



14 cybersecurity trends for 2024

Making your tech journey more secure



What are the main cybersecurity trends that we should pay attention to in 2024?



Intro

In a world where technology has an increasingly significant impact on the daily lives of individuals and organizations, it is important to know the best practices for using technology more consciously and securely.

As technological advancements continue to rise, so do cyberattacks, and therefore, it is crucial to be vigilant about trends and how to prevent and mitigate their impacts.

Cyberattacks increased globally by 125% until 2021, and rising volumes of cyberattacks continue to threaten companies and individuals since then. The Russia-Ukraine conflict had a massive impact on the cyber threat landscape, with phishing being the most common form of online crime. In Europe, ransomware was the primary type of attack, representing 26% of incidents on the continent. Server access attacks (12%) and data theft (10%) were the most common attack types.

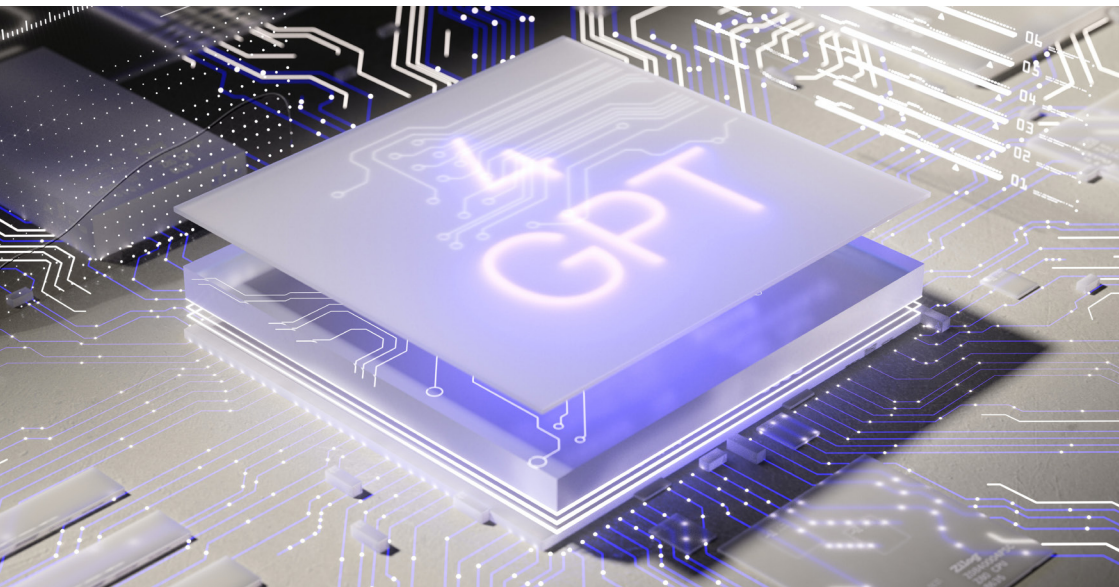
For 2024, we highlight some trends in the cybersecurity ecosystem:

1.

Adoption of Artificial Intelligence for Defense and Attack

Artificial Intelligence (AI) is becoming increasingly complex, and cyber attackers exploit this evolution to enhance cyber attacks. These attacks can **include deepfake or malware attacks**, as AI develops capabilities for attackers to create more accurate fake videos or audios and **deliver malware to outdated systems**.

On the other hand, AI is a tool to detect, prevent, and reduce cyber threats through intelligent authentication and automated response to potential cyber attacks. Therefore, AI provides strategic advantages for both attackers and defenders.





2.

Evolution of Phishing Attacks

Phishing, a type of social engineering attack that **involves deceiving users to grant access to attackers**, will continue to be a concern in 2024.

Attackers will leverage AI for more intelligent and personalized approaches, such as the use of ChatGPT. **Cybersecurity experts** become **essential in organizations to respond to these cyberattacks**, along with the development of awareness and education initiatives.

3.

Cybersecurity as a Priority in Organizations

With the increasing frequency of cyberattacks, cybersecurity should be a strategic priority in organizations rather than just an integral part of the IT department in 2024. **The Gartner report predicts that by 2026, 70% of boards of directors will include at least one member with cybersecurity expertise.**

Therefore, **cybersecurity training within organizations** becomes **crucial for combating cyber threats through employee awareness.**

4.

