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

Resilience

Culture

Awareness

Resilience

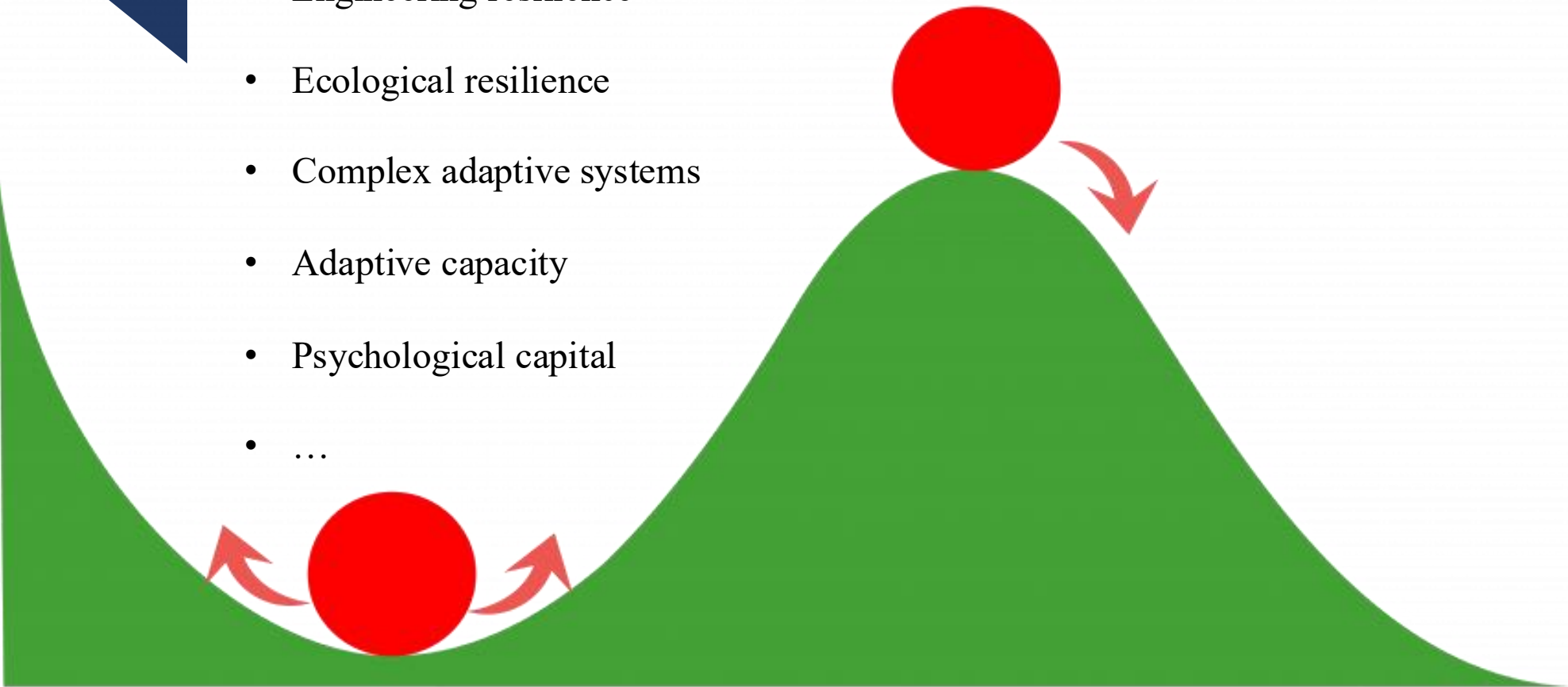
1) Resilience is a fundamental quality (...) to respond productively to significant change that disrupts the expected pattern of event without engaging in an extended period of regressive behavior (Horne and Orr, 1998)

2) Resilience is “the maintenance of positive adjustment under challenging conditions such that the organization emerges from those conditions strengthened and more resourceful” (Vogus and Sutcliff, 2007).

