University of Pisa
Department of Information Engineering
Master Degree in Cybersecurity
Organizational Sciences Module

Academic Year 2024 -25

Cybersecurity within organizational sciences – awareness, culture and resilience

ABOUT ME

- **Post-doctoral research** at the University Centre for Logistics Systems (University of Pisa) - “**MA**ritime and port cyber organizational **RES**ilience” **(MARES)**
- 2024 → Ph.D in Business and Management
- 2019 → Master Degree completed with honors in Strategy, Management and Control
- Since 2020 → **Projects**: **«Assessment Cybersecurity Readiness»**, University of Florence – **«cyber preparedness in healthcare (CAPSULE)»**, Department of Information Engineering, University of Pisa
- Collaborations: University of Florence – University of Geneva

PoLog

Università di Pisa
Polo Sistemi Logistici - Livorno

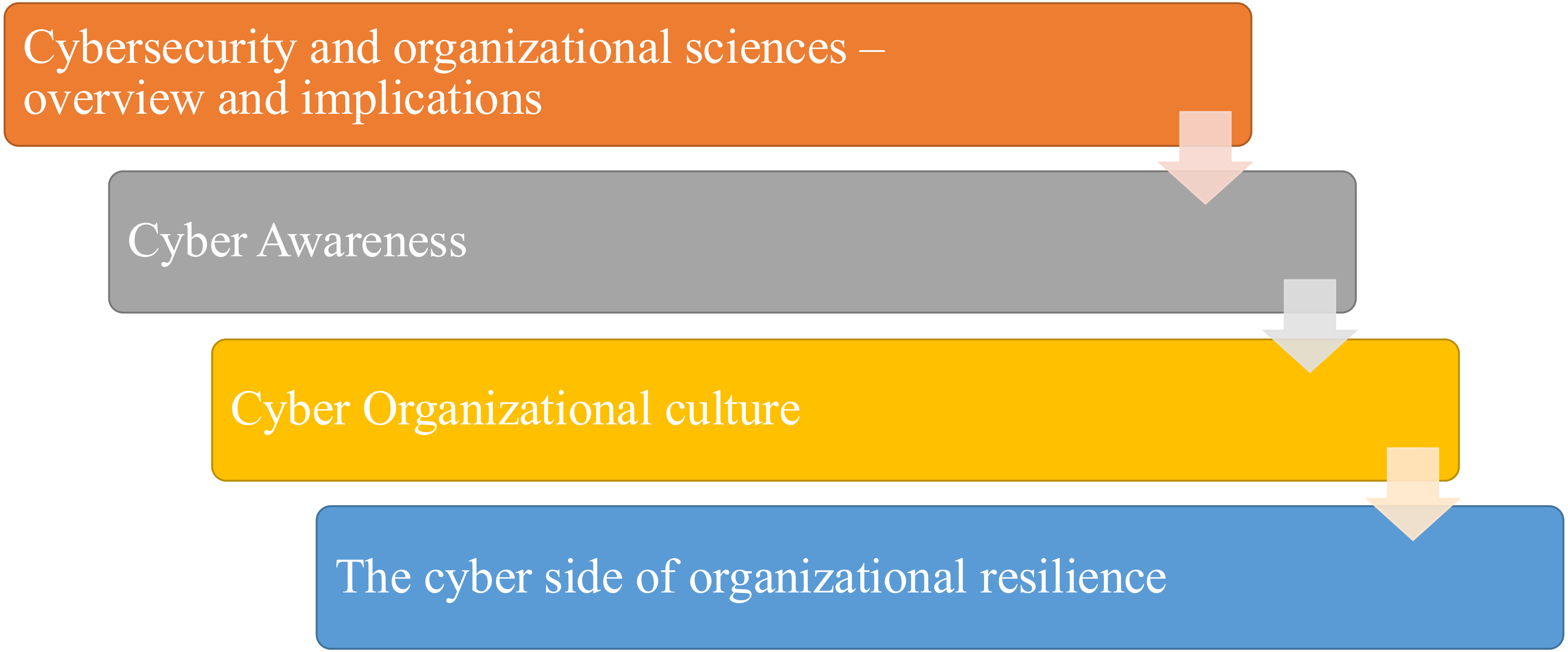
UNIVERSITÉ
DE GENÈVE

UNIVERSITÀ
DEGLI STUDI
FIRENZE

BIBLIOGRAPHY

- Duchek, S. (2020). **Organizational resilience: a capability-based conceptualization.** Business Research, 13(1), 215-246, paragraphs 3.1, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.3, 3.3.1, 3.4, 3.4.1, 3.4.2, 3.4.3, 3.4.4, pp. 223 to 232, and 234 to 237).
- Su, W., & Junge, S. (2023). **Unlocking the recipe for organizational resilience: A review and future research directions.** European Management Journal. https://doi.org/10.1016/j.emj.2023.03.002 (paragraph 5.1).
- -Huang, K., & Pearlson, K. (2019, January). **For what technology can't fix: Building a model of organizational cybersecurity culture.** In Proceedings of the 52nd Hawaii International Conference on System Sciences (sections 2 and 3, pp. 6399 to 6403).
- National Institute of Standards and Technology (2003). **Building an Information Technology Security Awareness and Training Program.** https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf (paragraphs 2, 3, 3.1, pp. 7 to 16).
- Materials provided by the teacher during the course **(slides).**

OUTLINE



Cybersecurity and organizational sciences – overview and implications

Cyber Awareness

Cyber Organizational culture

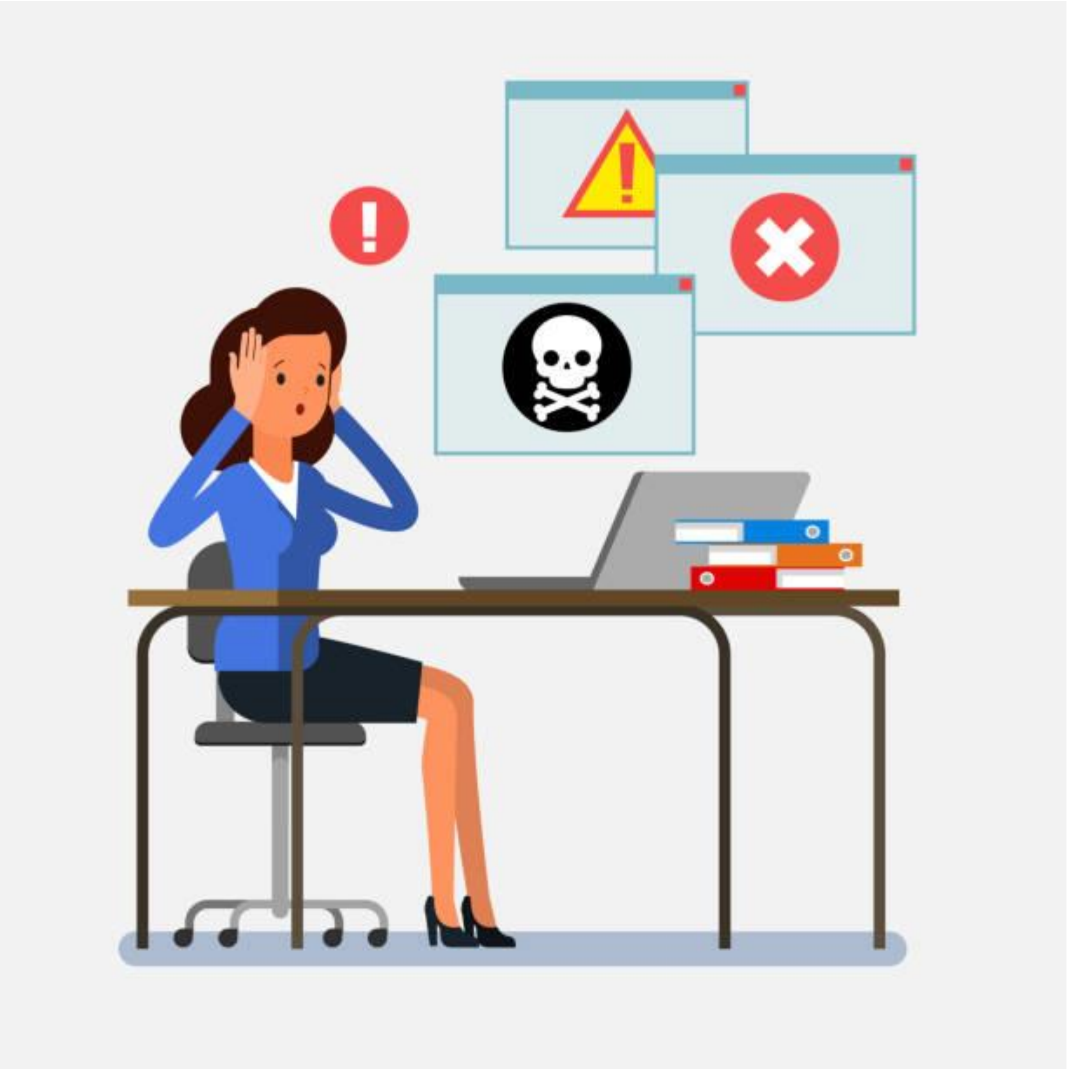
The cyber side of organizational resilience

Why?

A: Practical
B: Theoretical

Human error

- Vulnerability
- Malicious and non-malicious noncompliance with cybersecurity policy
- Skill based errors
- Decision-based errors



Cyber-risks

- Inside threats
- Outside threats
- How are they interconnected?
- Geographical boundaries

SMEs vs Big companies

- Global cybercrime costs are expected reach ***$13.5 trillion annually by 2028.***

- Data breaches and cyberattacks continue to impact organizations large and small and in particular ***very small one*** (CLUSIT 2021, 2022; Verizon 2022).

