

Key Findings from

THE INFLUENCE OF SECURITY RISK MANAGEMENT

Understanding Security's Corporate Sphere of Risk Influence

Funded by



FINDING SEVEN:

SECURITY AS A BRAND LACKS PROFESSIONAL RESPECT, COMPARED TO TRADITIONAL PROFESSIONS

The study uncovered a perceived degree of professional disrespect for corporate security. Many participants acknowledged that security professionals often learn their business through policing or military careers, as opposed to formal university education. Participants noted that professional certification on its own does not engender, at senior levels, the same respect as formal university education. It was therefore expressed that fostering the security “pracademic” is a key to developing appropriate business skills and respect, coupled with security industry certification, practical experience, and individual expertise. While the research indicated this is changing, such change was seen at the individual level rather than culturally at the industry or sector levels, resulting in a perception of an educationally inferior profession.

Perception of security played a salient role in the influence given to the function, and participants agreed that security is subject to several negative connotations. Most participants, including those from the regulatory risk-mature industries, acknowledged that the inherited stereotypes of security continue to be a significant hurdle in security achieving stronger organizational influence. Participants discussed the security function as being seen as the “corporate police,” “naysayers,” “doomsayers,” “...just guards, gates, and guns,” “a paramilitary role,” and “dark figures,” among others.

Furthermore, it was highlighted that in the C-suite, the security function is rarely seen or heard from unless there has been a significant incident that has a strategic implication or loss. The negative connotation was also frequently paired with the notion that security is perceived as providing little value; being dubbed “a drain to the bottom line,” where “security always comes at a cost...it never actually gives you anything.” This narrative linked the negative connotations of the security function to the fact that if physical security is being done correctly then it is invisible and the visible elements such as the

guards and gates, typically control areas, reduce access and limit freedoms. Corporate security managers said the negative perception of security is the most significant issue, as one manager stated “I genuinely think the optics of the role is the biggest hurdle we’ve got.”

Participants also highlighted the perception of risk from security managers as a limitation. A tangible lack of understanding of risk beyond the matrices used led to security managers desiring to be called “security risk professionals” instead of a more accurate description: that they are security managers with an understanding of security risk. Nonsecurity executives suggested that security professionals using the title “security risk professional” would be met with derision among their peers specifically qualified as risk managers. While this view was not consistent across all participant, it was held by participants in the executive and nonsecurity roles, uncovering a significant negative perception of the security function from more senior managers. Such attitudes reinforce the notion that security risk assessment is a box that needs to be checked by following a template, and that security risk should be disconnected from the broader organizational risk context. This issue was discussed by one participant, stating:

The security perception of risk is just using a template that identifies impact and likelihood and using that to justify whether to have one guard or two. Security is no more risk focussed or linked than the layman doing an HSE [health, safety, and environment] assessment for a school sports day. Security should be a specialist risk type, under a broader operational risk framework.

The poor understanding of the corporate security function at the board level is also

a barrier. A disconnect emerged between the perception of the security managers and the executive or nonsecurity: Corporate security managers often expressed that C-suite or board-level decision makers do not value security risk because they do not fully understand it or its importance. Conversely, when discussed at executive and external consultant level, the response centred on there being no need for the board to understand security in this way—this was the role of the specialist—with the crucial requirement being not the ability to translate specialist security knowledge for the board to understand, but the ability to communicate the security risk in business organizational risk terms and language for the board to be able to compare and utilize.

Professional disrespect was also highlighted during the discourse as a significant barrier to risk influence. Our research showed that the role of the security professional often is seen with a degree of disrespect, and despite the accepted growing awareness of risk, participants found that the role of security was discounted in discussions of risk at the board level, with participants attributing this lack of respect to numerous factors. The factors included the perceived misuse of the term security risk professional and the traditional trajectory into security, with many security managers emerging from military or law enforcement backgrounds with significant operational, but very limited corporate or business, experience. Embedded in this view was that the board often perceived the security professional as educationally inferior to other organizational professionals, such as lawyers or accountants, who have sound vocational degree qualifications.

The study recommends engaging with renowned business schools and associations through membership and educational opportu-

nities, to learn business metrics and language. Additionally, embracing formal registries for members who hold recognised tertiary degree qualifications as a mandatory requisite. This approach would enhance and reinforce their status of the registered security professional towards overcoming disrespectful negative perceptions of educational inequality.

Furthermore, professionals should strive to improve communication and imbed understandings of how security contributes to corporate success across all levels of business. It is only through such engagement that the benefits of enterprise security risk management can be communicated, and influence achieved with general managers and boards.



This is part of a series of nine short synopses, this paper explores the findings of an ASIS Foundation study conducted by Dr. Michael Coole, Nicola Lockhart and Jennifer Medbury of Edith Cowan University in Australia in 2022.

The ASIS Foundation, an affiliate of ASIS International, helps security professionals achieve their career goals with certification scholarships, practical research, member hardship grants, and more. The Foundation is supported by generous donations from ASIS members, chapters and organizations. Online at www.asisfoundation.org.