

# THE FUTURE OF SECURITY: A CALL FOR PROACTIVE ACTION



Toro recently held a lively panel discussion with our partners Wilson James and Summis, featuring input from a room full of security experts. The conversation was dynamic, with insightful exchanges on how the threat landscape is evolving and the steps we collectively must take to stay ahead.

As the threat landscape changes many organisations still see security as a grudge purchase - something done out of obligation rather than as a strategic necessity. This mindset is creating significant roadblocks, particularly in securing budgets, educating key stakeholders, and implementing holistic risk management strategies. As security leaders we must drive the conversation forward, shifting the perception of security from a reactive fix to an essential enabler of long-term business resilience and success.

Security must no longer be viewed as a box-ticking exercise. The reality is that every organisation will face a breach at some point. Rather than waiting for that day to arrive, we must guide organisations to be proactive in embedding security into the culture, processes, and strategies of every business. This requires more than just technology - it demands an understanding of risk, the empowerment of people, and a commitment to ongoing education and awareness.

## Don't Scaremonger – Educate and Empower

Using fear to drive security decisions is an outdated and ineffective strategy, with security experts often not realising they are scaremongering when communicating security. Scaremongering often leads to resistance, especially from decision-makers who may not fully understand the complexities of modern threats. Instead of relying on fear, we need to frame security in terms of measurable outcomes that resonate with business objectives. Demonstrating the potential cost of inaction – whether it's financial losses, operational downtime, or reputational damage – can be far more persuasive than catastrophic predictions of disaster.

This approach requires better communication around risk management. Many organisations still struggle to grasp the full scope of their vulnerabilities or how to manage risk holistically. It's not just about identifying threats; it's about helping decision-makers understand the real-world impact and showing them how security investments can mitigate those risks. Rather than talking about theoretical dangers, leaders must present realistic scenarios and actionable solutions that reflect the current threat environment.

## Find a Common Language – Improve Communication in Risk Management

Effective communication is often the missing piece in security strategies. Technical jargon can alienate stakeholders who don't understand the nuances of security threats, leaving them disengaged, or sceptical, about the value of investing in new solutions. It's critical to bridge this communication gap by finding a common language that everyone – whether in security, IT, finance, or the boardroom – can understand.

Risk management is not a one-size-fits-all approach; it's about understanding the specific pain points, weaknesses, and what opportunities can be taken from the risks within each individual organisation. Leaders must shift their focus from isolated fixes to developing a comprehensive strategy that integrates risk management across all departments. This requires a change management approach where security is seen as a collaborative effort, rather than an isolated function.

Moreover, a significant challenge is getting buy-in from those who control the purse strings. Many still see security as a budgetary burden rather than a long-term investment. Security leaders need to do more than explain threats and vulnerabilities – they need to advocate for risk management as a value-added component of the organisation's strategic goals. By aligning security investments with business priorities, they can drive home the point that robust security enhances overall business performance and resilience.

## Extend Expertise – Leverage a Holistic Approach

Whilst technology is making great waves in driving security forward – it's not enough in isolation. A holistic approach is necessary, one that extends beyond the technical aspects to include human factors, cultural considerations, and ongoing education. Far too often, organisations install sophisticated security systems but fail to provide adequate training for the teams who will be using them. Without providing ongoing training for the end-user, even the most advanced technology can become ineffective.

Investing in continuous training and upskilling is essential. Security is not static, and the threats we face today are vastly different from those of even a few years ago. Social engineering, for example, is a growing concern, and the easiest way for attackers to break into an organisation is often through human error. Employees must be empowered to recognise these risks and respond appropriately. This requires not only technical training but also behavioural awareness – teaching staff to understand what to look for and how to act when faced with potential security threats.

It's also important to create a culture of security within the organisation. Security should not be seen as a box to tick, but as an ongoing responsibility shared by everyone. People are often the greatest vulnerabilities, but with the right training and support, they can also become the organisation's biggest protectors.



