



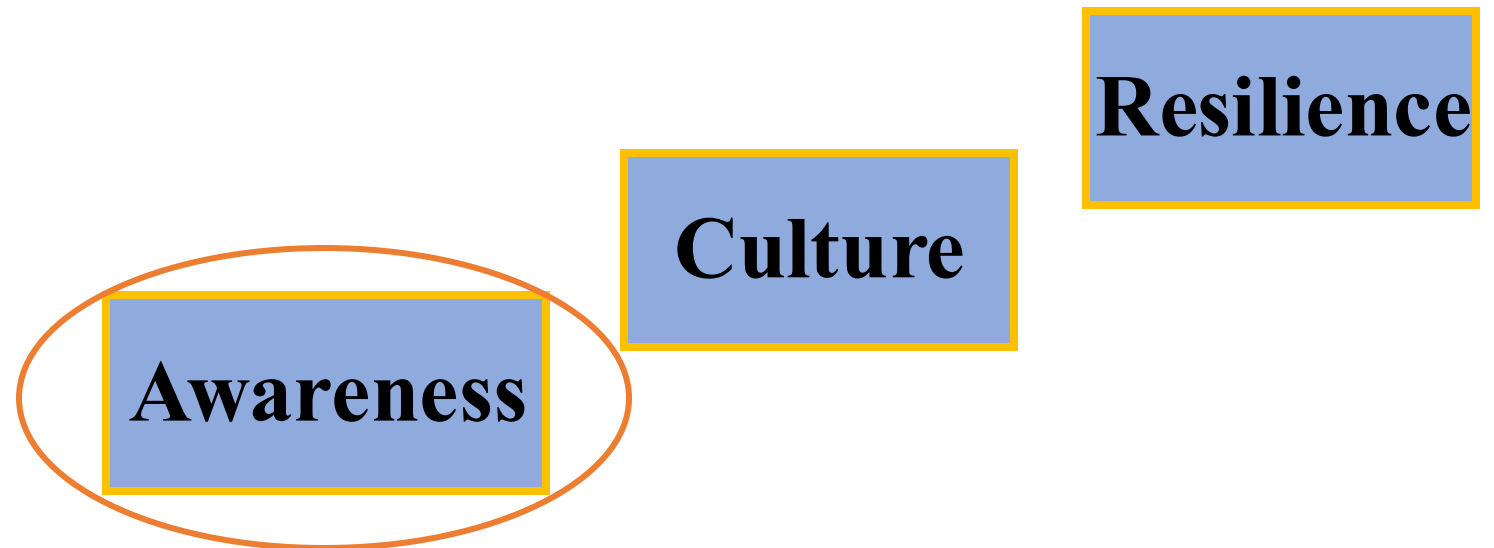
University of Pisa
Department of Information Engineering
Master Degree in Cybersecurity
Organizational Sciences Module

Academic Year 2024 -25

**Cybersecurity within organizational
sciences – awareness, culture and
resilience**



People, not only technology



Awareness

- An ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organization from lasting behavioral change (ENISA).
- Awareness refers to a continuous and regular attention that protects the organization (Safa et al., 2015).
- It's not just knowledge. Knowing isn't doing. Security awareness is knowledge combined with attitudes and behaviors that serve to protect. (Security Intelligence).



Core idea



Knowledge

Behaviour

Key features

- Password Management
- Personal devices
- Internet Use
- Data storage
- Incident report

Enhancing tools

- Training
- Cybersecurity policy



Cybersecurity awareness

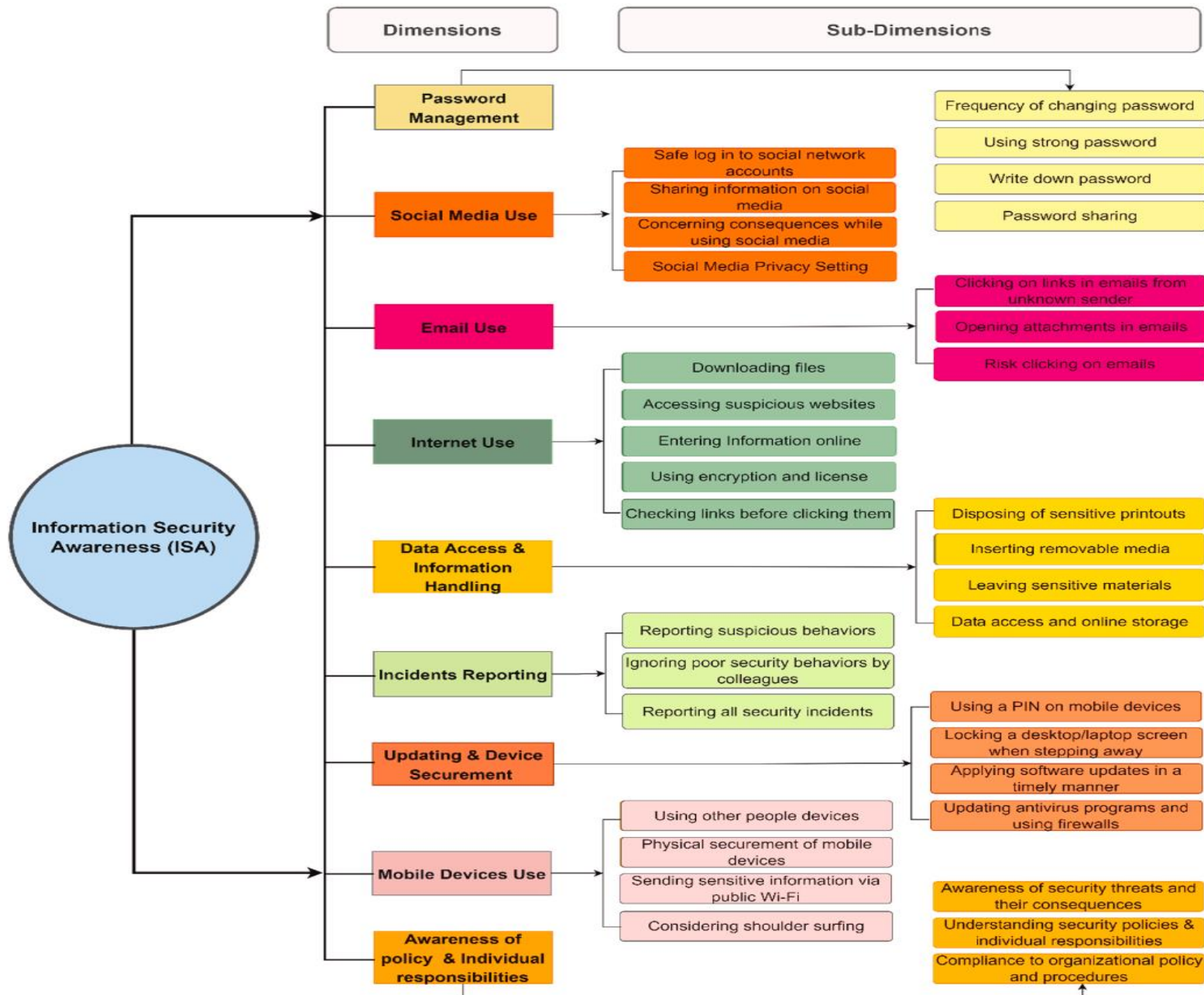


Fig. 5. Dimensions of the ISA and their respective Sub-dimensions, based on the selected 24 articles.

Cybersecurity awareness - A literature review on its dimension

Source: Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W. and Thapliyal, H. (2023), "A systematic literature review of cybersecurity scales assessing information security awareness", *Heliyon*, Vol. 9 No. 3, p. e14234, doi: [10.1016/j.heliyon.2023.e14234](https://doi.org/10.1016/j.heliyon.2023.e14234).

1) Password management refers to the awareness, usage, and management of passwords in general. Some examples include how a computer user can create a good and strong password, change it regularly, not share the work password with others, and be aware of the negative consequences.

2) Social Media Use is mainly related to the awareness and usage of social networking sites (e.g., Facebook, Instagram, LinkedIn, etc.). For instance, not accessing these sites during work time in organizations, considering the negative consequences before posting private and sensitive information, and regularly updating the privacy setting are some of the aspects considered by this dimension.

3) Email Use is relevant to the awareness and usage of emails. For example, employees in organizations should be aware not to click on links in emails from an unknown sender and consider not to download risky attachments (files) into a work computer. Further, social engineering is one of the most dangerous attacks, which is mainly carried out by phishing emails, so employees should understand not to be deceived by hackers.

