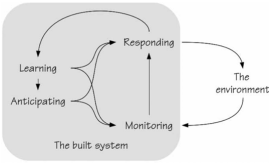
Neri V2

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

Cyber Resiliency Engineering Framework

- Anticipate
  - Understand + Prepare + Prevent
  - Maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks
- Withstand
  - Understand + Continue + Constrain
  - Continue essential mission/business functions despite successful execution of an attack by an adversary
- Recover
  - Understand + Continue + Reconstitute
  - Restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary
- Evolve
  - Understand + Transform + Re-architect
  - Change mission/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted cyber-threats



- 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 developments, 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 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

Adverse events differentiation criteria

Emergence → How quickly and visible does the adversity unfold?

- Gradual: creeping, accumulated, ordinary
  - Examples: capacity overload
  - Implication for resilience: likely to be anticipated owing to monitoring and warning systems; collective response requires synchronization
- Acute: sudden, unexpected, traumatic, high impact
  - Examples: terrorist attack, natural disaster
  - Implication for resilience: low chance of being avoided; collective response facilitated by a shared sense of fate

Novelty → Do knowledge and solutions already exist?

- Non-novel: controllable circumstances, existing solutions
  - Examples: floods in coastal regions
  - Implication for resilience: absorptive response based on predefined processes and routines
- Novel: usual circumstances, no existing solutions
  - Examples: new diseases
  - Implication for resilience: time-consuming sensemaking; tendency for adaptive response

Severity → How severe is the adversity (matter of life and death?)

- Livelihood-threatening: economic loss, impact on business survival, discriminate
  - Examples: financial crisis
  - Implication for resilience: rational response based on existing or new resources
- Life-threatening: impact on physical and emotional well-being, indiscriminate
  - Examples: war, natural disasters
  - Implication for resilience: collective, emotional response; rational response not fully applicable

Resilience properties

Capacity: potential to do something

Ability: something already in use of existing

Capability: refer to specific organizational abilities underlying resilience

Organizational resilience

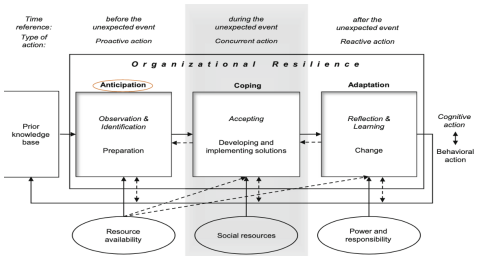
Resilience means to **EFFECTIVELY** respond to adverse events, **not only after adverse events, but before, during, and after as well**

Resilient organizations respond **not only** to the past (**reactive action**) or to current issues (**concurrent action**), but also to the future (**anticipatory action**)

The first stage of the resilience process refers to the **attempt to anticipate critical developments and potential threats and be prepared**

An **offensive response** comprises a **purposeful coping during critical situations** as well as some kind of **adaptation, transformation, or learning after** critical situations have occurred

💡 Organizational resilience is a set of organizational capabilities that allow for a **successful accomplishment of the three resilience stages**



Anticipation capabilities

Anticipation is the first stage of organizational resilience, focusing on the ability to proactively detect, identify, and prepare for potential threats or critical developments. It involves three key capabilities:

1. **Observation and identification**: The ability to recognize early signals of crises through practices such as environmental scanning (acquiring external knowledge) and scenario planning. Organizations must recognize early signals of crisis to respond quickly and avoid escalation
2. **Preparation**: The ability to develop resources necessary in times of crisis (recovery plans). Preparation includes risk management, training and simulation practices. Being prepared means that an organization is **equipped to deal with unforeseen adversity**. Organizations prepare without knowing **if, when, or where** an unexpected event will occur in the future (by expanding general knowledge and technical facility, and generalized command over resources)

Coping capabilities

Coping is a critical dimension of organizational resilience, focusing on managing unanticipated events once they occur. It encompasses two primary capabilities:

1. **Accepting the problem**: Organizations must overcome denial and accept critical situations to react quickly. Acceptance requires understanding the operational environment, defining system reference states, and acknowledging failures. This process, linked to anticipation capabilities, involves developing an attitude of wisdom — balancing confidence with caution and embracing doubt
2. **Developing and implementing solutions**: This involves **sensemaking** (understanding and interpreting the crisis through constant feedback), improvisation, and collective problem-solving. Practices like "**bricolage**" (creative improvisation) and expert networks enable rapid adaptation. Quick and precise implementation is vital, with coordination mechanisms (e.g. team collaboration and knowledge sharing) ensuring a unified and effective response.

