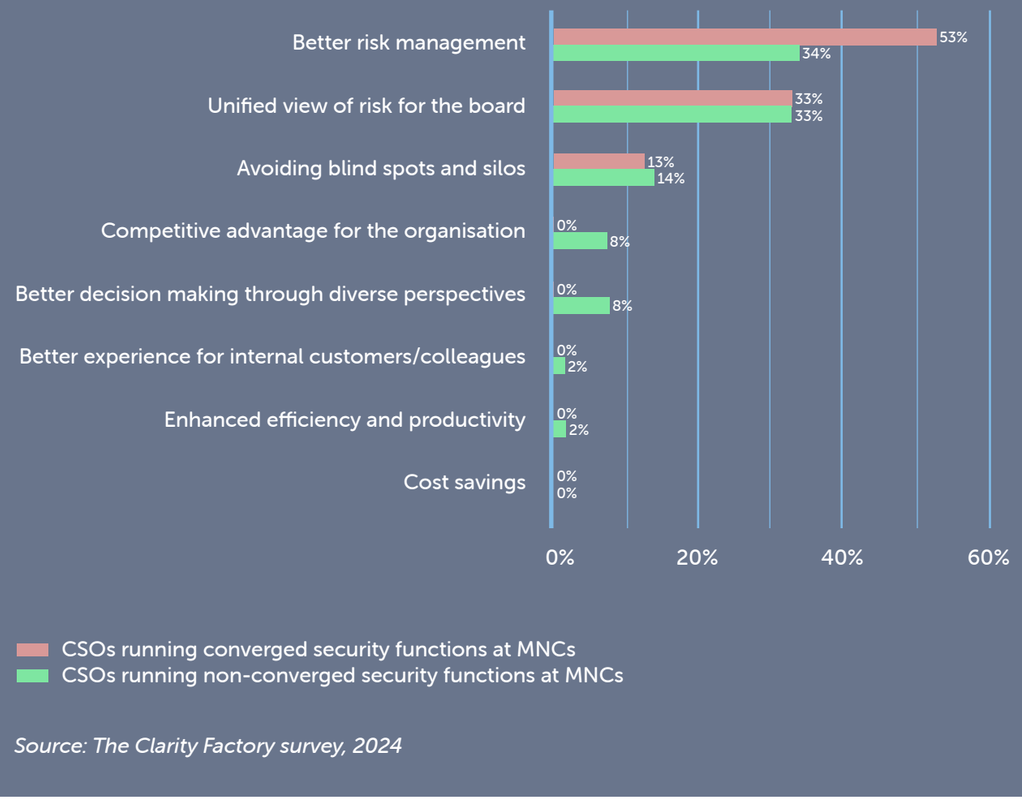
C-Suite demand for holistic security tends to be triggered by three things: a) an enterprise-level security event, b) pressure from regulators to achieve operational resilience, and c) the arrival of a business leader who has seen the value of partnership. A C-Suite member who operates a holistic model told us, 'If one of them [CSO or CISO] leaves, I will make my expectations clear that the successor needs to collaborate. I might not have made as much of a point of them working together if I hadn't seen it in practice.'

Security leaders see the risk management benefits of holistic security, with the vast majority ranking 'better risk management' as the top benefit of partnership (Fig. 2). A CSO told us, 'The bottom

line is that the risks we are exposed to are increasingly connected between physical and cyber and therefore to understand them, mitigate them, and explain them to leadership, we need people with a skillset in both or collaborating daily on these issues.' A CISO reflected, 'Fragmentation doesn't help risk management because you end up with siloed thinking and what we want is more integrated approaches and processes.'

Figure 2

What is the most important benefit of collaboration between corporate/physical security and cyber security?



Source: The Clarity Factory survey, 2024

Holistic security improves operational resilience processes

Both physical and cyber security are usually centrally involved in the three key processes of operational resilience: business continuity, crisis management, and disaster recovery. By working in partnership, they can improve the efficacy of each of these business-critical processes, as well as drive better alignment between them.

