Example: Creating a cybersecurity persona for a System Administrator

Step 1: Data gathering

The objective of this step is to collect comprehensive information about the systems administrator's role, daily activities, and interaction with security measures.

Activities:

- **Job description analysis:** Review detailed job responsibilities such as managing server environments, network configurations, and data backups.
- **Interviews and surveys**: Engage with systems administrators to gather insights on their day-to-day tasks, security concerns, and preferences.
- **Observation**: Observe administrators in their work environment to understand their workflows and interactions with security protocols.

Output:

- Job responsibilities: Server management, cloud management network configuration, regular system updates, and data backup.
- Survey insights: Most admins feel that security protocols can be cumbersome and sometimes slow down their tasks. They prefer hands-on and interactive training over reading manuals.

Step 2: Employee segmentation

Categorize systems administrators based on similar characteristics that influence their security needs and risks.

Criteria for segmentation:

- Level of Access – Distinguishing between those with access to critical vs. non-critical systems based on business processes.
- Experience and Training – Segmenting based on years of experience and previous security training.

Output:

- Group A: High-level access, over 10 years of experience, previous advanced security training.
- Group B: Less critical system access, 1-5 years of experience, basic security training.

Step 3: Developing persona profiles

Create a detailed persona for each segment that includes both professional and psychological traits to tailor the training effectively.

Profile Components:

- Professional Attributes – Specific system responsibilities and typical daily tasks.
- Psychological Traits – Attitudes towards security, work habits, and preferences.
  Behavioral Patterns – Any common shortcuts or bypasses in security procedures.

Mock Output Group A:

- Persona: Chris, 35, mid-level systems administrator with 10 years at the company.
- Professional Attributes: Manages important internal servers and cloud services, responsible for system updates and security patches.
- Psychological Traits: Detail-oriented, values efficiency, somewhat resistant to frequent procedural changes.
- Behavioral Patterns: Occasionally bypasses minor security steps to speed up work.

Step 4: Risk assessment

Identify the specific security risks associated with each persona based on their access level, responsibilities, and behaviors.

Risk Identification:

- Threat – Phishing and spear-phishing
- Vulnerability: need to assess susceptibility through advanced phishing simulations.
- Insider Threats: Consider risks due to high-level system access and occasional procedural bypasses.
- Compliance Risks: Potential for non-compliance given their views on security measures as cumbersome.

Mock Output:

- **Chris's Risk Profile**: High risk for phishing attacks due to access to critical systems, moderate risk for insider threats due to occasional security bypass, high compliance risk due to procedural views.

Step 5: Scenario planning

Develop training scenarios that are directly applicable to the persona's daily work and risks.

Scenario Development:

- Create scenarios that mirror real-life situations Chris might encounter, which also test his decision-making in terms of security.

Mock Output:

- **Scenario 1**: Chris receives a phishing email mimicking a common software vendor asking for credentials to resolve a licensing issue.
- **Scenario 2**: Chris needs to install a critical update but faces the choice of following a lengthy security procedure or bypassing some steps to expedite the process.

Conclusion

Through this detailed step-by-step process, the persona "Chris" is now a cornerstone for developing targeted, effective security training that addresses specific behaviors and risks. This approach ensures that the training is relevant, engaging, and practical, leading to improved security behavior across the organization. By continuously updating and refining these personas based on new data and feedback, the security training program remains dynamic and aligned with actual working conditions and evolving security threats.

Training examples:

Training Example 1: Decision-making workshop

Scenario: Chris has to decide whether to follow a lengthy security procedure or take shortcuts during a critical system update.

Training Activity: Host a workshop that presents 'Chris-like' employees with a series of decision-making scenarios. Use role-playing or a digital simulation that allows Chris to choose different paths and see the potential outcomes of each decision, highlighting the risks of non-compliance with security protocols. This can reinforce the importance of following security procedures fully, regardless of perceived time constraints.

Training example 2: Interactive phishing simulation

Scenario: Chris receives an email that looks like it's from a common software vendor requesting login credentials due to a licensing issue.

Training activity: Conduct a simulated phishing attack using a mock email designed to mimic common phishing tactics. After Chris interacts with the email, provide immediate feedback on indicators he should have noticed that it was a phishing attempt, such as suspicious sender addresses, generic greetings, and urgency claims. This activity will help Chris recognize and react appropriately to phishing attempts in the future.