Adaptation capabilities

Adaptation is a key dimension of resilience, enabling organizations to adjust to crises and use change as an opportunity for advancement. This long-term learning process expands organizational knowledge and strengthens anticipatory capabilities.
Adaptation involves two main capabilities:

1. **Reflection and Learning**:
    a. **Reflection**: Organizations must critically evaluate crisis experiences and integrate insights into their knowledge base. This involves a structured process, such as problem articulation, analysis, theory

formulation, and action. Practices like after-action review, incident reports, and informal discussions enhance this learning process.

b. **Learning**: Effective learning occurs through reflection, feedback, and experimentation. Organizations not only learn from their own failures but also through *vicarious learning* — analyzing failures in similar industries or systems.

2. **Organizational Change:** This involves cultural transformation, shifting norms, values, and practices. Organizations must balance belief in past experiences with openness to new approaches, as crises often present novel challenges requiring innovative solutions. To embed new knowledge, organizations must act on insights, transferring solutions to various departments. Robust change management processes, strategic planning are crucial. Practices such as effective communication and change agents can facilitate this process.

Interaction of resilience capabilities

The three stages of resilience are interdependent and overlapping. Anticipation helps organizations act quickly and effectively on changes, while a broad range of actions enhances the ability to perceive threats. Coping, in turn, lays the groundwork for reflection, learning, and adaptation, as organizations draw lessons from both successes and failures during crises. This learning process strengthens future coping capabilities.

Potential and realized resilience

To achieve high levels of organizational resilience, it is crucial to develop all three stages of resilience capabilities: anticipation, coping, and adaptation, forming a meta-capability. **Anticipation capabilities** help identify risks and take proactive measures, creating a resilience potential, which is the foundation for future responses. Organizations also need coping capabilities to effectively apply crisis plans and develop solutions during crises. Additionally, learning from critical events is crucial to adapt, transform knowledge, and enhance capabilities.

Cognitive and behavioral dimensions

The three stages of resilience — anticipation, coping and adaptation — require an interplay of cognitive and behavioral capabilities. Cognitive capabilities, such as mindfulness, sensemaking, and critical reflection, are essential for understanding environmental changes and making informed decisions. Behavioral capabilities, including improvisation, experimentation, and knowledge implementation, ensure actions are taking effectively. Resilient organizations arise when cognition and behavior work in conjunction, as neither cognitive development nor behavorial change alone is sufficient. Additionally, contextual factors like resources, social capital, and power play a vital role in supporting resilience processes and capability development.

Main antecedents and drivers

The development of organizational resilience capabilities, which support the three resilience stages, is influenced by key contextual factors. These include antecedents like the organization’s knowledge base and drivers such as resource availability, social resources, and power or responsibility. Since resilience capabilities are complex and deeply embedded in social contexts, identifying specific factors and conditions for their development remains challenging.

Knowledge base

The organization’s knowledge base plays a crucial role in all stages of resilience. While a firm’s prior knowledge base facilitates acquiring new knowledge by guiding its search, it can also limit exploration to familiar areas, potentially leading to narrow perceptions ill-suited for uncertain environments. To enhance resilience, organizations should cultivate a broad and diverse knowledge base, supporting the anticipation of internal and external changes. This diversity also aids in developing effective crisis responses, improving decision-making, fostering creativity, and promoting learning from experiences.

The knowledge base connects the adaptation and anticipation phases, as learning from crises expands knowledge and strengthens anticipation capabilities. Learning occurs throughout all resilience phases: anticipating crises

(learning for crisis), coping with them (learning as crisis), and adapting afterward (learning from crisis). This continuous feedback loop ensures that each phase enhances the organization's knowledge base, further boosting its resilience capabilities.

Resource availability

A broad and accessible set of resources, including time, financial, and human resources, is essential for building organizational resilience. These resources support effective anticipation, coping, and adaptation by enabling activities such as environmental scanning, crisis preparation, and recovery.

Social resources

Social resources are critical for organizational resilience. Deep social capital fosters coordination, shared goals, and mutual respect, enabling organizations to implement solutions and recover effectively. Trust, open communication, and a learning-oriented culture enhance these resources, while respectful interactions and shared cognitive frameworks strengthen organizational networks and crisis response.

