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

Culture

- Cybersecurity Culture (CSC) of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behavior with information technologies (ENISA)

- The beliefs, values, and attitudes that drive employee behaviors to protect and defend the organization from cyber attacks (Huang & Pearlson)

- There are three components of culture: 1) the belief systems forming the basis for collective action; 2) the values representing what people think is important; and 3) Artifacts and creations which are the art, technology, and visible and audible behavior patterns as well as myths, heroes, language, rituals and ceremony. (Edgar Schein)

Cybersecurity culture levels

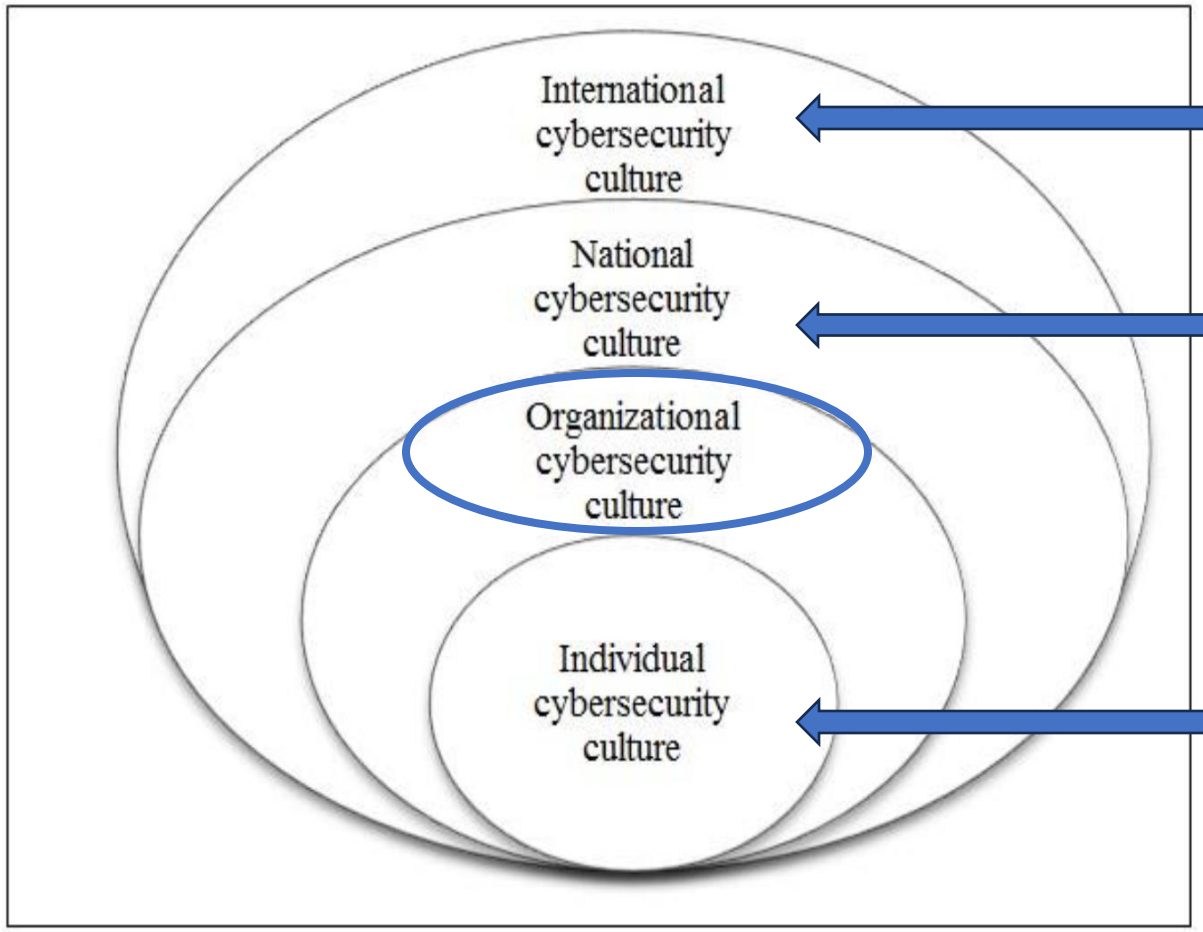


Fig. 1. Cybersecurity culture levels

Includes **all devices and people that are connected** globally

Maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while **promoting safety, security, business confidentiality, privacy, and civil liberties**