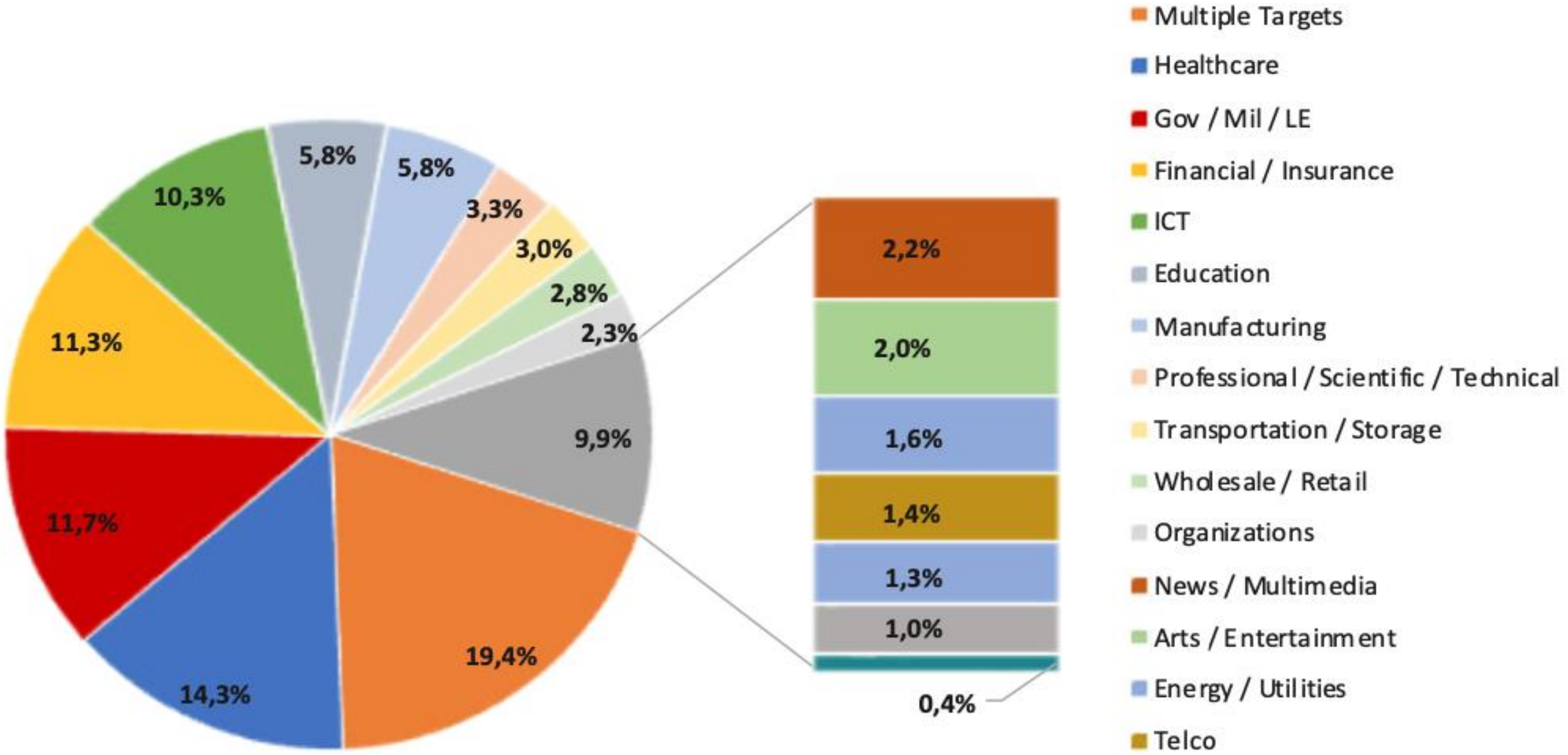
Sector

- ***Healthcare:*** HCA Healthcare, 2023, 11 million patients

- ***Port and Logistics:*** Moller Maersk, 2017, 10 billion dollars in damages

- ***Tourism:*** Sabre Booking Company, 1.3 terabytes of data stolen

- ***Finance:*** First American Financial Corporation, 2019, 885 million credit card applications



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Cybersecurity is…

- ➢ Complex
- ➢Uncertain
- ➢Evaluative

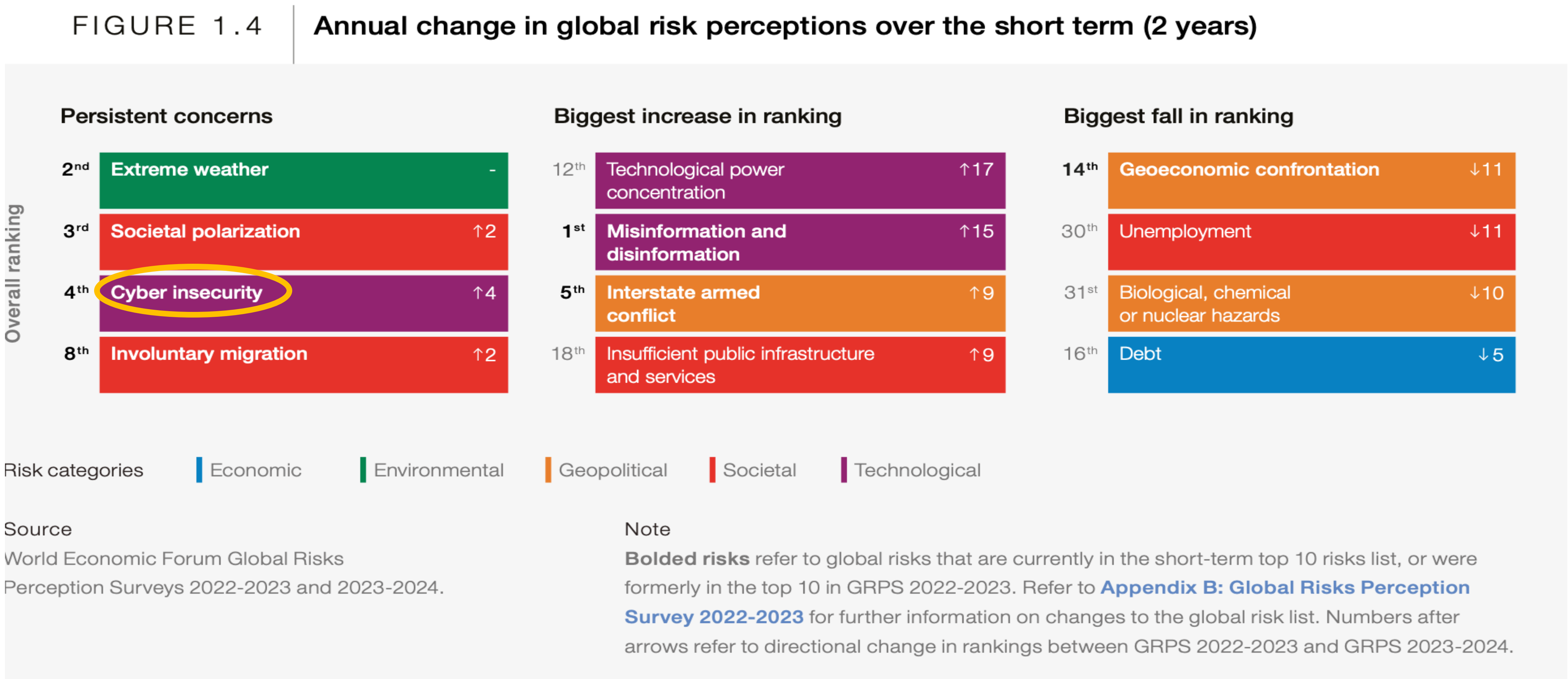


FIGURE 1.4 **Annual change in global risk perceptions over the short term (2 years)**

Overall ranking

Persistent concerns			Biggest increase in ranking			Biggest fall in ranking		
2nd	**Extreme weather**	-	12th	Technological power concentration	↑17	14th	**Geoeconomic confrontation**	↓11
3rd	**Societal polarization**	↑2	1st	**Misinformation and disinformation**	↑15	30th	Unemployment	↓11
4th	**Cyber insecurity**	↑4	5th	**Interstate armed conflict**	↑9	31st	Biological, chemical or nuclear hazards	↓10
8th	**Involuntary migration**	↑2	18th	Insufficient public infrastructure and services	↑9	16th	Debt	↓5

Risk categories | Economic | Environmental | Geopolitical | Societal | Technological

Source
World Economic Forum Global Risks Perception Surveys 2022-2023 and 2023-2024.

Note
Bolded risks refer to global risks that are currently in the short-term top 10 risks list, or were formerly in the top 10 in GRPS 2022-2023. Refer to **Appendix B: Global Risks Perception Survey 2022-2023** for further information on changes to the global risk list. Numbers after arrows refer to directional change in rankings between GRPS 2022-2023 and GRPS 2023-2024.

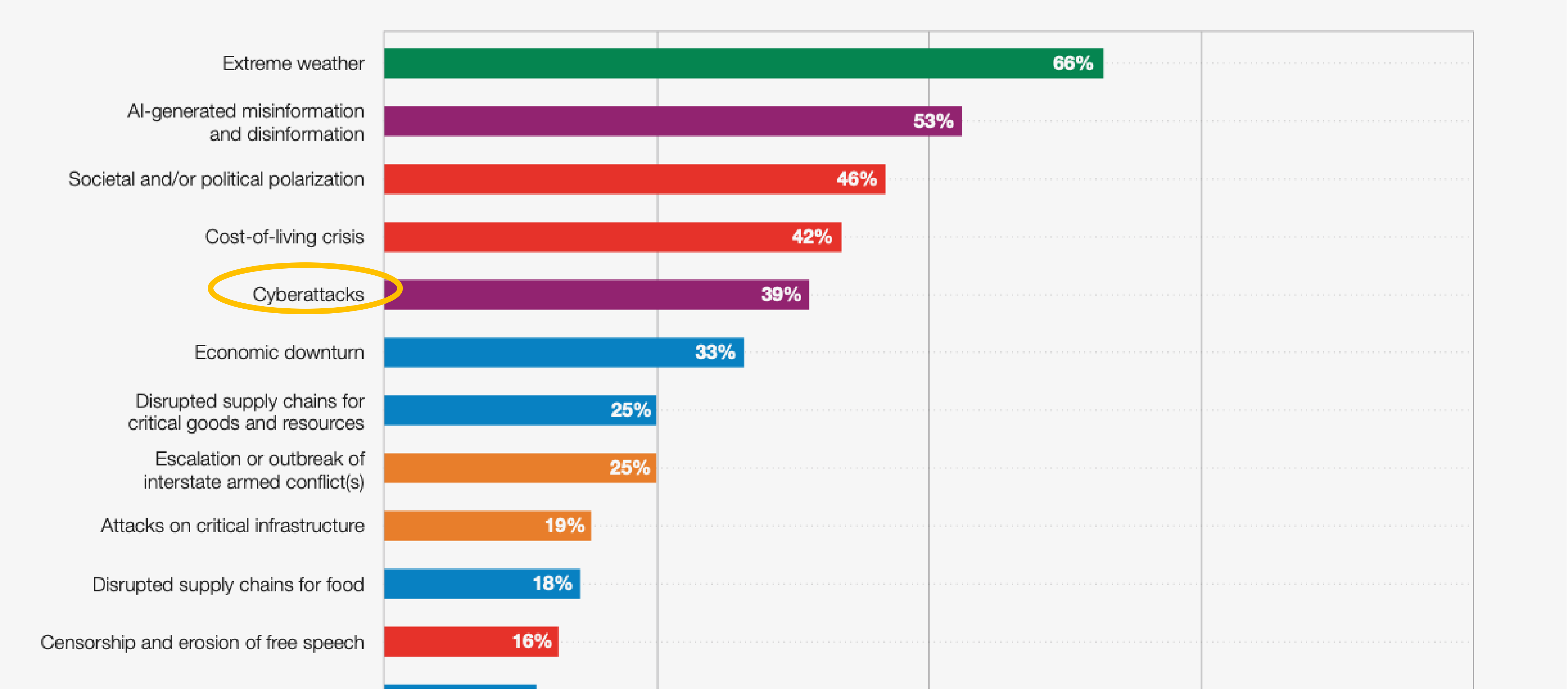
Cyber insecurity: Use of cyber weapons and tools to conduct cyberwarfare, cyberespionage and cybercrime to gain control over a digital presence and/or cause operational disruption. Includes: ransomware, data fraud or theft.

