Takeways from Infosecurity Europe 2026

In early June 2026, Infosecurity Europe once again brought together many companies and experts to explore the latest trends in the increasingly complex cybersecurity landscape. Here are our takeaways.

Marina Koytcheva, Research Director

Nicola Warren, Senior Analyst

June 2026

Introduction

Amongst the usual sea of Lego competitions, branded socks and stress toys, Infosecurity Europe 2026 presented an atmosphere of high energy and an underlying sense of urgency. As usual, it allowed us to test the temperature of the cybersecurity market for new themes and trends.

Cyber remains firmly part of the geopolitical confrontation.

This is not new- it's been a major theme this decade. And adversaries are not giving national cyber agencies any respite, as cyber attacks can enable broader sabotage (e.g. infiltrating supply chains to result in physical harms). We are in a time of "maximum uncertainty", as Paul Chichester, a cyber veteran from the UK's National Cyber Security Centre put it. Of course, offence is the best defence: we assume that all organisations have a role to play to reduce attack surfaces, address legacy systems, strengthen identity and access controls and prepare for incidents. Chichester's message to business: Don't wait for certainty before taking action.

The number of criminal AI-based cybersecurity tools for sale has exploded

Former FBI cyber deputy director Cynthia Kaiser highlighted that 60% of activity on the dark web is devoted to selling tools that enable cyber attacks. New AI-based tools include weaponised large language models, tools that enable identity fraud (e.g. voice cloning), AI-augmented malware and attack infrastructure, and jail-broken or stolen credentials for AI services. Ironically, criminals often target each other. Kaiser called on organisations to be ready for the increase in non-professional attacks and to improve coordination between defenders, model providers and payment companies to respond to the threat.

Speed is everything

Models are evolving quickly, leading one presenter to claim that all large language models are getting better at cyber; it is not just Mythos that CISOs should worry about. There is a sense of acceptance that AI is, or will soon be, able to exploit vulnerabilities almost instantly, at machine speed. We saw companies on the floor that offer patching within a few hours. Given that a human element might be the current patching bottleneck, this time frame doesn't sound too bad. But it might not be good enough either.

Offence is the best defence

The flip side is that AI can be used while building digital assets and solutions to avoid these vulnerabilities in the first place. For example, thanks to AI, in April 2026 Mozilla issued 423 security patches, compared to 76 in March, 61 in February and an average of about 20 in 2025 (source: here). Companies need to keep testing their preparedness constantly to ensure there is no open door that the next large language model can detect and enable criminals to exploit.

Securing non-human identities (NHI) is the next challenge

People may no longer be the easiest target for threat actors. Companies now face the task of securing an explosive number of non-human identities: AI agents and other machines. In his presentation, Darren Guccione, CEO of Keeper Security, shared that in the average company, there are 92 non-human identities for every human identity. He also claimed something quite intuitive but also seriously disturbing: that most organisations simply don't know the number of NHIs they need to secure. Organisations are struggling to deal with the sheer volume but also with the speed at which these NHIs proliferate. And so are their identity security solutions, which were not designed to account for them. But cybersecurity specialists are responding, and we saw several companies focusing on securing NHIs.

The increasing challenge of the CISO/defender role

Corporate defenders require expertise and knowledge related to geopolitics and technology, both of which are evolving fast. This is further complicated by an increasing level of system inter-connectedness, which is hard to identify and track. Security leaders have this in mind, while at the same time being under pressure to enable organisations to innovate with AI.

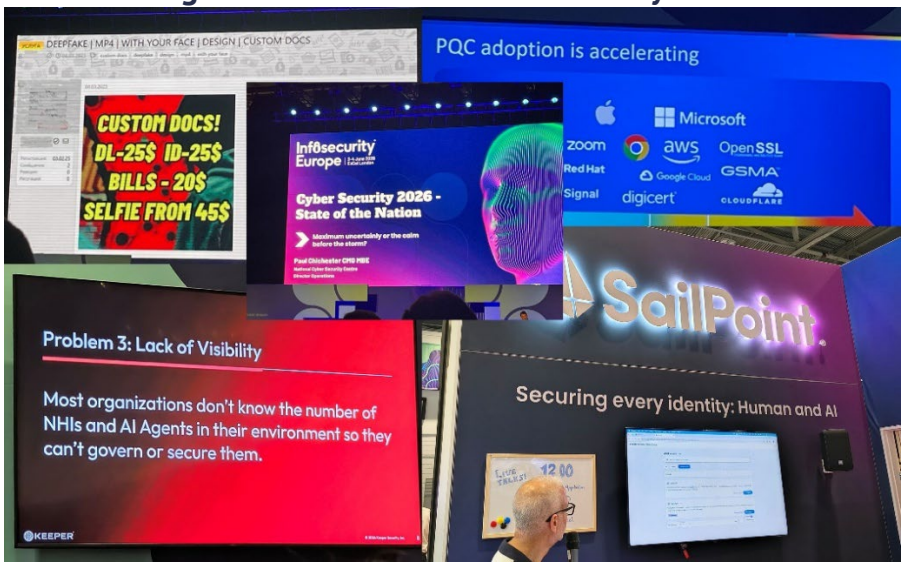
Telcos are recognising the opportunity to sell cybersecurity to small and medium businesses (SMBs).

At STL Partners, we have been advocating for telcos to address the untapped part of the SMB market. SMBs need more cybersecurity to protect their own businesses, but also to not become the weakest cyber link in the complex supply chains of major enterprises and the public sector. Cynthia Kaiser reported that there are four times as many SMBs that are targets of ransomware attacks compared to larger organisations. KDDI and Vodafone were the only telcos at the event. Vodafone has had a focus on SMBs for a while, while KDDI launched a new SMB solution a few months ago.

Post-quantum cryptography (PQC) is waiting for its turn

Last year, PQC was a major topic at this event. In contrast, this year it was hardly mentioned. A representative from DigiCert said "[companies] can see it in the distance, but it is not driving action yet". This doesn't mean that cybersecurity companies are not working on PQC. For example, Christian Reilly from Cloudflare even floated that the date for PQC migration might move forward. But the market can handle only a small number of hot topics, and at present, the imminent concern is securing against fast-developing AI capabilities. We expect PQC not to wait too long before coming back into the spotlight, though: in the same week as the Infosecurity Europe 2026, Microsoft unveiled its Majorana 2 quantum chipset and said it expected to achieve a "scalable quantum computer" by 2029.

Figure 1: Pictures from an industry show



Source: STL Partners

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

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' Strategy hub
https://stlpartners.com/telecoms-strategy/