ayesa

Cybersecurity 2025

Key predictions and trends

ayesa.com

Cibersecurity 2025:
Key predictions and trends

Complex and evolving scenario

Cybersecurity in 2025 is regarded as a critical and dynamic field, characterised by rapidly evolving threats and the complexity of the defence strategies. As the technology continues to evolve at an unprecedented rate, organisations are faced with a more interconnected digital environment, but also a more vulnerable one. Cybercriminals, driven by technological innovation, are taking their tactics to a new level of sophistication, making full use of advanced tools that challenge the capabilities of traditional security solutions.

The digital transformation, accelerated by the widespread adoption of technologies such as cloud computing, the Internet of Things (IoT) and hybrid systems, have broadened the attack surface significantly. Companies and public bodies are now facing the challenge of managing distributed and complex infrastructures that may provide great operational benefits but which also expose weak points that can be exploited. Security is no longer limited to protecting defined perimeters; it now includes a global network of interactions, remote accesses and shared ecosystems.

In this context, cybercriminals do not just make use of technical vulnerabilities, they also resort to more elaborate social engineering techniques to exploit the human factor. This underlines the importance of a comprehensive security strategy that combines advanced technology with education and awareness within organisations. Innovation by itself is not enough; a holistic approach is needed that considers people, the processes and the technologies as collective whole.

Furthermore, the global nature of the current threats has shown the need for closer collaboration between sectors, governments and regions. Cybersecurity is no longer seen as an isolated responsibility of the companies; it has become a collective force that requires the sharing of information, experiences and best practices. This collaborative approach is essential for anticipating emerging threats and responding efficiently to incidents in an ever more interconnected environment.

Resilience also covers an increasingly important aspect in the cybersecurity landscape. It is not just about preventing attacks, but about being prepared to quickly respond and recover from any disruption. Organisations must develop robust capabilities for business continuity that will allow them to mitigate the impact of incidents and guarantee operability at all times. These range from the planning of contingencies to the implementation of regular drills that strengthen their responsiveness.

Ultimately, 2025 will mark a turning point for cybersecurity, where the combination of technological innovation, continuous training and strategic consolidation will determine the success of organisations in their efforts to protect critical assets and build a more secure digital environment. Adapting to this complex, constantly changing scenario will not be an option, but a necessity for guaranteeing sustainability and competitiveness in a digital world.

Proliferation of attacks driven by Artificial Intelligence (AI)

Artificial intelligence has become a fundamental tool, both for improving cyber defences and for carrying out more sophisticated cyber attacks. In 2025, we will see an escalation in the use of AI by cybercriminals, who will use it for:

The automation of phishing attacks on a grand scale

personalising messages in real time based on stolen data.

The design of adaptable malware

that learns and evolves in order to evade traditional detection systems.

Carrying out mass data analysis

Identifying vulnerable patterns and points in complex networks.

Conversely, organisations will turn to AI to bolster their security systems, implementing solutions that can analyse anomalies in real time, anticipate possible threats and reinforce their capacity to respond to incidents. However, the race between defenders and attackers will be a dynamic battle ground where cybercriminals will continue to try to overcome the most advanced measures.

AI is not only changing the rules of the game in terms of the speed and precision of such attacks, but also in the ability of attackers to personalise specific campaigns based on behaviour analysis. Cybercriminals are also beginning to use generative systems, like deep learning, to create more convincing deceptions, such as images, texts or simulated voices. To counteract this threat, organisations must invest in detection systems based on artificial intelligence that are capable of analysing patterns and predicting the attacker's movements.

Cybersecurity 2025: Key predictions and trends

Evolution of ransomware and threats to the supply chain

Ransomware will continue to evolve as one of the most devastating threats. In 2025, it is anticipated that cybercriminals will target their attacks towards critical supply chains, using increasingly advanced techniques to disrupt essential operations. The new approaches will include:

Use of 'ransomware as a service' (RaaS)

democratising access to attack tools for inexperienced criminals.

Implementation of deepfakes

to manipulate identities and gain access to restricted systems.