Source: World Economic Forum (2024). Global Risk Report. https://www.weforum.org/publications/global-risks-report-2024/

FIGURE 1.2

Current risk landscape

"Please select up to five risks that you believe are most likely to present a material crisis on a global scale in 2024."

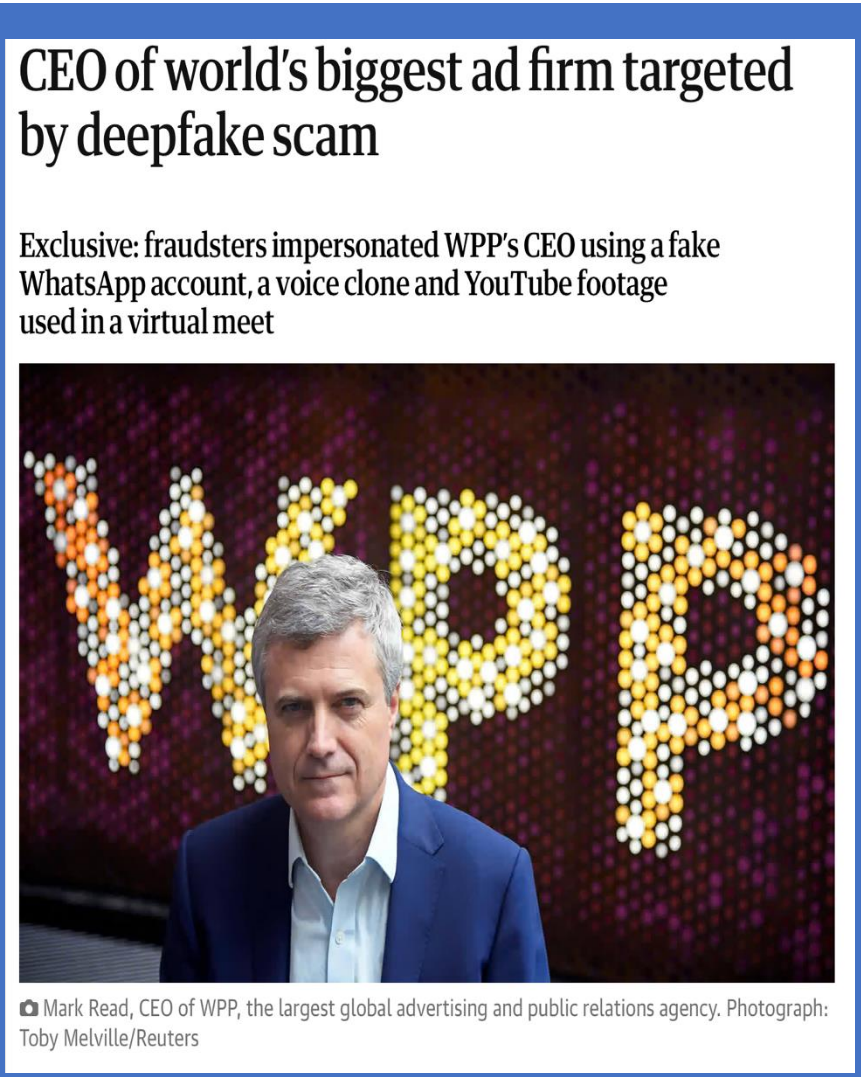


Source: World Economic Forum (2024). Global Risk Report. https://www.weforum.org/publications/global-risks-report-2024/

- ***Reinforcing mechanisms*** → while new technologies are developed and implemented as solutions for cyber incidents, the same brought ***side effects*** (e.g., being employed by cyber-criminals to convey more effective cyber-attacks).

- ***World Economic Forum*** → «the same attack vectors that have been employed by cybercriminals are still being used; however, new technology paves the way for nefarious activity» (p.15).

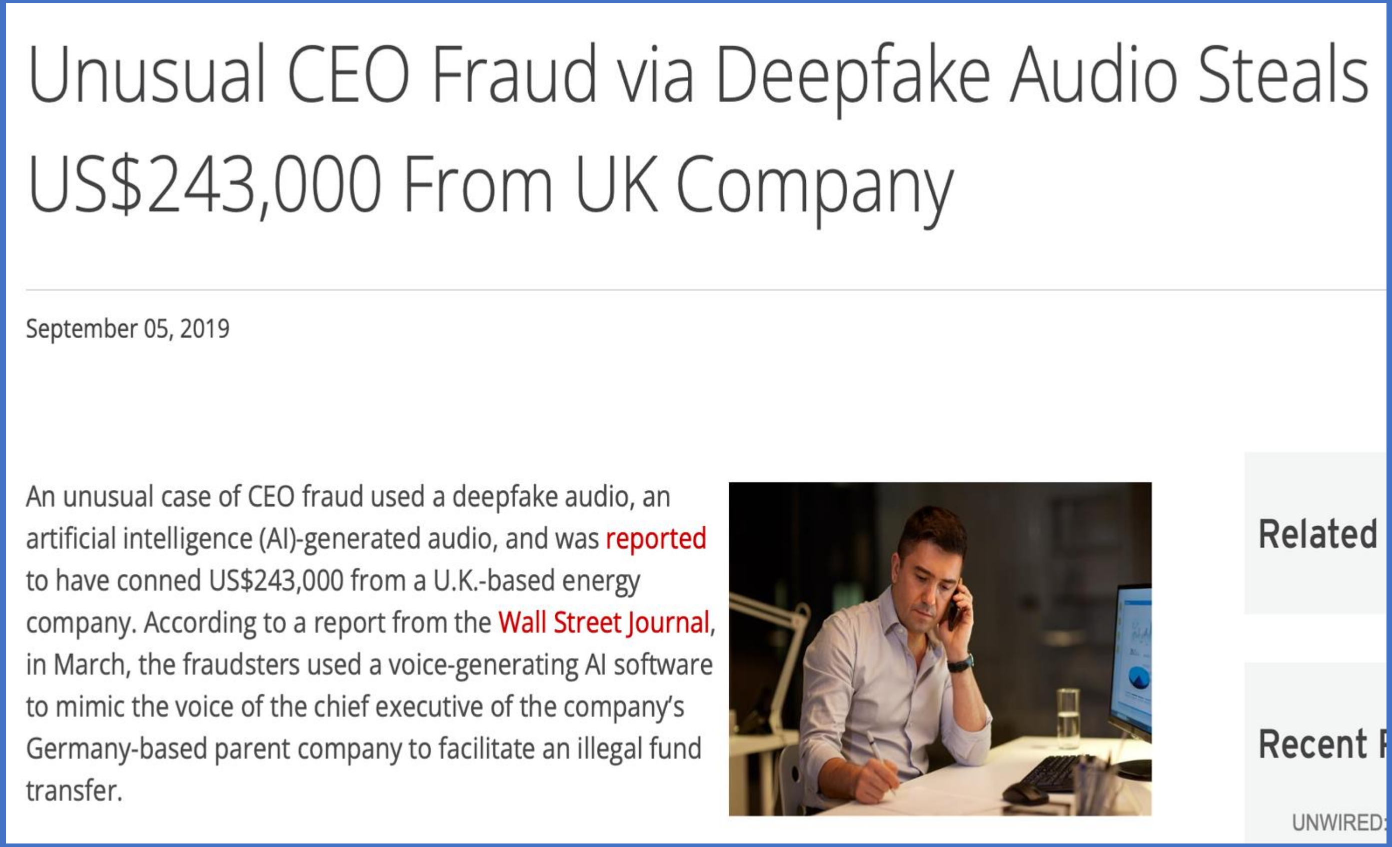
Complex



CEO of world's biggest ad firm targeted by deepfake scam

Exclusive: fraudsters impersonated WPP's CEO using a fake WhatsApp account, a voice clone and YouTube footage used in a virtual meet

Mark Read, CEO of WPP, the largest global advertising and public relations agency. Photograph: Toby Melville/Reuters



Unusual CEO Fraud via Deepfake Audio Steals US$243,000 From UK Company

September 05, 2019

An unusual case of CEO fraud used a deepfake audio, an artificial intelligence (AI)-generated audio, and was reported to have conned US$243,000 from a U.K.-based energy company. According to a report from the Wall Street Journal, in March, the fraudsters used a voice-generating AI software to mimic the voice of the chief executive of the company's Germany-based parent company to facilitate an illegal fund transfer.

Related

Recent

UNWIRED

Sources: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company
https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam

- ***Social factors*** have been depicted as hindering any technological prediction which «depends on an ***interplay between many factors***, some of which are much ***less predictable than the activities of an industrial laboratory***» (Hansson, 2011).

