

TAKEAWAYS FROM INFOSECURITY EUROPE 2025

The 30th edition of Infosecurity Europe took place from the the 3rd to the 5th of June 2025 in London. The discussion was dominated by growing threats from advancements in AI and quantum computing, as well as the worsening geopolitical landscape in the context of tight budgets. Here are our seven takeaways.

Marina Koytcheva, Research director

Nicola Warren, Senior analyst

December 2019

© STL Partners

Post-quantum cryptography (PQC) is the new hot topic

Getting ready for the world when quantum computers can be used by malicious actors to decrypt data harvested today was one of the hot topics, highlighted at the recent Infosecurity Europe event.

There is no consensus on exactly when that day will come: some say it will be around 2030, others think it might be even earlier. It is unlikely that we'll be able to point to a specific date and call it 'the Q-Day' either. For one, criminals will not announce it on social media and it might be a while before it is clear that they have started using quantum computing.

Big players such as Amazon Web Services (AWS), Google and others, are well-advanced in their preparation for the post-quantum future. Some security companies also claim to offer PQC-ready solutions.

It is now clear that the security industry is stepping up its efforts to convince enterprises that they need that extra layer of security, for which they have to pay a premium, naturally. This is particularly necessary for two types of industries: those of strategic national importance (financial services, telecommunication, healthcare, etc.) and those that are required to hold data for a very long time (financial services are an example here again – people take mortgages for decades ahead).

The problem for the security industry is that budgets are not growing. Many enterprises face much more immediate risks, and with limited budgets, shortsightedness is all but guaranteed. We expect that the shift to post-quantum security, unless orchestrated from the supply side or mandated by law, will be slow.

The global context is fuelling cyber risk

Rory Stewart, academic, political commentator and podcaster, eloquently outlined four shifts to explain this:

- Politics: The prevalence of liberal democracies is increasingly giving way to populist regimes focused on defending national interests.
- Economics: The principles of privatisation, deregulation and free trade are being reconsidered, as they have resulted in growing inequality – and the 2008 financial crisis – while China has been on the ascendant.
- Geopolitics: International bodies and laws have been ineffective in resolving crises such as the ones in Afghanistan and Ukraine, leading to countries increasingly acting alone and in conflict with each other.
- Media tech: The rise of social media – and its algorithms – has impacted politics and facilitated ideological spread beyond national boundaries.

Businesses should expect country differences in regulation, brought about by changing political views, which poses difficulties with compliance and law enforcement. The introduction of protectionist economic measures such as the tariffs in the US can facilitate a China-led globalisation and interoperability/ vulnerability issues later on. Geopolitical pressures will continue to drive more state-on-state cyberattacks. AI developments including deep fake technology will escalate the potential for misinformation and manipulation in politics.

State-sponsored cyber threats have become commonplace

The presence of state-sponsored bad actors, especially from North Korea, Russia, China and Iran, was widely discussed at the event. Understanding their motivation is really important to the ability to counteract them. Some pursue political outcomes, as in the case of the Russian attacks on Ukrainian infrastructure before the

© STL Partners

invasion of Ukraine in February 2022 or in instances where there has been meddling in democratic processes. Others pursue traditional espionage outcomes – knowledge about defence strategies and infrastructure. But financial gain is also a motive for some – for example, ransomware is believed to finance North Korean government initiatives.

That (almost) every country uses cyber tools against its enemies was also openly acknowledged. But the threats that we, as society, need to prepare for go beyond the realms of spy movies. Critical infrastructure, both physical and digital, can be targeted by bad actors – examples include tampering with the water supply for the civilian population. Clearly, protection against such threats forms part of the national defence, but lines may be blurred if a major enterprise, be it a big retailer or a bank, is targeted.

Cybercrime, and in particular ransomware, has evolved into a business – and a risk to be managed

In the early noughties, cyberattacks were fairly innocent – before their potential for nefarious ends was recognised (e.g., to make money or to be used for political gains). The emergence of Bitcoin enabled hackers to monetise their attacks in a non-traceable way, which resulted in targeted efforts to get into consumer home computers and demand money to end attacks. In 2020, cybercriminals began targeting the enterprise and the public sectors with ransomware.

Cybercrime gangs have built strong brands (to validate that they will do as they say on receipt of payment), they have HR departments and they are very rich (they keep wealth in blockchain for security – which increases the value of Bitcoin). Ransomware-as-a-service providers (e.g., GhostLocker) will write ransomware code and help attackers with the Bitcoin capabilities necessary to set up a hack.