Protect all **of the user's assets** (e.g. devices, household equipment) that can be connected to cyberspace and **the user's personal information** shared in cyberspace has to be protected

The organizational culture that develops on the basis of exhibited behavior is evident…

in **artifacts** (using encryption, dedicating times to cybersecurity during meetings)

values (the privacy of customer data is respected)

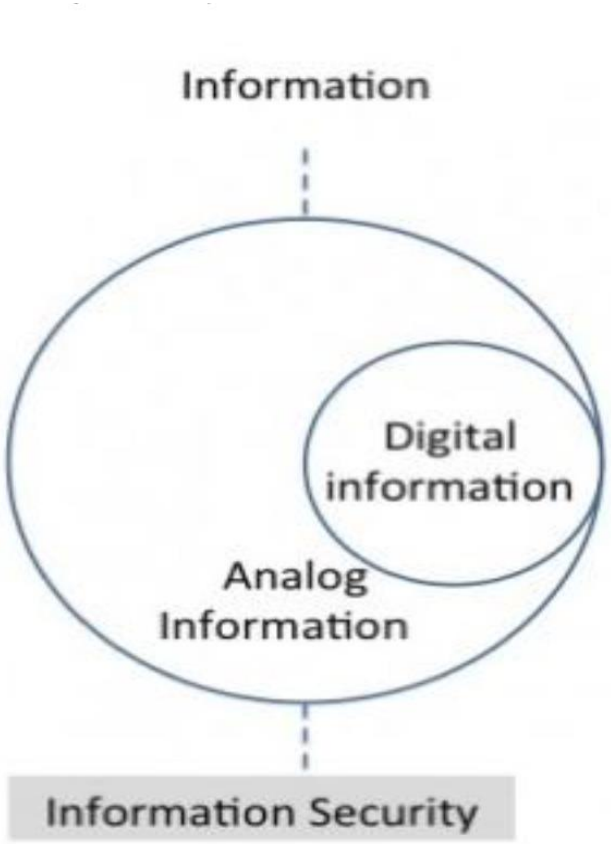
and **basic assumptions** (executive management understand the risk to information)

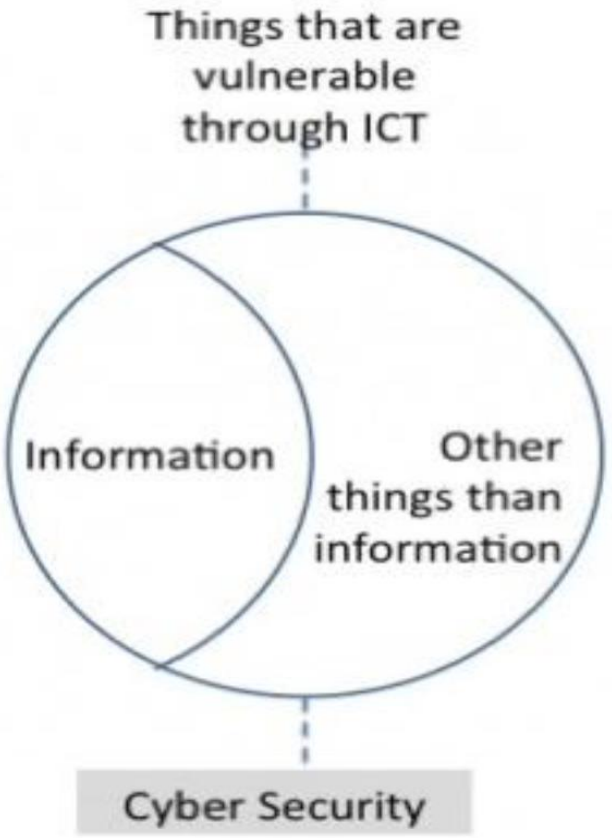
Cybersecurity culture vs information security culture

Information security culture consist of perceptions, attitudes, assumptions, values and knowledge that guide the ***interaction*** of people with organizational ***information assets*** with the mandate of securing information

