A complex and dynamic landscape

Peter French MBE, Managing Director, SSR Personnel examines industry trends and highlights some of the challenges facing security professionals in Europe

The World Economic Forum convened its 54th Annual Meeting in Davos in January 2024 on the theme 'Rebuilding Trust', emphasising the need for cooperation and shared solutions in a world facing challenges such as climate change, geopolitical issues and cost of living crises. This built on the World Economic Forum Global Risks Report 2023, which uses Polycrisis to explain how "present and future risks can also interact with each other to form a 'polycrisis' – a cluster of related global risks with compounding effects, such that the overall impact exceeds the sum of each part".

> "EUROPE IS DELIVERING INNOVATIVE SECURITY SOLUTIONS ACROSS MANY AREAS OF PUBLIC AND PRIVATE LIFE."

At the heart of the research is the annual Global Risks Perception Survey which brings together insights from over 1,200 experts across the Forum's diverse network. When asked to rank the most severe short and long term risks, respondents identified cost of living crises as the most severe, immediate risk but saw failure to mitigate the climate crisis as the biggest risk ten years from now.

Europe is delivering innovative security solutions across many areas of public and private life. There has been an unprecedented period of job growth and unfilled vacancies after a period of accelerated growth following the pandemic. The war in Ukraine and a cost of living crisis is fostering civil unrest. Some economies have tipped into recession or heading for stagflation. Public finances will overspend from prudent fiscal targets, yet we are not experiencing commercial demand reducing.

ESG (Environmental, Social and Governance)

Ethical investors harassing corporations to polish their sustainability and ESG credentials has weakened in the first half of 2024. We have seen a growing emphasis on corporate sustainability and ESG considerations among investors, consumers and regulators. Corporate officers have been under pressure to integrate sustainability principles into their business strategies, address environmental and social impacts and report transparently on ESG performance. There is also an increasing corporate pushback against many agendas.

Fund managers are swayed by sustainability and risk resilience; employees of today and tomorrow want to know in general that they work for organisations that have good governance and project a compassionate profile. Most security professionals have progressed well in such organisations as this fits into their work areas. Boosted as well by political instability, CSOs we speak to have received additional analyst resources, providing the executive suite with real time demographics.

The world of cybersecurity

The future of cybersecurity in Europe is likely to be shaped by a combination of technological advancements, regulatory developments and evolving threat landscapes. Most corporations have been slow to appreciate they are being attacked, not just by high street gangsters, but those assisted by hostile nations for a myriad of reasons.

It has taken time to realise that the files being accessed during attacks on insurance companies were cyber-policies. Information available would be the level of cover held by corporations should data be locked in a ransomware attack; there is no point asking for €25m when cover was only for €20m. Obtaining a ransom, guaranteed by a third party, reduces operation time and lowers the chances of law enforcement intervention.

The EU has been at the forefront of implementing robust data protection regulations, such as the General Data Protection Regulation – a responsibility picked up by most security functions. Future regulations will continue to emphasise data protection and privacy, impacting how businesses operate in Europe approach cybersecurity.

Countries are enacting cybersecurity legislation to protect infrastructure and ensure the resilience of digital systems. This includes measures to combat cyber-threats, enhance incident response capabilities; this promotes information sharing among public and private sectors. As tech evolves, cyber-threats are becoming more sophisticated and diverse. Europe is likely to see an increase in cyber-attacks targeting sectors including government, finance, healthcare and energy. ▸

These attacks may range from malware and phishing campaigns to advanced persistent threats and ransomware. The adoption of emerging technologies such as AI, and the introduction of Gen AI, brings both opportunities and challenges for security. Europe should focus on leveraging this tech to enhance security capabilities while addressing risks and vulnerabilities. The European Union Agency for Cybersecurity (ENISA) is dedicated to achieving a high common level of cybersecurity across Europe and this year predicts that €130b will be spent to mitigate EU countries' cyber-risks.

Business landscape

Private and public sector CEOs face a complex and dynamic business environment characterised by technological disruption, regulatory scrutiny, geopolitical uncertainty and shifting stakeholder expectations. Success requires visionary leadership, strategic agility and a focus on innovation, sustainability and customer value. They will seek board expertise in emerging areas and a more dynamic board composition.

This is an opportunity for security leaders who face challenges holding the attention of their executive boards as their pandemic halo dims. Key to this is having a seat at the executive table or working with a board champion who can translate risk temperature for areas of the business.

The pandemic exposed vulnerabilities in global supply chains, prompting organisations to reassess strategies and enhance resilience against future disruptions. CEOs need to optimise supply chain operations, diversify sourcing and leverage digital technologies to improve visibility and agility.

> **"SUCCESS REQUIRES VISIONARY LEADERSHIP, STRATEGIC AGILITY AND A FOCUS ON INNOVATION, SUSTAINABILITY AND CUSTOMER VALUE."**

As workforce dynamics evolve, CEOs need to address challenges related to talent acquisition, retention and development in a competitive labour market. They need to embrace flexible work arrangements, invest in upskilling and reskilling initiatives and foster a culture of diversity, equity and inclusion to attract and retain top talent. Part of this is presenting security colleagues as integral for the area of operations they are responding to.

Meeting evolving customer expectations and preferences is essential for business success. CEOs will prioritise customer centricity, leverage data driven insights to

personalise experiences and invest in omnichannel capabilities to engage and retain customers in a competitive marketplace. Yet, the greatest danger to reputations could be a B2B transaction, which then becomes the other party's B2C transaction. This is where AI could transform oversight, monitoring social media platforms: Where are your brands being traded? Are there spikes in complaints?

The chief executive is fully accountable for ensuring corporate compliance with a myriad of regulations spanning areas such as finance, accounting, employment and industry-specific requirements. They need to maintain strong governance structures, foster a culture of ethics and integrity and proactively manage regulatory risks. This remains a strong suit for the security business manager negotiating with the business to undertake programs for protection. Moreover, today we still find corporations with no coherent travel safety programs.

Statista predicts the European physical security industry spend will reach over €34b by 2027 against a global expenditure of €117b. Just under 50% will be spent in guarding services in Europe. In Northern European countries, the hourly costs will exceed €30. There is cost disparity, but we are running out of quality labour to export across countries as employment costs rise. Therefore, it is for asset protection groups, even when outsourced, to integrate technical ways to monitor security into core ways of working and adapting to their environment. ■