Power and responsibility

Crises can create opportunities for adaptation, but learning and change are not automatic. **Power and responsibility** significantly influence whether new knowledge is utilized. Power dynamics can either support or hinder organizational learning and adaptation, with expertise-based power fostering resilience more effectively than hierarchical authority. Resilient organizations emphasize decentralization, self-organization, and shared decision-making, enabling flexibility in dynamic environments.

Antecedents of organizational resilience

Organizational resilience is shaped by antecedents that determine its ability to respond to crises. These antecedents include **pre-disruptive phases** (like preparation and planning) and **response phases** during and after adverse events. They influence how organizations adapt and recover, playing a critical role in ensuring sustainability and renewal.

Cyber Organizational Resilience

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

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 fall in a controlled way, rather than being designed to soleley 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

Cybersecurity and cyber resilience differ in both focus and approach. Cybersecurity prioritizes protecting IT systems with a fail-safe intention, aiming to prevent breaches or disruptions by applying security externally. Its architecture is single-layered, focusing on isolated organizational protection.

In contrast, cyber resilience shifts the focus to ensuring business delivery despite disruptions. It adopts a "safe-to-fail" mindset, emphasizing the ability to recover and adapt. Security is built from within, with a multi-layered architecture that acknowledges the interconnected nature of modern organizations. Cyber resilience operates holistically, considering networks of organizations rather than individual entities alone.

💡 **Organizational resilience** focuses on the broader ability of an organization to adapt, recover, and thrive in the face of disruptions, whether they are internal or external. Characteristics like **self-efficacy**, **bricolage (improvisation)**, a **transformative mindset**, and **empathy** are essential in this context. These traits reflect an organization's capacity to leverage internal strengths, adapt creatively, and maintain a human-centered approach during challenges.

Cyber organizational resilience zooms in on the ability to prevent, withstand, and recover from disruptions specifically within the digital and technological landscape. As such, it emphasizes more structured and technical measures, like **situational awareness** (knowing your digital environment), **planning** (strategic preparation for cyber incidents), **training** (building cyber skills and awareness), and **vulnerability assessment** (identifying and mitigating system weaknesses).

Cyber resilience phases

Before an incident, the emphasis is on proactive measures such as planning, applying frameworks, assessing vulnerabilities, building situational awareness, and conducting training. These activities are foundational to preparing the organization for potential disruptions.

During an incident, the focus shifts to maintaining critical functions through the involvement of cybersecurity specialists, leadership, and collaborative efforts. This phase prioritizes immediate response and ensuring continuity under pressure.

After an incident, the organization concentrates on recovery, learning from the experience, and implementing changes to improve resilience against future threats. This phase underscores adaptation and growth based on the lessons learned.

Cyber OR Anticipation

Themes	Objectives	Tools
Situational Awareness	- Cyber threats frequency and trends identification - Quickly and accurate detection of 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
Training	- Increase awareness - Cyber-attack prevention and mitigation - Cyber-risk learning - Roles and responsibilities clarification	- Resilience plan education - Cyber-risks training - Social engineering, phishing attacks simulations
Resources	- Better defense against cyber-attacks - Enhanced Cyber Resilience strategies	- Dedicated budget allocation - Dedicated resources

Cyber OR Responding

Themes	Objectives	Tools
Roles and responsibilities	- Absorption - Mitigate cost - Increased agility (quickly adapt to changing cyber threats, vulnerabilities)	- Cybersecurity role - CISO - Cybersecurity expertise

Leadership	- Enable employee's cyber-resilience - Strategies implementation	
Maintain function	- Ensure business continuity - Deliver the intended outcome	
Collaboration	- Adequate and appropriate strategy implementation - Shaping cybersecurity knowledge in the environment	- Social networks - Networks and alliances

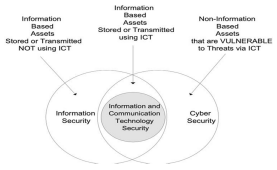
Cyber OR Recovering and Learning

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

Culture

Cybersecurity Culture 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

Information security culture (NIST): information security refers to the protection of information and information systems from unauthoritzed access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Cybersecurity is "the ability to protect or defend the organization from cyber-attacks"



