EXECUTIVE SUMMARY

SECURITY CULTURE

A STRATEGIC CAPABILITY THAT BUILDS RESILIENCE IN A VOLATILE WORLD

Rachel Briggs OBE
the clarity factory

The ASIS Foundation is sponsored by

EXECUTIVE SUMMARY

A woman claiming to be a contract cleaner calls the organization's helpdesk late at night to request her security pass be reissued. The operative, who is just about to finish his shift, goes ahead with the authorization as he's keen to close the matter and get home to catch the end of the football game. The following morning, CCTV footage shows expensive equipment being removed from the building, and the real cleaner turns up to find her pass is not functioning.

A team member holds the door open for a builder carrying equipment who signals he can't get to his security pass in his pocket. When they break for lunch, colleagues realize wallets and handbags have been stolen from their desks.

Colleagues notice that John doesn't seem himself. He's staying late after the end of his shift at the warehouse, keeping to himself on breaks, and yesterday turned up to work in an expensive new car. When a routine stock count reveals a significant amount of high-value product is missing, colleagues wonder whether John is involved. But he's a nice guy and they don't want to get him in trouble, and the local security manager tends to overreact. They decide to stay quiet.

Many organizations today operate in a complex and volatile security environment, facing a wide range of threats, including everything from crime, terrorism, espionage, and cyberattack to activism, workplace violence, and supply chain disruption. These threats present physical, digital, geopolitical, and insider risks the organizations must manage.[1][3] Security teams play a critical role in preventing, mitigating, and responding to these threats as they protect people, assets, information, and operations.[2]

Security teams are only part of the story. No matter how well-designed security governance structures, controls, and technologies may be, they cannot on their own deliver secure outcomes at scale. Security is ultimately enacted through the everyday actions, decisions, and behaviors of employees, contractors, and partners. As the fictional examples above demonstrate, when people feel pressured, confused, disengaged, or fearful of consequences, even the strongest security frameworks can be undermined.

WHAT IS SECURITY CULTURE?

This report uses the term "security culture" to describe the behavioral and social infrastructure that enables security strategies to function in practice and draws on the definition of the International Civil Aviation Organization (ICAO): Security culture is "a set of security-related norms, values, attitudes, and assumptions that are inherent in the daily operation of an organization and are reflected by the actions and behaviors of all entities and personnel within the organization, from the ground up and top down."[3]

The behavioral models examined in the report, such as human factors in security, psychological safety, environmental influences, social proof, and rational choice theory, have several implications for security culture:

- Controls do not guarantee compliance.
- Employees balance secure behaviors against competing priorities: commercial urgency,

pressure from managers, staffing constraints, or pressure to find workarounds when security systems are not user friendly.

- Employees may also lapse in their practice of secure behaviors if they are distracted or fatigued in fast-paced or stressful work environments.
- Employees don't generally "think security." They need security teams to make it easy for them to play their part through sensible policies and clear communication.
- Incentives are more important than penalties in influencing behavior.
- Employees need to feel positively towards security and be confident of the difference they can make.
- People influence people—especially leaders, managers, and workplace influencers.
- Knowing the right thing to do is a prerequisite, but knowledge alone does not change behavior. Employees must also understand the threat is real, be reminded to play their part, feel that others are doing likewise, and be subject to user-friendly policies that are easy to understand.

A healthy security culture is one where most employees, most of the time, confirm the following statements:

- I have a role in keeping our organization safe and secure.
- I understand why it matters for me to play my part.
- I know what I must do to play my part.
- Playing my part is worth it.
- I can do what's needed of me with minimal friction in terms of time and effort.
- I feel incentivized and recognized to play my part.
- I believe others are also playing their part.
- I feel comfortable speaking up if I have made a mistake or notice something that might impact safety and security.

THE EVOLUTION OF SECURITY CULTURE

The understanding of what security culture is has evolved in recent years. It was once treated as little more than an issue of training and awareness, however experience shows knowledge alone does not reliably change behavior and culture cannot be "trained into" an organization without attention to environment, incentives, accountability, and psychological safety.[4] Security culture is now increasingly recognized as a multifaceted program reinforced by leadership and governance, and one which sits at the heart of organizational resilience.

A FRAMEWORK FOR SECURITY CULTURE

The report sets out a framework for security culture that encompasses six factors, and provides supporting data, academic concepts, and practical examples for each one:

1. **Attitudes:** Do employess care about security?
2. **Knowledge:** Do employees know what is expected?
3. **Behavior:** Do employees do what is expected? What do they see others doing?