**“Investing in continuous training and upskilling is essential.”**

## Focus on Solutions, Not Fixing Single Problems

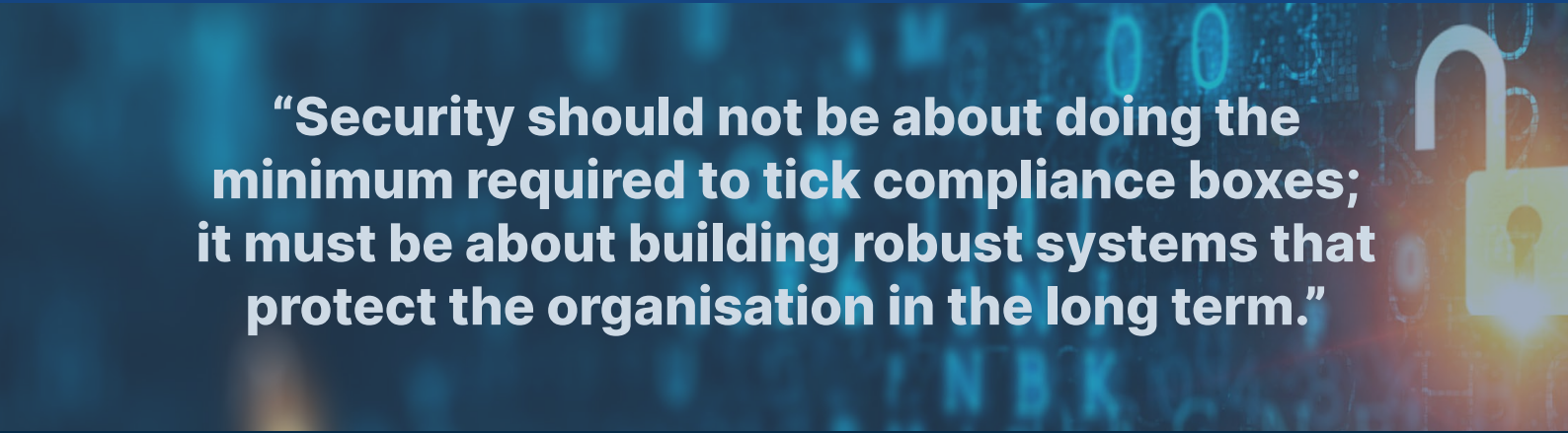
A common mistake in security strategy is focusing on single problems rather than adopting a solution-oriented approach. Too often, security teams find themselves reacting to the latest vulnerability or the most recent breach, addressing individual issues as they arise. However, this reactive approach is short-sighted. Organisations must instead focus on developing comprehensive solutions that address the root causes of their security challenges.

Risk management should be about building resilience, not just plugging holes. Security leaders must take a step back and consider the bigger picture: What are the most critical assets? What are the most significant threats? And how can the organisation protect against those threats while still enabling business operations? By thinking strategically and focusing on long-term solutions, rather than quick fixes, organisations can create more sustainable security practices.

## Stop Doing Security to a Budget

One of the biggest challenges security teams are facing is operating under tight budgets, often imposed by stakeholders who don't fully understand the scope of the risk. Security is frequently treated as a grudge purchase – a necessary but begrudgingly allocated expense. This mindset needs to change. Security should not be about doing the minimum required to tick compliance boxes; it must be about building robust systems that protect the organisation in the long term.

Many organisations make the mistake of waiting for a security incident to occur before investing in the necessary resources. The reality is that it's not a matter of "if" but "when" a security breach will happen. Waiting until after an attack to address vulnerabilities can be far more costly – both financially and reputationally – than investing in a proactive security strategy. Budget constraints shouldn't dictate the effectiveness of security measures. Instead, organisations must allocate resources based on risk assessments and the potential impact of security failures.



**“Security should not be about doing the minimum required to tick compliance boxes; it must be about building robust systems that protect the organisation in the long term.”**