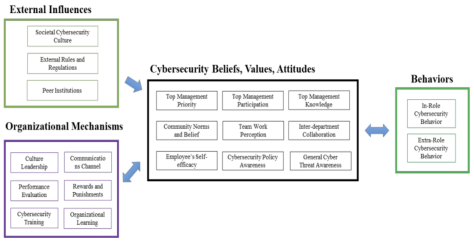
Cybersecurity culture practices

- 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**
- Involvement and communication → promotes a continuous reflection on own behavior, how that may influence security, and what they themselves can do to **improve security**. Whether 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

Cybersecurity Culture Model



To model a **cybersecurity culture**, three key concepts were analyzed:

1. **Organizational Culture**: Defined as the shared beliefs, values, and artifacts shaping collective behavior. It can be categorized into different orientations emphasizing trust, innovation, rules, or goal-driven approaches.
2. **National Culture**: Influences how employees comply with organizational rules and policies, shaped by broader cultural dimensions such as individualism, time orientation, and restraint.
3. **Information Security Culture**: Refers to the attitudes, values, and knowledge influencing employee behaviors regarding information systems, ensuring compliance with policies to protect organizational assets.

Cybersecurity Culture vs. Information Security Culture:

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

Cybersecurity 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 Model

The ultimate goal of managers is to promote **cybersecure behaviors**, which are driven by an organizational **cybersecurity culture**—comprising beliefs, values, and attitudes. This culture is shaped by:

- **External Influences**: Factors outside the organization's control.
- **Organizational Mechanisms**: Tools and strategies managers can implement internally.

The conceptual framework (illustrated in Figure 1) outlines these relationships, emphasizing how external and internal factors collectively influence the culture, which in turn shapes behaviors. Further details on the model and its constructs are explored in subsequent sections.

Behaviors

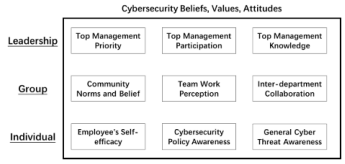
Cybersecurity is not solely a technical issue—it heavily depends on **employee behaviors** to reduce or create vulnerabilities. A **cybersecure culture** fosters two key types of behaviors:

1. **In-Role Cybersecurity Behaviors**: Actions directly related to an employee's official responsibilities, such as complying with security policies, avoiding misuse of systems, and reducing policy violations. These behaviors are essential for maintaining organizational security.
2. **Extra-Role Cybersecurity Behaviors**: Voluntary actions beyond job duties, including:
    - **Helping**: Supporting colleagues with cybersecurity questions.

- **Voicing**: Sharing ideas, feedback, or knowledge to improve cybersecurity.

Extra-role behaviors, particularly voicing, are highly valuable for addressing the complexities of cyber threats, encouraging innovation, and identifying emerging vulnerabilities across all organizational levels.

Beliefs, Values and Attitudes



At the core of the model is **cybersecurity culture**, which comprises values, attitudes, and beliefs that guide behaviors within an organization. While these cultural elements are often unwritten and implicit, they manifest in the actions of leaders, groups, and individuals. Leadership plays a critical role in shaping and reinforcing this culture by setting examples, allocating resources, and fostering shared understanding.

The leadership's influence on cybersecurity culture is assessed through three constructs:

1. **Top Management's Priorities**: Reflects the importance leaders place on cybersecurity, evident in strategic decisions and resource allocation.
2. **Top Management's Participation**: Measures leaders' direct involvement in cybersecurity activities, such as policy communication, training, or proactive actions to secure the organization.
3. **Top Management's Knowledge**: Refers to leaders' understanding of cybersecurity vulnerabilities and their ability to foster a cyber-resilient organization.

Effective leadership aligns organizational efforts with cybersecurity priorities, shaping beliefs and driving employee engagement in securing the organization.

At the group level, **shared values and beliefs** emerge through collaboration, communication, and teamwork. These cultural artifacts are influenced by group interactions and are summarized by three key constructs:

1. **Community Norms and Beliefs**: The collective ideas a group holds about cybersecurity, which influence individual attitudes. Social theories highlight how group norms shape personal beliefs, such as valuing information protection.
2. **Teamwork Perception**: How teams work together to enhance cybersecurity. Effective collaboration fosters shared understanding and situational awareness of threats, enabling teams to incorporate cybersecurity considerations into their activities.
3. **Inter-Department Collaboration**: Cross-functional efforts among departments to improve cybersecurity. Collaboration extends beyond IT and information security to involve business sectors, emphasizing the organization-wide value placed on cyber resilience.

Group norms and collaboration strongly influence the organization's cybersecurity culture, particularly when cybersecurity discussions and actions involve employees beyond dedicated cybersecurity professionals.