3) Resilience “is more than mere survival; it involves identifying potential risks and taking proactive steps (...) to ensure that an organization thrives in the face of adversity” (Somers, 2009)

Different theories of resilience

- Engineering resilience
- Ecological resilience
- Complex adaptive systems
- Adaptive capacity
- Psychological capital
- …



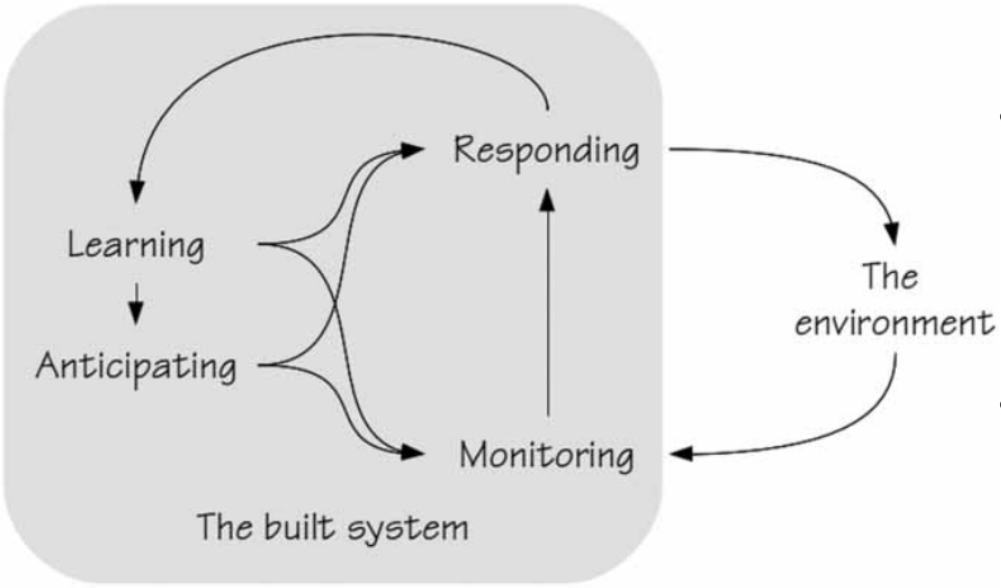


Figure 1 Dependencies among resilience abilities

- Knowing **what to do**: how to respond to regular and irregular disruptions and disturbances either by implementing a prepared set of responses or by adjusting normal functioning. This is the ability to **address the actual.**

- Knowing **what to look for**: how to monitor that which **is or can become a threat** in the near term. The monitoring must cover both events in the environment and the performance of the system itself. This is the ability to **address the critical.**

- Knowing **what has happened**: how to learn from experience, in particular how to learn the right lessons from the right experience – successes as well as failures. This is the ability to **address the factual.**

- Knowing **what to expect**: how to anticipate devel- opments, threats, and opportunities further into the future, such as potential changes, disruptions, pressures and their consequences. This is the ability to **address the potential**.