Cyber security culture is defined as the beliefs, assumptions, attitudes, values, perceptions, and knowledge that people ***have pertaining to cyber security*** and how these manifest in their interaction with ***ICT***

Cybersecurity culture
vs
information security culture





Cybersecurity culture vs information security culture

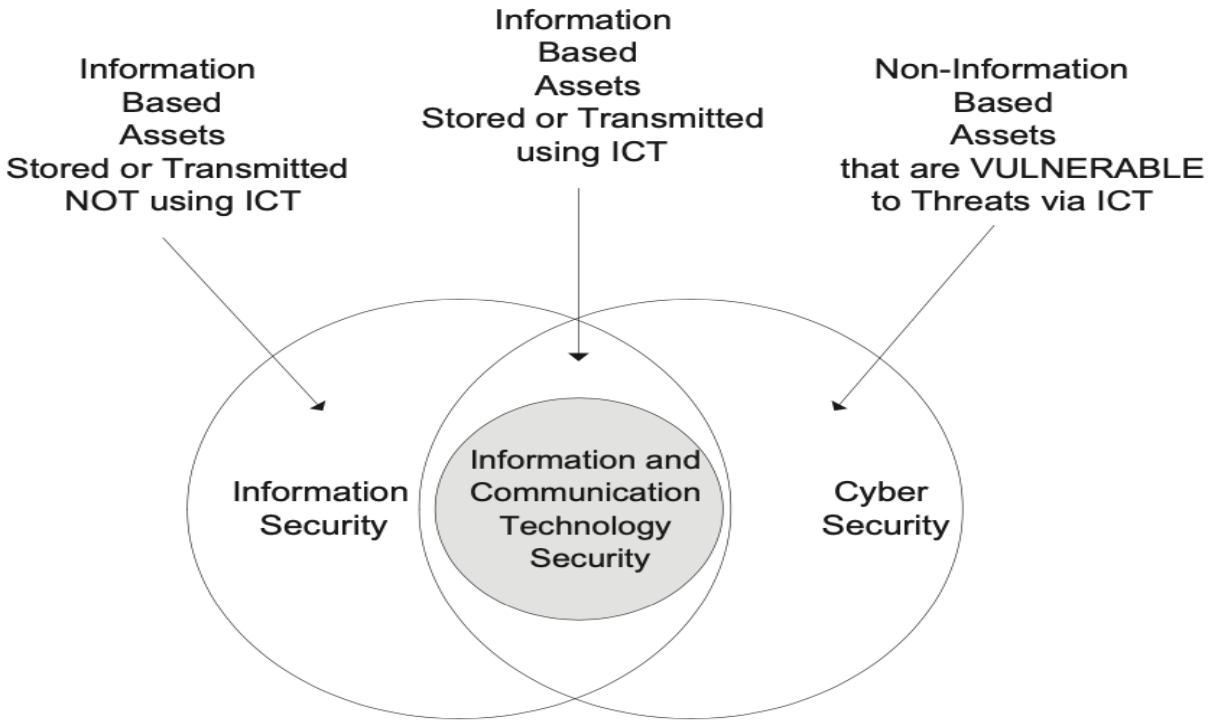


Fig. 4 — The relationship between information and communication security, information security, and cyber security.

Cybersecurity culture vs information security culture

Information Security → protection of the underlying ICT assets, and then goes beyond just the technology to include **information that is not stored or communicated directly using ICT**

Information and Communication Technology Security → ICT security, the asset(s) that need to be protected are the underlying information technology infra-structure, thus protecting the **ICT itself**

Cybersecurity → Cyber security is also about the protection of the person(s) using resources in a cyber environment and about the protection of any other assets, including those belonging to society in general, that have been exposed to risk as a result of **vulnerabilities stemming from the use of ICT.**

To summarize

In the case of information security, the asset(s) to be secured are the **information together with the underlying technologies.**

In information and communication security the asset to be secured is **the underlying technology**

In the case of cyber security, the goal is clearly not to secure cyberspace but rather to **secure those that function in cyberspace, whether individuals, organisations or nations.**

Information Security Culture

IPCA dimension	Description
Information security commitment	The perception on the commitment from an organisational, divisional and employee perspective regarding the protection of information and implementation of information security controls.
Management buy-in	The perception on management buy-in towards information security and the importance attached to the concept by senior managers and executives. The concept of management adherence to the information security policy is also established.
Information security necessity and importance	Information security necessity is established by focussing on specific concepts such as people, time, money and the impact of changes.
Information security policy effectiveness	The effectiveness of the information security policy and the communication thereof is established.
Information security accountability	Individual accountability to compliance and the requirements for information security training.
Information usage perception	The perception on information security and privacy usage requirements.