At the individual level, **cybersecurity culture** is influenced by employees' **beliefs and knowledge**. Understanding cyber threats, being aware of policies, and having a sense of self-efficacy increase the likelihood of behaviors that enhance organizational security. The model includes three key constructs:

1. **Employee's Self-Efficacy**: An individual's confidence in their ability to take effective cybersecurity actions. Higher self-efficacy leads to greater efforts in maintaining cybersecurity.
2. **Cybersecurity Policy Awareness**: The understanding of organizational policies and their importance. Employees who are aware of policies are more likely to follow them, contributing to overall cybersecurity.

3. **General Cyber Threat Awareness**: An employee's knowledge of cyber threats. Greater awareness helps employees identify and respond to potential risks, such as suspicious communications, enhancing the organization's security posture.

These factors empower employees to act in ways that contribute to increasing cyber resilience within the organization.

Organization Mechanisms

Organizational culture, shaped by beliefs, values, and attitudes, can be cultivated through six **managerial levers** that foster a strong cybersecurity culture:

1. **Cybersecurity Culture Leadership**:
   - Assigning a dedicated leader or team to focus on developing and maintaining a cybersecurity culture ensures consistent efforts to integrate security practices organization-wide.
2. **Performance Evaluations**:
   - Incorporating cybersecurity behaviors into employee evaluations sets clear expectations and emphasizes secure practices, such as policy compliance and phishing simulation performance.
3. **Rewards and Punishments**:
   - A balanced system of recognition and consequences motivates employees to follow secure practices and discourages risky behaviors, reinforcing accountability.
4. **Organizational Learning**:
   - Building processes for continuous learning, such as mentorship, knowledge-sharing, and access to expertise, helps the organization adapt and improve cybersecurity resilience.
5. **Cybersecurity Training**:
   - Regular, varied training ensures employees stay informed about threats and best practices. Periodic updates and targeted sessions foster lasting behavioral changes and awareness.
6. **Communication Channels**:
   - Using diverse methods to share cybersecurity messages—like updates, incident reporting, and campaigns—ensures consistent communication, proactive engagement, and swift threat response.

These levers help managers shape behaviors, instill values, and sustain a proactive cybersecurity culture across the organization.

External Influences

An organization's attitudes, beliefs, and values about cybersecurity are shaped by both internal and **external factors**, including societal culture, regulations, and peer influence. Key external influences include:

1. **Societal Cybersecurity Culture**: Communication plays a key role in shaping societal perceptions of cybersecurity. The media, public discussions, and awareness campaigns influence how individuals and organizations perceive cyber threats. Regular communication about cyber risks, breaches, and best practices helps create a societal culture that prioritizes cybersecurity.

2. **External Rules and Regulations**: Effective communication between regulatory bodies and organizations is essential for compliance with cybersecurity laws and regulations. Communication helps ensure that organizations understand and implement the required cybersecurity measures, such as data protection regulations like GDPR. This communication may occur through official channels like governmental publications, legal advisories, or industry-specific guidelines.
3. **Peer Institutions**: Communication among peers, including trade associations, conferences, and social interactions, facilitates the sharing of cybersecurity practices and experiences. These interactions provide a platform for learning, benchmarking, and adopting successful strategies. Communication channels within and between industries allow organizations to understand the cybersecurity concerns of their peers and influence their own practices accordingly.

Cybsersecurity awareness

Ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organization from lasting behavioral change (ENISA)

- **Password Management** emphasizes creating strong passwords, changing them regularly, not sharing them, and being aware of potential risks.
- **Social Media Use** highlights responsible use of social networks, avoiding access during work, cautious posting of sensitive information, and updating privacy settings.
- **Email Use** focuses on avoiding phishing and risky attachments, and being vigilant against social engineering attacks.
- **Internet Use** stresses safe browsing, avoiding suspicious sites, not sharing sensitive information, and using content filtering.
- **Data Access and Information Handling** involves securely handling sensitive materials, verifying file authenticity, and properly disposing of sensitive documents.
- **Incident Reporting** involves promptly reporting security incidents, suspicious behaviors, or rule violations.
- **Device Securement and Updating** emphasizes updating software, locking devices when idle, and using secure passwords.
- **Mobile Device Use** includes securing mobile devices physically, using secure networks, and being aware of risks like shoulder surfing.
- **Awareness of Policies and Responsibilities** encourages employees to follow security rules, understand risks, and adhere to organizational policies.