Resilience engineering

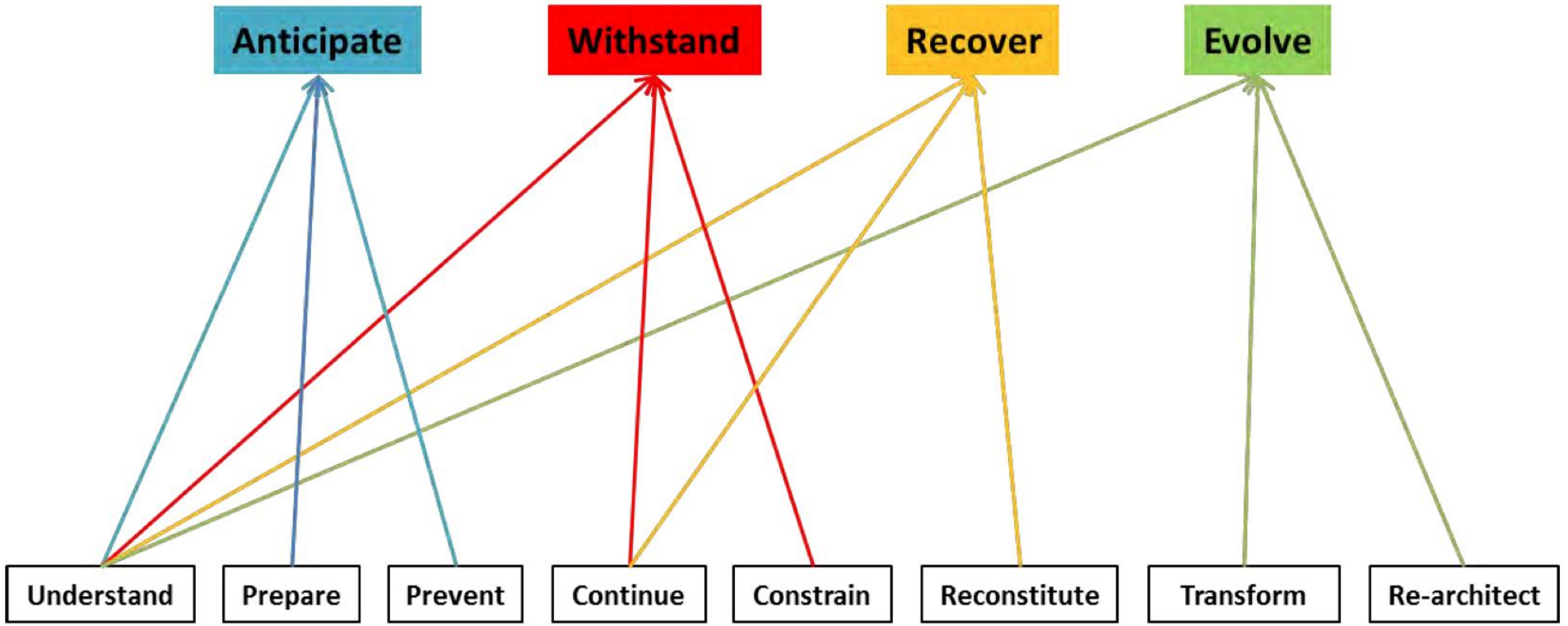


Figure 4. Cyber Resiliency Goals and Objectives

Cyber resiliency Engineering Framework

Anticipate	• maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks
Whitstand	• continue essential mission/business functions despite successful execution of an attack by an adversary
Recover	• restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary
Evolve	• Change mission/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted cyber-threats

Cyber resiliency Engineering Framework

CHALLENGES

- Resilience to what?
- Property
- Single or multi-level concept
- Heterogeneity

Resilience to what?

References	*Event*
Horne and Orr (1998)	**significant change**
Linnenluecke et al. (2012), Sullivan-Taylor and Branicki (2011)	**extreme event**
Lengnick-Hall et al. (2011)	**disruptive surprises**
Ates (2011)	**disaster**
Vogus and Sutcliffe (2007) and Sutcliffe and Vogus (2003)	**challenging conditions**
Somers (2009), Kahn et. Al., (2018)	**adversity**
Bhamra et. al., (2011)	**disruptions**
Chewing et. al., (2012)	**rapid change/chaos**
Ortiz-de-Mandojana and Bansal (2016)	**shocks in their environment**
Annarelli and Nonino (2016)	**disruptions and unexpected events**
Hillman et al., (2018)	**unexpedcted events/changes**

Resilience to what?

An important question that remains is **whether** organizational resilience developed in relation to one type of adversity will lead to **greater resilience in relation to other types of adversity**.

Would, for instance, an organization that has experienced a cyberattack and developed new capabilities in response to that threat become more resilient in relation to a global pandemic?