1. Business continuity

In today's volatile business operating environment, a company's ability to maintain operations and minimise disruption when faced with unexpected events, such as cyber-attacks, natural disasters, or system failures, is critical to success. Physical security functions are central to business continuity. According to our survey, almost half are accountable for the process and one-third are involved. As companies become increasingly dependent on technology, cyber security and IT must be fully integrated into business continuity. A CSO told us, 'We need to partner with cyber and technology teams to understand the vulnerabilities and ensure our business continuity processes are properly calibrated to respond quickly and effectively in the event of outages.'

The 2024 CrowdStrike outage revealed the vulnerabilities created when partnership between physical and cyber security and IT is lacking. Many CSOs with accountability for business continuity told us they felt unable to challenge IT decisions impacting continuity, such as the reliance on a single source supplier. One told us, 'Business continuity processes are sacrosanct, unless technology says we need something, and then nobody questions it.'

CSOs must step forward to advocate for a holistic approach to business continuity – and the CrowdStrike outage has created an opportunity to do so. One CSO told us, 'I wasn't asking questions ahead of time because we were told CrowdStrike was the answer and that we had to rely on it for everything. There was never a conversation about it. CrowdStrike has now opened the door for me to get more involved in these conversations, and we are doing a review on this.'

A holistic approach to business continuity is also a source of competitive advantage. A CSO told us, 'In the US during the hurricanes, a number of plants were put out of action. Because our continuity plans were better than our competitors', we were up and running quicker and able to supply to customers before our competition. As a result, customers switched to us and subsequently stayed with us because they trusted our ability to continue operating, allowing them to stay open for business. It's the same for a major IT outage or cyber-attack; it's the company that is up and running fastest that will enhance their reputation and be more competitive in the market.'

2. Crisis management

> *A robust and integrated security approach instils confidence in our partners and investors.*
>
> — CSO

Crisis management is no longer just a standalone process – it is also a core skill for all leaders. As the former Dean of the Harvard Business School put it, '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.'[22] One executive told us, 'Every element of the business needs to be able to do crisis management.'[23]

Corporate security functions are normally at the heart of their organisation's crisis management capability. According to our survey, three-quarters are accountable for crisis management and one-fifth are involved. Business dependence on technology means that IT and cyber security must be key partners for physical security in crisis management.

Building partnership muscle memory can pay dividends during a crisis. One CSO described the importance of being able to lean on cyber security and IT colleagues during a large-scale physical security crisis when he and his team were overwhelmed dealing with the immediate response. He told us, 'I was comfortable with my peers leading on aspects of our response because I had limited bandwidth. You need to utilise the influence, support, and intellectual capacity of your peers to get the best outcome for the business.' A seamless handoff between physical and cyber security is also important because what starts as one risk can quickly morph into another. When a company is in crisis, it needs a whole-of-company approach.

3. Disaster recovery

Boards increasingly seek assurance that the company's IT and data systems can be recovered in the event of a major cyber-attack. Disaster recovery is usually led by the IT function, but the crisis-management expertise of physical security can add value, and two-fifths of CSOs say their team contributes consistently to disaster recovery. CISOs and business leaders recognise this value; as one executive told us, 'I think corporate security has a unique set of assets when it comes to crises.'[24] Some companies see disaster recovery as the totality of operational resilience, rather than just one element of it. In fact, operational resilience is only achieved when these three processes are fully joined up.

Holistic security helps to build cross-cutting resilience

The challenges of partnership between physical security and cyber security can be converted into opportunities and strengths by those companies that get it right. Bringing together physical security's horizontal/geographical structure with cyber security's vertical one can create a resilient web across a siloed multinational corporation. The combination of the two groups' skills, perspectives, and working styles can create a more nuanced and complex risk picture to drive better decision making. And the combination of cyber security's shorter-term focus with physical security's medium-term gaze enables companies to see both around corners and over the horizon at the same time, which improves scenario planning.