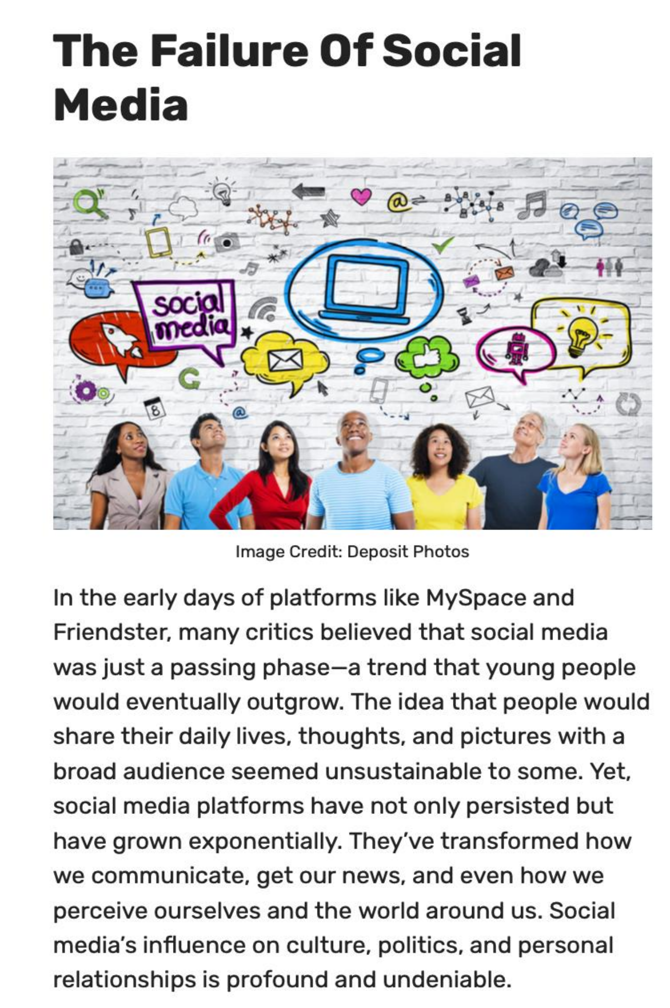
- Samuel (2019) reported that «humans determine not only which (and how) technologies get created, but also, ***how technologies get disseminated and used***» (p.1).

- At each stage of digital technology development, «although there have been glimmers of this future, by and large, ***it has taken us by surprise***» (Batty, 2021).

Uncertain

Uncertain

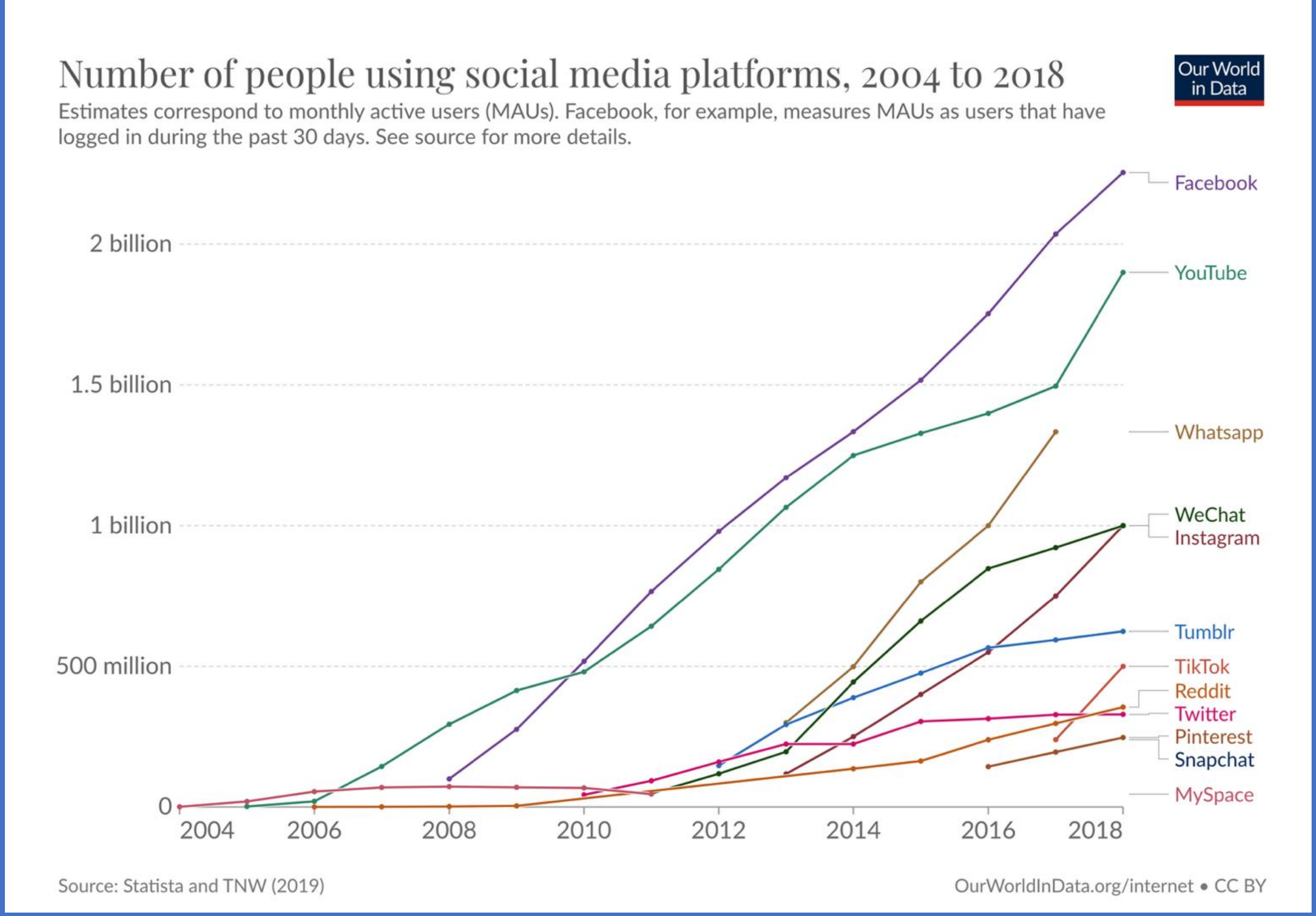
Example



The Failure Of Social Media

Image Credit: Deposit Photos

In the early days of platforms like MySpace and Friendster, many critics believed that social media was just a passing phase—a trend that young people would eventually outgrow. The idea that people would share their daily lives, thoughts, and pictures with a broad audience seemed unsustainable to some. Yet, social media platforms have not only persisted but have grown exponentially. They've transformed how we communicate, get our news, and even how we perceive ourselves and the world around us. Social media's influence on culture, politics, and personal relationships is profound and undeniable.



Number of people using social media platforms, 2004 to 2018

Estimates correspond to monthly active users (MAUs). Facebook, for example, measures MAUs as users that have logged in during the past 30 days. See source for more details.

Source: Statista and TNW (2019)

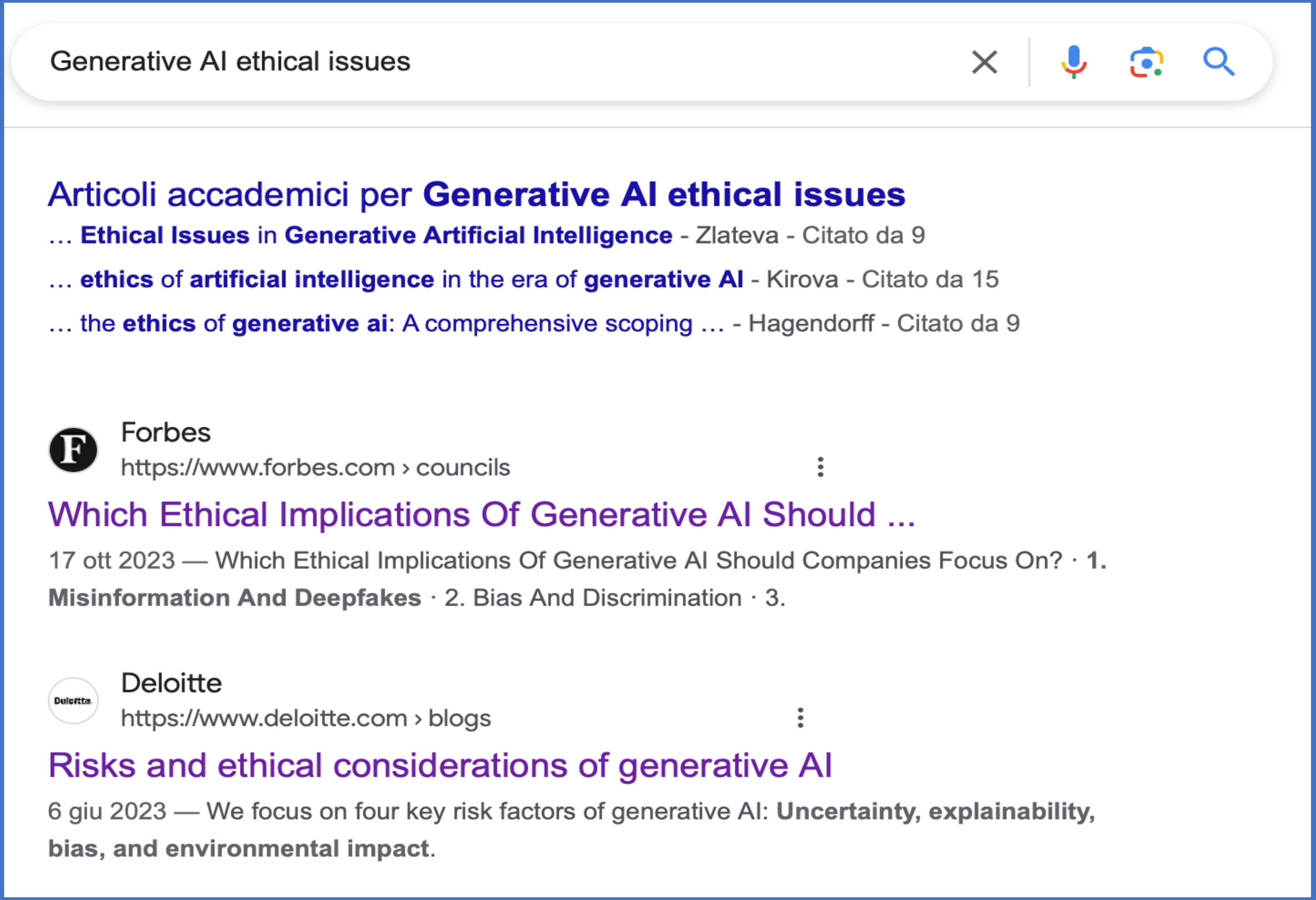
OurWorldInData.org/internet • CC BY

Sources: https://stemeducationguide.com/tech-predictions-2000s/
https://ourworldindata.org/rise-of-social-media
https://www.weforum.org/agenda/2020/11/heres-how-technology-has-changed-and-changed-us-over-the-past-20-years/

Example

Ethical concerns

- Academic research
- Environmental impacts
- DeepFakes contents
- ….