Source: Hepfer and Lawrence (2022). The Heterogeneity of Organizational Resilience: Exploring functional, operational and strategic resilience. *Organization Theory*, 3(1), 1-29.

Adverse events differentiation criteria…

- **Emergence**
- **Novelty**
- **Severity**

Source: 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

Emergence

Differentiation criteria	*Forms and properties*	*Examples*	*Implication for resilience*
How quickly and visibly does the adversity unfold?	**Gradual:** creeping, accumulated, ordinary	Capacity overload	Likely to be anticipated owing to monitoring and warning systems; collective response requires synchronization
	Acute: sudden, unexpected, traumatic, high impact	Terrorist attack, natural disaster	Low chance of being avoided; collective response facilitated by a shared sense of fate

Novelty

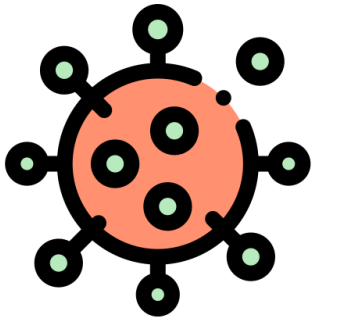
Differentiation criteria	*Forms and properties*	*Examples*	*Implication for resilience*
Do knowledge and solutions already exist?	**Non-novel:** controllable circumstances, existing solutions	Floods in coastal Regions	Absorptive response based on predefined processes and routines
	Novel: usual circumstances, no existing solutions	New diseases	Time-consuming sensemaking; tendency for adaptive response

Severity

Differentiation criteria	*Forms and properties*	*Examples*	*Implication for resilience*
How severe is the adversity (i.e., is it a matter of life and death)?	**Livelihood-threatening:** economic loss, impact on business survival, discriminate	Financial crisis	Rational response based on existing or new resources
	Life-threatening: impact on physical and emotional well-being, indiscriminate	War, natural disasters	Collective, emotional response; rational response not fully applicable

Resilience to what? Black swan vs cyber-attack

Black swan: a random event with a large impact, incomputable probabilities, and surprise effects (Taleb, 2007)



Cyber-attack: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself (NIST)

Resilience as a property?

Reference	*Property*
Coutu (2002), Linnenluecke et al., (2012)	**capacity**
Ates (2011), Chewing et al., (2012), Jiang et al., (2019), Kahn et al., (2018), Lengnick- Hall and Beck (2005), Lengnick-Hall et al., (2011), Whitman (2012)	**ability**
Annarelli and Nonino (2016), Hillman et. al., (2018), Ma et. al., (2018), Sullivan-Taylor and Branicki (2011)	**capability**

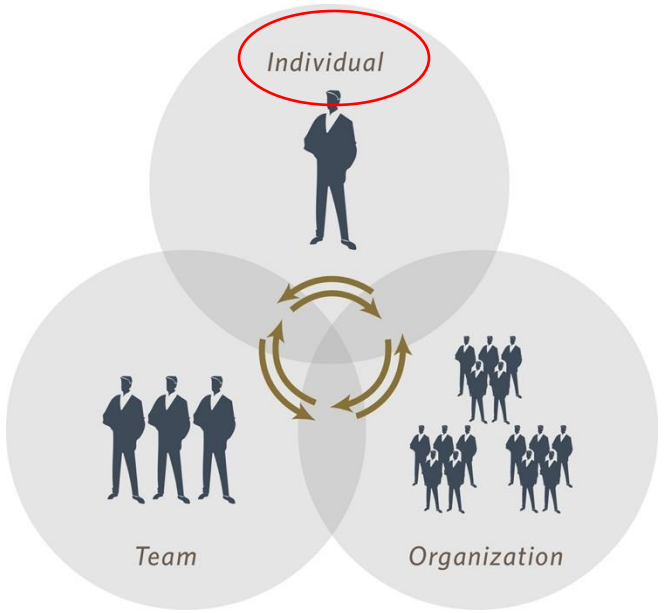
Resilience as a property?