Cybercrime gangs don't choose a target – they seek out vulnerabilities. They are often capable of stealing a company's financial information to know how much they can expect a business to pay.

Digital fraud has the potential to affect any business/entity at any time and presents a risk to be managed, alongside risks of fire and floods. Unlike those, however, the difference is that the risk from cybercrime presents itself daily. Regulators increasingly want to know that companies have thought about cyber impacts and have planned responses that are commensurate with their company risk appetites.

Laws and regulations do not equate to resilience – despite security improvement

Tech lawyer Jonathan Kewley from law company Clifford Chance made the point that laws, regulation and compliance manuals are not enough to protect companies from cyberattacks. While cyber is a key priority for governments and regulators, legislation creates costs and complexity for businesses. And laws very seldom provide the practical guidance necessary to provide envisaged levels of resilience. He strongly recommended that businesses endeavour to co-create regulation with the government for greater effectiveness.

Despite the headaches that they create, legal requirements are one way to ensure that due consideration is given to security by businesses and their boards, with all enterprises required to invest in it. In this respect, a speaker from IBM suggested that legislation could be a friend to the dissemination of PQC, for example.

Conflicting views were expressed in terms of how legislation will impact the industry in the near future, especially in the context of geopolitical shifts. Will the post-quantum regulation by the US National Institute of Standards and Technology (NIST) spill over to the rest of the world? Will the slimmed-down US regulators

© STL Partners

have the capacity to influence regulation worldwide as much as it had in the past? Will the European Union (EU)'s emphasis on citizen safety and sovereignty over innovation be adopted by the UK and other countries?

As the future unfolds, companies will do well to build cyber resilience into the corporate culture – ensuring that security becomes a core business value.

New approaches to AI

Undoubtedly, AI remains both the main risk driver and security driver in the industry. On its own, it wasn't even a huge topic at the show anymore, unlike a year ago when companies proudly announced that their solutions were AI-enabled. This has since become a hygiene factor.

One interesting example of using generative AI (GenAI) was presented by Dutch cybersecurity company Hadrian. It is building its own, lighter large language model (LLM) trained on cybersecurity data only. The company claims that its LLM works for cybersecurity purposes much better than a generic LLM does, plus it is cheaper to train and operate.

Another interesting example – using AI for predictive defence – was discussed by Dataminr, a company that analyses real-time data to predict when and where an attack is likely to happen. It said it knew something was wrong with the British retailer Marks & Spencer a few days before the company announced it had become a victim of an attack in April 2025. It also brought up a case study of preemptively protecting an airport in the US at the time when a similar-sized airport came under a cyberattack. Clearly, it is better to go 'shields up' before the attack happens.

SMBs are a weak link in cybersecurity terms

As STL Partners' recent survey showed, while small and medium-sized businesses (SMBs) may be aware of the cybersecurity risk, they are frequently challenged in terms of what to do about it: where to find expertise and how to free up necessary funds – particularly once they have become a victim of crime. They find it difficult to adhere to cyber regulations when they may not have an IT person, let alone cybersecurity personnel on their payroll, and frequently run into obstacles when navigating cybersecurity checks while being onboarded as a new supplier.

There may be government support for SMBs once they have experienced an attack (e.g., Cyber Resilience Centres in the UK), but the information landscape for the proactive amongst them is very confusing. For example, there is no single information source that covers all aspects of security.

A Cyber Security Communities of Support (CyCOS) project has been set up in the UK to address this issue. Due to pilot in August, it aims to build an SMB community around the topic of cybersecurity, making free information available and facilitating peer-to-peer learning in order to improve SMB understanding and normalise security practices. It also plans to offer training and certification in cybersecurity. The intention is to create a platform that can scale to reach the large number of SMBs that exist in the UK.

Initiatives such as these are critical to enable the participation of SMBs in supply chains and prevent them from being locked out due to non-compliance with new supplier screening criteria.

© STL Partners

Figure 1: Impressions from the show floor



Source: STL Partners

© STL Partners

Marina Koytcheva is a Research director at STL Partners specialising in strategy, cybersecurity, AI and consumer services.

Nicola Warren is a Senior Analyst at STL Partners specialising in strategy, transformation and cybersecurity.

Get in touch with the authors to learn more

marina.koytcheva@stlpartners.com

nicola.warren@stlpartners.com

Or visit STL Partners' Consumer Services
https://stlpartners.com/telecoms-strategy/

© STL Partners