Generative AI ethical issues

Articoli accademici per **Generative AI ethical issues**

… **Ethical Issues** in **Generative Artificial Intelligence** - Zlateva - Citato da 9

… **ethics** of **artificial intelligence** in the era of **generative AI** - Kirova - Citato da 15

… the **ethics** of **generative ai**: A comprehensive scoping … - Hagendorff - Citato da 9

Forbes
https://www.forbes.com › councils

Which Ethical Implications Of Generative AI Should ...

17 ott 2023 — Which Ethical Implications Of Generative AI Should Companies Focus On? · **1. Misinformation And Deepfakes** · 2. Bias And Discrimination · 3.

Deloitte
https://www.deloitte.com › blogs

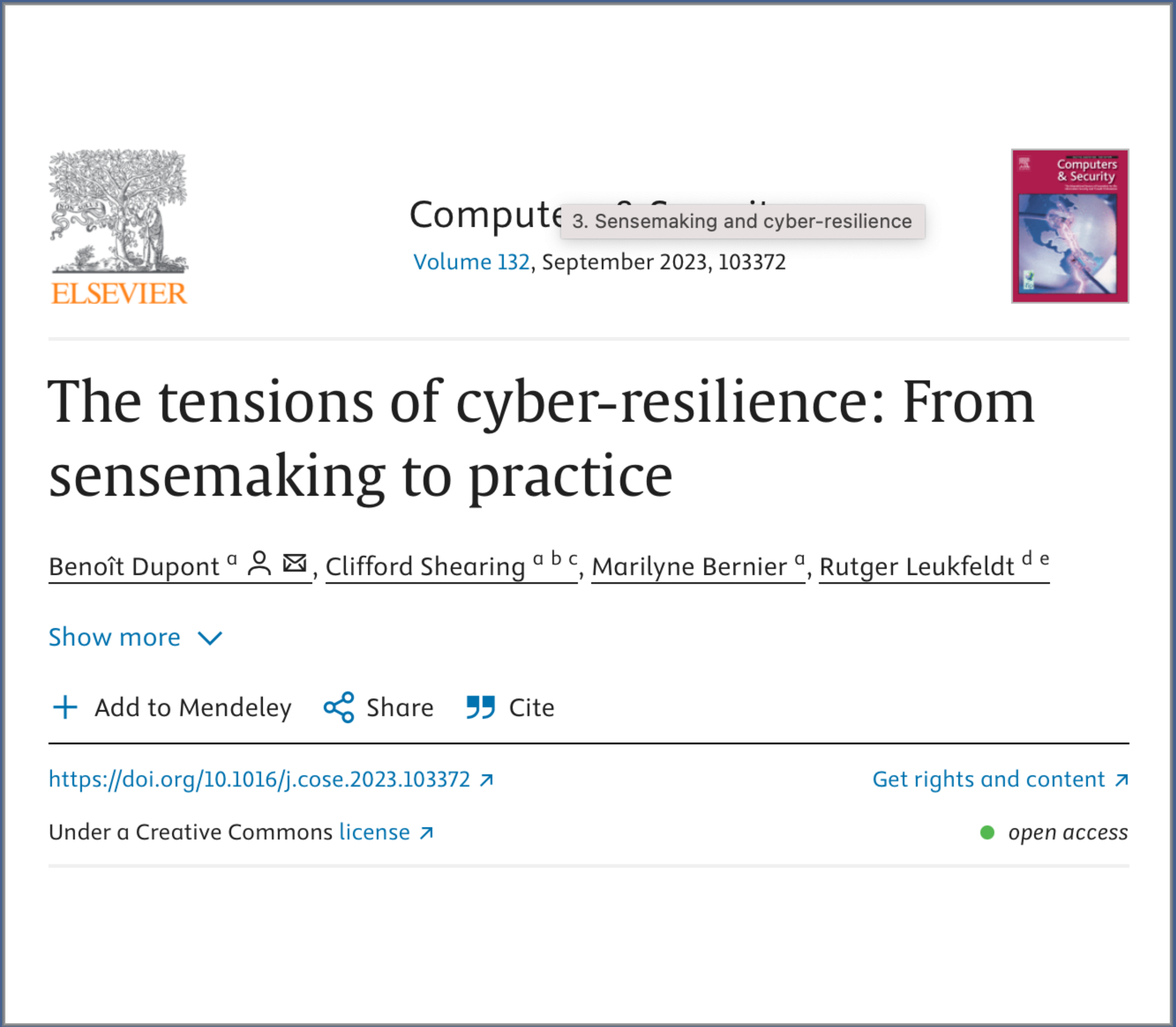
Risks and ethical considerations of generative AI

6 giu 2023 — We focus on four key risk factors of generative AI: **Uncertainty, explainability, bias, and environmental impact**.

- Cybersecurity could be depicted as ***multidisciplinary***, thus involving different fields such as ***social sciences, organization studies, law, and engineering*** (Ferdousi, 2024).

- As an example, the so-called human factor has brought organization studies into the arena of cybersecurity since "***technical expertise is not the only commodity that can aid in understanding and ameliorating cyberattacks***" (Dalal et al., 2021, p. 2).

Evaluative



ELSEVIER

Compute

3. Sensemaking and cyber-resilience

Volume 132, September 2023, 103372

The tensions of cyber-resilience: From sensemaking to practice

Benoît Dupont [a], Clifford Shearing [a b c], Marilyne Bernier [a], Rutger Leukfeldt [d e]

Show more

+ Add to Mendeley · Share · Cite

https://doi.org/10.1016/j.cose.2023.103372 ↗ · Get rights and content ↗

Under a Creative Commons license ↗ · ● open access

JOINT NATIONAL CONFERENCE ON CYBERSECURITY
ITASEC25
Italian Conference On Cybersecurity
SERICS
Conference On Security And Rights In The Cyber Space
FEBRUARY 3-8, 2025 - BOLOGNA

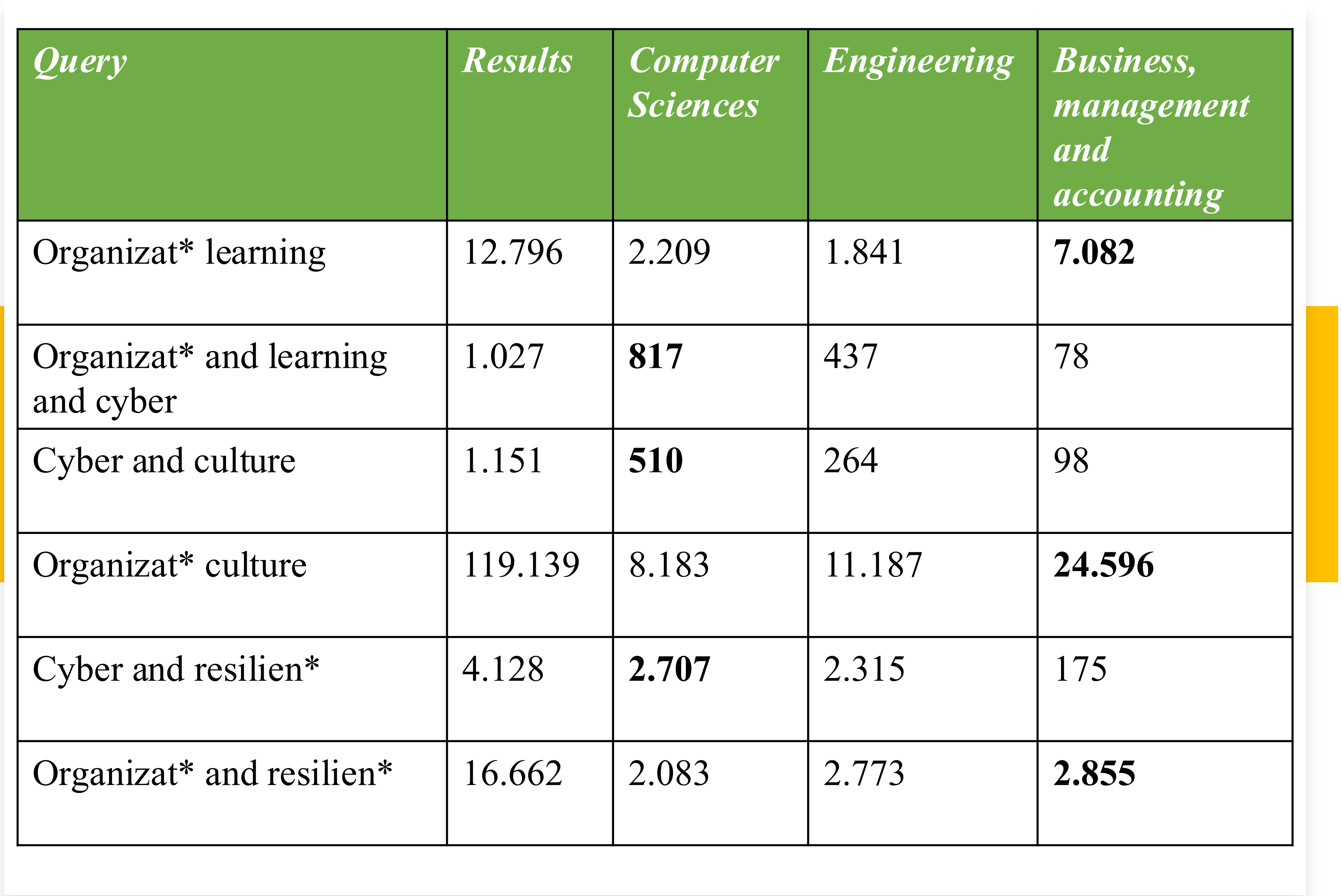
Human, social and legal aspects:

- Disinformation, fake news and deep fakes
- Human issues and awareness
- Security management and governance
- Cyber education and training
- Legal aspects, compliance and regulation

