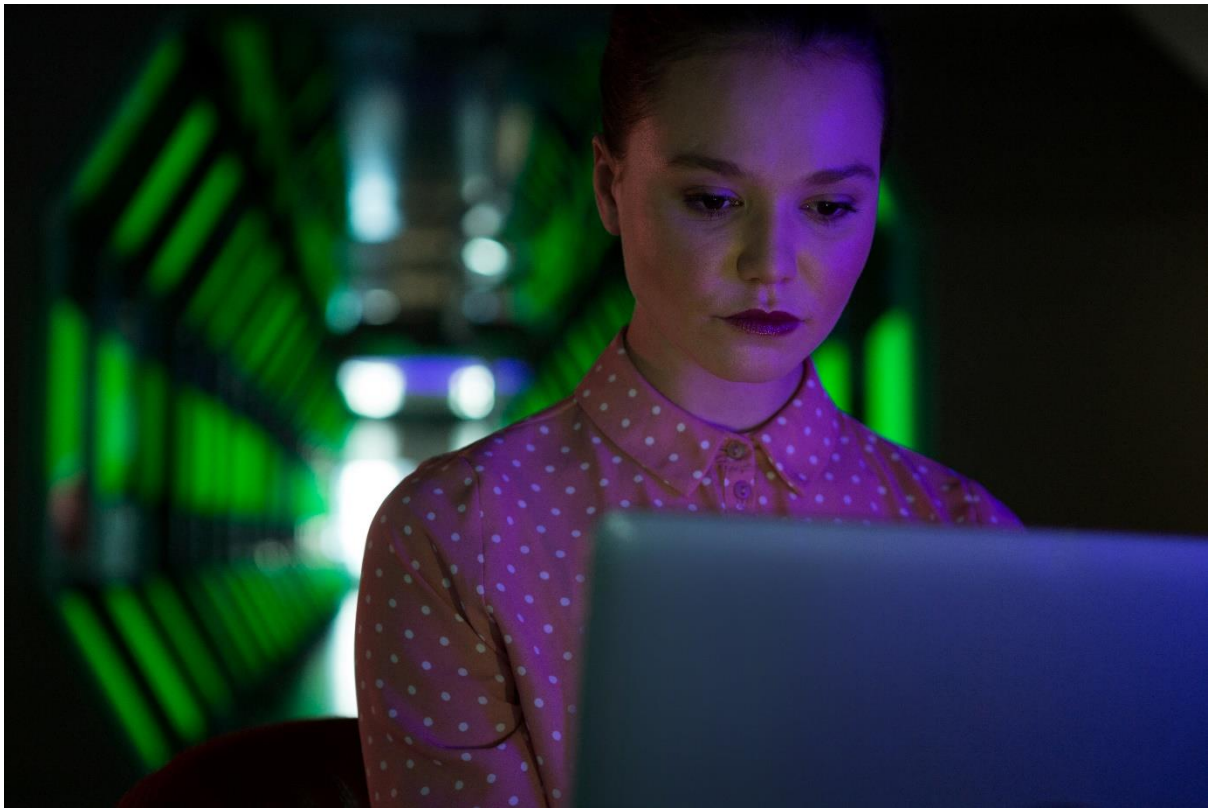
Information Security Leaders: Trailblazing Comprehensive Security Management

Written by Joshua Bucheli, AI Ethics Researcher and Fellow at the ForHumanity Center, in Collaboration with Dr. Doron Zimmermann, Chief Cybersecurity Officer, and Peter Kosel, Founder of cyberunity



Running a successful business largely comes down to setting the right priorities and mobilising the right people towards fulfilling them. While these priorities may vary considerably depending on sector, one remains ubiquitous, and yet underappreciated – security.

The issue of corporate- and cyber-security is often likened to a sort of silent war that rages all around us without most of us even noticing – a battle between those who protect our digital assets and those who aim to exploit them.

While cliché, there is something to be gleaned from this combative analogy for cybersecurity:

Just as an effective army consists of both well trained soldiers *and* shrewd generals, effective corporate cybersecurity comes down to both capable specialists *and* savvy leaders.

A business can have all the cryptographers, cloud security specialists, phishing experts, security scouts**,** and awareness specialists it wants at its disposal. Unless these human assets are recognised, hired, coordinated, and mobilised proactively by prudent leaders who genuinely understand and appreciate the needs of security, their potential will largely be rendered moot.

Where Does Corporate Security Stand Today?

According to Maslow's famous hierarchy, security ranks second only to physiological factors in the pecking order of human needs. What is often still underappreciated, however, is that the same holds true for businesses.

The advantages of an integral approach to security strategy are still not sufficiently recognized, even though this is the foundation for any sustainable relationship with employees and customers in terms of quality assurance. The burden of rectifying this rests primarily on the shoulders of boards of directors and c-suite management, who will need to define, design, and ultimately implement and emphasise the relevance of and demand for security throughout their companies.

Another key dimension of the implementation of comprehensive security strategies is the acquisition of specialists who can breathe life into this challenging and future-oriented issue. If companies only put out feelers when a need for additional expertise has been identified, it is already much too late, as Peter Kosel, founder of cyberunity AG, points out. A modern approach to recruiting is one that thinks at least one, if not two steps ahead, reaching out to and building relationships with potential future employees *before* vacancies arise. The name of the game is *KNOW* YOUR TALENTS not *WAR* FOR TALENTS.

Conversations about corporate security often focus on its piecemeal, bottom-up operational dimensions, saying little of how security ought to be approached holistically by executives, managers, and specialists.

Businesses will also often downplay risks, pointing to the considerable costs associated with comprehensive security strategies. But this is a mistake – bottom lines are jeopardised far more by a lax approach to security than by the short-term investment that it requires – not to mention the myriad hidden benefits that security can bring to a business.