4) Internet Use refers to the awareness of internet usage and accessing suspicious websites in general (downloading safe files, not accessing any suspicious websites, or not entering private and sensitive information online). Furthermore, internet users should understand the safe sources from which they download any file, not give private information on any website, and use content filtering programs.

5) Data Access and Information Handling refer to how a computer user can handle sensitive information and access or store data using online storage. For example, awareness of leaving sensitive materials (e.g., documents), downloading files from sources without checking their authenticity, and shredding sensitive printouts.

6) Incident Reporting is another dimension of information security awareness. It generally refers to reporting any security incident happening in a particular organization. Some examples include reporting suspicious behaviors of someone in the workplace, reporting the violation of the security rules of co-workers, or experiencing any security data breaches or incidents that should be reported.

7) Device Securement and Updating is a dimension where users/employees should understand and be aware of devices' security and regularly update the required software. For instance, internet users should regularly update the necessary software like antivirus, set a computer screen or other mobile devices to automatically lock while not using them, and use a password/passcode to unlock a computer or other mobile devices.

8) Mobile Device Use refers to the awareness of proper usage of mobile devices and keeping them secure. For example, using secure networks while sending important emails, considering shoulder surfing while working on a sensitive document, physical securement of mobile devices like not leaving a work laptop unattended, etc.

9) Awareness of policies and individual Responsibilities is another dimension where employees in the organization should be aware and understand their responsibilities and follow all the organizations' security policies, rules, and procedures. For instance, awareness of the potential security threats, their negative consequences, and adherence to the organization's security rules and regulations.

Key features

- Password Management
- Personal devices
- Internet Use
- Data storage
- Incident report