## From Reactive to Proactive Security – A Shift in Mindset

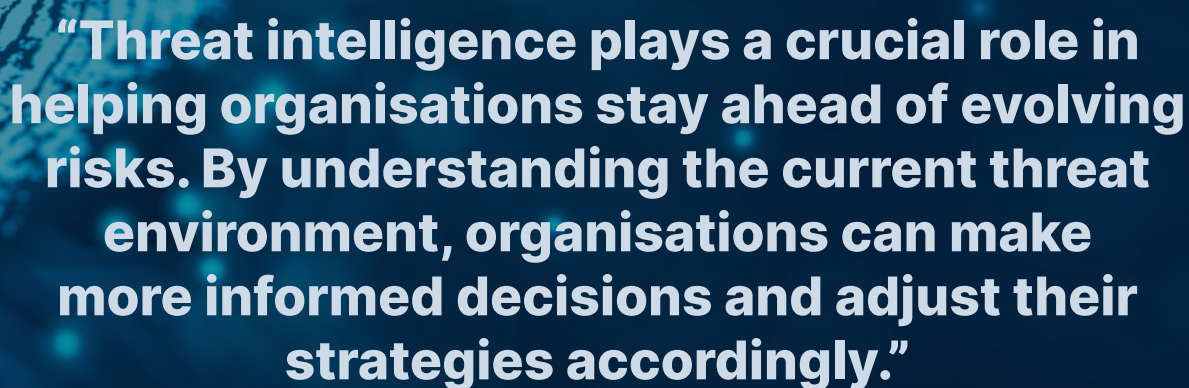
For too long, security has been reactive. Organisations tend to focus on responding to incidents rather than preventing them. To truly protect against evolving threats, there needs to be a fundamental shift from reactive to proactive security. This shift requires a mindset change – not just in security teams, but across the entire organisation.

Proactive security means anticipating threats before they happen, using threat intelligence to inform decision-making, and investing in the right tools, technologies, and training to stay ahead of attackers. It also means moving away from short-term fixes and embracing a long-term, strategic approach to security that aligns with business goals.

# The Role of Threat Intelligence and Regulation

As the threat landscape becomes more complex, the role of threat intelligence and regulation in shaping security strategies cannot be overstated. With regulations becoming increasingly stringent, organisations are now being held to higher standards of safety and risk management. This shift is a positive development, as it forces businesses to move beyond good practices and embrace mandatory security measures.

Threat intelligence plays a crucial role in helping organisations stay ahead of evolving risks. By understanding the current threat environment, organisations can make more informed decisions and adjust their strategies accordingly. This, combined with compliance-driven initiatives, ensures that security is treated not just as a reactive necessity but as an integral part of business strategy.



**“Threat intelligence plays a crucial role in helping organisations stay ahead of evolving risks. By understanding the current threat environment, organisations can make more informed decisions and adjust their strategies accordingly.”**

## Understanding the Human Element

Amidst the complexities of modern security, the human element remains pivotal. Individuals within an organisation can be both the greatest asset and the biggest vulnerability. Whether through insider threats, human error, or susceptibility to social engineering attacks, the human factor is often the weakest link in security defences.

Organisations must equip their teams with the tools and training needed to recognise and counteract these challenges. Continuous education, regular testing, and upskilling are essential to keeping employees informed about emerging threats and ensuring they can respond effectively. Building a culture of security within the organisation is key.

Security is everyone’s responsibility, not just the IT or security teams.

# Security Design – The Importance of Integration and Testing

During the discussion on security design best practices, experts highlighted the crucial role of proactive planning, collaboration with penetration testers, and utilising the latest technologies. By incorporating insights from offensive security specialists – who think like hostile actors – organisations can better anticipate and counter potential threats.

This approach enables a comprehensive, client-focused security design tailored to specific requirements and vulnerabilities. However, even the most advanced security systems must be subjected to regular testing throughout their lifecycle.

Testing is not a one-off event but a critical process to ensure that solutions remain resilient and adaptable to evolving threats. Without thorough, ongoing testing, even the best designed security measures may fall short when they are needed most.



# A Call to Action for the Future of Security

As leaders in security, we can help organisations navigate the complexities of today's threat landscape by driving this conversation forward.

Looking ahead, the future of security will require a balance of cutting-edge technology and human understanding. While AI and machine learning are transforming the threat detection landscape, these tools can only take us so far. To truly build resilient organisations, we must focus on holistic solutions that consider the human element. Security must be a shared responsibility, embedded into the culture and processes of the organisation.

It is our responsibility to guide businesses in integrating security into their core operations, moving beyond fear-driven responses and instead creating a culture of education, proactive risk management, and holistic solutions. By leading this charge, we can help organisations recognise that security is not just a defensive necessity, but a strategic enabler. Through collaboration, communication, and ongoing education, we can empower businesses to thrive while staying resilient against evolving threats.

**The conversation needs to evolve -  
let's lead the way.**



[www.torosolutions.co.uk](http://www.torosolutions.co.uk)



[info@torosolutions.co.uk](mailto:info@torosolutions.co.uk)



0208 132 9267

**Physical. Cyber. People.**