IoT-Driven Cyber Attacks

The IoT (Internet of Things) consists of more devices communicating with each other via the Internet, which means **more potential systems for cyber attackers to attack.**

With the further integration of **working from home,** the possible **risks that can exist through workers connecting or sharing data via improperly protected devices** could increasingly be a threat. Most of the time, these devices are developed for ease of use and convenience for workers and home **IoT devices can be at risk due to weak security protocols.**

However, the IoT has positive benefits and by 2024 it will have evolved significantly, particularly in terms of security protocols and measures. It

5.

Cyber Resilience and Cybersecurity

In 2024, a clearer distinction between **cyber resilience** and **cybersecurity** will emerge. While cybersecurity focuses on preventing cyberattacks, cyber resilience acknowledges that 100% security is not achievable.

Developing the ability to recover data quickly and effectively will be a key measure of cyber resilience to ensure operational continuity and minimize data loss. **Cyber resilience will be a strategic priority for organizations in 2024.**

6.

Zero-Trust Model

The **Zero-Trust model assumes that everything is a threat**, i.e. everything involved in a corporate network must be recorded and analyzed, including checking employee access.

Over time, **the concept of Zero-Trust has evolved as technological systems have become more complex** and their security more necessary. Since it is not possible to define a security “perimeter” in a network and threats are moving beyond the corporate network and extending to remote workers and IoT devices, **it is necessary to integrate cybersecurity into organizational contexts.**

In 2024, **Zero-Trust will cease to be a technical model** and will **become a holistic and easily adaptable model**, through **continuous authentication by AI and activity monitoring.**

7.

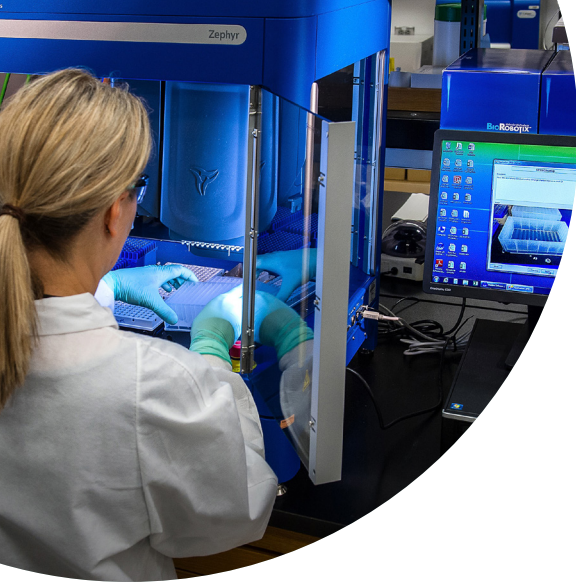
Cyber Warfare and State-Sponsored Cyber Attacks

With the war in Ukraine, **cyber warfare has become more popular and the evolution of cyber attacks is evident.**

Cyber-warfare attacks have been on the rise worldwide and cybersecurity experts predict that **attackers will increasingly use technology as a weapon.** In this sense, one of the **trends for 2024 will be to pay attention** to military operations that may be accompanied by cyber-warfare operations, such as **phishing attacks that aim to gain access to information systems in order to disable communications, public services, transport or security infrastructures.**

Also in 2024, **cybersecurity will play a key role in the world of politics,** as there will be elections in the US, the UK and India and there is likely to be an increase in cyber attacks to destabilise and disrupt democratic processes.





8.

Ransomware Evolution (Ransomware as a Service - RaaS)

Ransomware, **a type of cyberattack that consists of blocking access to a computer system until the user pays a ransom**, has been a worrying threat, **particularly for healthcare providers**, and **will continue to be a recurring attack in 2024**.

What will make **this type of cyber-attack even more dangerous is the growing number of businesses on the dark web** that sell malware, **making it harder to trace the source of the attack**. RaaS vendors work exactly like another type of business, where cyber attackers can buy and customize ransomware through a customer portal. In this sense, it will be essential to define cybersecurity practices, especially within an organization, in order to avoid negative financial impacts.

9.

