



HELLENIC

Connect | Educate | Inspire | Secure

Quo Vadis, CyberSecurity ?

Dr. John ILIADIS

CISSP, *rest of alphabet soup omitted*

President, (ISC)² Hellenic Chapter
&
IT Infrastructure Manager, TEIRESIAS S.A.



(ISC)² = International Information Systems Security Certification Consortium, established in 1989

Non-profit consortium of information security industry leaders

Supports security professionals throughout their careers

Global Standard for information security: (ISC)² CBK®

Over 300,000 members, associates, candidates; over 170 countries

300 members in Greece, established in 2015



HELLENIC



Ahoy Captain, Challenges ahead!

May you live in interesting times*

*Chinese curse



HELLENIC



Big Challenges *(some of them...)*

1. People

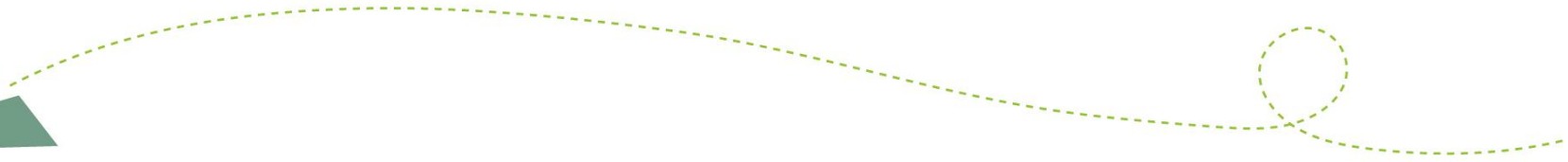
2. Processes

— **Risk**; not just a fun board game anymore

3. Technology

— **Cloud**: Welcome to





Challenge #1

People



HELLENIC



People, Part 1/3



- Attack surface ↑ - meanwhile:
 - We became more vulnerable to social engineering
 - 82% of breaches took advantage of the human factor
- Humans: the chain link that will become stronger





People, Part 2/3

- Workforce gap of 3.4 million CyberSecurity professionals
- (ISC)² migration pathway: CC - Certified in CyberSecurity.
free until Sep. 2023 or until coupon stock runs out





People, Part 3/3



- More professionals; is it better?
 - Not quite; we need more diversity!
 - Diverse groups [mitigate groupthink](#), but...
 - ...have [less confidence wrt their decisions](#) achieving the objective
- Managers beware!
 - Consider reduced confidence levels of diverse groups
 - Discuss ways to harness diverse groups' benefits





Challenge #2

Risk



HELLENIC



Risk, *the issues*



- » "Creative" Risk Management; common practice?
 - Unclear ways to estimate asset value, impact
 - Deliberate underestimation

- » Case Study: Cyber Risks in Canadian Banking Sector
 - “Known unknowns”; caution in relying on past data to predict future
 - Requires shift to resilience-centricity, continuous adaptation





Risk: regulating it

- "...security risk assessments of specific critical ICT ...supply chains"
([NIS2](#))
- ICT Third-Party Risk Management, [DORA](#)
- Guidance on Third-Party Relationships, [US Federal Reserve System](#)
- Outsourcing and third-party risk management, [Bank of England](#)





Risk: *directing it*

- Cyber-aware decision makers at the top
 - Call for Cyber-aware BoD members: [Consulting companies](#) and the [SEC!](#)
 - Minister for Cyber Security! ([Australia](#))
- Is Cyber Resilience integrated into enterprise risk* ?
 - Business executives: 92%
 - InfoSec-focused leaders: 55%
 - **Global Cybersecurity Outlook, World Economic Forum 2022*



