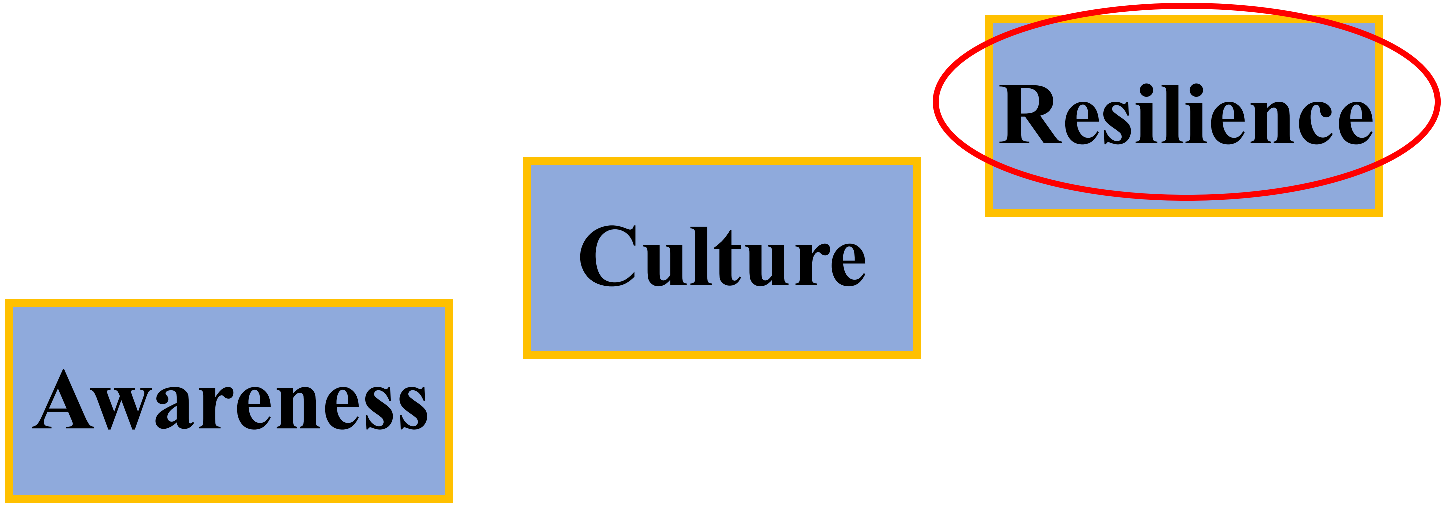
University of Pisa
Department of Information Engineering
Master Degree in Cybersecurity
Organizational Sciences Module

Academic Year 2024 -25

Cybersecurity within organizational sciences – awareness, culture and resilience

People, not only technology



Awareness

Culture

Resilience

Cyber organizational resilience

1) Ability to anticipate, withstand, recover, evolve (Bodeau and Graubart, 2011)

2) Ability to continuously deliver the intended outcome (Björck et al., 2015)

3) Ability to resist, respond, and recover from a cyber-attack (Hausken, 2020)

4) Ability to ensure business continuity in the face of attacks (Appiah et al., 2022)

Cyber organizational resilience – a broad conceptualization

*Cyber-OR is a **multifaceted concept***
that includes three stages, namely
anticipation and preparation, respond and withstand, and
recovery, change, and learn.