Organizational cybersecurity

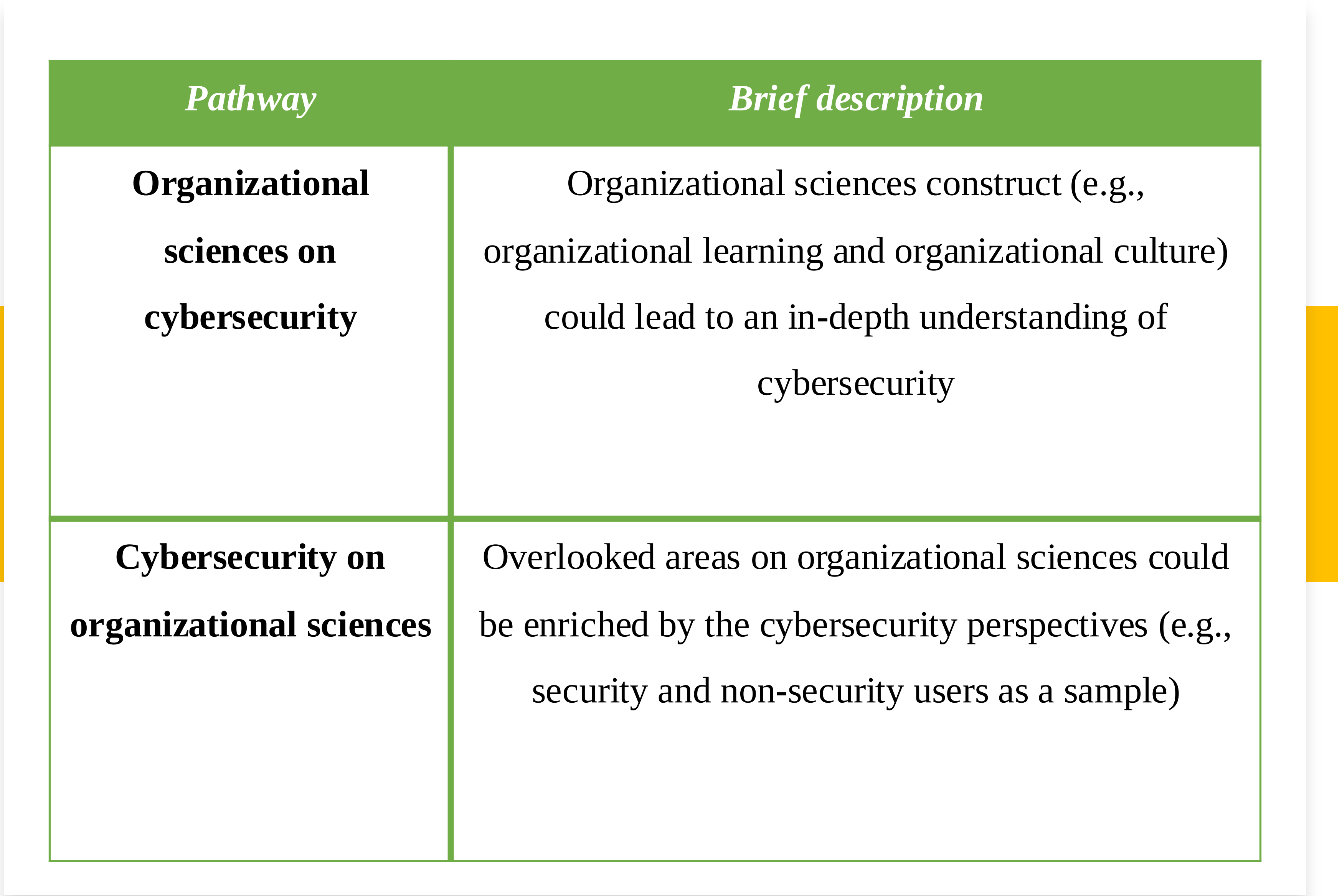
is broadly defined as «the efforts organizations take to ***protect and defend*** their information assets, ***regardless of the form in which those assets exist***, from threats ***internal and external*** to the organization»

Literature Research - Scopus



Query	***Results***	***Computer Sciences***	***Engineering***	***Business, management and accounting***
Organizat* learning	12.796	2.209	1.841	**7.082**
Organizat* and learning and cyber	1.027	**817**	437	78
Cyber and culture	1.151	**510**	264	98
Organizat* culture	119.139	8.183	11.187	**24.596**
Cyber and resilien*	4.128	**2.707**	2.315	175
Organizat* and resilien*	16.662	2.083	2.773	**2.855**

Multiple pathways for cross-contamination



Pathway	*Brief description*
Organizational sciences on cybersecurity	Organizational sciences construct (e.g., organizational learning and organizational culture) could lead to an in-depth understanding of cybersecurity
Cybersecurity on organizational sciences	Overlooked areas on organizational sciences could be enriched by the cybersecurity perspectives (e.g., security and non-security users as a sample)

- ***Multisciplinary and proactive approach*** → A comprehensive cybersecurity strategy normally includes ***physical, procedural, logical and organizational forms of protection***. This new approach is oriented not only to technologies, but towards ***learning through the adverse events*** that occur, thus evolving from a defensive attitude to a ***proactive one***

- ***Situational awareness and strategy***→ ***scenario planning***, environmental monitoring, anticipation, preparation, training and education

Organizational science

↓

cybersecurity

- ***Organizational culture*** → cybersecurity is a core value in the ***long-term run*** of the organization

- ***Organizational learning*** → the ability to ***learn from past events***, carry on the experience in future projects and arise more powerful and strong than before

- ***Network approach*** → develop an inter-organizational and networking approach, especially creating ***relationships*** with strategic partners and national authorities

Organizational science

↓

cybersecurity

- ***End-user vs cyber-focused user*** → going beyond the classic sample analysis focused on gender or age

- ***Training effectiveness*** → how ***different training methods*** could impact and effect employees?

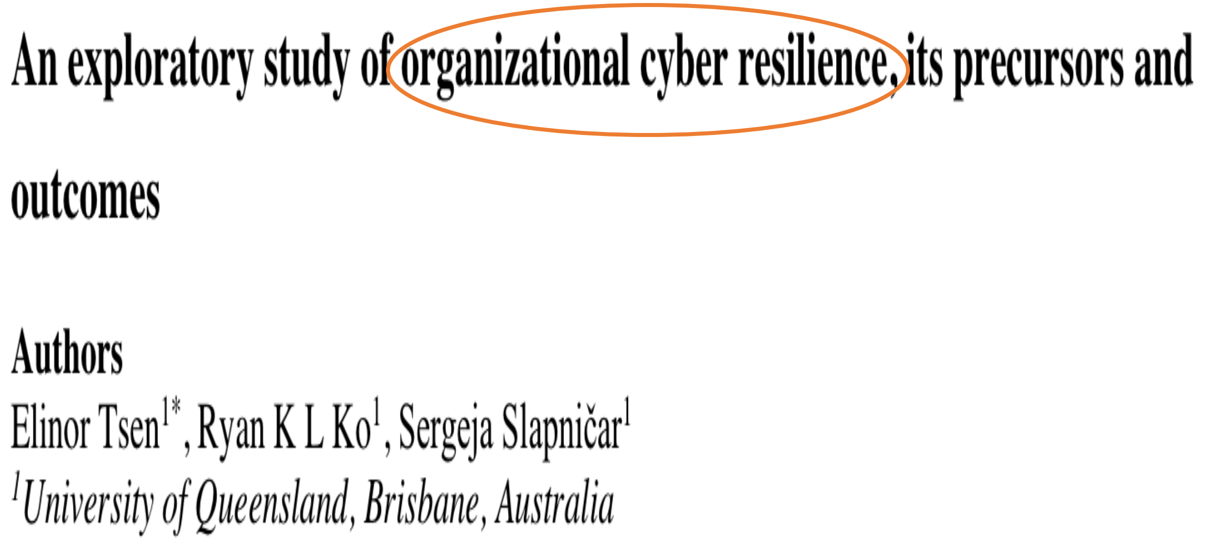
- ***Job performance*** → over training ***impede*** job performance (e.g., every email is suspicius)

Cybersecurity

↓

organizational sciences

SOME CONTRIBUTIONS ON THE ORGANIZATIONAL SIDE OF CYBERSECURITY

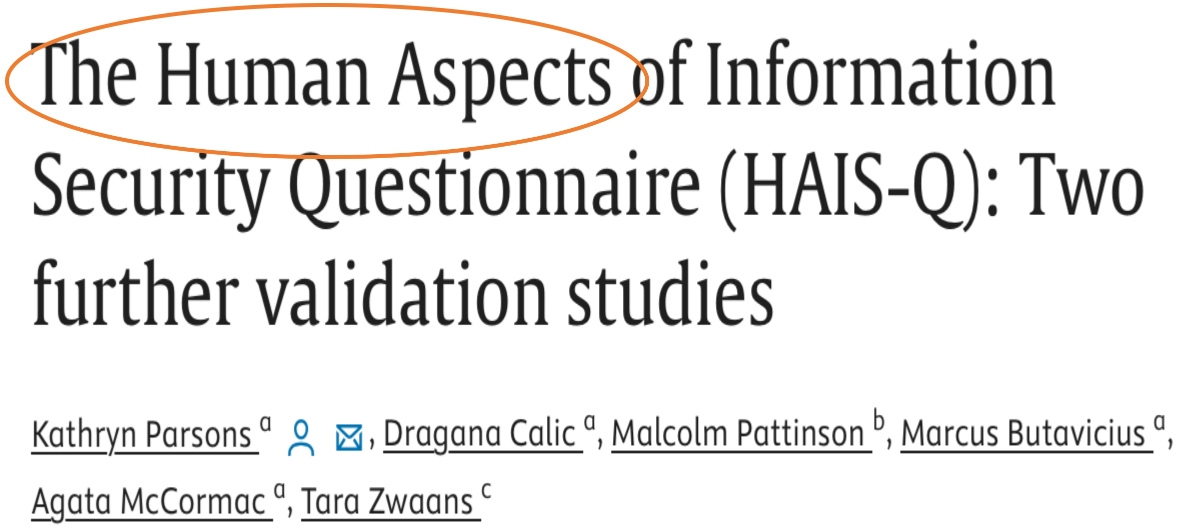


An exploratory study of organizational cyber resilience, its precursors and outcomes

Authors

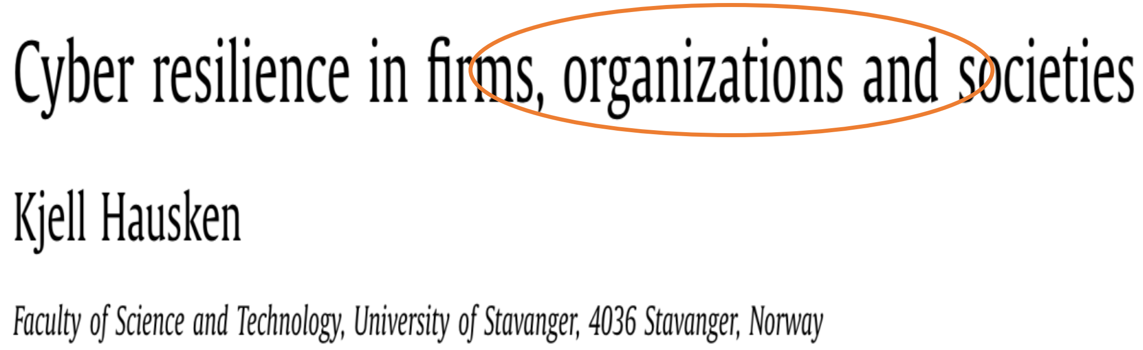
Elinor Tsen[1*], Ryan K L Ko[1], Sergeja Slapničar[1]

