



HELLENIC

16° IT Directors
Forum

Connect | Educate | Inspire | Secure

Post-COVID; waking up in the new threat landscape

Dr. Dimitrios Patsos

CISSP, CISM, CDPSE, CCSK
President, (ISC)² Hellenic Chapter
Sr. Specialist, Security, Microsoft

About Us

- » Official Chapter of (ISC)² – the largest information security community worldwide
- » 150,000 members in 80 countries
- » In Greece, since 2015: 280 members and intense activities
- » Promoting cyber security training and public awareness
- » Intense activities with deep industry link
- » No 5 in EMEA; No 31 WW

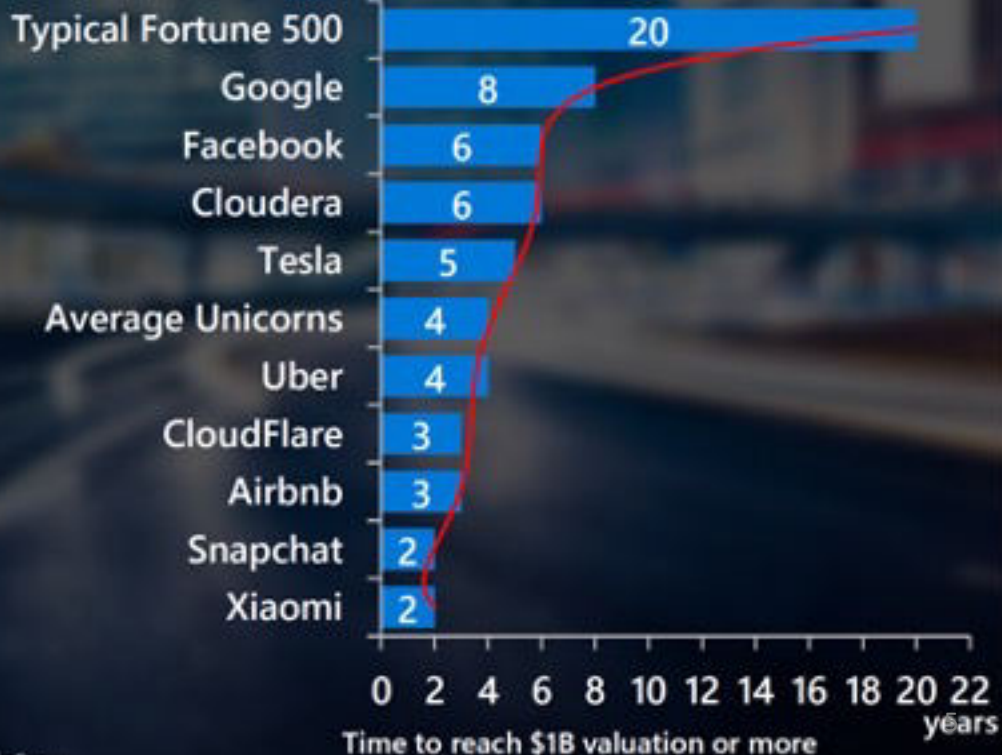


Vectors of Change

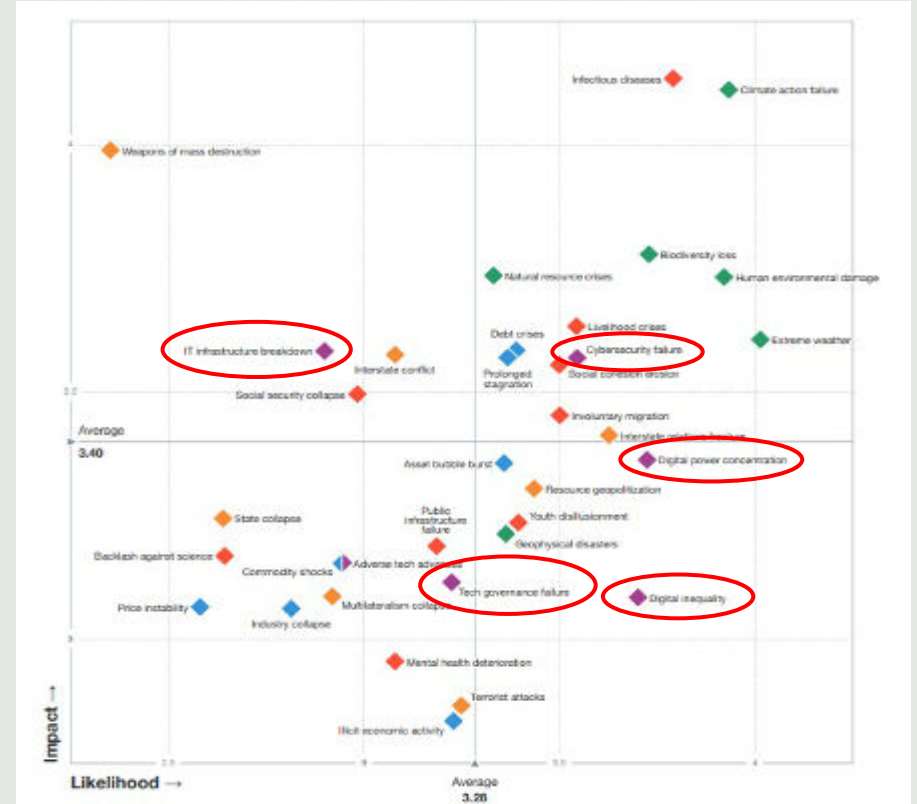


The scale and pace of change

An astonishing pace of change is accelerating transformation. Technology is more affordable and accessible than ever before.



Pre- and Post-Covid; Digital Risks



Source: World Economic Forum, Global Risks Landscape, 2020 & 2021



Post-Covid Threat Landscape

organized
crime



nation state
attacks



hybrid
work



converged
threats



information
integrity



HELLENIC

Sources:

Accenture, Threats Unmasked, 2021 Cyber Threat Intelligence Report

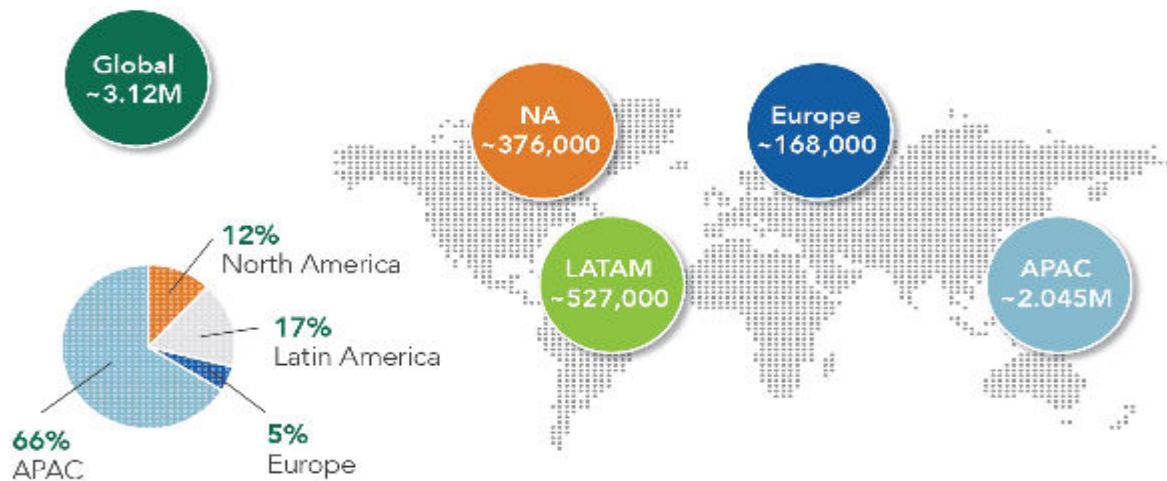
Microsoft Digital Risks Report 2021

Mc Kinsey and Company, COVID-19 crisis shifts cybersecurity priorities and budgets

Uncovering Key Issue

The Cybersecurity Workforce Gap by Region

The global gap in the cybersecurity workforce varies by region, dominated by a gap of more than 2 million in the Asia Pacific region.



Key Takeaways

The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks



Enable multifactor authentication

Make it harder for bad actors to utilize stolen or phished credentials by enabling multifactor authentication. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Apply least privilege access

Prevent attackers from spreading across the network by applying least privilege access principles, which limits user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive policies, and data protection to help secure both data and productivity.

Keep up to date

Mitigate the risk of software vulnerabilities by ensuring your organization's devices, infrastructure, and applications are kept up to date and correctly configured. Endpoint management solutions allow policies to be pushed to machines for correct configuration and ensure systems are running the latest versions.

Utilize antimalware

Stop malware attacks from executing by installing and enabling antimalware solutions on endpoints and devices. Utilize cloud-connected antimalware services for the most current and accurate detection capabilities.

Protect data

Know where your sensitive data is stored and who has access. Implement information protection best practices such as applying sensitivity labels and data loss prevention policies. If a breach does occur, it's critical that security teams know where the most sensitive data is stored and accessed.



HELLENIC

Source: Microsoft Corporation Digital Risks Report



Get In Touch !
www.isc2-chapter.gr
info@isc2-chapter.gr



Free Cyber Security Awareness Training; October 27th