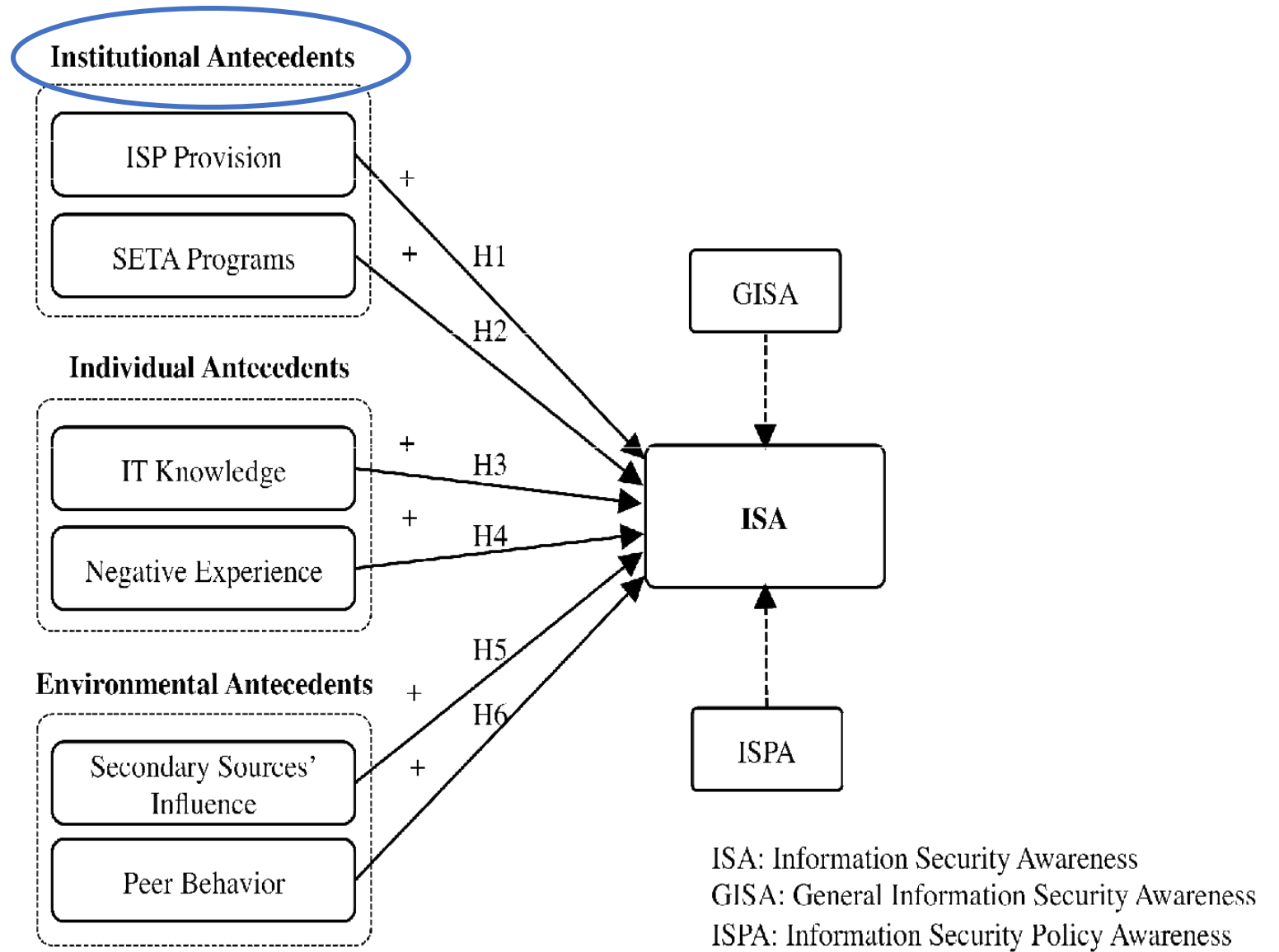
Enhancing tools

- Training
- Cybersecurity policy



Cybersecurity awareness

Training and policies

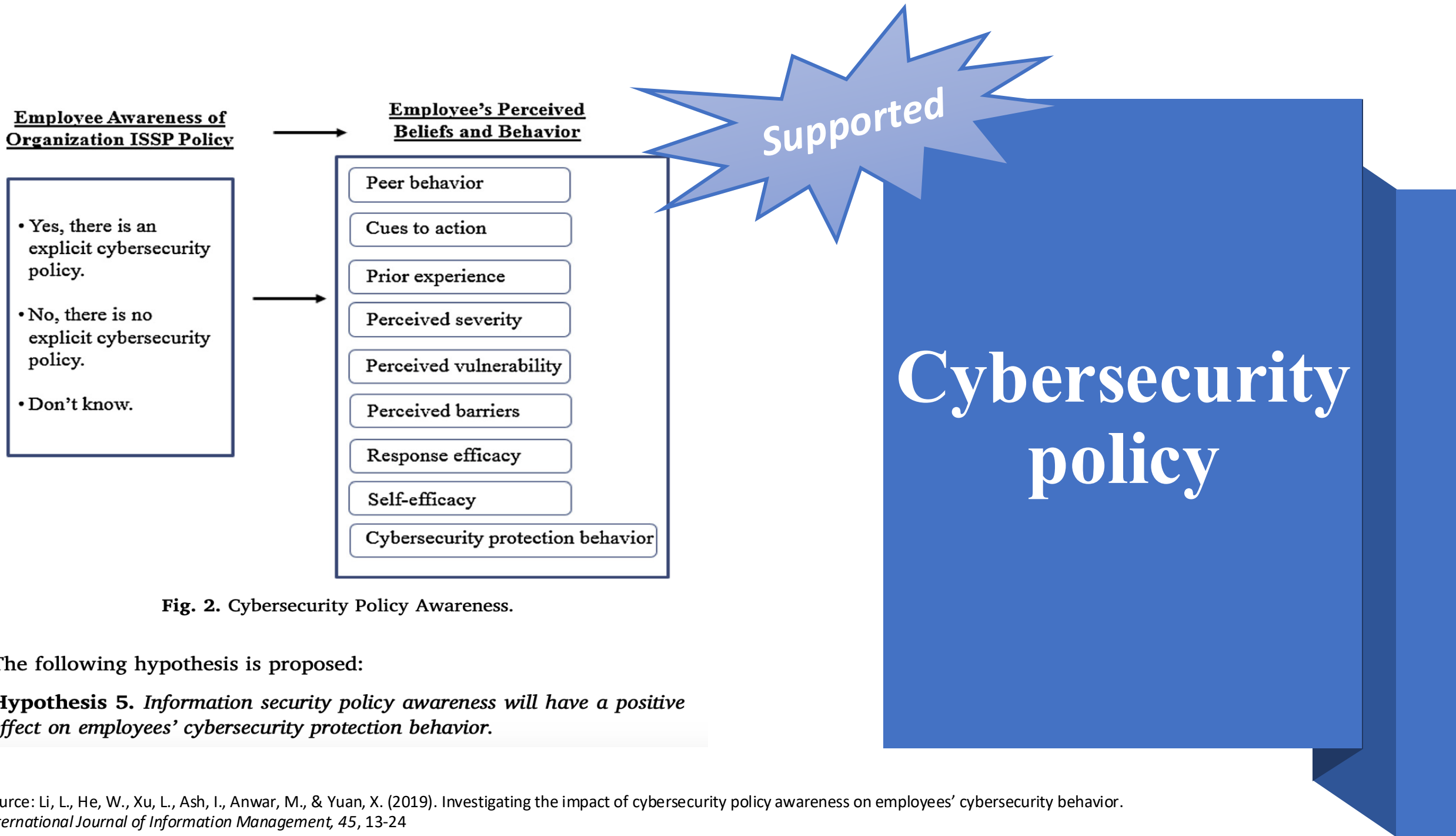




Training programmes & Education

- It cannot be assumed that the *average employee has the necessary knowledge* to perform his/her job in a secure manner
- Cybersecurity awareness training should consider that *different roles* may have *different knowledge* and training needs
- Persuade *people at all organizational levels* about what cybersecurity is and how the risks can affect their areas of responsibility
- Many forms of *training fail* because they are rote and do not require users to think about and apply security concepts
- Managers should *guide* the entire organization and *participate* in training activities

Training programmes & Education - An overview



The NIST perspective

Learning is a *continuum*: it starts with awareness, builds to training, and evolves into education.

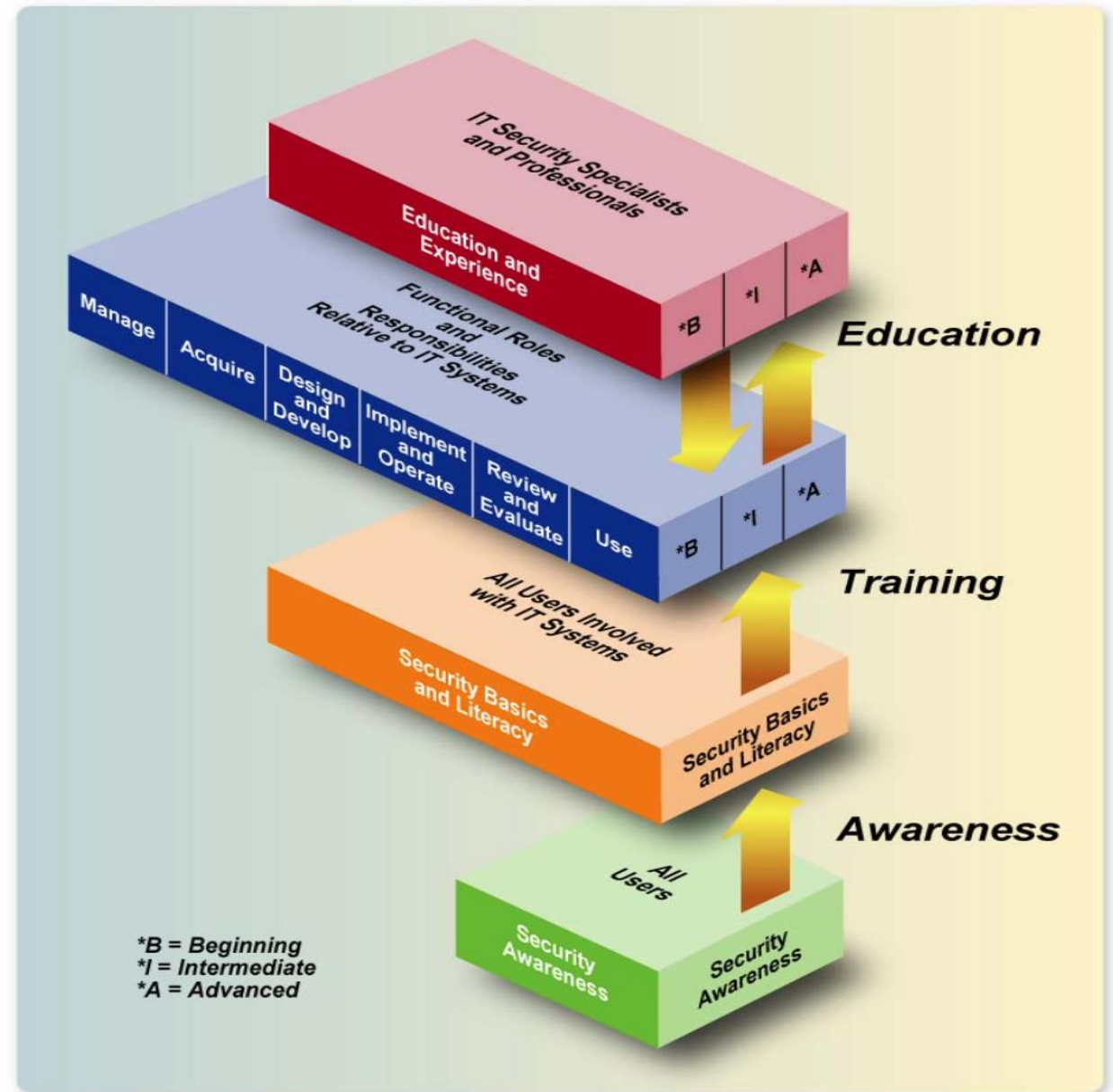


Figure 2-1: The IT Security Learning Continuum

Awareness

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.

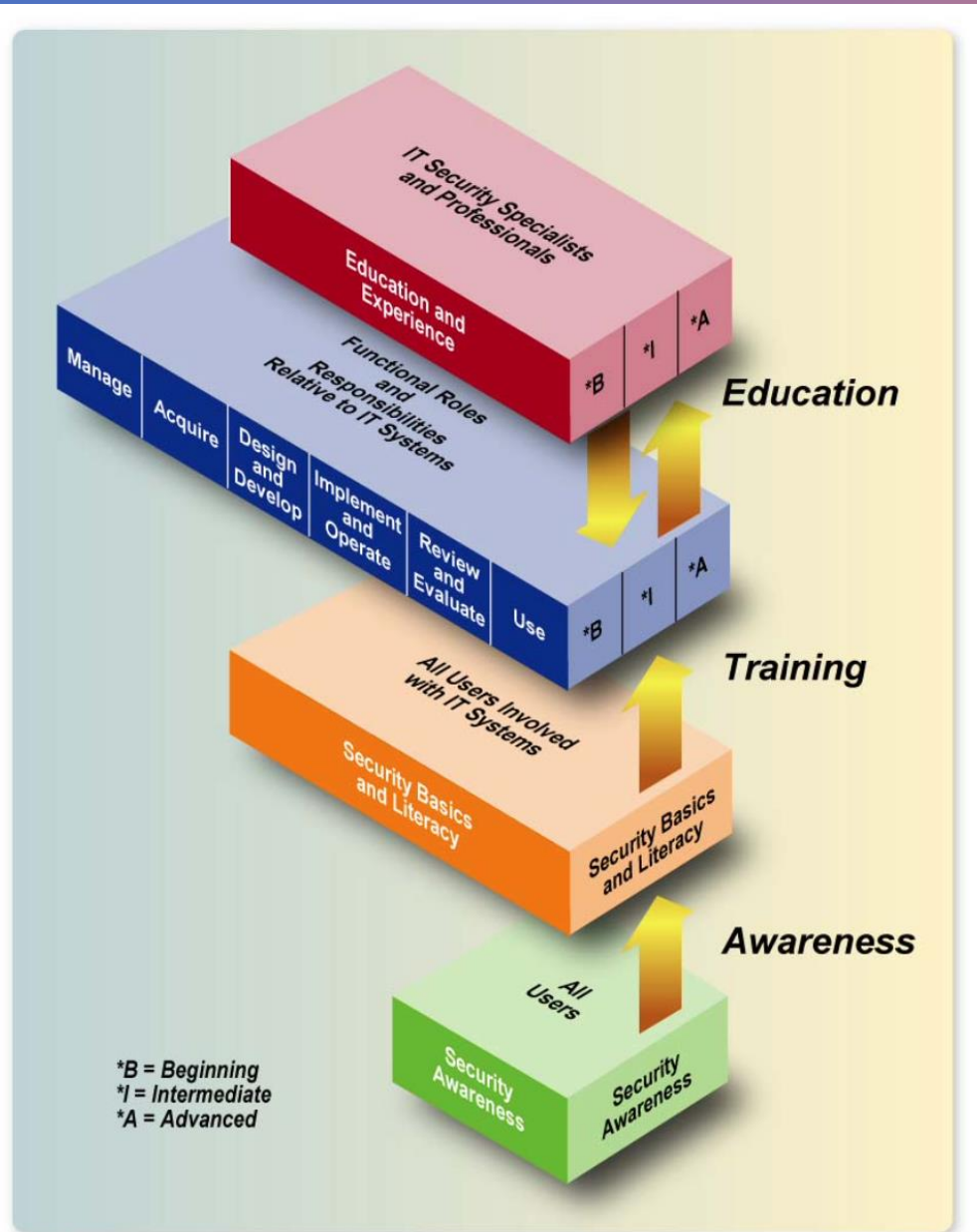


Figure 2-1: The IT Security Learning Continuum

Awareness

Example:
Virus protection.