[1]University of Queensland, Brisbane, Australia



The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies

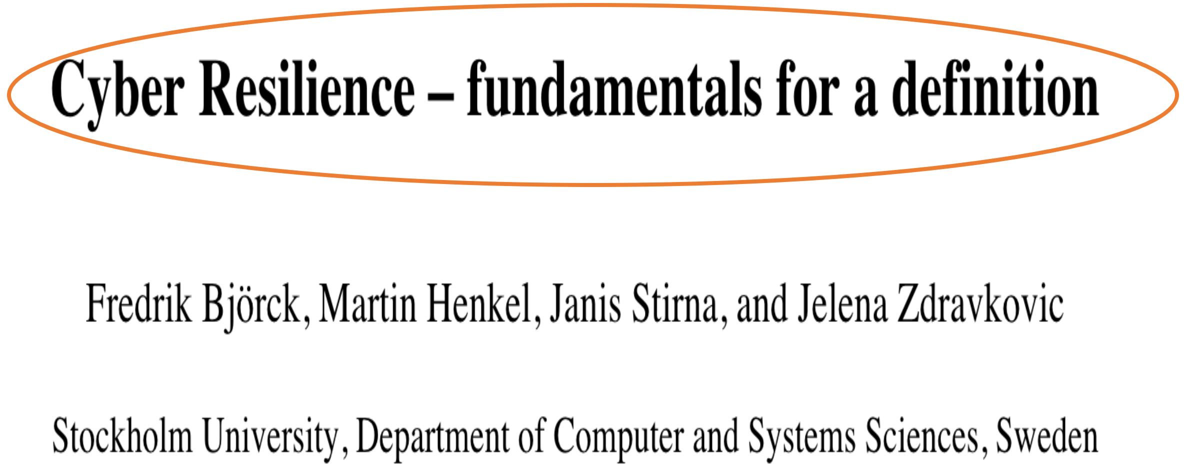
Kathryn Parsons [a], Dragana Calic [a], Malcolm Pattinson [b], Marcus Butavicius [a], Agata McCormac [a], Tara Zwaans [c]



Cyber resilience in firms, organizations and societies

Kjell Hausken

Faculty of Science and Technology, University of Stavanger, 4036 Stavanger, Norway



Cyber Resilience – fundamentals for a definition

Fredrik Björck, Martin Henkel, Janis Stirna, and Jelena Zdravkovic

Stockholm University, Department of Computer and Systems Sciences, Sweden

Contributions from international organizations

The WEF point of view

In collaboration with Accenture

WORLD ECONOMIC FORUM

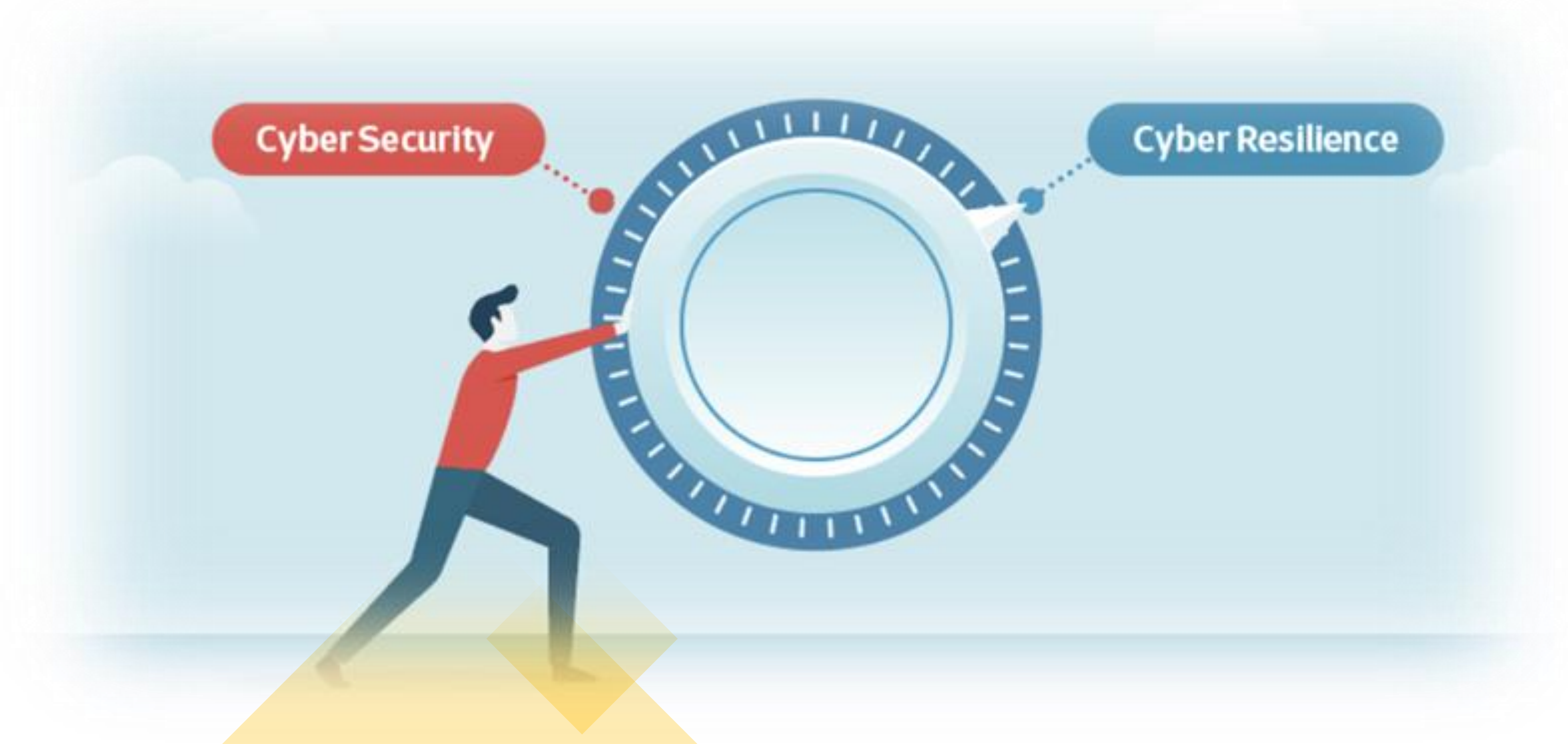
The Cyber Resilience Index:
Advancing Organizational Cyber Resilience

WHITE PAPER

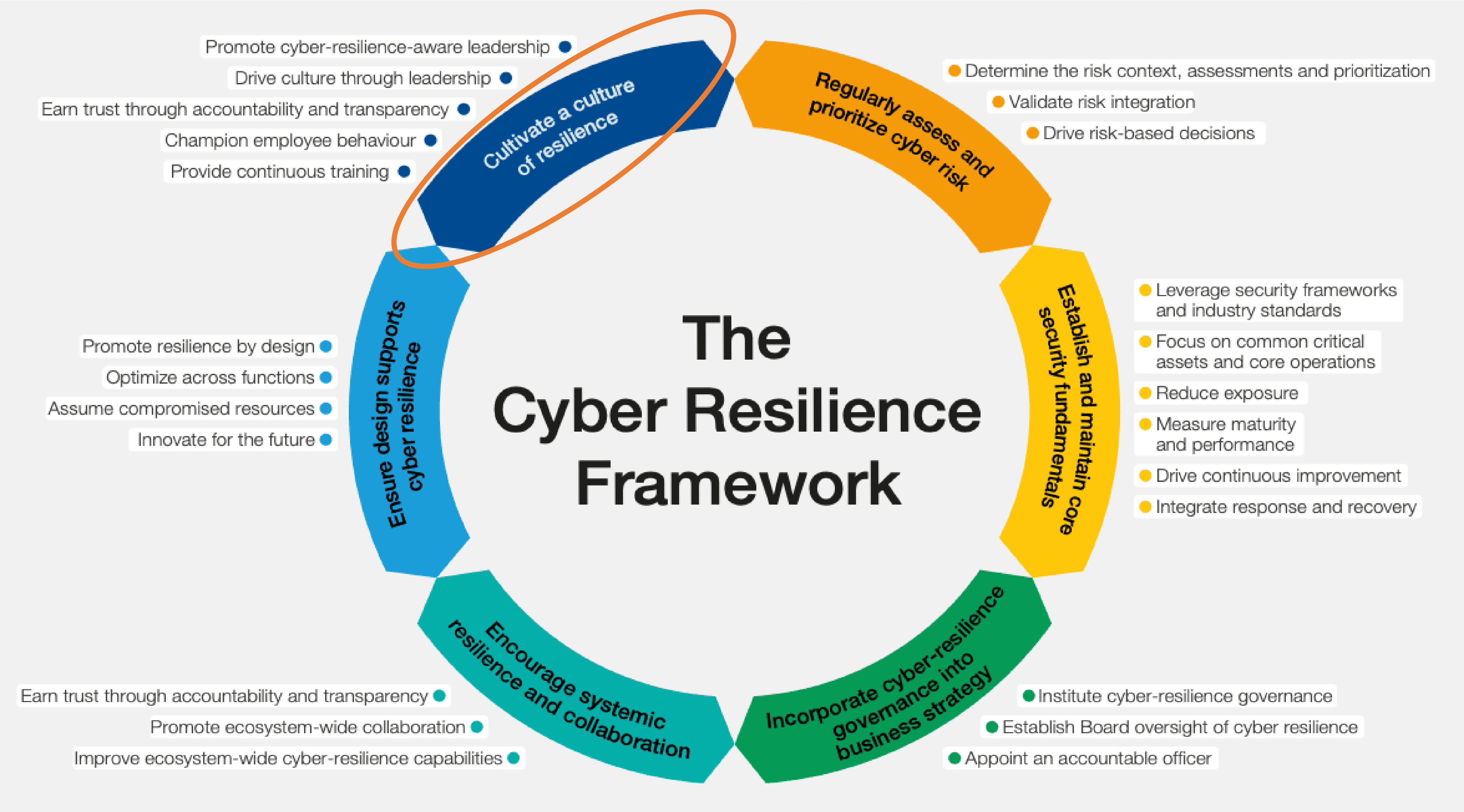
JULY 2022

Available at: https://www.weforum.org/whitepapers/the-cyber-resilience-index-advancing-organizational-cyber-resilience/

Cyber resilience is the ability of an organization to ***transcend any stresses, failures, hazards and threats to its cyber resources*** within the organization and its ***ecosystem,*** such that the organization ***mission,*** enable its ***culture*** and maintain can confidently pursue its its ***desired way of operating***.