Source: Da Veiga, A., & Martins, N. (2015). **Information security culture** and information protection culture: A validated assessment instrument. *Computer Law & Security Review, 31*(2), 243–256. https://doi.org/10.1016/j.clsr.2015.01.005

Cybersecurity Culture

Factor	Definition
Top management support, leadership or involvement	The support and engagement of C-suite executives, senior managers, department managers, in creating, practicing and maintaining a security culture.
Security policy	A set of guidelines and processes which are defined by an organisation in relation to security.
Security awareness	The understanding that employees of an organisation possess regarding security generally.
Security training	The provision of security education materials to, and general upskilling of, employees that would make them cognisant of security threats and the organisation's respective policies and procedures.
Change management	The process that guides and supports employees towards the change necessary to develop a security culture within an organisation.
Compliance	The process of ensuring employees and the organisation as a whole adhere to standards and regulations on security.
Knowledge	Employee understanding of security hygiene practices as well as an organisation's policies and procedures.
Accountability and responsibility	Accountability refers to an employee owning the outcome of an action/behaviour, while responsibility refers to the employee's obligation to carry out a task that may pertain to security.
Security risk	This factor refers to the security threats and vulnerabilities that an organisation (and its employees) is exposed to which can lead to intentional or unintentional impacts.
Commitment	Employees within an organisation understand the need for security and support practices to ensure security policies are adhered to and a security culture fostered.
Communication	The means utilised to share information between the organisation and its employees, for instance, means through which employees find out about security policies, procedures and practices and what is expected of them.
User management	The procedures that are in place to manage and monitor employee behaviour and compliance.
Motivation	Incentives provided to encourage employee adherence to security policies, practices, procedures and advice.
Trust	Employees and the organisation need to have confidence in each other both generally and as it relates to security activities. This confidence is two-way and can relate to any activities within or about the organisation (e.g., trust in the organisation generally, trust that its policies are well considered, employees trusting their employer, etc.)
National culture	This relates to the norms, values, beliefs and customs of the nation or region that an organisation or employee is based in; these can influence an organisation's security culture.
Ethical conduct	Behaviour and decision making within an organisation follow a moral code of right and wrong. Such code can impact how people adopt or engage with a security culture (especially if that culture is perceived as unethical or harmful).
Regulations	The legal provisions/directives in relation to safeguarding information technology and computer systems, which organisations and their employees need to abide by.
Establishing a network of champions	Champions are members of an organisation who support activities in raising security awareness and act as a point of contact. Champions within different sections, departments or offices of an organisation create a network.
Rewards and sanctions	Utilising an approach of rewarding employee behaviour which is security compliant, or penalising non-compliance which may result in a potential compromise (or compromise) of the organisation.

Source: Developing a **cyber security culture**: Current practices and future needs. (2021). *Computers & Security, 109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Man in the mirror or man in the middle? Digital artifacts as…

Vulnerabilities

- Exploited by cybercriminals
- Phishing
- Man in the middle
- BEC
- ….

Opportunities

- New value paradigm oriented toward cyber-resilience can be conveyed

- Through digital communication tools, procedures, policies, behavioral rules, national or industry cyber report, can be disseminated

Source: Neri, M., Niccolini, F. (2022). «Man in the mirror or man in the middle? Artefatti digitali e cyber resilienza». Prospettive in Organizzazione.