Meaning	*Property*
The potential to do something	**capacity**
Something already in use of existing	**ability**
Refer to the specific organizational abilities underlying resilience	**capability**

Single vs multi-level concept

- ***Individual*** → Psycologhical traits
- ***Team*** → Social relationships influence organizational outcomes such as resilience
- ***Organizational*** → routines, processes and capabilities
- Interdependency?

Single vs multi-level concept

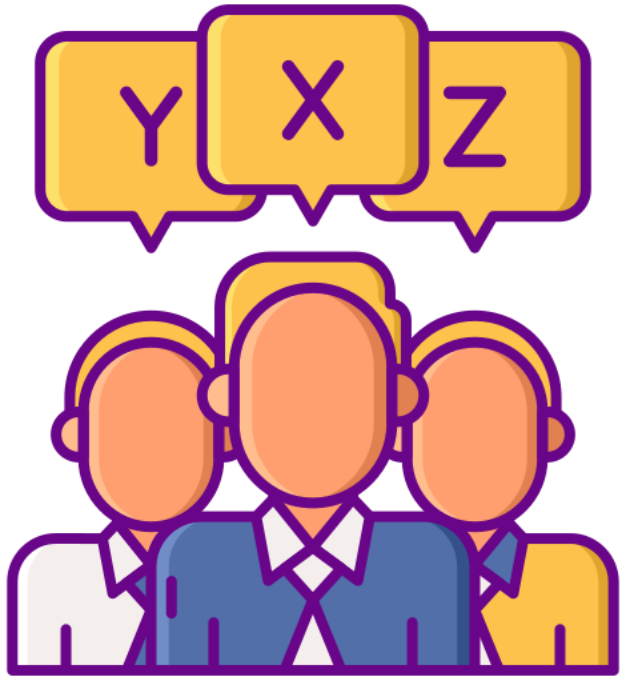


- **Self-efficacy** - belief in one's ability to succeed in adverse situations based on the past mastery of experiences
- **Bricolage (improvisation)** - remain creative in adverse situations and develop innovative solutions
- **Transformative mindset** - functions as the driving force and motivational frame for collective action in response to disasters
- **Empathy** - Empathic CEOs can quickly sense crises, provide meaning to various stakeholders, and mobilize a collective response

Single vs multi-level concept

- Groups' **capacity to improvise**
- **Group identity** creates cohesion and collaboration among individual
- **Group diversity** that is, heterogeneity among group members in terms of knowledge, experience, and competencies
- **Psychological safety** - group, members can voice their thoughts and concerns without the risk of negative social consequences

Heterogeneity



- **Equifinality**
- **Path dependency**
- **SMEs vs other companies**

International Journal of Production Research ›
Volume 49, 2011 - Issue 18: Creating resilient SMEs

Original Articles

Creating resilient SMEs: why one size might not fit all

Bridgette Sullivan-Taylor & Layla Branicki

Pages 5565-5579 | Accepted 01 Jan 2011, Published online: 19 Apr 2011

Cite this article https://doi.org/10.1080/00207543.2011.563837

SMEs challenges

- Adequate resources
- Optimistic outlook
- Focus on day to day business activities
- Lack of cybersecurity expert
- Misconception about being targeted from cyber criminals