Holistic security can increase confidence among investors, regulators and customers

Holistic security can improve a company's compliance with regulators, investors and customers, who demand a joined-up approach to operational resilience. For example:

- **Regulators**: Regulators increasingly look at risk management through the lens of operational resilience and the coordination of risk functions. Much of this is driven by cyber regulation, such as the SEC in the US, the EU's NIS2 Directive, Australia's Critical Infrastructure Act, and the Security Act in Norway. Holistic security can help to demonstrate compliance with the letter and spirit of this

regulation. As one CSO told us, 'One of the benefits of collaboration is better alignment with regulatory requirements through unified security policies and standards, consistent risk reporting to leadership, and joined-up innovation and knowledge sharing.'

- **Investors**: There was a six-fold increase in the number of mentions of 'cyber risk', 'cyber security' and 'cyber attacks' on earnings calls from 2017 to 2022, demonstrating rising investor concerns.[25] One of the main drivers of SEC regulation on cyber security is a desire to improve investor confidence through transparency in risk management and board governance. Holistic security is a signifier of a well-organised entity, which can be a business advantage. A CSO running a converged function told us, 'We have received feedback from our customers and investors that they like the fact we are able to report in a joined-up way; it gives them confidence in our security risk management. We are now working with the business to incorporate our integrated security management framework into our business pitch deck.'
- **Customers**: In some industries, such as defence or critical national infrastructure, customers have strict requirements about the governance of physical and cyber security and require specific measures that make holistic security the natural choice. And many customers stipulate that suppliers must meet certain standards. Widely used information security standards combine cyber and physical security controls. For example, one-third of the controls for ISO 27001 relate to physical security. A CISO told us, 'Our standards, like ISO, have elements of both physical and cyber, so it's vital we work together.'

Holistic security delivers productivity and efficiency gains

There are several areas where partnership between physical and cyber security can leverage efficiencies, including:

- **Security culture and awareness**: Security functions that work holistically can pool what are usually limited resources from each group to run joint campaigns, training and events, and create co-branded resources for the company intranet. A CISO told us, 'In my previous company, we worked closely on culture and awareness.

It didn't matter whose banner the messaging went out under, what mattered was that we were able to use what we were doing to have another bonus opportunity to get our message across.'

- **Assurance**: With both functions required to conduct assurance processes, working in partnership provides scope to combine efforts so that staff do not receive multiple requests for similar information. A CISO commented, 'What frustrates people in business is getting similar overlapping disjointed requests from multiple functions. We in cyber security worked with our physical security colleagues to offer a more joined up approach so colleagues got one assurance request rather than many.'
- **Red team testing**: Boards are requesting red team testing to provide assurance on disaster recovery. Given the linkages between physical and cyber security, and limited board time, there are benefits to running these exercises jointly.
- **Security team resources**: Some companies are combining all or some elements of intelligence and security operation centre (SOC) capabilities for physical and cyber security. Given cyber talent is expensive and in short supply, using physical security personnel across both intelligence and SOCs can lower staffing costs and improve retention.

> *I am a better risk owner as a result of having them [CSO and CISO] both report into me.*
>
> — C-Suite Executive

5 The Success Factors for Holistic Security

Summary

Our research identified eight success factors for holistic security that, together, create an identity based on partnership and make change easier than continuity.

1. Identity and culture
Teams understand the rationale for partnership.

2. Leadership
CSOs and CISOs see themselves as risk leaders.

3. Incentives
Teams have incentives for collaboration and leaders celebrate partnership wins.

4. Clarity of roles
Teams have clear roles and responsibilities.

5. Professional development
Leaders encourage cross-functional learning to enhance partnership.

6. Reporting lines
CSOs and CISOs report into the same C-Suite executive.

7. Operational
Teams establish structures for partnership, such as working groups and shared resources.

8. Governance
Teams are part of a shared governance framework that promotes partnership.

Eight success factors for holistic security

1. Identity and culture

Holistic security starts with culture and an identity where partnership is 'something that people like us do'. Culture is the cornerstone of effective change. Lou Gerstner, former CEO of IBM, said of his efforts to successfully turn around the company, 'I came to see, in my time at IBM, that culture isn't just one aspect of the game – it is the game.'[26]

2. Leadership

Functional leadership sets the tone for partnership. **CSOs and CISOs who see themselves as risk leaders first tend to be less territorial, more open to partnership, position themselves as enterprise-wide risk leaders, and inspire their teams to work across silos.** A C-Suite executive we interviewed who manages the CSO and CISO described how their leadership styles are critical to the success of their partnership: 'If they were not the leaders they are, and if they did not operate in the way they do, I can imagine that I would have had friction to resolve in bringing them together.' Leaders who are collaborative tend to be open, consultative, matrix-driven, curious, and put the organisation before function.