"Security is still often looked at as a low priority peripheral support process, when really it is a fundamental management process that necessitates careful investment in sustainable relationships with customers and stakeholders. Integral corporate security lies at the very foundation of any company's survival, whether or not that company's leaders realise it", says Dr. Doron Zimmerman, Chief Cybersecurity Officer.

Where is Corporate Security Headed?

As Doron points out, executives are getting more involved in conversations about security and businesses are beginning to look at security through the lens of risks and threats, rather than merely as a subsidiary responsibility of IT departments:

"Analysing what hazards exist, determining which are relevant, and then prioritising them accordingly is slowly becoming a standard part of management level responsibilities. Considering these threats in relation to the strengths and weaknesses of the company in question is also an increasingly common and encouraging development."

While limited in scope, such practices are a step in the right direction in terms of bringing business leaders into the security fold. A genuine commitment to security on the part of managers and an honest consideration of risks is the only thing that will allow companies to get ahead of the ever-evolving threats of the digital world.

Businesses are focused on ensuring a stable environment in which they can conduct their business:

“They want to make sure that their products, services, and solutions are so safe, that they are able to keep their existing clientele while at the same time gaining new customers. On top of this, it is well within the interest of any serious entrepreneur to provide appropriate security measures in the workplace so that employees can continue to rely on a secure workplace in the future. If, for example, a company is crippled by a cyber attack, then depending on the duration of the ensuing operational downtime, the very existence of the company itself, and the jobs it provides, is threatened”, says Doron.

The only way to achieve this security is through a comprehensive strategy, and this must be guided and managed. Effective security must be conceptualised broadly and actively not only from the bottom-up, but from the top-down, with executives and managers setting out a clear vision of what security is supposed to help a business achieve *before* they turn to the operational side of things and consult or hire specialists.

Information Security Leaders – Hard Skills and Qualifications

Because comprehensive and innovative security is such a fundamental aspect of corporate survival and success, technically savvy security strategists (CISOs) who can help internalise this reality into the very ethos of a business will be indispensable. Security is a dynamic issue and it is key that these individuals be able to foresee and respond to its evolving needs accordingly.

Nevertheless, CISOs with degrees in cybersecurity and the usual certificates like CISSP, CISA, CISM etc. will not be enough: “These are impressive titles and qualifications, but they do not guarantee that a comprehensive and holistic security imperative is being pursued and internalised”, cautions Doron.

In practice, it is still all too often the case that security managers with strong IT backgrounds are hired in order to quickly fix urgent security gaps, rather than security strategists who see the big picture and who can act proactively to avoid such situations in the first place.

As has already been emphasised, security is often approached too operationally. In order to rapidly address the issue of safety, where it has been neglected, and as a result of an understandable urge to quickly demonstrate initial successes, compromises in terms of standards and personnel are still all too commonplace. Admittedly, such approaches bring results, and have their place within corporate security strategies, but they can lack the long-term thinking that information security leaders need to bring to the table.

Such perspectives are best sourced from backgrounds in security-management and policy making. So called ‘Defence Intellectuals’ coming from highly strategic risk-mitigation fields ranging from ex-law enforcement or military personnel to foreign affairs professionals and intelligence analysts can bring robust strategic and analytical skills to corporate leadership teams.

Besides a general understanding of risk- and corporate-management, professionals hoping to help set the course for corporate security will need to be able to develop procedures and guidelines, mandate practically applicable trainings, oversee inspections and audits, set priorities, and innovatively dedicate limited resources accordingly.

When all is said and done, what corporate security leaders need to be able to do is bridge the gap between IT and management. Certifications that combine cybersecurity- and risk-management essentials, like CISSP, CRISC, and especially CISM, will give future leaders a considerable edge over the competition in this respect.

Beyond Technical Know-How:

Hard skills, certificates, and experience in approaching risk identification and management holistically can only take security leaders so far. Without people skills and an honest appreciation of the stakes at hand, the vital link that leaders represent between IT and management will remain tenuous at best.

For example, adaptability, out of the box thinking, and the ability to maintain a level-head under pressure are key attributes for anyone hoping to contend with the threat landscape of modern corporate security. A strong network in the security-community and a general passion for matters of security leadership demonstrated through attendance at functions like the ASIS Europe Conference will likewise be an undeniable asset.

Beyond this, an appreciation of the importance of security and the ability to act as an advocate for the change that needs to happen in the industry is also critical. Oftentimes security leadership job descriptions focus heavily on operational dimensions. In such cases, it will be up to aspiring corporate security leaders to help employers recognise the importance of a holistic approach to security.

“Human beings are the source of security, but they are also the source of vulnerabilities. In this sense, security is a ‘people-business’ – a social matter”, says Doron. Indeed, studies have shown that 99% of data security breaches are the result of human error.

In a world where something as innocent as plugging in an unknown USB drive can bring a business to its knees, defending against increasingly common threats ranging from phishing attacks and ransomware to full blown hacks is largely a matter of mitigating insider threats. This will come down to communicating effectively with both individual security teams and regular employees about how best to protect the business.

All said, there is no single formula for an effective security leader and this has a lot to do with the fact that it is a role that is still largely being defined. What is for sure though, is that it will be the very people who fill these roles, who will play the biggest part in defining them, not to mention the future of corporate security in general.

As Peter Kosel concludes, a strategic anchoring of the issue within corporate visions and missions is essential in order to satisfy the fundamental security needs of employees, customers, and of corporate environments as a whole – installing fire extinguishers makes sense as an emergency precaution, but what are companies doing to ensure that they never have to be used in the first place?