Privacy and Regulatory Compliance (DORA, NIS2)

NIS2, the Network and Information Security Directive, is one of the European Union's comprehensive efforts to improve cybersecurity and protect infrastructures against cyber threats.

In this sense, it aims to ensure that digital service providers have access to **adequate security measures to protect themselves against possible cyber incidents** and **ensure the cyber resilience** of networks and computer systems, establishing the liability of CEOs in the event of non-compliance with cybersecurity obligations.

The aim of **DORA, the Digital Operational Resilience Act, is to ensure that the digital operational resilience of the EU financial sector is functional**, through a regulatory framework that responds to the sector's dependence on technology, proposing that organizations have to comply with certain requirements.

In 2024, EU Member States may adopt the NIS2 standard, bringing significant benefits for organizations in terms of cybersecurity. According to NIS2, only individuals or systems with prior authorization can access an organization's network or system, reducing the risk of a cyberattack.

10.

Extended Detection and Response (XDR)

With **constant technological advancements**, traditional **cybersecurity tools** will become insufficient, **giving way to more comprehensive solutions.**

XDR platforms collect and correlate data automatically, integrating various security levels such as email, servers, cloud storage, and networks. This security analysis allows organizations to correlate data, predict threats, and respond quickly and efficiently.

11.

Increased Investments in Supply Chain Risk Management (Third Party)

Third-Party Risk Management **is the process of analyzing and reducing the risks associated with subcontracting suppliers or service providers to third parties.**

In 2023, there was an increase in attacks on data related to third parties and supply chains became a concern due to geopolitical issues. It is therefore expected that in 2024 there will be several trends in supply chain-related risks, **with cybersecurity threats standing out, with potential exposure to the confidentiality, integrity or availability of infrastructure and data and technological systems.** In addition to attacks on data, third-party cybersecurity risk involves attacks on supply chain software, theft of credentials and virtual access to systems that facilitate services or transactions.

As third-party cybersecurity incidents continue to recur, **the risk of supply chain cybersecurity will become increasingly critical and will tend to increase.**

12.

Privacy-Preserving Technologies

Data privacy and its regulation will drive the development of privacy-preserving technologies, such as **homomorphic encryption**. This **innovation enables secure computation on encrypted data**, safeguarding privacy without compromising utility.



13.

Integration of DevSecOps

DevSecOps will no longer be a concept but will become a **fundamental part of software development**.

DevSecOps, which stands for Development, Security, Operations, aims to incorporate security at all stages of the software development and operations process. Security will be integrated proactively in the development process through security measures.

14.

Security in Cloud and Multi-Cloud Environments

Security in cloud or multi-cloud environments has been mentioned as a trend to adopt in the **IT ecosystem**, remaining relevant in 2024. While **it facilitates data storage**, it also **exposes computer systems to cyber attackers**.

Therefore, **improvements and strengthening of cloud environments** are expected, along with an increase in cyberattacks on these environments.

bibliography

<https://www.cloverinfotech.com/blog/top-10-cybersecurity-trends-and-predictions-for-2024/#:~:text=2024%20will%20witness%20a%20surge,tool%20to%20a%20cyber%20entry>

<https://elevatesecurity.com/5-cybersecurity-trends-to-prepare-for-in-2024/>

<https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/?sh=143f8ccb5f13>

<https://www.cpomagazine.com/cyber-security/top-security-risk-management-trends-in-2024>

<https://www.watchguard.com/wgrd-news/blog/qual-e-o-papel-que-blockchain-desempenha-nos-ciberataques-e-na-ciberseguranca>

<https://www.checkpoint.com/cyber-hub/cloud-security/devsecops/>

<https://www.sitelock.com/blog/chatbot-security-risks/>


<https://www.prevalent.net/blog/third-party-risks-that-should-be-on-your-2024-radar/>

<https://www.okta.com/nl/blog/2023/09/nis2-and-dora-what-are-they-and-how-can-identity-help-compliance/>

<https://www.linkedin.com/pulse/an%C3%Allise-do-google-cloud-cybersecurity-forecast-2024-cxtte/?originalSubdomain=pt>

T: +351 21 33 03 740
E: info@integrity.pt

Present in 18 countries in the EMEA Region



Making your tech journey more secure