Campaigns aimed at software and hardware providers

to introduce vulnerabilities in your products.

The importance of protecting the supply chain will be crucial, given that one single point of failure could unleash catastrophic consequences in many areas, including the financial, energy and health sectors.

The professionalisation of ransomware, combined with inadequate preparation by small and medium-sized businesses, will expose the critical supply chains further. Targeted attacks on smaller suppliers may trigger a chain reaction with global consequences. Increasing digitisation is also creating new technological dependencies, which underscores the need to implement new strategies for network segregation and strict access controls to minimise risks.

Growth of vulnerabilities in cloud and IoT environments

The widespread adoption of cloud services and Internet of Things (IoT) devices will continue to expand the attack surface. Cybercriminals will be focused on exploiting poorly managed configurations, weak credentials and missing updates. In this context, several challenges are expected:

The complexity of managing hybrid infrastructures

that combine local and cloud solutions.

An increase in attacks directed at IoT devices

used in critical sectors such as health and manufacturing.

The need to implement specific security solutions

for multi-cloud environments.

In addition to configuration risks, the proliferation of unsafe IoT devices is creating a network of vulnerable points that cybercriminals can exploit. Many devices lack robust security standards, which increases the chances of unauthorised access. Organisations must prioritise monitoring tools that can constantly analyse network behaviours in search of irregularities, with frequent updates to mitigate these risks.

Emerging quantum computing threats

Although quantum computing is still in its early stages, its potential to break current encryption methods presents a significant worry. In 2025, greater focus is expected in:

Development of algorithms

resistant to quantum computing.

Updates to security protocols

in sectors such as banking, e-commerce and telecommunications.

Increases in research investment

to prevent the risks associated with this technology.

Quantum computing also poses challenges in terms of infrastructure, as organisations must adapt their systems to still-evolving technologies. This change will involve significant costs in terms of updates and technical training. Governments and private entities must work together on global standards to guarantee that these quantum-resistant solutions are adopted uniformly and efficiently.

A shortage of cybersecurity talent

The gap between the demands of cybersecurity experts and available supply will continue to be a challenge in 2025. This situation will have a direct impact on the capacity of organisations to implement effective security measures. Some key strategies for addressing this problem area include:

Investment in training and certification programmes

specialised in cybersecurity.

Promotion of public-private partnerships

to develop local talent in emerging markets.

Incorporation of artificial intelligence and automation

to partially cover shortfalls in specialised staff.

This talent shortage not only affects the immediate response to incidents, but also the capacity for innovation in cybersecurity. Companies must consider in-house training of non-technical staff to cover certain duties. Moreover, diversity and inclusion in training programmes could increase the professional base, attracting talent from various disciplines to address the challenges in a creative way.

Stricter regulations with emphasis on cyber resilience

The growing pressure from governments and international organisations to strengthen cybersecurity will lead to the adoption of stricter regulations. Most notably, regulations such as the NIS2 Directive in Europe will push for a more rigorous approach in:

Management of cyber-risks

as an essential element of corporate governance.

The implementation of cyber resilience frameworks

that will ensure operational continuity, even in the event of severe attacks.

Transparency in incident reporting

by promoting a more collaborative approach between sectors.

These regulations not only establish minimum security standards, but also require companies to redefine their strategic priorities with regard to data protection. In addition, compliance with these regulations is becoming a competitive differentiator, as customers and trading partners prefer to work with organisations that demonstrate a solid commitment to cybersecurity. The costs associated with non-conformity, such as fines and loss of reputation, further stress the importance of integrating cyber resilience in all levels of the organisation.

7

Automation and professionalisation of cybercrime

Cybercrime is evolving towards a highly organised business model, with specialised groups that provide services at every stage of an attack cycle. This professionalisation includes:

The use of automated tools

that increase the speed and precision of the attacks.

Sales of exploitation kits in clandestine markets

providing less experienced actors with access to cybercrime.

Collaboration between criminal groups

to maximise the efficiency of their operations.