3. Incentives

Holistic security is underpinned by incentives for collaboration:

- **Recruitment**: Prioritise collaborative and soft skills when selecting candidates.
- **Objectives**: Set objectives that go beyond the scope of an individual's role and relate to converged risks. Compared to non-converged security teams, twice as many members of converged teams have objectives that relate to converged risks.
- **Behaviour goals**: Set goals about the kind of behaviour that is expected in a holistic security model, as well as goals linked to outcomes.
- **Celebrate wins**: Celebrate and publicise successful partnership working to build momentum for change.
- **Recognise the inevitability of failure**: Communicate that failure will be a feature of the change process and is not a reason to return to old ways of working.

4. Clarity of roles

In large change processes, hands-on management helps people to navigate ambiguity. As Chip and Dan Heath put it in *Switch*, you must 'script the moves',[27] breaking down new habits into bite-sized chunks. A key part of this is clarity of roles and responsibilities, and how the partnership will work in practice. Effective leaders formally document this to ensure partnership working survives staff turnover, which is critical given cyber talent shortages and the fact that average CISO tenure is just over two years.[28] One CSO described the value of this document, 'It has become the north star for us. If someone new comes in, we are not starting from zero. We have a clear outline of how we work.'

5. Professional development

Effective leaders encourage and facilitate professional development to enable team members to learn about the roles and expertise of their colleagues in other areas of security. This helps to build empathy, reduce fear of the unknown, and grow confidence in partnership. For example, some CSOs are enrolling team members in university programmes to supplement their cyber knowledge.

6. Shared reporting lines

One of the most important success factors for holistic security is joint reporting for the CSO and CISO into the same C-Suite member, and two-thirds of CSOs we surveyed agreed this would enhance partnership. Sitting within the same part of the business, while remaining in separate functions, fosters enhanced understanding and empathy for one another's challenges, and creates opportunities to problem solve together. It also opens up options to share resources, such as intelligence analysts, security operation centres, and incident response teams. A senior executive who manages the CSO and CISO described some of the benefits, 'The two of them are doing a lot more things together, sharing more context, so they are acting a lot more united as a pair, solving problems and escalating issues as a partnership.'

> *"The extent of the interaction between me and the CISO means we are much more ready to support one another than we were before... That's game changing."*
>
> *— CSO*

The CSO told us,

> *'The CISO and I sit on the same leadership team, we are formally and informally engaging to a greater extent than ever we did before. Our ability to see risks requiring both our contribution, and opportunities requiring both of our support, is much greater than it was before. The extent of the interaction between me and the CISO means we are much more ready to support one another than we were before. We see the same issues at the same time, and then consider how we can work together to help the company manage risk. That's game changing.'*

Transitioning to joint reporting lines is outside the gift of CSOs and CISOs, and only 15% of CSOs we surveyed have this arrangement. One thing that security leaders can do in pursuit of this goal is to take the initiative to create a joint security strategy – formal or informal. This will communicate to the C-Suite the holistic nature of the risks, how their areas of responsibility interface, and how they will share resources for the benefit of the company. Only one company we interviewed had done this.