Cyber resilience in the environment

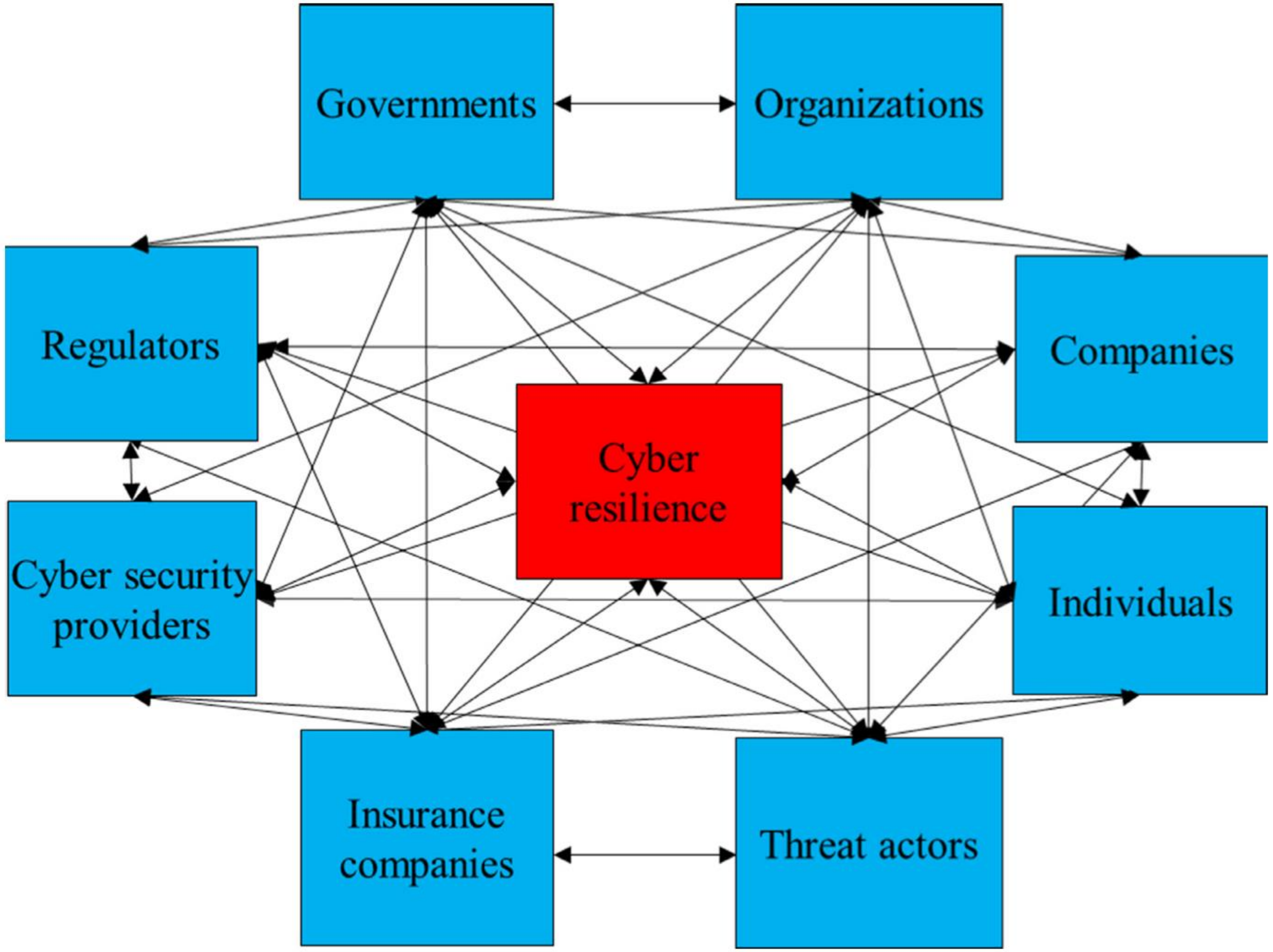


Fig. 1. Examples of actors involved in cyber resilience.

Source: Hausken, K. (2020). Cyber resilience in firms, organizations and societies. Internet of Things, 11, 100204. https://doi.org/10.1016/j.iot.2020.100204