Automation is enabling cybercriminals to reduce operational costs and increase the frequency of their attacks. Furthermore, the creation of well-organised, clandestine networks, operating as genuine companies, is facilitating the development of customised threats for specific aims. This model poses additional challenges for organisations, in that they must adapt their defences to counteract individual attackers as well as highly structured criminal operations.

8 Integration of physical and digital threats

The convergence between physical and digital threats will be a reality in 2025. Examples of this include:

Combined attacks

that disrupt IT systems as well as physical infrastructures.

The use of physical intimidation tactics

to extort digitally compromised companies.

The need for integrated defence strategies

that address both types of threat.

Digitalisation of critical infrastructures, such as energy and transport, converts those infrastructures into high-value objectives. Hybrid attacks that combine cyberattacks with physical sabotages may cause massive and prolonged disruption. What is more, industrial espionage, where adversaries combine physical and digital infiltrations to extract sensitive information, is on the increase. In this context, the integration of physical defence and cybernetic strategies will be key to guaranteeing overall security.

Risks associated with the improper use of AI

The prompt adoption of AI tools in business processes will involve risks, including:

Accidental exposure of sensitive data

through poorly configured platforms.

Excessive dependence on automated solutions

that could be manipulated by attackers.

The need for ethical and clear governance frameworks

to guarantee the safe and reasonable use of these technologies.

The absence of effective controls over AI may also pose regulatory and ethical risks, especially in sectors in which automated decision-making may affect consumers. E.g. errors in the AI used in financial or health processes may have serious consequences. Companies must prioritise the implementation of AI audits and establish clear policies for managing and supervising those technologies.

10 Prioritising proactive security strategies

Rather than limiting themselves to reacting to incidents, organisations should take proactive approaches, such as:

Implementation of zero trust architectures

to minimise risks.

Investment in cyberattack simulations and training

for employees.

Use of threat intelligence

to anticipate possible vulnerabilities.

These proactive strategies not only improve the capacity to respond to threats, they also significantly reduce the costs associated with security incidents. Advanced simulations, such as Red Teaming Exercises, also allow companies to identify internal weaknesses before the attackers exploit them. Investment in predictive analysis and in collaboration with specialist external teams will be fundamental for maintaining a solid security posture.

Cybersecurity 2025:
Conclusion

The year of 2025 is seen as a crucial period for cybersecurity, where threats will be more sophisticated and persistent than ever. The key to overcoming these challenges will be a combination of technological innovation, investment in human talent and collaboration between sectors to build a more secure digital ecosystem.

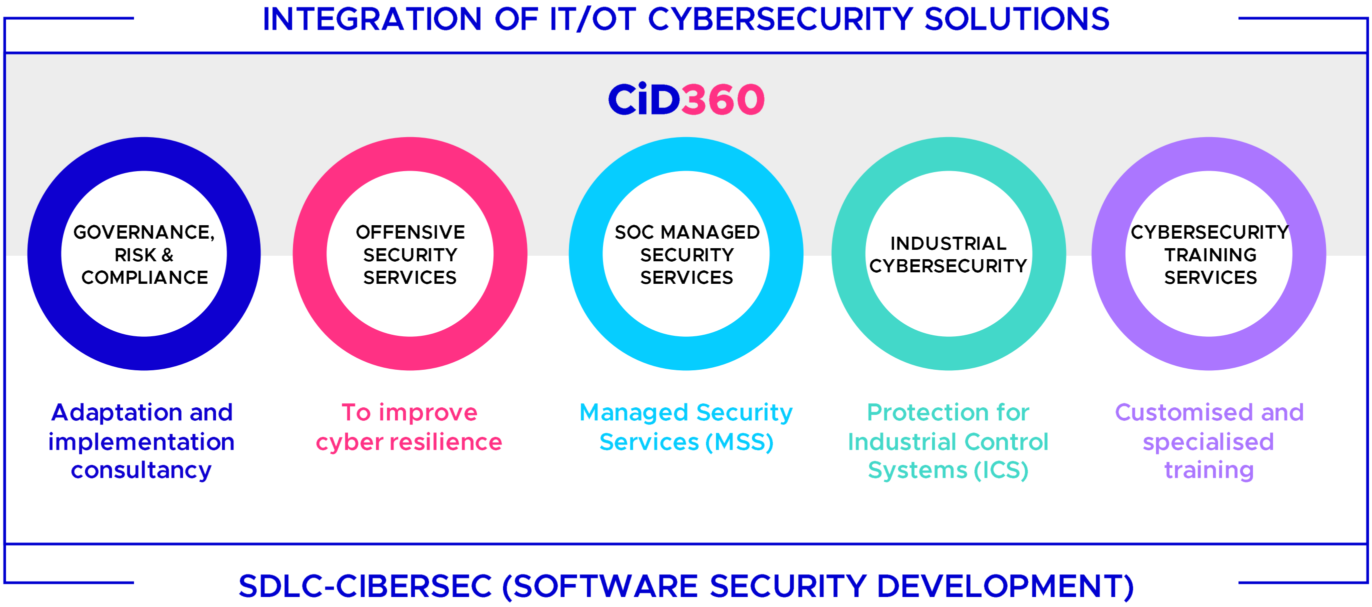
To guarantee their competitiveness, organisations must integrate cybersecurity into the core of their business strategies. This does not just mean the implementation of advanced technological solutions, but also the promotion of a culture of security at all levels of the organisation. Continuous training of professionals, combined with the raising of awareness to emerging threats, will be essential in order to strengthen the weakest links in the security chain.