7. Operational

Effective leaders establish organisational structures, processes and prompts that make partnership easier and siloed working harder. For example:

- **Joint working groups** to oversee co-working on specific priority issues (e.g. insider risk, or fraud prevention). As one CSO put it, 'You have to show people what they are missing by working in silos.'
- **Shared personnel**: security leaders can nominate personnel to work across both functions to connect the teams on priority issues, with dotted line reporting.
- **Proximity between teams**: co-location of physical and cyber security teams can foster empathy and relationships that make partnership easier and more natural. One CSO told us, 'Co-location

would accelerate the social interaction between the two teams that would help to build mutual trust, respect and understanding, which would free them from defensiveness.' According to our research, fewer than half of physical security teams are co-located with cyber security, and this will often be something security leaders cannot influence. Where co-location is not possible, face-to-face contact is desirable.

- **Shadowing**: requiring team members to cover for peers outside their own silo will increase knowledge and understanding.
- **Board briefing**: leadership team members from physical and cyber security can be required to cross-check one another's briefings and board notes.
- **Shared processes**: leaders can identify ways to share technology and data, including through the adoption of a single management system.
- **Shared resources**: the use of technology to share and collate information sources across physical and cyber security teams will provide a richer risk picture, such as in the domains of intelligence and security operations centres.
  - **Intelligence**: According to our research, almost half of converged security functions have brought together their physical and cyber security intelligence teams into a shared capability, compared to just 2% of non-converged functions. This is an untapped opportunity. As one CSO put it, 'Collaboration provides the highest fidelity of information with which to make better informed risk-based decisions that allows the organisation to take risks their competitors can't or won't.' When full partnership is not possible, share intelligence subscription services and team briefings.
  - **Security operation centres**: Two-thirds of CSOs we surveyed have a SOC. Almost no non-converged functions have merged their physical and cyber security SOCs, compared to one-fifth of converged functions.

> *"Collaboration provides the highest fidelity of information with which to make better informed risk-based decisions that allows the organisation to take risks that their competitors can't or won't."*
>
> *— CSO*

8. Governance

Effective holistic security is delivered under a joint governance framework, including:

- **Board reporting**: A majority of non-converged CSOs report into the board and/or board committees, but fewer than one-in-five report jointly with the CISO. This limits the board's ability to effectively manage risks impacted by both physical and cyber security. As a CSO put it, 'When we are managing organisations, we are managing risk. Your ability to present a holistic picture of risk is critical. You can't expect [the board] to translate.' The most effective risk management happens when cyber security and physical security leaders present jointly to the board.
- **Governance structures**: Just over half of non-converged CSOs have a coordinating body at corporate leadership level, compared to almost all CSOs from converged functions. These structures lock-in partnership and provide a formal process for joint information sharing, deliberation and decision making.

> *"Over half of non-converged CSOs have a coordinating body at corporate leadership level."*

CSOs and CISOs do not have the power to create governance structures, but they can advocate and share examples of how peers use them to manage risk more effectively.

6 The Clarity Factory Holistic Security Maturity Model

> *Security without partnership creates blind spots, silos and missed opportunities.*

The scale of the security risks faced by most multinational corporations, the fact that threat actors target silultaneously across both physical and digital domains, and the extent of the dependencies between physical and cyber security, make partnership an urgent imperative. Security without partnership creates blind spots, silos and missed opportunities. Holistic security also brings wider business benefits through enhanced operational resilience, better risk management, and efficiency and productivity gains.

Holistic security offers an approach to partnership that is nimble; organisational-model agnostic; can be started within security teams without requiring senior-executive sign-off; is flexible to organisational need, culture, and risk level and appetite; and is cognisant of the challenge of bringing together two divergent groups of professionals.

The Clarity Factory Holistic Security Maturity Model (Table 1) does not assume that all companies need to reach level four maturity. What 'right' looks like for each company will depend on the nature and scale of risks they face, their risk appetite, their current available resources, and the maturity of their physical and cyber security functions. It also does not assume that they should seek to achieve consistent maturity across all factors. These choices should be informed by the unique features and situational context of the business.

The model is intended to be used as a tool to facilitate conversations between the CSO and CISO, and between security leaders and business executives, prompting questions such as:

- What is the value of holistic security for our organisation? What opportunities can holistic security offer for us?
- How does our current model align or diverge from that of holistic security?