Cybersecurity culture practices

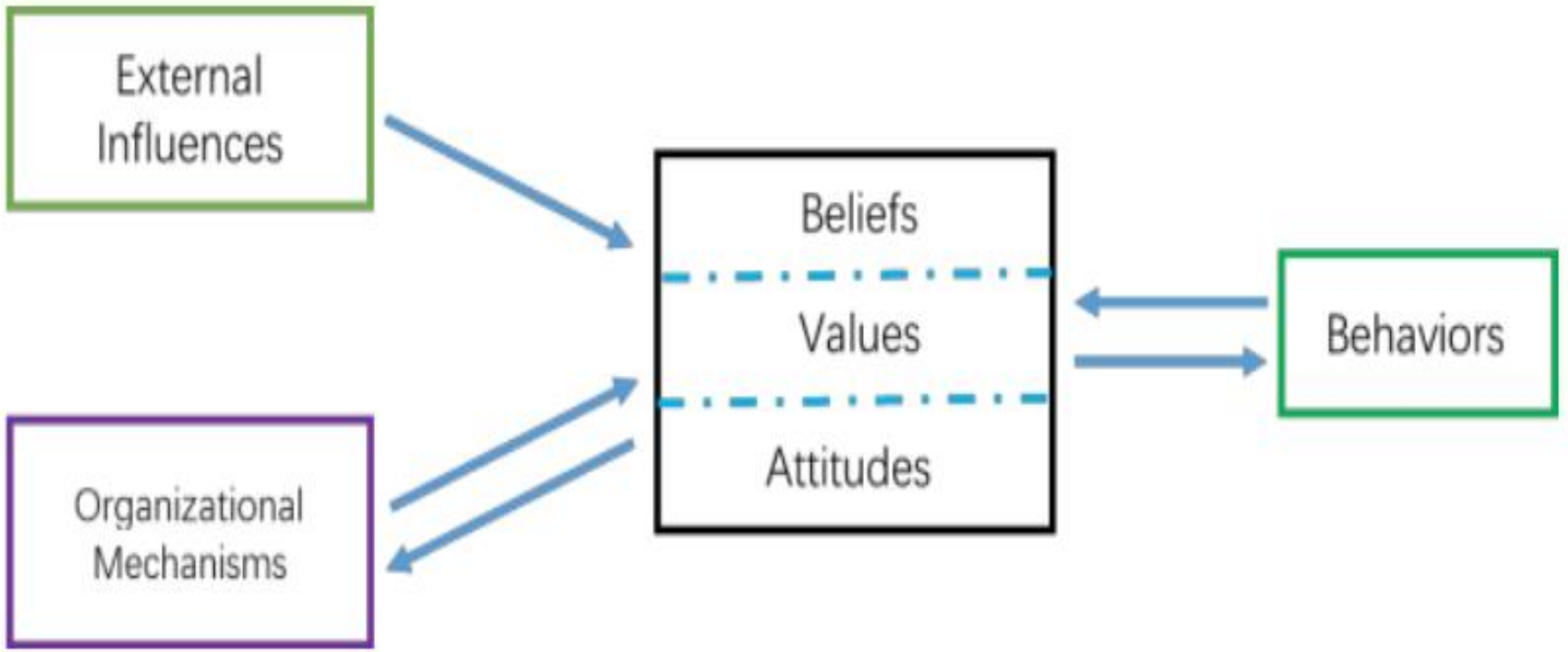
- ***Management support*** –> ***participation and visible support*** by top management, willingness of ***financial investment***
- ***Cybersecurity policy*** –> shows and demonstrate management intent and the importance of cybersecurity, as well as to ***provide overall guidance***
- ***Training and awareness*** –> To increase awareness of cybersecurity, the organization must ensure that the training is ***tailored to the target population***. One of the cornerstones in shaping cybersecurity culture is knowledge, both of ***management and employees.***