The subject can simply and briefly be addressed by describing **what a virus is**, what can happen if a virus infects a user's system, **what the user should do to protect the system**, and what the user should do if a virus is discovered.

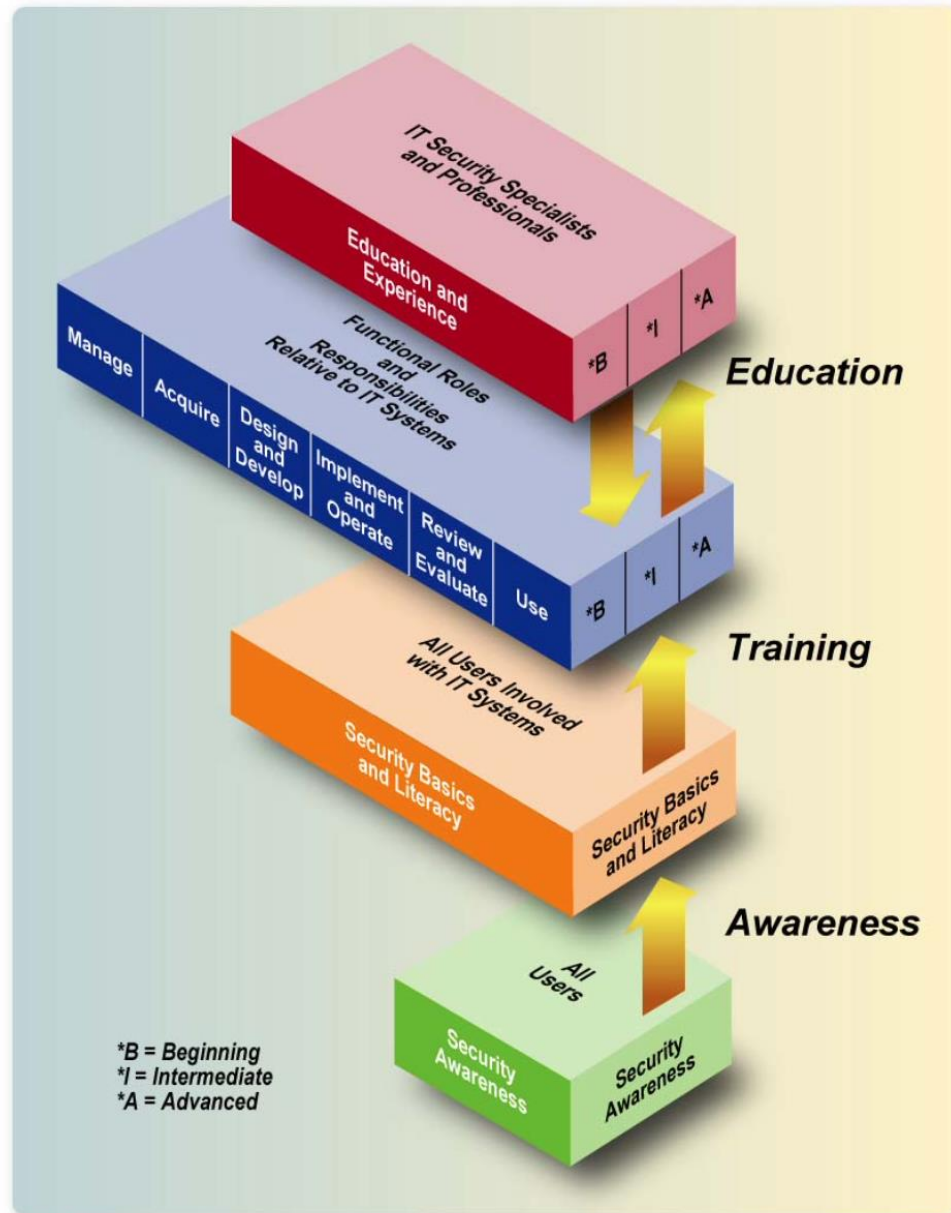


Figure 2-1: The IT Security Learning Continuum

Security Basics and Literacy

The basics and literacy material allow for the development or evolution of a more robust awareness program and provide the foundation for the training program.

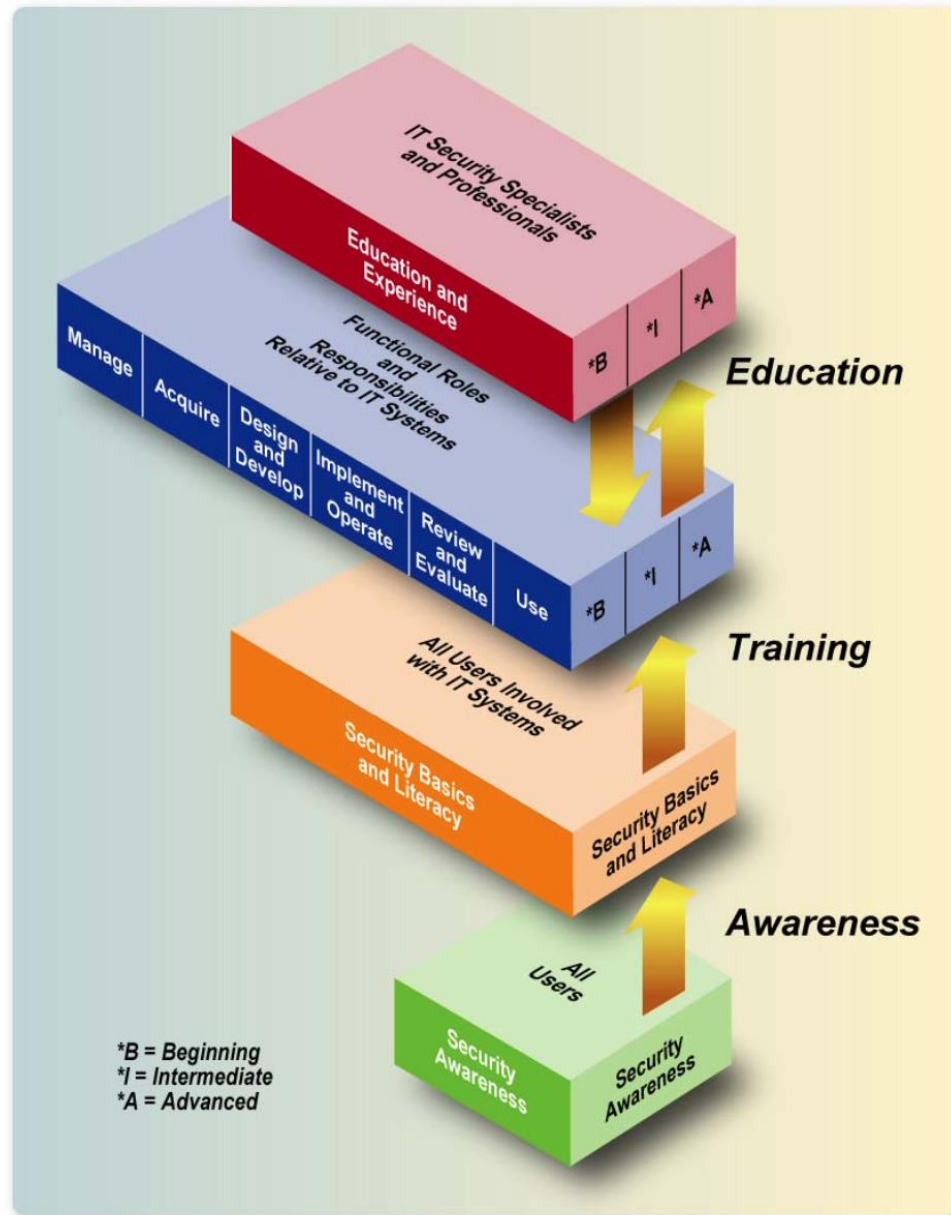


Figure 2-1: The IT Security Learning Continuum

Training

Training strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing).

