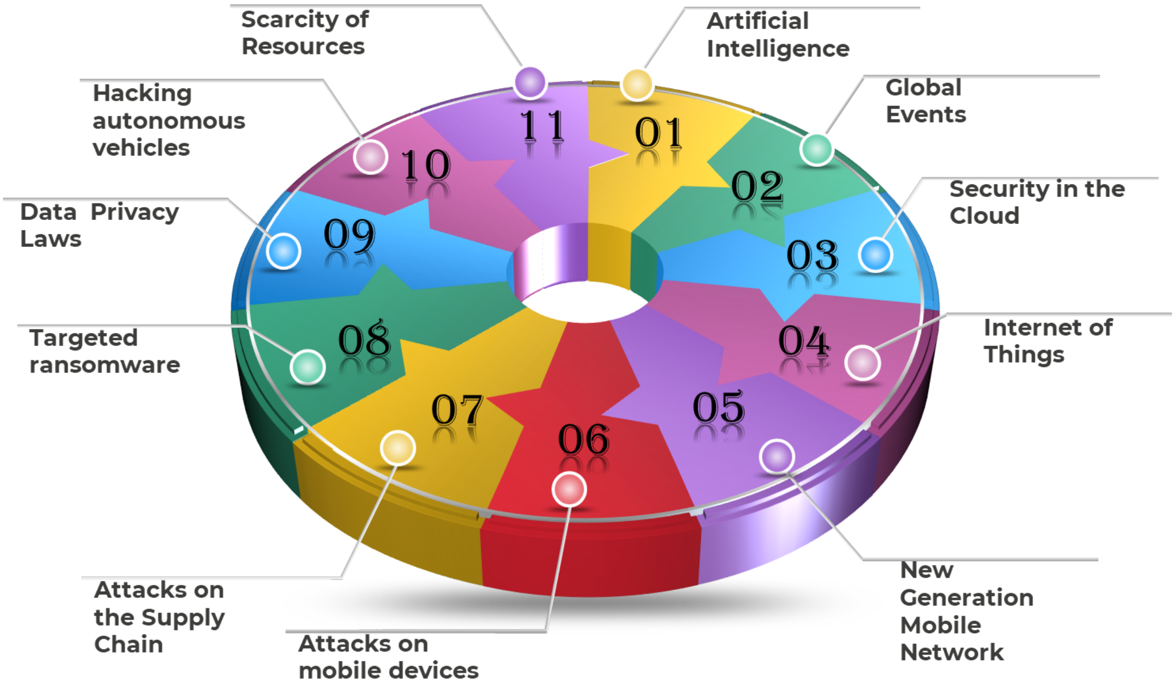
INTEGRITY
Part of Devoteam

11 cybersecurity trends for 2023

Securing your business

devoteam
Cyber Trust

11 cybersecurity trends for 2023



Every year, technology evolves and shapes the way we conduct business, manage tasks and store data. The digital environment and opportunities for attacks are constantly changing. Thus, it is important to be aware of technological trends, especially regarding cybersecurity, which currently have significant importance in management and business continuity. The prevention and defence of cybersecurity is intrinsically related to identifying trends, technologies and factors of potential threats. Based on these premises we highlighted those that we consider to be the trends for 2023.

1 The impact of Artificial Intelligence (AI)

Artificial Intelligence will continue to have a significant impact on the cybersecurity environment, taking on an important role in businesses, creating real-time solutions faster than a human. AI can perform various security-related tasks, including data analysis and *machine learning*.

AI can also be used by cybercriminals. In cybersecurity, incorporating automated AI-based solutions is a necessity at this time to save resources and for being more reliable against automated attacks.

Deepfake videos are popular on social media, and cybercriminals, knowing this, use them to manipulate information, destroy credibility and pose as reliable sources. According to experts, deepfake technology is currently the most worrying in the use of artificial intelligence, as it can have significant effects on terrorism and cybercrime.

It is estimated that more cybersecurity themes will be made available with AI systems, year after year.

2 Global Events

Global turbulence or politically volatile events can trigger serious cybersecurity risks. Moreover, events with potential international impact often set trends to shape action and response in the sphere of information technology and cybersecurity.

As a prime example, the COVID-19 pandemic created a fertile ground for cybercriminals and malware groups to develop virus-based threat campaigns and misinformation around treatment, such as vaccines. Whenever important issues arise, these provide ammunition to lead phishing, malware and other cyberattacks.

This is also why organisations had to adapt and set new security policies during the pandemic for their employees. Basic precautions included the use of dedicated devices, reserved access and guidance to employees on security. Today we are noticing an adoption of hybrid working, where possible, in organisations. Now that the pandemic is coming to an end, 2023 will show whether any of the precautions taken in these years will make a difference.

3 Security in the Cloud

As organisations migrate to the cloud, it is inevitable that cybersecurity will develop specific solutions. And the trend is for migration by entities to increase. It can be said that the cloud will continue to be a key component both for its business application and for ensuring business continuity. Today, the cloud is leading in ransomware protection, primarily due to its backup functionality and ability to build infrastructure quickly.

In recent years, there have been major developments in cloud security, one of which is the Zero Trust cloud security architecture. Zero Trust is a security framework that requires all users, on or off the organisation's network, to be authenticated, authorised and continuously validated before receiving or maintaining access to applications and data.

