SECURE, AWARE & RESILIENT

Security Awareness & Training are foundations for a resilient workforce!

etis | THE COMMUNITY FOR TELECOM PROFESSIONALS

Introduction

In an increasingly connected world where cyberattacks are becoming more sophisticated, building a resilient workforce is essential. For telecommunications and technology companies, resilience directly impacts brand stability, customer trust, and overall market position. Resilience is a dynamic interplay between people, processes, and technology — not a single point of failure or blame. This synergy ensures that organizations detect, recover from, and continuously improve after cyber incidents. An integral part of this resilience is the combination of security awareness, a positive security culture (open minded, employee orientated), psychological safety, and targeted training. These elements create an informed workforce capable of actively contributing to the organization's security and stability.

Contents

The Role of Security Awareness

Security awareness encompasses equipping employees with the knowledge and tools to recognize and address threats. For tech and telecom companies (and other organizations under the scope of NIS2), which manage infrastructure underpinning global communications, it is essential.

Through targeted awareness campaigns, organizations ensure their workforce identifies risks and acts appropriately, emphasizing the holistic coordination of people, processes, and technology. Regular campaigns, interactive training sessions, and accessible resources foster a pervasive sense of responsibility across all roles. Everyone has an important role in cybersecurity and must act accordingly.

Security awareness aligns with the NIS2 Directive's mandate (and other pieces of legislation such as DORA and the AI Act) to implement comprehensive programs addressing both technical and organizational aspects of cybersecurity. The NIS2 Directive is the first time that concrete requirements for security awareness are being set up throughout Europe, which can be exemplary for other scenarios (e.g. DORA).

NIS2 Directive Emphasis

The NIS2 Directive specifically emphasizes:

- **Regular Training for All Employees:** Impart knowledge on cybersecurity basics, incident handling, backup management, and business continuity (Article 21, Paragraph 2).
- **Specialized Training for Leadership:** Ensure management understands risks and implements suitable governance practices.
- **Tailored Programs:** Address the unique needs of employees across different departments and levels.
- **Periodic Updates:** Regularly review and update training programs to address new threats and compliance requirements.

For telecommunications and technology companies, adhering to these measures is not merely compliance — it is integral to sustaining customer confidence. One breach can erode years of trust and compromise market reputation.

Security Awareness & Culture Lifecycle Framework

A robust security culture harmonizes the values, attitudes, and behaviours of an organization concerning security. For tech and telecom companies, where customer trust is paramount, cultivating a collaborative and transformational security culture is vital.

"Culture eats strategy for breakfast," as management thinker Peter Drucker famously noted. Even the best technical defences falter without an engaged and informed workforce.

A strong and transformational culture encourages employees to collaborate on solutions and voice concerns proactively. This trust and transparency are particularly crucial for companies managing critical infrastructure. Security culture thrives when aligned with consistent, organization-wide reinforcement of psychological safety.

Psychological Safety: Encouraging Open Communication

Psychological safety, a concept championed by Amy Edmondson, ensures individuals feel confident raising concerns or reporting mistakes without fear. Telecommunications and technology companies benefit immensely when employees trust that their voices contribute to improved processes, not punitive measures.

By fostering this openness, organizations enable rapid identification and mitigation of vulnerabilities. For example, an employee who reports suspicious activity empowers the company to respond promptly, reducing potential harm. This dynamic approach strengthens resilience and supports a cooperative security environment.