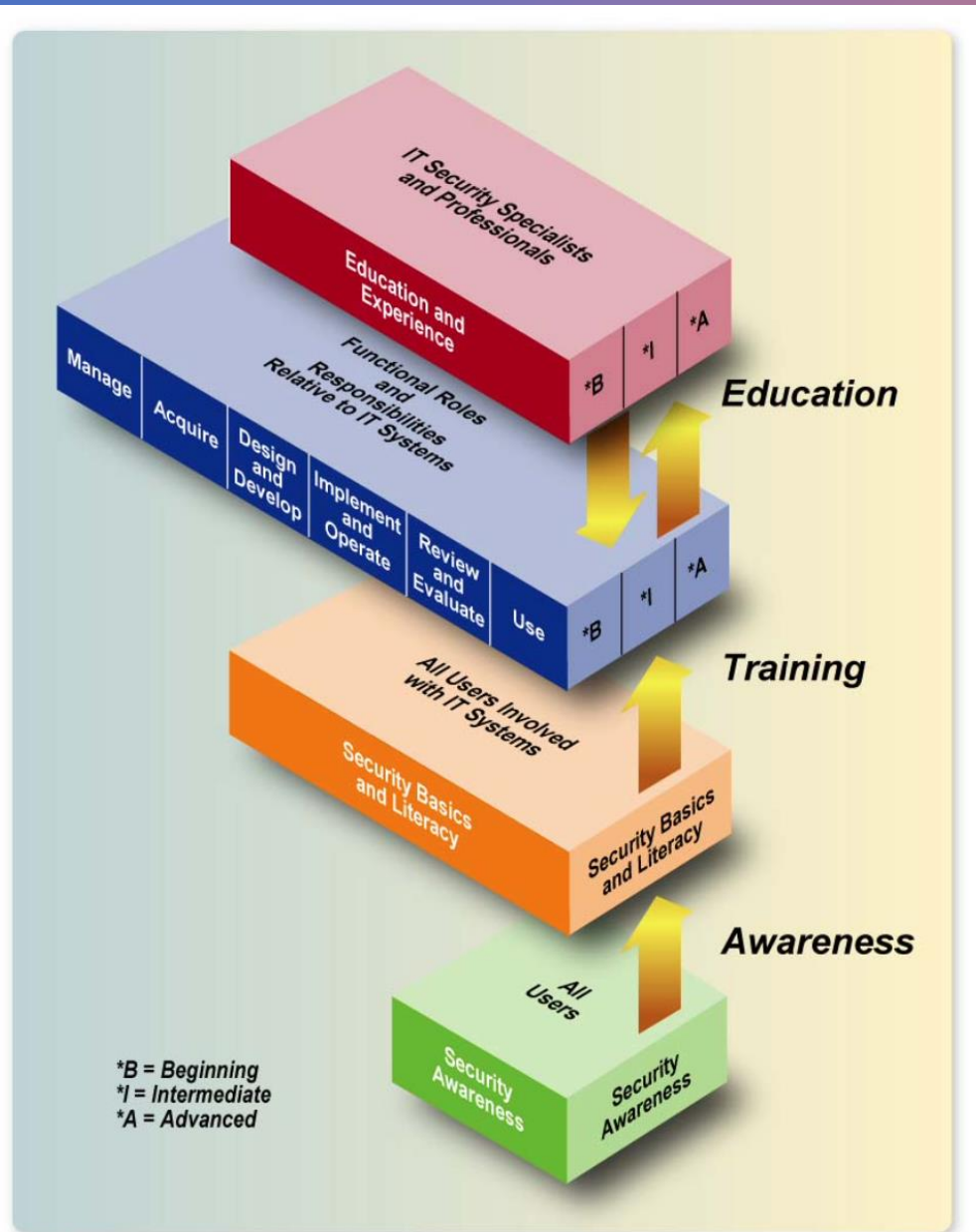


Figure 2-1: The IT Security Learning Continuum

Training

Example: IT Security course

IT security course for system administrators, which should address in detail the management controls, operational controls, and technical controls that should be implemented.

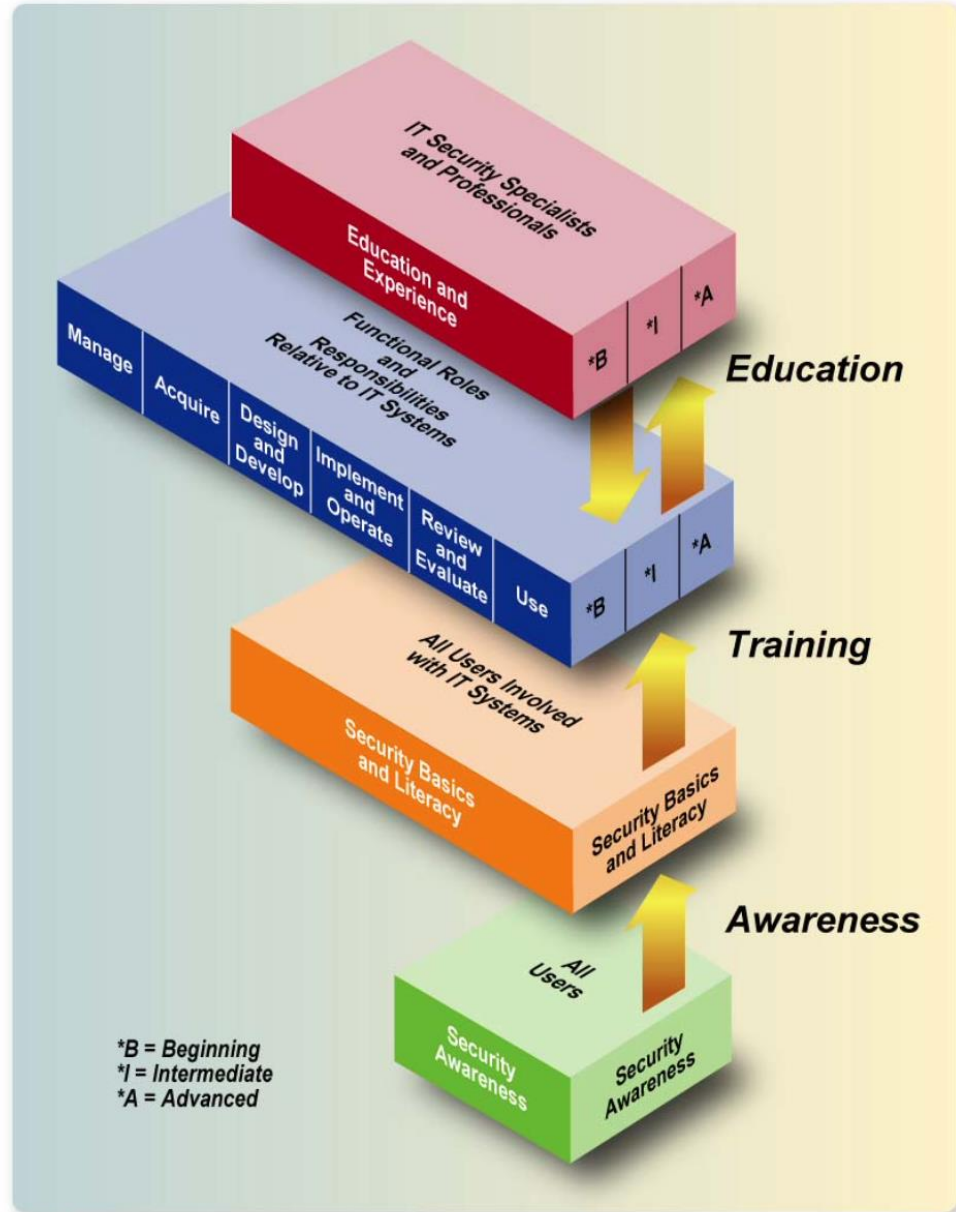


Figure 2-1: The IT Security Learning Continuum

Education

Integrates all the security skills and competencies of the various functional specialties into a **common body of knowledge**.