Some quotes from a recent research…

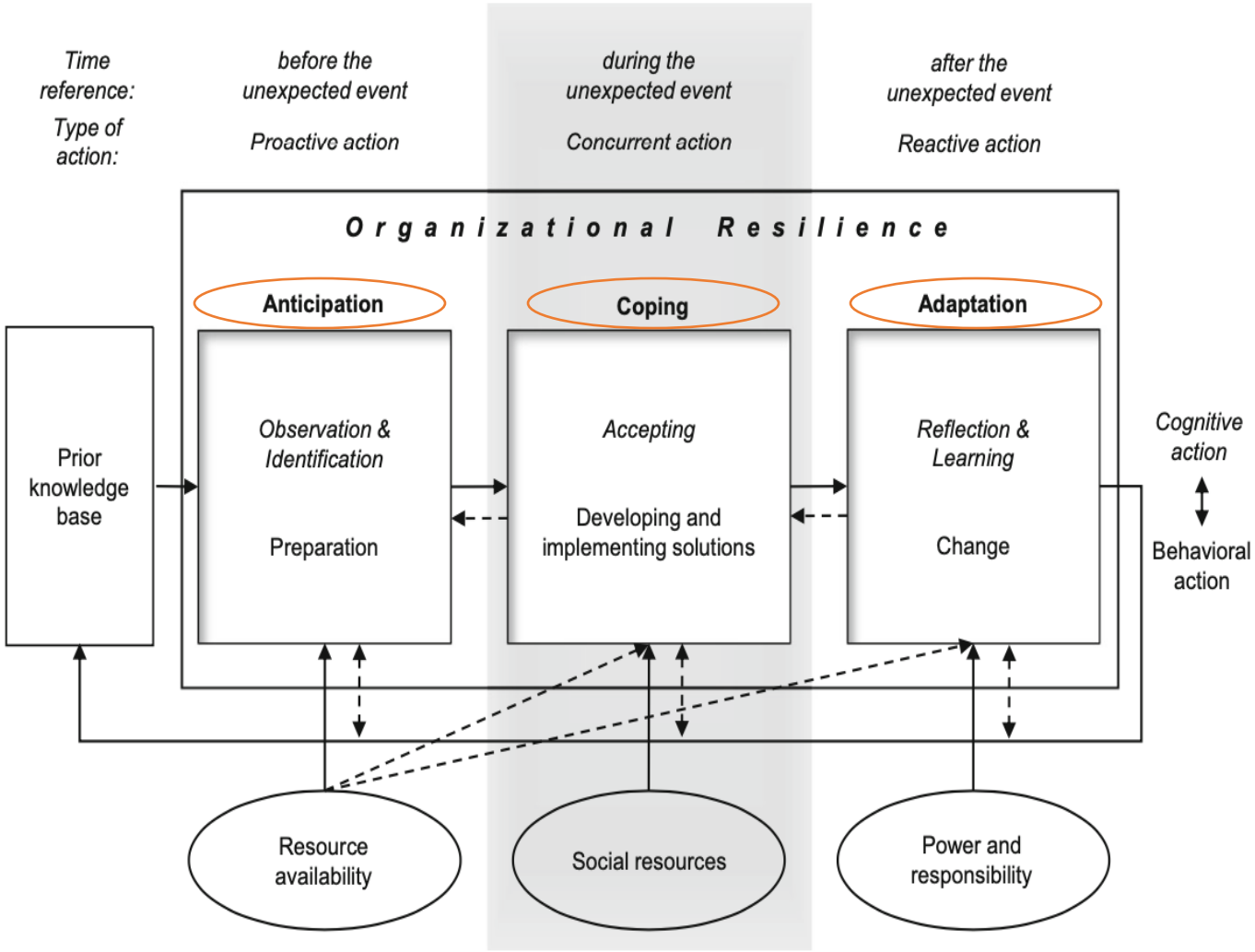
«**We believe the risk is pretty low** because we work in a mature industry, so it's not highly innovative so there's definitely no trade secrets to take from us»

«Of the IT part of the organization, **we don't have a dedicated manager**, let's say we have a team of people who deal with it but on an occasional basis, **that's not their role**»

«**Resources are limited** and so everything is always focused as much as possible toward what is the core of the business **aimed at generating profits.** Cybersecurity is not our priority»

«Being attacked by a cyber-criminal has always been seen as an **unlikely scenario**, and so for the same reason as above we have **not spent time and money in training**»

Organizational resilience: a capability-based conceptualization



Source: Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, *13*(1), 215-246.