4. **Communication:** Do executives and security leaders communicate security in a relatable and understandable way?

5. **Compliance:** Are policies sensible and easy to follow?

6. **Empowerment:** Do employees feel able to play their part?

Embedded in the framework is the conception that security culture needs to account for national cultural norms, applicable legal and regulatory requirements, third parties and the extended enterprise, and organizational change and transformation initiatives.

DESIGNING A SECURITY CULTURE STRATEGY

A security culture strategy provides the structure needed to define priorities, target specific risk related behaviors, and ensure that interventions reinforce rather than contradict one another. Without such a strategy, security culture efforts risk becoming reactive, fragmented, and dependent on individual enthusiasm rather than organizational commitment, which ultimately limits the impact of the effort.

The report sets out a five-point plan to build a security culture strategy:

1. ***Define the purpose and scope of the security culture program,*** being sure to align security culture with executive priorities and framing it as a lever for business advantage that supports operational resilience, strengthens business continuity, improves crisis response, and protects reputation and competitive position.

2. ***Understand the risk context,*** including grounding the strategy in the organization's risk profile and appetite, defining priority employee groups, and ensuring the strategy takes account of national cultural norms, applicable legal and regulatory requirements, third parties and the extended enterprise, and organizational change and transformation initiatives.

3. ***Incorporate all six factors of security culture:*** attitudes, knowledge, behavior, communication, compliance, and empowerment.

4. ***Measure, collect feedback, and learn and adapt,*** including a baseline measure against which to track progress, a cadence for measurement, and a small but manageable set of metrics that can grow as the program matures.

5. ***Plan for sustainability across sites and time*** by incorporating redundancies, local capabilities through security champions networks, and building a multilayered program.

MEASURING SECURITY CULTURE

Measuring security culture is challenging[5] and cannot be captured in a single measure, but organizations can combine data across the six factors to build a picture of the health of security culture and where they should prioritize their efforts. Security leaders should assemble a range of measures to set a baseline and track performance against the six factors of security culture. Organizations should look first to use existing datasets such as incident reporting, GSOC data, access control data, or requests for travel security briefings. Organizations can then consider if other data sources need to be developed to enhance how security culture can be measured. In addition to determining what measurements apply, organi-

zations need to determine how the data will be used and by whom. At the outset, organizations should develop a baseline so they can track progress and understand which interventions are making a difference.

Security leaders must grapple with several challenges in relation to security culture metrics, including the risk of designing metrics that distort behaviors in unintended ways;[6] misreading increased reporting as a sign of deteriorating security performance rather than better employee engagement;[7] attributing cause and effect too liberally, which can dent credibility with executives;[8] generalizing findings from data in a way that obscures local trends and can lead to blunt interventions;[9] evoking metrics fatigue, ethical concerns about surveillance, or blame culture, which can erode trust and reduce employee engagement;[10] and focusing on lagging versus leading indicators that provide a more forward-looking view of security culture.[11]

THE CASE FOR SECURITY CULTURE

The current global operating environment strengthens the case for treating security culture as a strategic capability rather than a supporting activity because of increased vulnerability at the physical-cybersecurity interface, heightened regulatory and governance expectations, and accelerated adoption of AI and other emerging technologies. Evidence points to the role of security culture in improving crisis response and resilience and reducing the likelihood and cost of security incidents.

ABOUT THIS REPORT

The primary audience for this report is ASIS International members, the majority of whom are physical security professionals. The report provides a framework that can be adapted to any organization regardless of size, type, or sector.

While the report is written with physical security practice in mind, it draws on insights, frameworks, and evidence from cybersecurity. There are many reasons for greater partnership between physical and cybersecurity teams: the converging threat environment requires joint approaches to tackling behavioral challenges; research and practitioner interviews suggest some cybersecurity teams are more advanced in how they approach security culture and therefore have useful lessons to share; while some tactics may differ, overall approaches are similar across both disciplines; and physical and cybersecurity teams can achieve economies of scale by cooperating rather than competing for employee attention on what are often similar and complementary messages.[12]

By the end of this report, readers should have a clearer understanding of how to develop and sustain a healthy security culture, how to make security culture work in their organizations, and how to share the value of security culture with senior leaders and boards in meaningful ways. The ultimate aim is to equip security practitioners with the skills and knowledge needed to embed security culture as a normal, supported, and effective part of everyday work, thereby strengthening organizational resilience, security performance, and crisis capability.