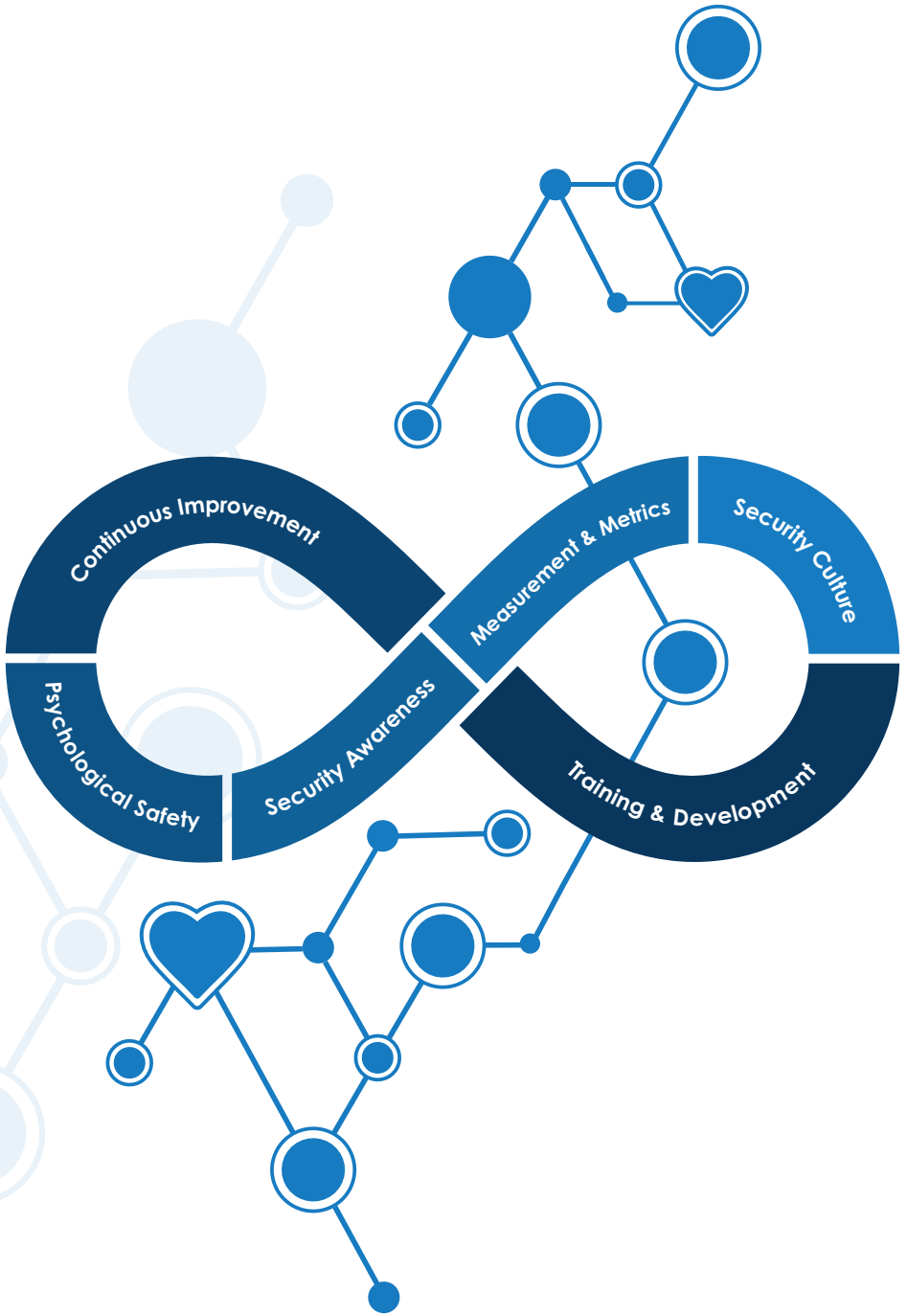
Training:
Bridging Knowledge and Action

Training transforms theoretical knowledge into actionable expertise. Employees practice real-world responses to potential threats in controlled, safe environments, enabling them to address incidents effectively.

The NIS2 Directive mandates that organizations prioritize training efforts:

- **Cyber Hygiene Practices:** Promote multi-factor authentication, secure email use, and awareness of social engineering tactics.
- **Incident Response Protocols:** Ensure employees across roles know their responsibilities during security events.
- **Leadership Engagement:** Encourage senior management to participate actively in awareness and training initiatives.

By focusing on collaboration between people, processes, and technology, training programs foster a well-rounded, prepared workforce.



Effective Measures to Support Resilience

Integrating security awareness, culture, and training into operational frameworks enhances brand integrity and builds trust. Telecommunications and tech firms benefit from:

1. Regular Awareness Campaigns:
- Be a security influencer – one who generates a desire for security competences and skills (The Why?, How? & What?).
- Develop memorable messages and tell stories (e.g., "Think Before You Click").
- Find and communicate links towards private life situations.
- Use videos, posters, and newsletters to reinforce core concepts.

2. Interactive Training:
- Implement gamification elements like escape rooms or role-playing scenarios.
- Provide online courses emphasizing real-world relevance.

3. Simulations and Safe-Environment Tests:
- Conduct phishing simulations to evaluate responses.
- Use tabletop exercises to rehearse incident response scenarios.

4. Feedback Mechanism:
- Establish channels for reporting concerns and risks.
- Recognize and reward proactive reporting.

5. Crisis Drills:
- Regularly test and refine incident response plans.
- Encourage cross-department collaboration during exercises.

6. Engaged Leadership:
- Provide role-specific training for decision-makers.
- Encourage executives to model compliance with security policies.

7. Supportive Communication:
- Train managers and leadership to cultivate open discussions on cybersecurity.
- Emphasize learning from, not penalizing, mistakes.

8. Continuous Evaluation:
- Periodically assess security culture effectiveness.
- Update strategies based on evolving threats and internal feedback.

