Telefónica Tech

Cyber Security in 2022 and Beyond

2022

Where are you today?

"The risk landscape is changing, and uncertainty about the future of work postpandemic is impacting business and IT plans." (1)

80%

of respondents viewed cyber security-related risk as a **business risk**, not just a technology risk.

51%

of respondents had experienced a **cyber security risk incident** in the past two years. (2)

The Landscape

The perimeter is dead - long live the new perimeters

The security perimeter is now everywhere, especially with increased employee mobility, therefore security affects every aspect of a company and everyone within it, not just the IT department.

Confronting the challenges of the new wave of digitalisation

Digital transformation means the number of connected devices is growing exponentially and the attack surface is expanding, whether it's across IoT, OT or even robotics.

New types of adversaries

Ransomware is still at large, but new attacks include Malware infecting Dockers server in cloud platforms, attacks on APT & supply chains, or attacks leveraging & targeting AI.

A move from attacks on infrastructure to attacks on individuals

While attacks on system vulnerabilities continue to be a staple of nefarious activities, there's been a renewed focus on attacks against individual employees via mobile devices. The upturn in BYOD and IoT devices will create further headaches for IT departments in 2022. (3)

Phishing for SaaS credentials

More than ***75%*** *of targeted cyber attacks start with someone at an Organisation opening a malicious email....****1/4*** *of all employees have noticed an increase in fraudulent emails, spam, and phishing attempts in their corporate inbox since the beginning of the COVID-19.* (4)

Zero Trust

Assume the network is hostile and only give entities the least privileged access – the minimum permissions they need to fulfill their function. This framework is predicted to become essential in stopping identity from being exploited through various avenues in 2022. (3)

By 2024

organisations adopting a cyber security mesh architecture will reduce the financial impact of security incidents by an average of

90% (5)

By 2024

30%

of enterprises will adopt cloud-delivered Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA) and Firewall As A Service (FWaaS) capabilities from the same vendor. (6)

By 2025

70%

of CEOs will mandate a culture of organisational resilience to survive coincident threats from cyber crime, severe weather events, civil unrest and political instabilities. (5)

Take the Lead

By 2024

60%

of organisations in highly regulated industries will create a dedicated **cyber risk management** — or equivalent function — providing cyber risk expertise, support, monitoring on cyber risks and challenging risk-related decisions by security and risk management leaders. (2)

Security and risk management leaders must:

Develop

a culture of cyber judgment and align this culture with evolving talent needs.

Prioritise

customers and market-facing executives (including the CFO, CMO and CEO) in communication and stakeholder relationship plans.

Position

the enterprise for a secure future by choosing cyber security technologies that offer high levels of integration, automation and orchestration capabilities. (6)

Telefónica Tech

We unlock the power of **integrated technology**, bringing together a unique combination of the **best people**, with the **best tech** and the **best platforms**, supported by a dynamic partner ecosystem, to make a real difference to **our customers, every day**.

We're here to **help**.

Visit **telefonicatech.com**
for more information on Cloud Technology.

@TefTech_EN

Telefónica Tech

Telefónica Tech

Sources:

[1] https://www.forbes.com/sites/bernardmarr/2021/10/25/the-5-biggest-cloud-computing-trends-in-2022/?sh=7d2c7ceb2267

[2] https://www.accenture.com/gb-en/insights/strategy/green-behind-cloud

[3] Gartner Forecast Analysis: Public Cloud Services, Worldwide, 3Q21 Update October 2021

[4] https://www.apper.ph/2021/09/17/10-future-cloud-computing-trends-in-2022/

[5] Gartner, 2022 Planning Guide for Cloud and Edge Computing October 2021

[6] Gartner Forecast Analysis: Cloud Consulting and Implementation Services, Worldwide July 2021

The information disclosed in this document is the property of Telefónica Cybersecurity & Cloud Tech S.L.U. ("Telefónica Tech") and/or any other entity within Telefónica Group and/or its licensors. Telefónica Tech and/or any Telefonica Group entity or Telefónica Tech's licensors reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use and sales rights thereto, except to the extent said rights are expressly granted to others. The information in this document is subject to change at any time, without notice. Neither the whole nor any part of the information contained herein may be copied, distributed, adapted or reproduced in any material form except with the prior written consent of Telefónica Tech. This document is intended only to assist the reader in the use of the product or service described in the document. In consideration of receipt of this document, the recipient agrees to use such information for its own use and not for other use. Telefónica Tech shall not be liable for any loss or damage arising out from the use of the any information in this document or any error or omission in such information or any incorrect use of the product or service. The use of the product or service described in this document are regulated in accordance with the terms and conditions accepted by the reader. Telefónica Tech and its trademarks (or any other trademarks owned by Telefónica Group) are registered service marks.

Telefónica Tech