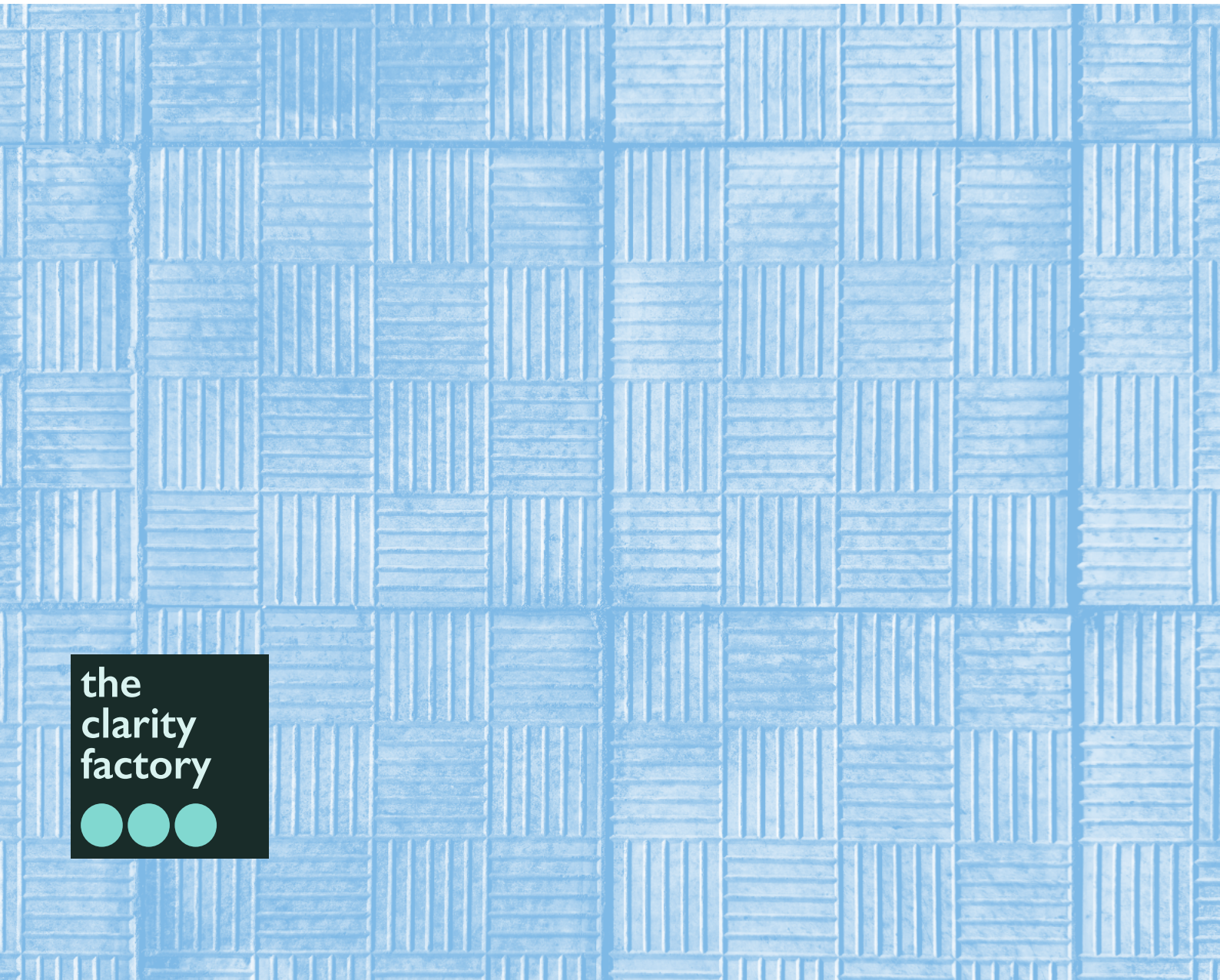
June 2025

Rachel Briggs OBE

Executive Summary

Holistic Security

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



the clarity factory

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.

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

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

1 *Global Risks Report 2024*, World Economic Forum

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.

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.

bp BARCLAYS JM Johnson Matthey SCENTRE GROUP

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.**