4 Internet of Things

The common usage of IoT creates an attractive attack base for cybercriminals. According to Insider Intelligence, there will likely be 64 billion IoT devices deployed worldwide in the next five years. An organisation's opportunity for attack grows as more devices are connected to the internet.

Computers or smartphones have better security precautions compared to other IoT devices. With this in mind, one of the critical cybersecurity topics to watch in 2023 is IoT and increased digitisation.

5 New Generation Mobile Network

As 5G is a very new technology, it is difficult to predict what effects it will have on cybersecurity.

Unprecedented new levels of wireless connectivity and speed are introduced with 5G. There are more opportunities to initiate larger attacks at faster speeds. Like IoT, 5G is still a new architecture, so it will take some time to adapt and protect. Early adopters should be cautious when integrating cutting-edge technology and even limit the use of 5G-based devices.

6 Attacks on mobile devices

Cyber criminals attack mobile devices through various methods, such as phishing and unauthorised applications. Today, these devices can store large amounts of valuable data and perform functions remotely, and often have a low level of security. Mobile security is often undervalued, and with mobile devices being yet another potential gateway to network breaches despite manufacturers' efforts to implement security, it is very likely that phishing and malware attacks on these devices will increase.

7 Attacks on the Supply Chain

Supply chain attacks can use vulnerabilities in third-party software and cause substantial financial losses. Today's business operations are primarily supported by the global network of suppliers, third-party services and supply chains. Unfortunately, this dependency increases the possibilities for attacking businesses and provides cybercriminals with more entry points for exploitation.

According to open source reports, the number of supply chain attacks has increased 430% by 2021.

While supply chain attacks are no longer a novelty, other opportunistic and financially motivated cybercriminals will be alert to the potential that exists and the impact it can unleash. Cybercriminals are more willing to apply a strategy they see succeeding.

8 Targeted ransomware

Ransomware, the biggest threat raising the most visibility, is one of the big issues that cybersecurity has to deal with.

Ransomware campaigns require resources and, therefore, high impact attacks can be sponsored by terrorists looking to inflict a massive attack on a territory or organisation. With the current war situation in Ukraine we have seen this happening with cyber warfare. With increasing resources, sponsored and targeted ransomware cases (e.g.: Colonial Pipeline incident), are expected to increase proportionately.

These ransomware attacks may even become a regular scenario.

9 Data Privacy Laws

At a time when we share our personal information across almost every service, governments have started taking strict measures on data security.

By the end of 2023, 75% of the world's population will have their personal information protected by modern data privacy legislations established by various data protection authorities (such as RGPD).

Consumers will be able to know what kind of data is collected about them and for what purpose. Organisations will begin to manage various data protection laws and will focus on automating their approach to data privacy.

10 Hacking autonomous vehicles

Autonomous vehicles are a topic that has us all curious and excited. But is cybersecurity ready for this technology?

Cars often have automated software, enabling features such as cruise control, engine timing, airbags, automatic door locking and driving support systems.

Currently, it is believed that cyber criminals will be able to control vehicles or listen to conversations through microphones.

It is therefore crucial to be aware of the numerous risks associated with the purchase of these new autonomous vehicles.

11 Scarcity of Resources

In order to respond to regulatory requirements and the challenges of cybercriminals with increasingly ingenious and creative attacks, the demand for cybersecurity experts and talent has increased considerably.

Many organisations lack cybersecurity talent, knowledge and expertise - and the shortfall is growing. Overall, cyber risk management has not kept pace with the proliferation of digital and analytic transformations, and many companies are unsure how to identify and manage digital risks. To face the challenge, regulators are increasing the targeting of corporate cybersecurity resources, generally with the same level of oversight and focus applied to credit and liquidity risks in financial services and to operational and physical security risks in critical infrastructure.

At the same time, companies face stricter compliance requirements as a result of growing privacy concerns and high profile security breaches.

By 2023 that challenge remains, and it is anticipated that it may increase the demand for talent and the demand from regulators.

Understanding trends, especially cybersecurity threats, means staying aware of the world around us.

Sources:

- https://www.insiderintelligence.com
- https://www.techtarget.com/searchsecurity/tip/5-steps-to-help-prevent-supply-chain-cybersecurity-threats
- https://www.computerweekly.com/news/252500508/Colonial-Pipeline-ransomware-attack-has-grave-consequences
- https://opensource.googleblog.com/2021/10/protect-your-open-source-project-from-supply-chain-attacks.html
- https://infosecwriteups.com/car-hacking-cyber-security-in-automotive-industry-e9a7a4ffd6bb
- https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html
- https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

Portugal	United Kingdom	España
Edifício Atrium Saldanha Praça Duque de Saldanha, nº 1, 2º andar 1050-094, Lisboa | Portugal T: +351 21 33 03 740 E: info@integrity.pt www.integrity.pt	5th Floor, Cottons Centre Hay's Lane London, SE1 2QG | United Kingdom T: +44 20 7288 2800	Calle Cronos 63, 4ª planta Oficina 2 28037, Madrid | España T: +34 91 376 88 20

Content produced by Integrity part of Devoteam