Conclusion

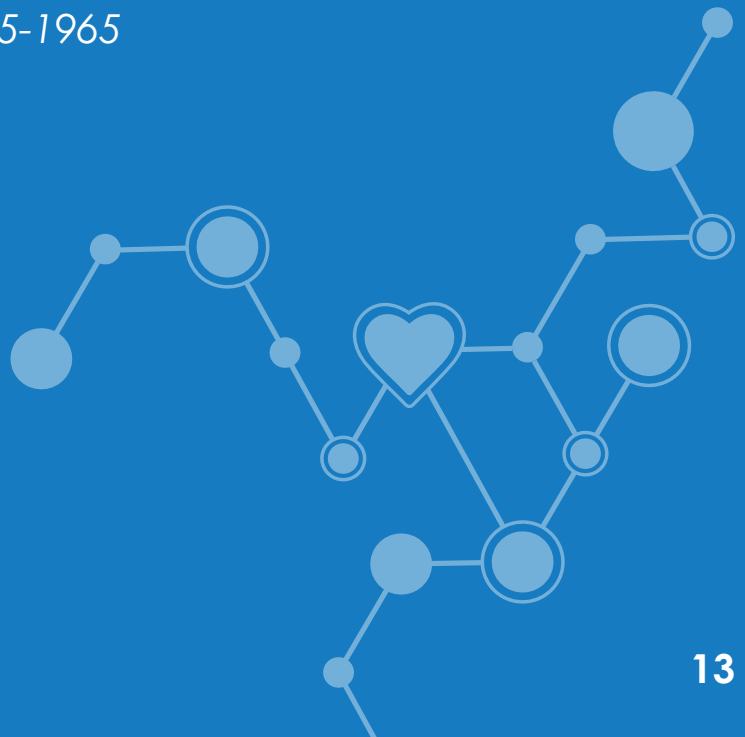
For telecommunications and technology companies, resilience is a strategic imperative. By integrating security awareness, a strong culture, and ongoing training with psychological safety, organizations empower their workforce to collaborate effectively. This holistic approach ensures brand stability, strengthens customer trust, and prepares the organization for evolving cyber challenges.

As psychologist Abraham Maslow noted, "If all you have is a hammer, everything looks like a nail." By fostering a collaborative synergy of people, processes, and technology, companies ensure robust, adaptive security strategies capable of navigating complex cyber landscapes.

"Example is not the main thing in influencing others. It is the only thing."

Albert Schweitzer

1875-1965



The promise from the Security Awareness Working Group:

A resilient workforce is at the heart of effective Security for telecommunications and technology companies. Security culture forms the foundation of this resilience, fostering an environment where employees feel empowered and equipped to address cyber threats collaboratively. By integrating psychological safety, ongoing training, and open communication, organizations create a culture that prioritizes vigilance and proactive engagement. For the first time on the European level, the NIS2 Directive underscores the importance of these measures, ensuring that employees across all roles understand their responsibilities and feel supported in addressing potential threats. Building resilience against security threats is not just about processes or technology — it's about creating a workforce that adapts, collaborates, and strengthens the organization's ability to withstand risks. This comprehensive approach enhances not only security but also trust, stability, and the long-term success of economy & society.

Notes:

Publisher: ETIS – The Community for Telecom Professionals / European Telecommunications ISAC – www.etis.org

Editor: ETIS Security Awareness Working Group

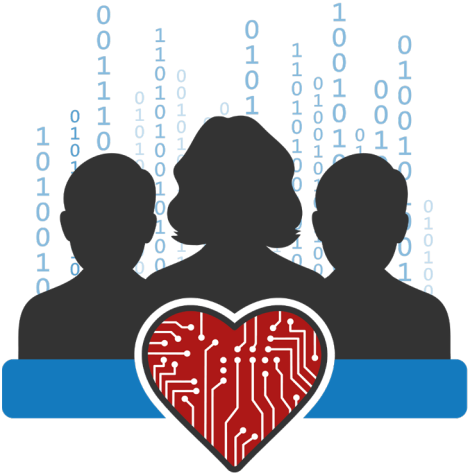
Layout: Marc Roux, Swisscom (Schweiz) AG

Contact: isac@etis.org

Release date: 26th May 2025

Take our survey!

etis THE COMMUNITY FOR TELECOM PROFESSIONALS



www.etis.org

Security Awareness Working Group

Mission of the ETIS Security Awareness Working Group is to expand the reach of achievements in building collaboration and knowledge transfer among security awareness professionals in the European telecom ecosystem and for their workforce.

- We discuss openly and transparently about security awareness and behaviour issues. Every participant in this task force is an advisor and bring their own expertise into this group.
- We share our achievements, failures and lessons learned to make each other better. We want to support each other in our roles, as responsible for security awareness and Human Risk Management, to change security behaviour in our organisation.
- We inspire each other to create the right contents and prepare programs and measures for our internal workforce including partners and also external customers.

To join, contact Andrija Višić, Senior Community & Programme Manager, ETIS, av@etis.org