- Where are we currently on the holistic security maturity model?
- What is the appropriate level of maturity for us, given our risk profile and appetite and our current business conditions?
- Which aspects of the maturity model matter to us, given our culture, organisational structure, resourcing, and security strengths and weaknesses?
- How do we get started? What changes would bring the best return on investment?
- How would we generate buy-in for change among our teams and senior executives?
- How mature are our peers in our sector?

Not all factors on the holistic security maturity model are created equal. Our research suggests companies should target the following as a matter of first-order priority:

- **Identity and culture**: fostering a sense that partnership is how you do business;
- **Incentives**: such as behaviour goals and objectives related to holistic security;
- **Clarity of roles**: articulated in a shared document; and
- **Operational**: creating working groups to tackle low-hanging fruit where joint working will deliver fast wins.

One of the most promising success factors is joint reporting lines for the CSO and CISO. This is outside the gift of security leaders, but it should remain a north star as a company travels through the maturity levels. All the CSOs and CISOs we interviewed who had achieved joint reporting – whether their functions were converged or not – said it was a game changer.

Holistic security delivers a holistic response to today's holistic threat environment. Those companies that achieve maturity will also boost operational resilience.

6 The Clarity Factory Holistic Security Maturity Model

Table 1
The Clarity Factory Holistic Security Maturity Model

	Level 1 >>>>>>>>>>>>	Level 2 >>>>>>>>>>>>	Level 3 >>>>>>>>>>>>	Level 4
Identity and culture	People identify with their own team and see partnership as a distraction Leaders celebrate their own wins, but don't acknowledge other security team success	People identify with their own team and see partnership as an ad hoc 'nice to have' Leaders celebrate their own wins and acknowledge other security team success	Partnership is part of how the team works Leaders celebrate wins by both security teams	Partnership is non-negotiable Leaders celebrate success through partnership
Leadership	Leaders strongly identify as functional heads; incurious about partnership Separate functional strategies; no areas of partnership identified	Leaders identify as functional heads; see limited value in partnership Separate functional strategies; disjointed approach to third parties and vendors	Leaders identify as risk leaders; value partnership across security functions Separate functional strategies; elements of partnership; disjointed approach to third parties and vendors	Leaders identify as enterprise risk leaders; partner across business with other functional risk leaders Joint cross-functional strategy; shared approaches to technology, third parties, government contacts and vendors
Incentives	Team members have outcome goals linked to their role	Team members have outcome goals linked to their role and functional objectives	Team members have outcome goals linked to their role, functional objectives and cross-functional work	Team members have behavioural goals as well as outcome goals, and objectives related to holistic risks
Clarity of roles	No discussion about respective areas of accountability	Ad hoc partnership; no clarity of accountability	Clear roles and areas of accountability	Clear and documented accountability of roles; regular reviews
Professional development	Learning focused on individual roles Focus on role-specific technical skills	Learning focused on individual roles; limited learning across functions Focus on role-specific technical skills; social skills 'nice to have'	Learning about other areas of security actively encouraged Social skills 'desirable'	Dedicated resources for cross-functional learning Social skills 'essential'
Reporting lines	Separate reporting lines, no supervisor expectation of collaboration	Separate reporting lines, some supervisor expectation of collaboration	Joint reporting lines, limited effort to realise opportunities of partnership	Joint reporting lines, opportunities for enhanced insight are embraced
Operational	No joint working groups Separate functional processes and resources	Ad hoc joint working groups in limited areas Separate processes and resources; ad hoc input from other function (e.g. intel, SOC, technology, data)	Working groups in critical areas and effort to co-work in same location Separate processes and resources; active input from other function (e.g. intel, SOC, technology, data)	Established working groups and co-location of teams Co-design of processes to benefit from diverse views and joint decision-making
Governance	Separate board reporting No governance structures to coordinate security No governance oversight to coordinate physical- and cyber-security roles in operational resilience processes (business continuity, crisis management, and disaster recovery)	Separate board reporting; joint discussions with board Nascent governance structures to coordinate security Operational resilience is aspirational; board and risk committee take ad hoc interest in operational resilience processes	Separate board reporting; proactive coordination of data Governance structures to coordinate security Expectation of joined up approach to operational resilience; limited governance structures to drive and incentivise partnership	Joint board reporting presenting holistic view of risk Mandated governance structures to coordinate security Established oversight of operational resilience processes; expectation of partnership across risk functions