Cybersecurity culture practices

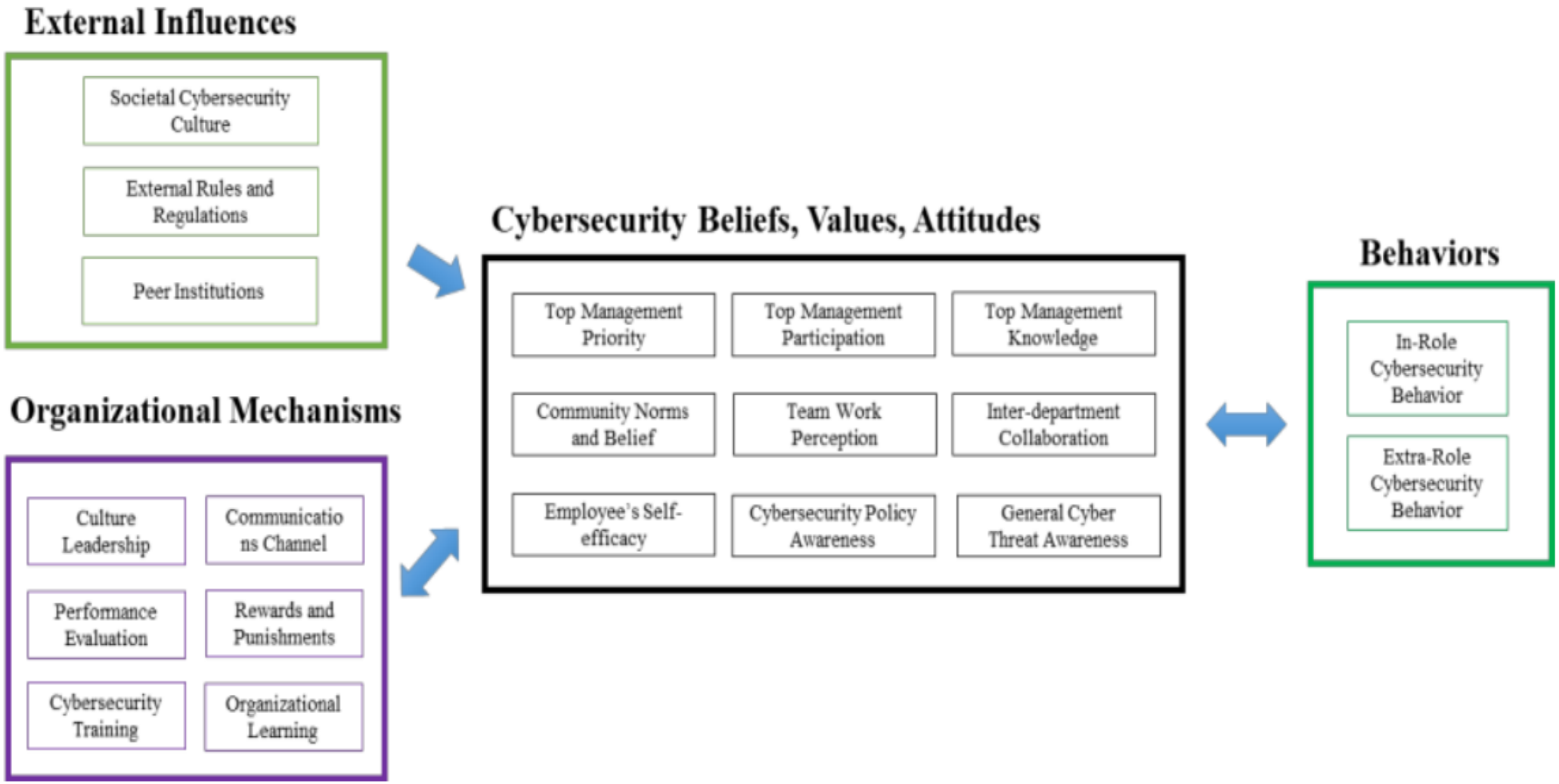
- ***Involvement and communication*** –> promotes a continuous reflection on own behavior, how that may influence security, and what they themselves can do to ***improve security***. Wether employees have the potential to positively contribute to information security if their participation is encouraged which, in turn, promotes ***proactivity***

- ***Learning from experiences*** –> maturity model, incident reporting system, auditing mechanism…

Conceptual Model



Conceptual Model



Behaviors

In role

Actions and activities an employee takes as part of their official role in the organization

- Complying with formal organizational security policies
- Decreasing the computer abuse
- Avoiding policy violation

Extra role

Actions and activities an employee does that are not part of their job description

- ***Helping:*** cooperative behavior to aid others who might ask a cybersecurity question
- ***Voicing:*** speaking up to offer comments and knowledge to improve cybersecurity

Cybersecurity Belief, Values and Attitudes

Leadership

When top managers believe that cybersecurity is important, **they will make cybersecurity a priority for the organization** (e.g., resources allocation)

Personal involvement in the cybersecurity-related activities (e.g., communicating cybersecurity policies, funding/attending training, creating games, participating in other cybersecurity activities)