Cyber resilience vs cybersecurity

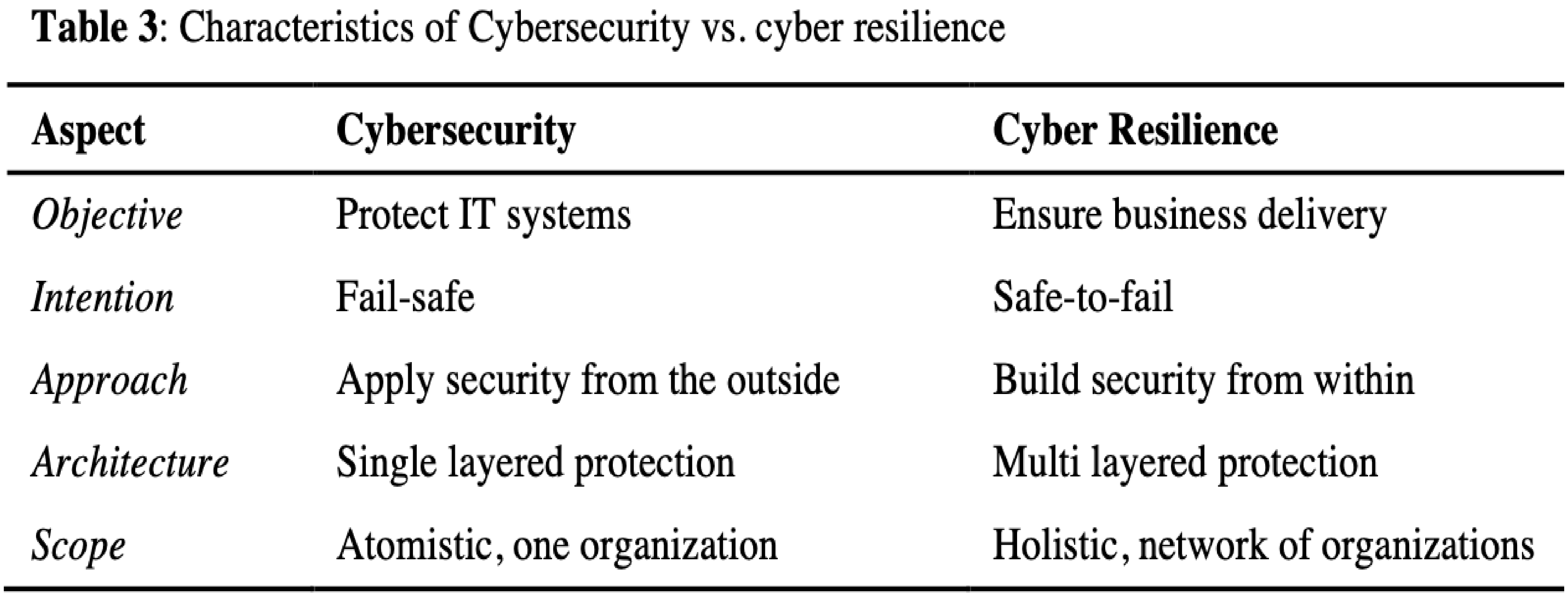


Table 3: Characteristics of Cybersecurity vs. cyber resilience

Aspect	**Cybersecurity**	**Cyber Resilience**
Objective	Protect IT systems	Ensure business delivery
Intention	Fail-safe	Safe-to-fail
Approach	Apply security from the outside	Build security from within
Architecture	Single layered protection	Multi layered protection
Scope	Atomistic, one organization	Holistic, network of organizations

Source: Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), *New Contributions in Information Systems and Technologies* (pp. 311–316). Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_31

Cyber resilience vs cybersecurity

Aspect	Meaning
Objective	1) Resilience focuses **on keeping business goals intact**, rather than IT systems, during adverse cyber events 2) Resilience analysis needs to have the **business as a starting point**, rather than the IT systems
Intention	3) Resilient systems should be **designed to be able to fail in a controlled way**, rather than being designed to solely protect against failure
Approach	4) Resilience is **built into organizations and IT systems**, rather than added as separate functions or teams
Architecture	5) A resilient architecture contains **several layers, each capable of protection** and recovery, rather than having a single layer of protection. The architecture needs to be structured to allow for partial failure.
Scope	6) To manage resilience, the business and IT systems need to be viewed as an **interconnected network**, rather than as a single unit of analysis with an environment 7) Resilience is viewing networked **interconnection of organizations** and systems as both a strength and a weakness, rather than just a source of threats

Key features

When	*Features*
Before	Planning, framework application, vulnerability assessment, situational awareness, training
During	Cybersecurity specialist, function maintenance, leadership, collaboration
After	Recover, learn, change

Anticipation

Themes	Objectives	Tools
Situational awareness	• Cyber threats frequency, sophistication, and trends identification • Quickly and accurate detection of cyber-attack and malicious activities	• Interaction with the operating environment • Monitoring procedures • Environmental monitoring
Vulnerability assessment	• understand the vulnerabilities in the organization • identify the cybersecurity organizational status • prevent threat vulnerability exploitation	• Vulnerability assessment • Penetration and red team testing • Asset vulnerability inventory
Planning	• prevent and minimize cyber incidents • quick recovery from cyber-attacks • threats' anticipation and a better planning • appropriate emergency response	• Physical and cybersecurity plans • Business continuity plans Mitigation and recovery plans • cybersecurity framework (e.g., NIST, COBIT, ISO)

Anticipation

Themes	Objectives	Tools
Training	• Increase awareness • Cyber-attack prevention and mitigation • Cyber-risk learning • Roles and responsibilities clarification • Proper policy adoption • Shape a cyber-resilient organizational culture	• Resilience plan education • Cyber-risks training • social engineering, phishing attacks simulations • scenario based wargaming • Report procedure
Resources	• Better defend against cyber-attacks • Enanced CR strategies	Dedicated budget allocation Dedicated resources

Main differences

- Planning vs improvisation
- **Training contents** more specifics
- A specific unexpected event enables to define the **desired outcome of monitoring activities** more clearly

Anticipation

Responding

Themes	Objectives	Tools
Roles and responsibilities	• absorption • mitigate cost • support -and monitor- CR control measures effectiveness • great communication during a cyber-attack • increased agility	• cybersecurity role • chief Information Security Officer • cybersecurity expertise
Leadership	• enable employee’s cyber-resilience • strategies’ implementation	• // (absence of identified organizational mechanism)

Responding

Themes	Objectives	Tools
Maintain function	• Ensure business continuity • Deliver the intended outcome	• // (absence of identified organizational mechanism)
Collaboration	• Adequate and appropriate strategy implementation • Shaping cybersecurity knowledge in the environment • Enables a resilient digital ecosystem	• Identify any preferred third-party • Communication channel with stakeholder • Social networks • Networks and alliances

Main differences

- Roles and responsibilities
- External resources dotation vs network collaboration
- **Agility** topic is underrepresented

Responding

Recovery and learn

Themes	Objectives	Tools
Learning	• Improvement and avoidance for future cyber incidents	• Incident report
Change	• Evolution • Adaptation	• Threat environment changes • System environment changes • Technology environment changes
Recovery	• Restore to the regular mechanism	• Updating • Reviewing • Optimization • Damage identification • Capabilities restoration

Main differences

- More specific content design for being resilient to a specific event (i.e., cyber-attacks)

Recovery and learn