Appendices

Appendix 1: Methodology

The research for this report was conducted by 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 CSOs and CISOs**: structured interviews with 27 CSOs and CISOs from the following sectors: agriculture, automotive, consulting, consumer goods, energy, finance, food and beverage, manufacturing, media, pharmaceuticals, real estate, retail, technology, and transport.
- **Interviews with a handful of C-Suite executives from multinational corporations**.
- **Expert interviews with a range of relevant professionals**: informal interviews with 10 experts across a range of relevant fields.
- **Survey of CSOs**: an anonymous survey was conducted, for which we received 151 responses, of which 90 were from CSOs at multinational corporations. Where relevant, we separated responses for CSOs that were converged and non-converged. The survey data quoted in this report refers to this sample from multinational corporations.

Appendix 2: Project Partners

This research is kindly supported by partners, including Barclays, BP, Johnson Matthey and Scentre Group. The views experessed in this report are those of The Clarity Factory and do not necessarily reflect the views or positions of the companies who supported the work.

The following individuals 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: Alex Hawley, Derek Porter, Steve Brown, Matt Sinden and John Yates.

Appendix 3: Author Acknowledgements

I would like to extend my sincere thanks to the companies who supported the research. They recognised the importance of independent research and provided help without a desire to influence the findings. They include BP, Barclays, Johnson Matthey and Scentre Group.

A huge thank you to the members of the Advisory Council who dedicated significant time and attention to the study: Alex Hawley, Derek Porter, Steve Brown, Matt Sinden and John Yates.

Most of the people I interviewed did so on the condition of anonymity, so I cannot thank them individually. The study has been improved as a result of their willingness to share their expertise. I am always impressed with the way in which security professionals are willing to collaborate for the common good.

I would like to thank a number of individuals who contributed in a variety of ways: Brian Allen, Matt Grant, Jon Gregory, Tim McNulty, Christian Plate, Tim Rawlins, James Smith, Oliver Tattersall, James Turner, Simon Vaughan-Edwards, and Harriet Wood.

Thanks to those who have helped with the production and dissemination of this report: Tom Hampson (Hampson Studio), Sophie Gillespie (Inkwell Communications & Design), and Jo Sayer (Virtual Alchemists).

Finally, I would like to thank Paul, Bandit and Dot for making life joyful.

All errors are, of course, my own.

Rachel Briggs OBE, 14 April 2025

Endnotes

1 *Global Risks Report 2024*, World Economic Forum

2 *Global Risks Perception Survey 2022–2023*, World Economic Forum

3 *Black swans, gray rhinos, and silver linings: Anticipating geopolitical risks (and openings)*, Grant, Haider, and Raufuss, McKinsey & Company, 2023

4 *Global Risks Report 2024*, World Economic Forum

5 *Global Cybersecurity Outlook 2024*, World Economic Forum

6 *Global Risks Perception Survey 2022–2023*, World Economic Forum

7 *Board members seek ERM benchmarking data*, Diligent, 2024

8 *Break Down Silos for Visibility into Enterprise Risk*, Richard Chambers, MIT Sloan Management Review, 2025

9 *Global Risks Report 2025 Insight Report*, World Economic Forum

10 How cybersecurity boosts enterprise reinvention to drive business resilience, State of Cybersecurity Resilience 2023, Accenture, 2023

11 *Former contractor shuts down British Museum's IT systems, gets arrested*, DCD, 2025

12 Insider threat a hidden risk to organizational growth, Forbes Magazine, 2024

13 *Voice Phishing (Vishing) Response Report*, Keepnet, 2024

14 Finance worker pays out $25 million after video call with deepfake 'chief financial officer', CNN, 2024

15 Global Cybersecurity Outlook 2025, World Economic Forum, 2025

16 *The Business Value of Corporate Security: Sustainable commercial success through resilience, insight, and crisis leadership in a volatile world*, Rachel Briggs, The Clarity Factory, 2023

17 Security Convergence and Business Continuity, ASIS 2022. Please note, the ASIS study looked at convergence of two or more of physical security, cyber security and business continuity.