Adds a **multidisciplinary** study of concepts, issues, and principles (technological and social).

Strives to produce IT security specialists and professionals **capable of vision and proactive response**

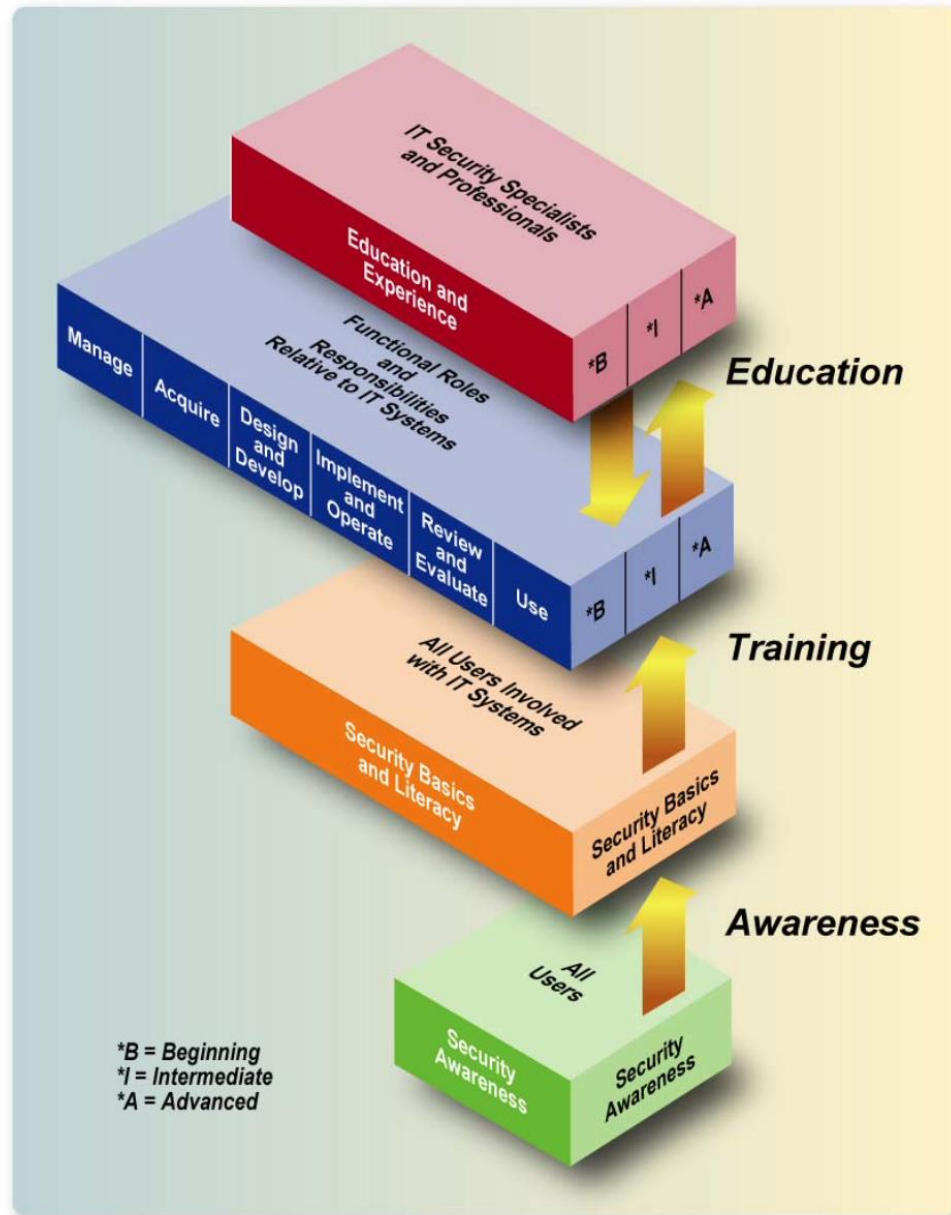


Figure 2-1: The IT Security Learning Continuum

Education

Example College degree

Some people take a course or several courses to develop or enhance their skills in a particular discipline. This is training as opposed to education.

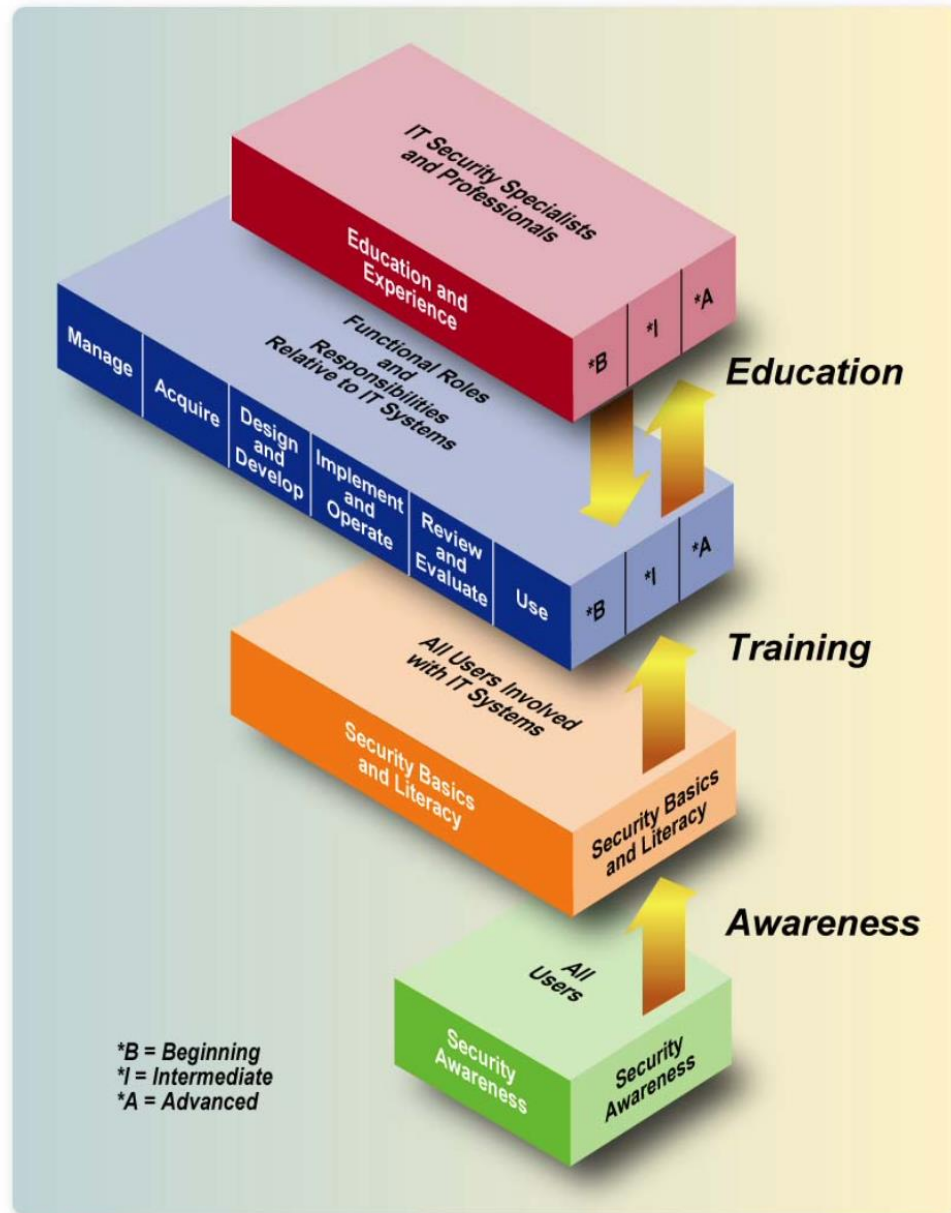
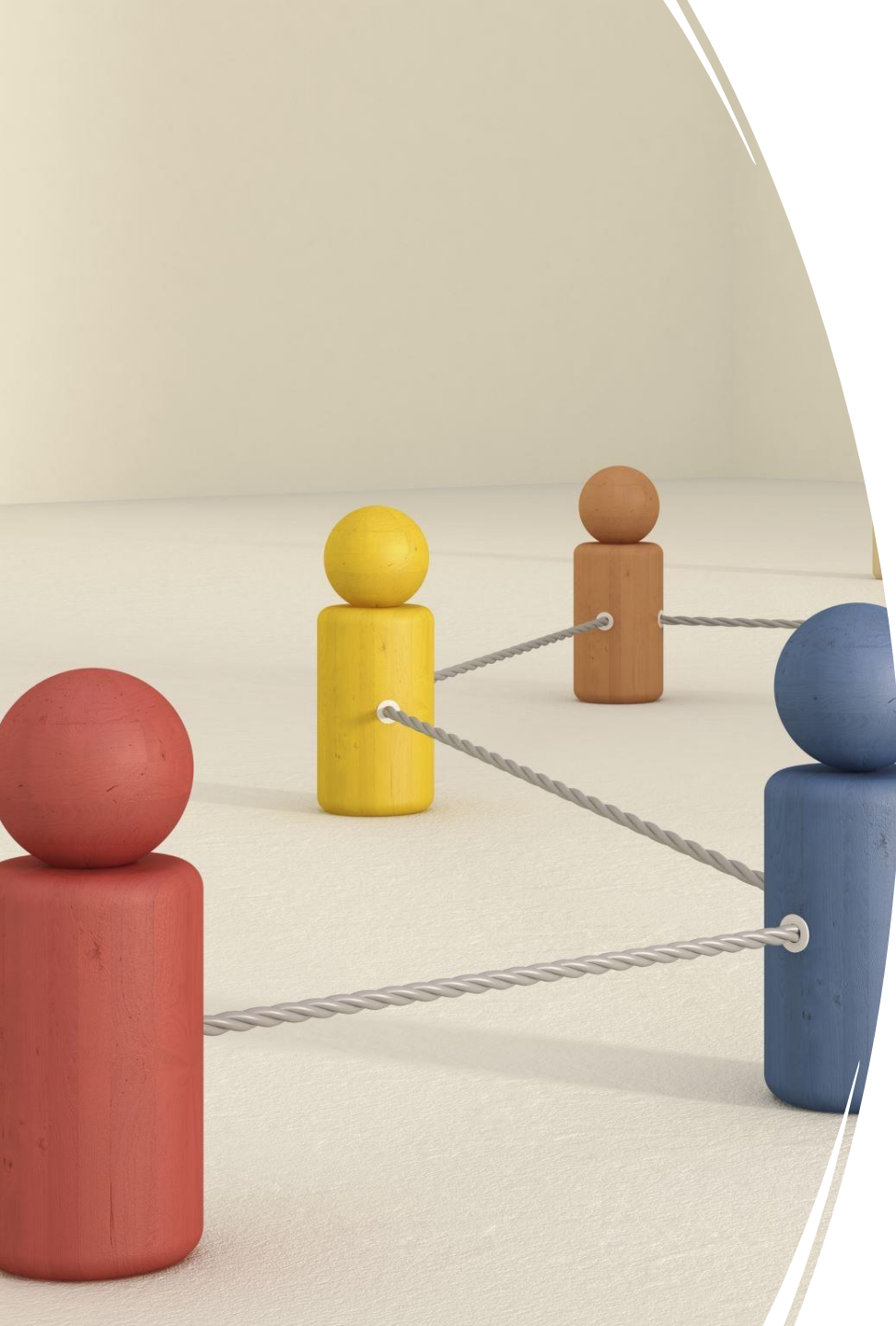


