Expert Insight

Leadership skills *for* tomorrow

Peter French MBE, Chief Executive, SSR Personnel discusses how blending professional experience with continuous qualifications shapes security leadership and drives the convergence of cyber and physical security amid evolving regulatory and skills gaps

Balancing experience and underpinning qualification through continuing professional development is the bedrock of professional sectors. Add personal experiences and you will begin to see how that moulds into organisational influence. It is people that drive corporate culture and most security leaders know that as they seek to protect the corporation from any of the Chief Executive's top five risks, they are protecting the corporation from its people. The world of security, like any other function, works overtime to attract, retain and promote talented people and develop leadership role models.

Security convergence

The reference to "security convergence" started to emerge in the 1970s as physical security systems began to incorporate more computing, networking and communication technologies. This included the development of computer-based access control and alarm systems. The term "cybersecurity" emerged in the 1980s.

The first commercial antivirus software appeared in 1987, marking a significant milestone in the formalisation of the field. Before this, the focus was more on protecting individual networks, rather than the broader cybersecurity network. The term was coined by William Gibson in 1983 in his novel entitled Neuromancer.

CISO v CSO

As technology continues to evolve, so does the need for cyber-protection professionals. The mantle of which emerges as the Chief Information Security Officer, alongside the Chief Technical Officer and Chief Information Officer. Today's digital protection leaders have a myriad of regulatory fences to navigate. Organisations are legally responsible for managing cybersecurity risks, particularly when processing personal data under EU regulation. A CISO position is not mandated, but having someone with strong cybersecurity expertise is crucial for compliance, good governance and essential when trading in multiple EU countries.

The World Economic Forum (WEF) established the Centre for Cybersecurity at the forefront of addressing these challenges. In their Cybersecurity Outlook 2025, they examined the trends and the impacts on economies and societies. The WEF this year highlighted the global talent shortage in cybersecurity; currently 3.5 million vacancies exist and it seeks to address it through frameworks and initiatives like the Cybersecurity Learning Hub. It hosts a CISO community to facilitate knowledge sharing and collaboration among cybersecurity leaders.

Convergence and opportunities

The convergence of cyber and physical security has been a trend integrating digital and physical security measures to address complex threats in an interconnected world.

Whilst security budgets are increasing for the protection of online commerce and data, the Chief Security Officer with a combination of professional experience – combined with an MSc in a technical field like organisational risk and resilience, or an MBA – helps make them business ready. Increasingly, we see CSO leaders choosing to take cyber-related qualifications as they are called upon for a risk review or may be involved in digital supplier due diligence. Their learning hubs are well catered for Europe and the U.S., to blend compliance, security and risk management.

A recent Information Systems Security Association (ISSA) report notes that the CSO tenure in post is typically longer than that of the average CISO. The CSO will build a unique relationship with senior management as they move towards the C-suite. This is a professional bond that is not readily replicated as the CSO accumulates a trusted role with the Board. ▸

> **"Balancing experience and underpinning qualification through continuing professional development is the bedrock of professional sectors."**

How will you double your digital protection budget every two years?

From the SSR Personnel European Insights report, spending in 2025 on digital protection budgets will exceed €45 billion. Statista predicts that when adding AI protection, Agentic AI and hardware upgrades by 2030, it will have increased to €100 billion. The UK National Cyber Security Centre (NCSC) has reported that in the past 12 months, there were 7.7 million cyberattacks in the UK. NCSC has launched Connect Inform Share Protect (CISP), a free platform for security professionals to collaborate on cyber threat information in a secure and confidential environment.

> **"ISSA research indicates that due to the age demographics of CISOs, there is a higher incidence of retirement."**

What is the effect?

How is the CISO coping with increasing legal scrutiny and regulatory cyber oversight? Not well, according to ISSA, over half of those surveyed claim that their job is stressful most of the time due to overwhelming workload, working with disinterested business managers and keeping up with the security requirements of new business initiatives. A third say it is very likely or likely that they will leave their current job within 12 months. Nearly half have considered leaving cybersecurity altogether, and most claim that they are frustrated because their organisation does not take cybersecurity seriously.

How is the CSO coping with increased regulation, reductions in physical budgets and consistency of threats balanced against the Boardroom's increasing risk appetite to deliver greater shareholder and executive wealth? In general, they are frustrated with unnecessary budget withholding (until a crisis response is required). Both operate in an increasingly interconnected, matrixed, technology-driven and polycrisis global environment.

ISSA research indicates that due to the age demographics of CISOs, there is a higher incidence of retirement, while others will move to lucrative portfolio or field CISO positions with security technology vendors.

The future deployment of AI

Khalifa Ibrahim Al Saleis, CEO of the Security Industry Regulatory Agency, addressed delegates at the Dubai ISJ Leaders in Security Conference 2025. His theme on AI in the workplace connected with leadership in the room, foreseeing a five-year timeline and introducing Vanguard AI, a developing self-learning intelligence system that will power the UAE in its goal to become a world leader in AI by 2031. Should we be considering the 1968 film 2001: A Space Odyssey and HAL (Heuristically Programmed Algorithmic Computer), a sentient artificial general intelligence computer that defends itself against astronauts?

Vanguard presented a real-world example that when designing the Burj Khalifa Skyscraper, it took three years and one million labour hours. Vanguard boasted it could have completed the design in a 24-hour AI day! Following Donald Trump's visit to the UAE, both countries signed an AI agreement that supports a US$1.4t investment commitment, to build and finance U.S.- operated regional data centres, the first being established in Abu Dhabi with five-gigawatts of capacity - enough to power a major city.

Many see trust in AI as the momentous point that humans will accept its rapid deployment and organisations will have to be ready to take opportunities. Security leadership must be ready to reconcile anomalies with co-working personnel and machines. One of which will work 24/7.

Leading law firms are now offering AI Solicitors for you to consult with. The AI accuracy prediction is 99.8%. The defendant is given an AI defence team. The AI prosecution presents its case and both sides will interview witnesses, video statements are taken and an AI magistrate supervises proceedings. Gone is the courtroom theatre, the surprise revelation. Will this lead to quicker justice?

If your career needs revitalising, consider undertaking the ISC2 Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM), addressing GDPR, NIS2, EU AI Act and other compliance frameworks. ■

About the Author

Peter J French was awarded the Member of the British Empire in 2010. He is the Chief Executive of SSR Personnel, a leading recruitment consultancy in the field of security risk, permanent or interim hire, with a significant workforce presence in Europe and the Middle East.