The WEF point of view



The Cyber Resilience Framework

Cultivate a culture of resilience

- Promote cyber-resilience-aware leadership
- Drive culture through leadership
- Earn trust through accountability and transparency
- Champion employee behaviour
- Provide continuous training

Regularly assess and prioritize cyber risk

- Determine the risk context, assessments and prioritization
- Validate risk integration
- Drive risk-based decisions

Establish and maintain core security fundamentals

- Leverage security frameworks and industry standards
- Focus on common critical assets and core operations
- Reduce exposure
- Measure maturity and performance
- Drive continuous improvement
- Integrate response and recovery

Incorporate cyber-resilience governance into business strategy

- Institute cyber-resilience governance
- Establish Board oversight of cyber resilience
- Appoint an accountable officer

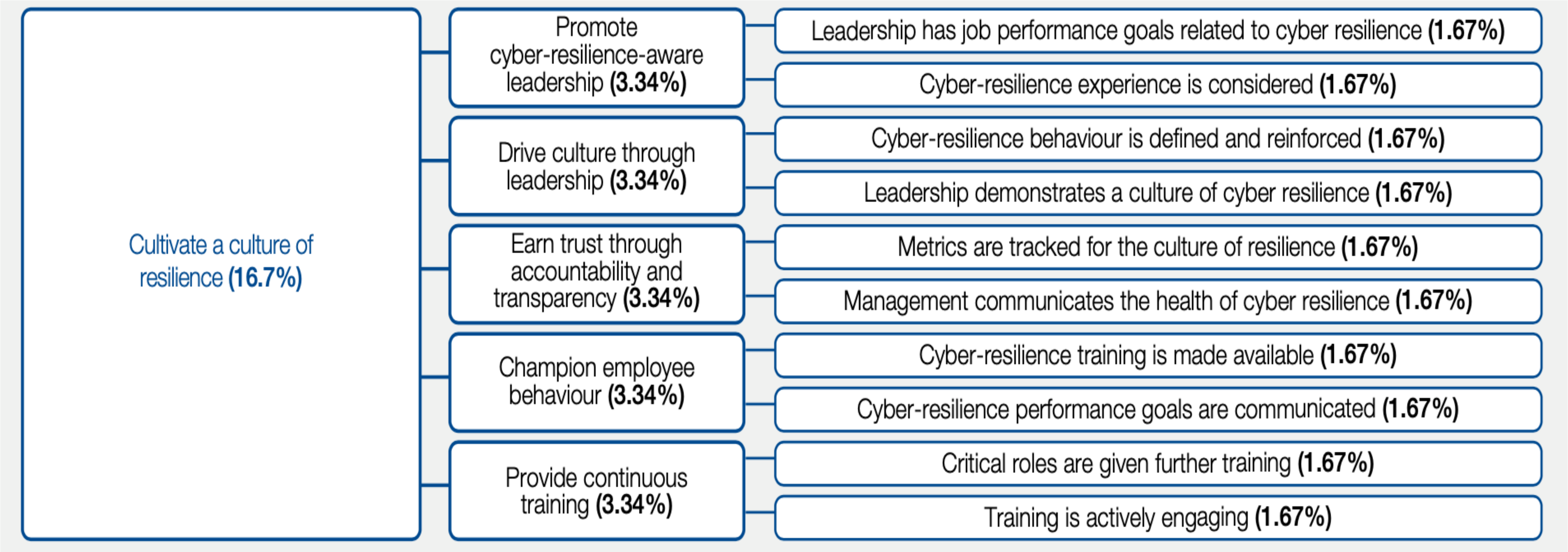
Encourage systemic resilience and collaboration

- Earn trust through accountability and transparency
- Promote ecosystem-wide collaboration
- Improve ecosystem-wide cyber-resilience capabilities

Ensure design supports cyber resilience

- Promote resilience by design
- Optimize across functions
- Assume compromised resources
- Innovate for the future

The WEF point of view



Cultivate a culture of resilience **(16.7%)**

Promote cyber-resilience-aware leadership **(3.34%)**

Leadership has job performance goals related to cyber resilience **(1.67%)**

Cyber-resilience experience is considered **(1.67%)**

Drive culture through leadership **(3.34%)**

Cyber-resilience behaviour is defined and reinforced **(1.67%)**

Leadership demonstrates a culture of cyber resilience **(1.67%)**

Earn trust through accountability and transparency **(3.34%)**

Metrics are tracked for the culture of resilience **(1.67%)**

Management communicates the health of cyber resilience **(1.67%)**

Champion employee behaviour **(3.34%)**

Cyber-resilience training is made available **(1.67%)**

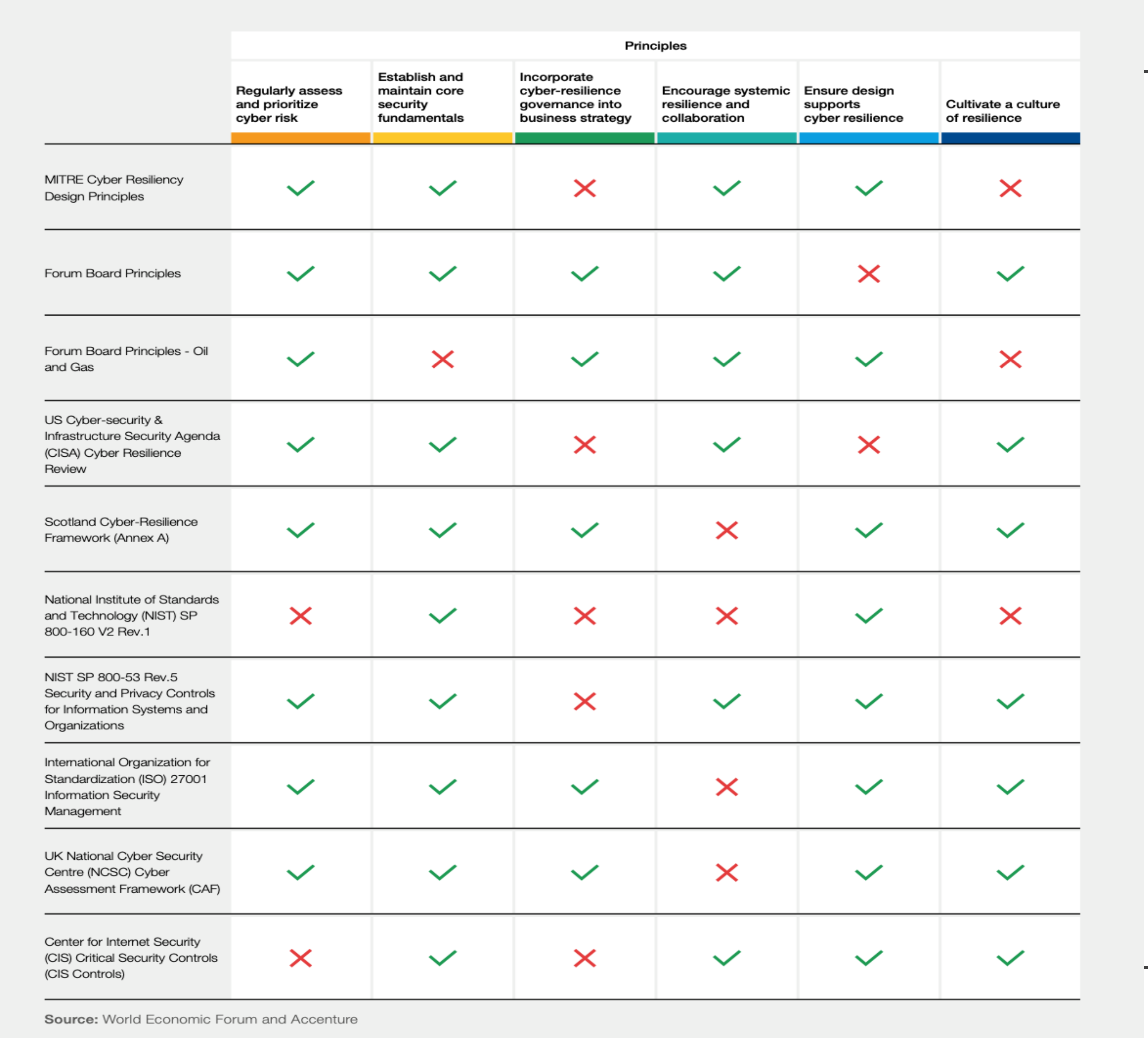
Cyber-resilience performance goals are communicated **(1.67%)**

Provide continuous training **(3.34%)**

Critical roles are given further training **(1.67%)**

Training is actively engaging **(1.67%)**

The WEF point of view



	Principles					
	Regularly assess and prioritize cyber risk	Establish and maintain core security fundamentals	Incorporate cyber-resilience governance into business strategy	Encourage systemic resilience and collaboration	Ensure design supports cyber resilience	Cultivate a culture of resilience
MITRE Cyber Resiliency Design Principles	✓	✓	✗	✓	✓	✗
Forum Board Principles	✓	✓	✓	✓	✗	✓
Forum Board Principles - Oil and Gas	✓	✗	✓	✓	✓	✗
US Cyber-security & Infrastructure Security Agenda (CISA) Cyber Resilience Review	✓	✓	✗	✓	✗	✓
Scotland Cyber-Resilience Framework (Annex A)	✓	✓	✓	✗	✓	✓
National Institute of Standards and Technology (NIST) SP 800-160 V2 Rev.1	✗	✓	✗	✗	✓	✗
NIST SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations	✓	✓	✗	✓	✓	✓
International Organization for Standardization (ISO) 27001 Information Security Management	✓	✓	✓	✗	✓	✓
UK National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)	✓	✓	✓	✗	✓	✓
Center for Internet Security (CIS) Critical Security Controls (CIS Controls)	✗	✓	✗	✓	✓	✓

Source: World Economic Forum and Accenture

«Technology is a critical piece of the cybersecurity puzzle, but just like a car with the most advanced technology the best defense is a well-trained driver»

People, not only technology

Awareness

Culture

Resilience