Training programs & Education

It cannot be assumed that the **average employee has the necessary knowledge** to perform his 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

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

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

Security Basics and Literacy
The basics and literacy material
allow for the development or evolution of a more robus awareness program and **provide the foundation for the training program**

Training

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

The difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues.

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

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**

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.

Professional Development

Ensure that users, from beginner to the career security progessional, possess a required level of knowledge and competence necessary for their roles. Professional development validates skills through certification. Such development and successful certification can be termed "professionalization". The preparatory work to testing for such a certification normally includes study of a prescribed body of knowledge or technical curriculum, and may be supplemented by on-the-job experience

Two types of certification: general and technical

- The general certification focuses on establishing a foundation of knowledge on the many aspects of the IT security profession
- The technical certification focuses primarily on the technical security issues related to specific platforms, operating systems, vendor products, ecc

Awareness and training programs

- Input
  - The size and geographic dispersion of the organization
  - Defined organizational roles and responsibilities

    - Budget allocations and authority
- 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

Communication between central authority (CA) and organizational units (OU) travels both ways: CA communicates the agency's policy directives regarding IT security awareness and training, strategy, for conducting the program, material and methods for implementation to the OU; OU provide information requested by the CA. OU can provide feedback on the effectiveness of awareness and training material and teh appropriateness of the method used to implement the material

Deployed by agencies that:

- 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
- Have a **higher degree of similarity in mission and operational objectives** across all of its components

Partially Decentralized Program Management

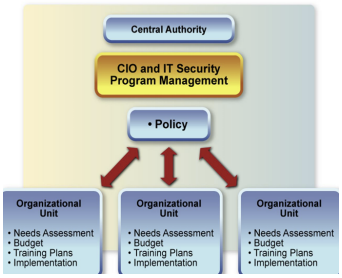
Communication between the CA and the OU travels in both directions in this model. The CA communicates the agency's policy directives regarding IT security awareness and training, the strategy for conducting the program, and the budget for each OU. the CA may also advise the OU that they are responsible for developing training plans and for implementing the program, and may provide guidance or training to the OU so that they can carry out their responsibilities

Deployed by agencies that:

- 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**
- Have **organizational units with diverse missions**, so that awareness and training programs may differ significantly, based on unit specific needs

Fully Decentralized Program Management



Communication between the CA and the OU travels in both directions in this model. The CA communicates the agency's policy directives regarding IT security awareness and training, and the budget for each organizational unit. The CA may also advise the OU that they are responsible for conducting their own needs assessment, developing their strategy, developing training plans, and implementing the program. The CA may provide guidance or training to the OU so that they can carry out their responsibilities

Deployed by agencies that:

- 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**
- Have **quasi-autonomous organizational units** with separate and distinct missions, so that awareness and training programs may need to differ greatly

Evolving the CISO role

The role of the Chief Information Security Officer (CISO) is evolving from a primarily technical focus to a strategic leadership role that bridges business transformation and cybersecurity. Modern CISOs must connect cybersecurity efforts with organizational goals, driving initiatives that enable success.

Effective CISOs are fluent in both business and technology, adept at collaborating with C-suite executives and boards, and navigating complex regulatory and privacy challenges. They also foster a shared-risk perspective across risk management, compliance, and leadership teams. However, only 26% of organizations currently see developing cybersecurity risk metrics as a core responsibility, though this shift reflects growing integration of cybersecurity with overall risk management and data governance.

Organizations often recruit CISOs externally, though some internal promotions occur, particularly from technology, compliance, or consulting roles. As the role grows strategically, building a company-wide cybersecurity culture and formulating strategies are becoming critical responsibilities. Routine technical tasks, like threat identification, are expected to become more automated and less central to the CISO's role.

Key challenges include the lack of CISO involvement in early product development stages, with less than half participating in product testing, development, or strategy. This limits the organization's ability to embed security from the outset, missing opportunities to leverage the CISO's expertise.

To address these gaps, organizations should:

- Develop a strong business case for organization-wide cybersecurity programs.

- Empower CISOs to focus on strategy and fostering a cybersecurity culture.
- Decouple the CISO role from IT and promote closer engagement with executives and boards.
- Involve CISOs earlier in product and application development.
- Invest in recruiting, training, and providing adequate resources for cybersecurity leadership.

This evolution positions the CISO as a key driver of strategic resilience in an increasingly digital and risk-intensive environment.