SSR Personnel recently carried out research into how technological innovation is transforming security and providing practitioners with powerful new capabilities. We have extracted five key pieces of wisdom from their contributors on how to understand the threats and benefits technology can bring security..

It is clear that the security sector is more technology driven than ever before. As Niall MacGinnis, Director of Group Security at Sky, says: "The future of security can be summed up in one word: technology. Technology will be the biggest asset to securing businesses and organisations and pose the biggest threats. Today's security professional needs a clear understanding of security technology and how to maximise its benefits."

So, how can security practitioners capitalise on the benefits and mitigate the threats that technology brings?

Here are five pieces of security wisdom:

One: Support the business

Two: Understand the expanded nature of the security risk

Three: Embrace the convergence of physical security and cyber security

Four: Integrate Systems

Five: Don't forget the human touch

One: Support the business

For businesses to survive, they must continually exploit the opportunities that technology brings. Today this is facilitating automation, enabling frictionless business activity, making it easier to demonstrate compliance with policy and regulations, and driving efficiency. Innovation will continue in delivery methodologies, particularly though biometric technologies and the adoption of cloud computing (including the challenges that go with this).

At the same time, businesses must operate securely and have efficient security environments. The best security systems support and sometimes enhance the business. Alistair Enser of Reliance Hi Tech says: "What benefits can we create for our customers through the smart use of technology, for example using footfall and behaviour analysis to predict events or manage building energy and usage? If we build smart, connected and highly integrated ecosystems with the many different types of sensors and devices available, we can not only secure a building or a company, but we can add value to their marketing, save them energy, increase their productivity, improve health and safety. The list is endless."

Michael Barley, Master of the Worshipful Company of Security Professionals, adds: "The security practitioner's approach internally, now and going forward, needs to be as a business partner rather than a provider of services. Greater integration in the day-to-day business is key. Security should be so embedded in the business that it works to take the risks out in order to help protect the bottom line."

Two: Understand the expanded nature of the security risk

Cyber threats resulting in breach or data loss and infrastructure failures impacting the business objectives are not new areas of risk to most organisations; however, the impact of these threats to the P&L objectives of the organisation are more severe than ever for both financial and reputational reasons.

The multiplied threat that technology brings cannot be underestimated. Werner Cooreman, Group Security Director, Solvay, says: "Expansion of cloud technologies, in combination with artificial intelligence (unleashed on all that cloud data) and creation of the Internet of Things (once 5G is fully deployed), will multiply the vulnerabilities. And security threats are already taking big advantage of the expanded attack surface of companies as a result."

He continues: "Taking a holistic enterprise security risk management approach has become the only way to stand a chance of increasing a company's security resilience. Focusing on mitigation of priority security risks (be they cyber, physical or other in nature), whilst enhancing the capacity to rebound from inevitable incidents, will be essential."

James Mulheron, technology, cyber and data risk professional says: "Emerging technologies, big data, advanced analytics and a deluge of regulation has changed forever how businesses need to address future cyber and technology risk landscapes. The threat landscape is changing daily and with that comes the need for individuals of strategic mindset and with a broad range of technology and data expertise to take hold of the organisation's technology risk portfolio and provide the Board with appropriately risk assessed and commercially viable solutions."

Alistair Enser, CEO, Reliance Hi Tech, concludes: "Today with the IoT, nearly everything we touch is networked. A lot of business is now less worried about the theft of a laptop or physical device than the data on it or disruption caused. The threats may come in through the network, not the front door, and often the damage can be reputational as well as physical.

capitalising on the benefits technology brings security

Three: Embrace the convergence of physical security and cyber security

The future of security will be dominated by the need to have physical security capabilities integrated with, and protected by, cyber security capabilities. Tony Anderson, G4S Fire & Security Systems, says: "In a world where every device is now IP connected, with online connectivity and remote diagnostics, the clear line that divided the two sectors is becoming blurred."

Four: Integrate Systems

Integrated security systems can bring multiple layers of security for greater effectiveness, efficiency and ease of use. This can involve integrating security systems such as video surveillance, access control, intrusion alarm, public address systems, automatic number plate recognition and tracking systems, together with corporate databases and systems, such as HR and facilities management.

Andy Ellis from Johnson Controls says: "Integrated systems are becoming more and more important as smart buildings start to dominate our cities' skylines. The future of security is knowing who is in your building, where, and when – and having instant access to every piece of data a building holds. This requires the best possible system integration, bringing together access management and cybersecurity with HVAC, lighting, fire safety and energy management in one central place."

Jamie Allam, Amthal Fire & Security, adds: "In commercial settings, intelligent buildings and corresponding management systems are quickly evolving to create smart workspaces. These now embrace flexible working and 'free flow' spaces to encourage productivity, collaboration and growth in a safe and secure environment."

Five: Don't forget the human touch

John Sheeran, Northern Trust Corporation, says: "The days of gates, guards and guns are long gone, replaced with facial recognition, biometrics and other state-of-the-art physical security detection systems; however, what cannot be replaced is the human element. The human will always be required as the start and end user to influence the systems we are using as the security landscape changes on an unprecedented basis."

Summary

Today's security professionals need to maintain a clear understanding of the business they are part of and how security and risk management can be of support. The key role of technology, both in terms of business enabler and top threat, must be recognised and prioritised in their approach. However, they must never forget that security is all about the people.

Eduardo Jany, Bloomberg Inc., concludes: "Today's security practitioners must have a solid understanding of their organisation's needs, their environment and an ability to look at things holistically, to determine what is available, what can be most reasonable and most practical. AI and automation combined with the IoT can mean improved efficiency and savings. The future of security operations, however, will not be one where machines or robots will be in total control. Machines will never deliver empathy or be capable of making decisions with flexibility based on the spirit of the law versus the letter of the law."

Peter French MBE oversaw this research for SSR® with this group of professionals and thanks all those that shared their visions of the future. Initial results of this research were originally published on IFSEC Global.

Peter French MBE
SSR® Personnel

www.ssr-personnel.com