18 *The Heart of Change: Real-life stories of how people change their organizations*, John P Kotter and Dan S Cohen, 2002

19 Quoted in *Switch: How to change things when change is hard*, Chip Heath and Dan Heath, 2010

20 Quoted in *Switch: How to change things when change is hard*, Chip Heath and Dan Heath, 2010

21 Security Convergence and Business Continuity, ASIS 2022

22 'As the World Shifts, So Should Leaders', Nitin Nohria, Harvard Business Review, July-August 2022

23 *The Business Value of Corporate Security: Sustainable commercial success through resilience, insight, and crisis leadership in a volatile world*, Rachel Briggs, The Clarity Factory, 2023

24 *The Business Value of Corporate Security: Sustainable commercial success through resilience, insight, and crisis leadership in a volatile world*, Rachel Briggs, The Clarity Factory, 2023

25 How cybersecurity boosts enterprise reinvention to drive business resilience, State of Cybersecurity Resilience 2023, Accenture, 2023

26 *Switch: How to change things when change is hard*, Chip Heath and Dan Heath, 2010, p.242

27 *Switch: How to change things when change is hard*, Chip Heath and Dan Heath, 2010

28 Cyber Security Leadership is Broken: Here's how to fix it, Richard Brinson and Rachel Briggs, Savanti 2022

About The Clarity Factory

The Clarity Factory is an engine room generating knowledge, insights, and practical solutions for our increasingly complex world. We use our data to help clients benchmark against peers, stay on top of best practice, and strive for continual improvement and innovation. We run workshops and training to grow and develop the skills and competencies that security leaders and their teams need to deliver maximum value for their organisations.

The Clarity Factory creates clarity from complexity – to enable our clients to thrive.

The Clarity Factory can help you in the following ways

- Consult on ways to optimise the relationship between your physical and cyber security teams by using our Holistic Security Maturity Model.
- Deliver a benchmarking study to help you understand how you compare to your peers, with actionable insights to improve either your overall programme or a specific area of work.
- Work alongside you to improve your programme.
- Deliver training to elevate your team, such as our Storytelling for Security Leaders workshop in partnership with HumanStory.

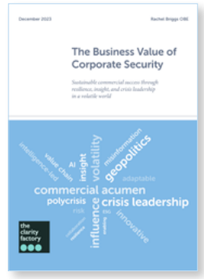
Sign up to our monthly newsletter

https://www.clarityfactory.com/subscribe

Get in touch

info@clarityfactory.com

Other reports by 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, 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

Connected Corporate Security: How to manage threats and risks with a unified model

The Clarity Factory and Ontic, 2024

Corporate Security: Securing Future Talent,

With Kathy Lavinder,
SI Placement and
The Clarity Factory, 2024

the clarity factory

Holistic Security

Major multinationals face elevated and interconnected security risks. As criminals, terrorists and nation states target across digital and physical domains, a siloed approach to security leaves companies exposed.

Convergence is a proposed solution, but only 15% of companies have merged their physical and cyber security teams due to the sizeable effort involved in organisational restructuring. Companies need a more nimble and flexible way to achieve joined-up security.

***Holistic Security* is a pragmatic framework to achieve partnership between physical and cyber security.** Holistic security is an outcome, not an organisational structure, drawing together the knowledge, data, and resources of both functions through smart team working and shared technology.

The Holistic Security Maturity Model is a tool for companies and offers practical and proportionate steps to optimise the partnership between physical and cyber security to deliver better security outcomes and enhanced operational resilience.

***Holistic Security* delivers a holistic response to today's holistic threat environment.**

ISBN 978-1-7384176-1-2
9 781738 417612

www.clarityfactory.com