Figure 2-1: The IT Security Learning Continuum



How to establish and oversee awareness and training programs

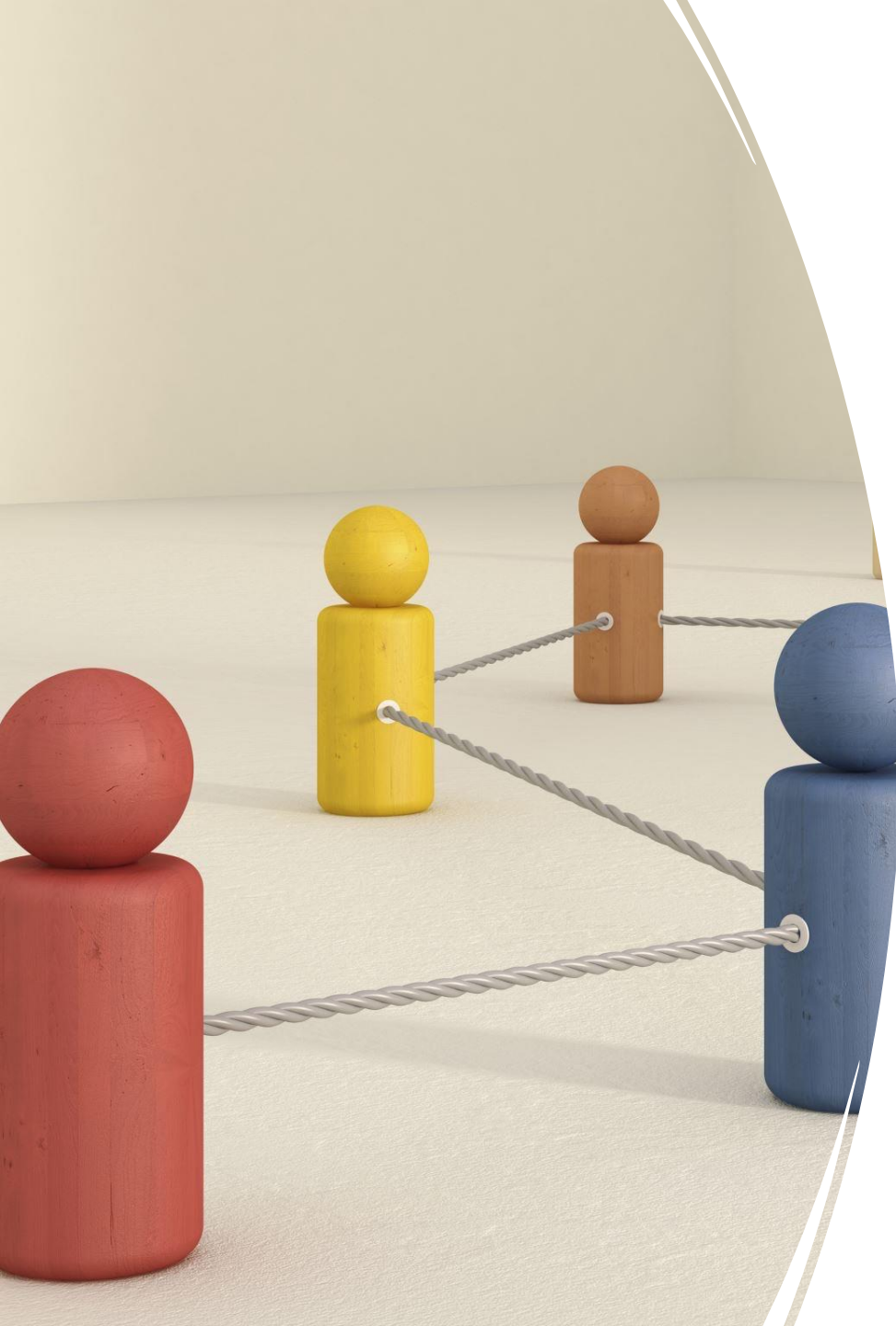
Input

- The size and geographic dispersion of the organization
- Defined organizational roles and responsibilities
- Budget allocations and authority

How to establish and oversee awareness and training programs

Output

- **Model 1:** Centralized policy, strategy, and implementation
- **Model 2:** Centralized policy and strategy, distributed implementation
- **Model 3:** Centralized policy, distributed strategy and implementation



Centralized Program Management

- Are **relatively small** or have a **high degree of structure** and central management of most IT functions
- Have, at the headquarters level, the necessary resources, expertise, and knowledge of the mission(s) and operations at the unit level; or
- Have a **high degree of similarity in mission and operational objectives** across all of its components



Figure 3-1: Model 1 – Centralized Program Management

Partially Decentralized Program Management

- Are **relatively large** or have a **fairly decentralized structure** with clear responsibilities assigned to both the headquarters (central) and unit levels;
- Have functions that are **spread over a wide geographical area**: or
- Have **organizational units with diverse missions**, so that awareness and training programs may differ significantly, based on unit-specific needs.