Cybersecurity-related **knowledge, skills and competencies** leaders have. Leaders who know and understand their cybersecurity vulnerabilities are more likely to have values, beliefs and attitudes around building a more cyber resilient organization

Group

Collective set of ideas the group has about cybersecurity that influences individuals (i.e., if the group values information protection, individuals in the group will more likely value information protection)

The way teams within the organization work together to be more cyber secure (e.g., To be situationally aware about a cybersecurity threat, team collaboration provides a way to continuously process and update information)

The work done between groups of individuals from different parts of the organization (e.g., an individual in each department participating on a task force to find ways to be more cybersecure across the organization)

Individual

Refers to a person's **knowledge about how well he or she can personally execute actions to increase cybersecurity** (e.g., when an individual feels his actions keep data safer, he is more likely to make the effort to do so, resulting in stronger cybersecurity attitudes)

Individual's **knowledge of what to do, what is right or wrong and why it is important** (e.g., employees who know that their organization has a policy of locking a computer every time it's left alone is more likely to believe that locking the computer is important

Individual's **knowledge and understanding of threats** (i.e., be suspicious of unusual emails, texts, attachments, and other communications)

Organizational Mechanism

Organizational Mechanism

Culture Leadership

- An **individual or team** with formal responsibility for building a cybersecurity culture (e.g., CISO)
- A very large agenda with responsibility to **cultivate** cybersecurity culture with **direct power and authority** to impact the cultivation process
- Without a leader with specific responsibility for building the culture, the activities will be **haphazardly executed and sometimes skipped entirely**

Organizational Mechanism

Performace evaluation

- Inclusion of **measures of cybersecurity compliance** and behaviors in the employee's **formal evaluation processes**
- Managers use the performance evaluation process to clarify what behaviors are **required, nice to have, and not acceptable** for the employees (e.g., results of the phishing exercises regularly carried out by management)
- Alerts employees about **the organization's ability to observe cybersecurity behaviors, which can in turn influences the employees' values**

Organizational Mechanism

Rewards and punishments

- The design of the rewards and punishments can impact the individual decisions in many different contexts
- Rewards include **social events, proclamations, and certificates acknowledging exemplary behaviors**
- Punishments include **remedial training, reprimands, or at an extreme, firing the offending employee**
- To be most effective, rewards and punishments must **match the severity of the behavior** (e.g., failing a phishing test vs purposefully failing a phishing test with many management warnings)

Organizational Mechanism

Organizational learning

- How organization **builds and retains cybersecurity knowledge** and it is «*the intentional use of learning processes at the individual, group, and system level to continuously transform the organization in a direction that is increasingly satisfying to its stakeholders*»
- Helps **manage continuous change** which is also characteristic of cybersecurity
- Examples of organizational learning for cybersecurity include **mentors** who work with individuals to help them build skills, processes that encourage **information sharing**, consultants that bring new knowledge to the team

Organizational Mechanism

Cybersecurity training

- Courses and exercises that **develop cybersecurity skills and knowledge**
- Training **fosters** information security awareness, **educates** users on the importance of information security, and **trains** insiders to take on information security roles
- Examples include make new hires complete a cybersecurity training module as part of the onboarding process, make employees take an annual update course or online training program to ‘refresh’ their knowledge of cybersecurity practices, additional training offerings such as just- in-time learning pop-up windows

Organizational Mechanism

Communications channel

- **Coherent and well-designed** messages about cybersecurity **communicated using multiple methods and networks**
- **The right information is heard by the right person at the right time over the right channel.**
- Managers must create **multiple formal and informal channels** for reporting cyber incidents, sharing dynamic cyber information, and even identifying potential vulnerabilities.
- Examples include creating cybersecurity-based marketing-like campaigns to influence behaviors by keeping the issues front and center for employees, include short communication moments at the beginning of every company meeting to share a cybersecurity message.

External influences

Societal cybersecurity culture

The differences among nations and societies can impact individual's perception about online threat

External rules and regulations

Laws, guidelines, and regulations imposed by government and other industry organizations (e.g., financial services)

Peer instituions

The pressure felt by managers in an organization from actions their peer organizations have taken (institutional mimicry theory)