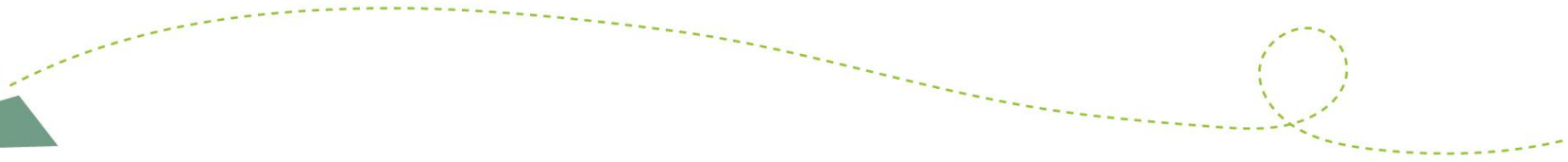


Risk: *harmonising it*



- Interoperable Risk Management Framework ([ENISA](#))
 - Unified risk assessment scale; results' comparison
 - Baseline security controls
 - Guidelines for evaluating and comparing risk appetites
- Using BIA to guide Risk Prioritisation/Response ([NIST](#))
 - Identify assets enabling mission objectives
 - Leaders deciding on risk appetite/tolerance
 - System owners applying BIA to develop asset protection requirements
 - BIA becoming an input to Enterprise Risk Management





Challenge #3

Cloud



HELLENIC



Cloud: *who consumes whom?*

Businesses consume a lot of Cloud

Cloud spending surpasses on-premise since 2020

or

Cloud consumes a lot of businesses?

Predictable OpEx costs?

Cloud impact on profit margins?



HELLENIC

Biggest threat in Cloud



62%

Misconfiguration
of the cloud
platform/wrong setup



54%

Insecure
interfaces/APIs

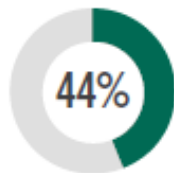


51%

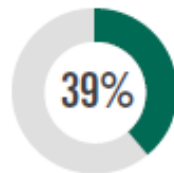
Exfiltration of
sensitive data



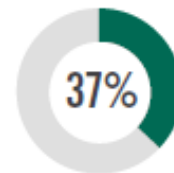
Unauthorized
access



Hijacking of
accounts,
services, or traffic



External
sharing of data



Foreign
state-sponsored
cyber attacks



HELLENIC

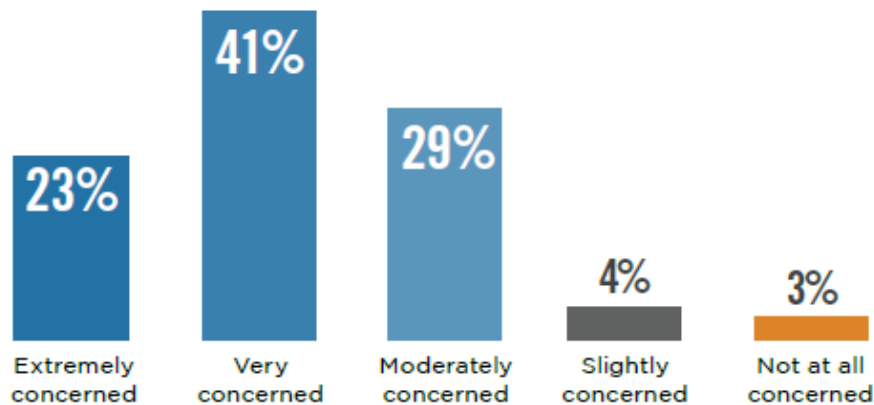
Source: Cloud Security Report 2022, (ISC)²

Cloud's missing ingredient



93%

of organizations are moderately to extremely concerned about the shortage of qualified cybersecurity professionals



HELLENIC

Source: Cloud Security Report 2022, (ISC)²



Where to?



- Many emerging cyber battlefields
 - supply chain, ransomware, cloud, regulations, professionals' gap, etc...
- Starting point? Security Culture; the road to maturity...
 - Culture eats strategy for breakfast
 - Security awareness on all levels
 - Security pros: hone communication skills, adapt per audience
- Security maturity; where does it lead?
 - [66% of C-suite](#) view cybersecurity as a revenue-enabler
 - [Only 34%](#) of C-suite view cybersecurity as a cost-center



Thank you !

[j.iliadis {at} isc2-chapter.gr](mailto:j.iliadis@isc2-chapter.gr)



HELLENIC