Figure 3-2: Model 2 - Partially Decentralized Program Management

Fully Decentralized Program Management

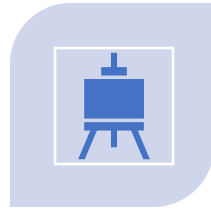
- Are **relatively large**;
- Have a very **decentralized structure** with general responsibilities assigned to the headquarters (central) and specific responsibilities assigned to unit levels;
- Have functions that are spread over a **wide geographical area**; or
- Have *quasi-autonomous* **organizational units** with separate and distinct missions, so that awareness and training programs may need to differ greatly.



Figure 3-3: Model 3 – Fully Decentralized Program Management



Conduct an initial assessment of employee security awareness.



Design for cultural context and employee cultural diversity.



Make a yearly plan to align goals and objectives.



Know your audiences to ensure content suitability.





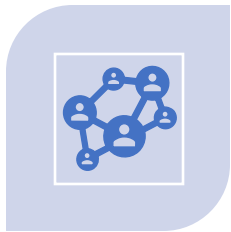
Sustain communication of relevant messages.



Maintain quarterly evaluation of employee performance.



Measure employee reporting of security incidents.



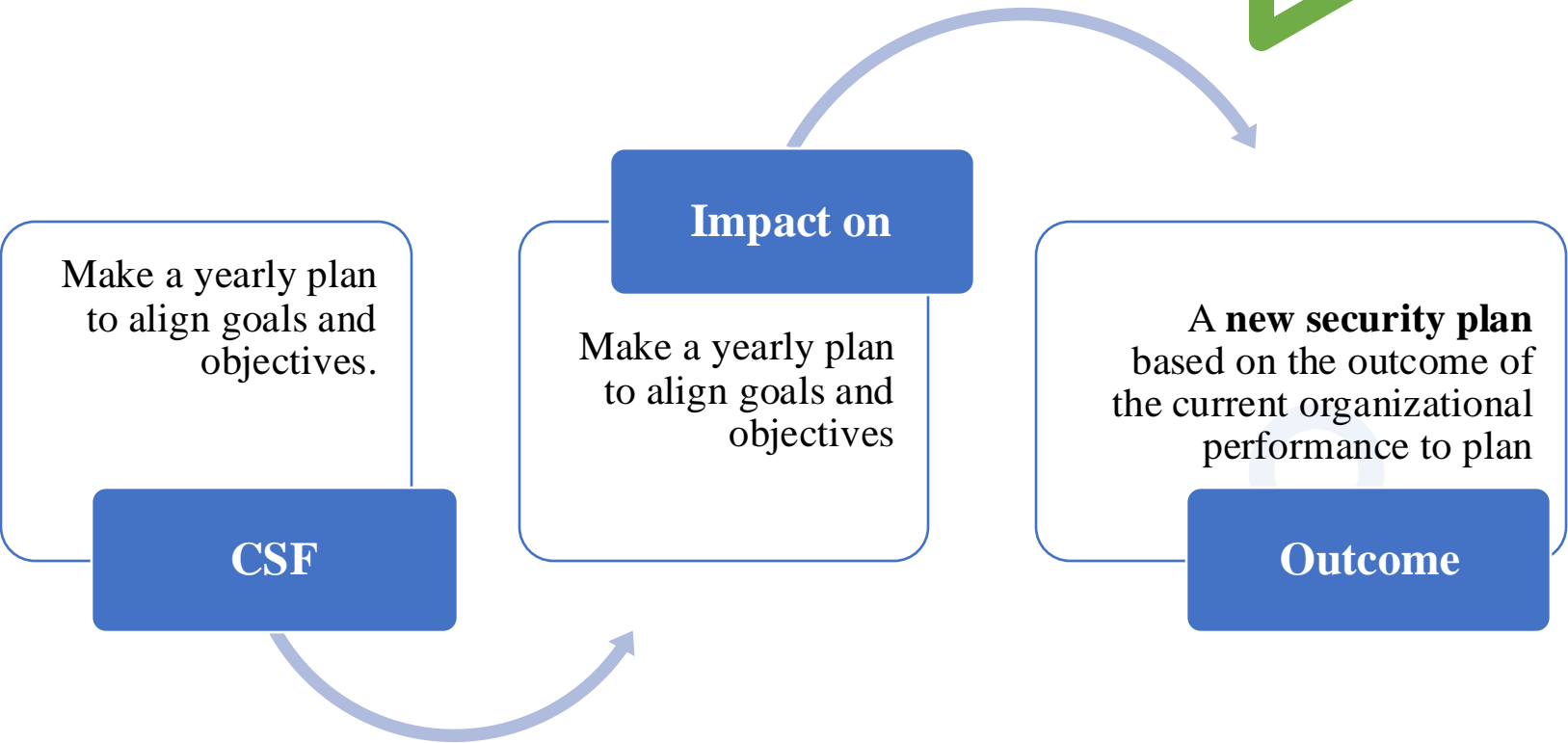
Motivate employees to engage in security awareness.



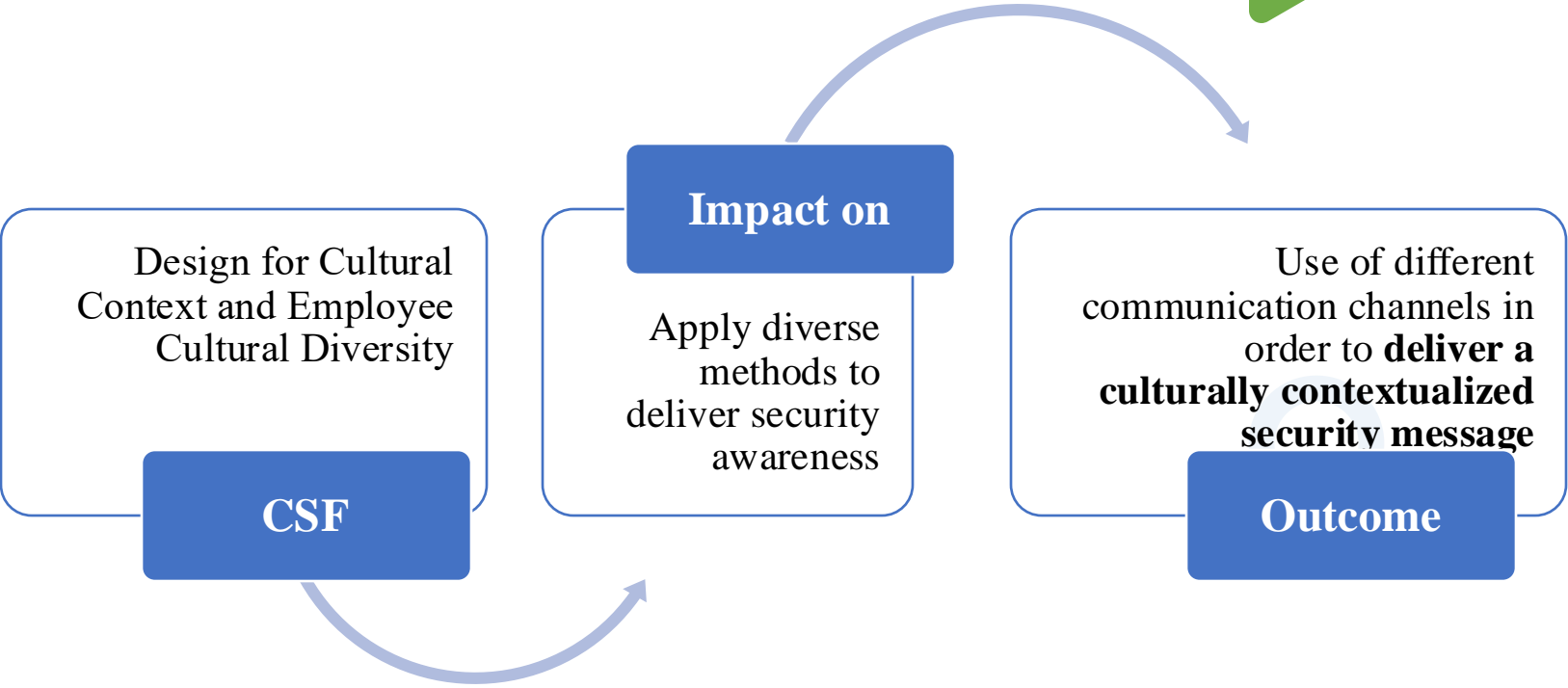
Apply diverse methods to deliver security awareness messages.



Some interactions: *Scheduling*



Some interactions: *Contextualizing*



Some interactions: *Informing*