Furthermore, collaboration between public and private sectors will play a fundamental role in the detection and mitigation of threats. Joint initiatives for sharing information surrounding incidents and best practices will allow companies to forestall attacks. Meanwhile, governments must take a more active role, promoting clear regulations and investment in cyber defence.

Ultimately, cyber resilience will be the distinguishing factor between the organisations that prosper in the digital landscape of 2025, and those that fall behind. Beyond the prevention of attacks, companies must be capable of recovering quickly, reducing the impact on their operations and reputations. This comprehensive approach will not only guarantee the protection of assets, but also the trust of customers and partners, consolidating their position as leaders in an evermore digital, connected world.

Our Cybersecurity services 360º

AUTHORIZED TO USE CERT · FIRST · TF-CSIRT Trusted Introducer · CSIRT.es · Red Nacional de SOC · CCN-cert



INTEGRATION OF IT/OT CYBERSECURITY SOLUTIONS

CiD360

GOVERNANCE, RISK & COMPLIANCE — Adaptation and implementation consultancy

OFFENSIVE SECURITY SERVICES — To improve cyber resilience

SOC MANAGED SECURITY SERVICES — Managed Security Services (MSS)

INDUSTRIAL CYBERSECURITY — Protection for Industrial Control Systems (ICS)

CYBERSECURITY TRAINING SERVICES — Customised and specialised training

SDLC-CIBERSEC (SOFTWARE SECURITY DEVELOPMENT)

Author

Álvaro Fraile
Global Cybersecurity Services Director

Founded in 1966, Ayesa is a global technology and engineering services company, with 13,200 employees and a direct presence in 23 countries in Europe, Africa and Asia. Led by José Luis Manzanares, its turnover exceeds 717 million euros, and it has established itself as one of the main consultancy and IT services companies in the Spanish market.

It provides a broad range of advanced Digital Transformation solutions (projects with disruptive technologies and solutions) and core service lines (traditional IT services) to improve competitiveness in all business sectors through the application of technology and knowledge.

Industry 4.0, Analytics, Cloud, Hybrid IT, Cibersecurity, Quantum Computing, Blockchain, IoT, AI, RPA, Bimodal IT, Mobility or Digital Experience are some of the technologies available to their customers to cope with the new digital era.

It is also a benchmark engineering company, working to build a fairer and more efficient world through the application of engineering and cutting-edge technology in an integrated manner. It assists companies, institutions and organisations to become what they want to be. It works in space between the now and the future, applying, with the best talent, the latest technology.