Finally, the report highlights several challenges and calls for more research to address knowledge gaps, including an imbalance of data relating to cybersecurity over physical security, limited exchange between these two security groups about ways to collaborate on security culture, a paucity of data on executive attitudes to security culture, the need for more examples of security culture in action, and the fact that AI is developing at exceptional speed, meaning that some elements of the report may feel dated quickly.

The report is based on several research methods, including interviews with security leaders and security culture practitioners in organizations from a range of sectors; work with twenty companies as part of a security culture roundtable facilitated by The Clarity Factory; interviews with experts in security culture, behavioral science, user design, security champions networks, human risk, metrics, and organizational culture; and a thorough and wide-ranging literature review.

ENDNOTES

[1] *The Global Risks Report 2026,* World Economic Forum, 2026

[2] *Annual Chief Security Officer Survey 2025,* Rachel Briggs, The Clarity Factory, 2025

[3] International Civil Aviation Organization Security Culture Definition, ICAO, 2017

[4] The Security Culture Playbook: An Executive Guide to Reducing Risk and Developing Your Human Defense Layer, Perry Carpenter and Kai Roer, 2022

[5] "The New Analytics of Culture," Matthew Corritore, Amir Goldberg and Sameer B Srivastava, *Harvard Business Review,* Jan-Feb 2020 - https://hbr.org/2020/01/the-new-analytics-of-culture

[6] *Problems of Monetary Management,* Charles Goodhart, 1975

[7] *Psychological Safety and Learning Behavior in Work Teams,* Amy Edmondson, 1999

[8] *Organizational Culture and Leadership,* Edgar Schein, 2010

[9] *Sensemaking in Organizations,* Karl Weick, 1995

[10] *The Ethics of Workplace Surveillance,* Lyon, 2007

[11] *Leading and Lagging Indicators in Safety Management,* Hopkins, 2009

[12] *Holistic Security,* Rachel Briggs, The Clarity Factory, 2025

ABOUT THE AUTHOR: RACHEL BRIGGS OBE

Rachel Briggs OBE is a leading expert on security and advises corporate and cybersecurity leaders from some of the world's largest multinational corporations. She is author of *The Annual Chief Security Officer Survey 2025 and 2026, The Business Value of Corporate Security and Holistic Security,* whose Holistic Security Maturity Model is used by CSOs to measure the collaboration efforts of their teams. Rachel received the International Security Management Association (ISMA) Outstanding Achievement Award in 2016, is a board member of the Risk and Security Management Forum (RSMF) in the United Kingdom, and an Associate Fellow of Chatham House. She was awarded an OBE by Her Majesty the Queen in 2014 for her services to hostages and their families. https://www.linkedin.com/in/rachel-briggs-obe/

ABOUT THE CLARITY FACTORY

The Clarity Factory is a research and consultancy firm serving physical and cybersecurity teams in multinational corporations. Its purpose is to enhance resilience by helping corporations to keep their people, assets, facilities, systems, data, and intellectual property safe and secure. It does this by delivering research and benchmarking data, consulting and advisory services, and training and professional development workshops.

The Clarity Factory's Annual CSO Survey has become the go-to resource for CSOs and their teams on corporate security management trends. It provides data on security and geopolitical risks, use of technology and AI, talent and teams, resourcing, the role and scope of corporate security teams, reporting levels, KPIs, and more. The survey report is published free of charge in September to promote learning within the security industry.

The Clarity Factory works with some of the world's largest corporations, who rely on its extensive data, thought leadership, and expertise to help them deliver mature, business-aligned security and resilience programs. It runs benchmarking studies, maturity assessments, and bespoke advisory and consulting projects. It also convenes industry roundtables to promote peer learning and networking on specific priority topics. This includes a Security Culture Roundtable, comprised of twenty companies.

The Clarity Factory also runs webinars, in-person events, and storytelling workshops. It provides briefings for CSOs and their teams on corporate security trends and best practices.

The Clarity Factory was founded by Rachel Briggs OBE, a recognized thought leader on security, who has advised dozens of Fortune and FTSE 100 companies over 25+ years. The Clarity Factory has teams in the UK and US.

Subscribe to The Clarity Factory's monthly newsletter for data, insights, and news: https://www.clarity-factory.com/subscribe. Access The Clarity Factory's data and insights: https://www.clarityfactory.com.