Funded by the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

SECURITY DESIGN

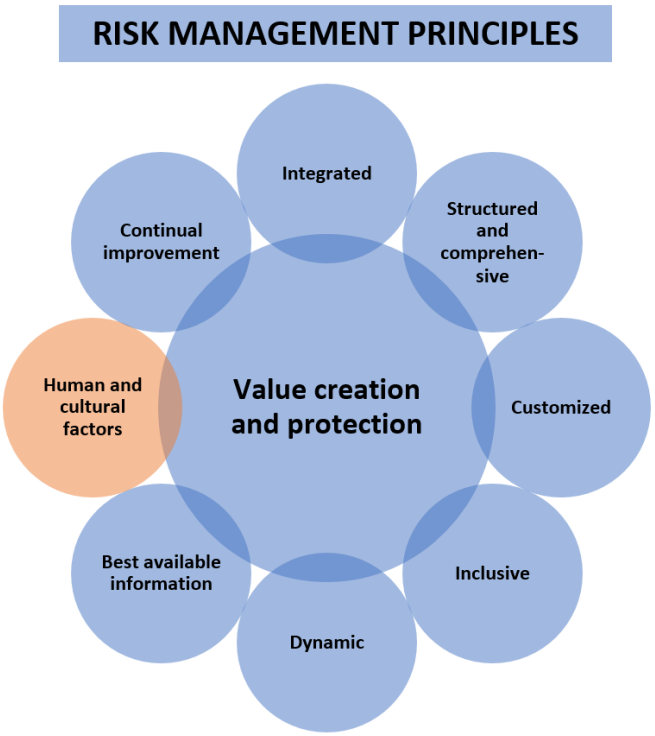
Kārlis Apalups / Turiba University / 2024

ABSTRACT

Designing security training for universal risk readiness is essential for any organization. The process begins with a commitment from top management, recognizing that without their backing, no substantial progress in training design can occur. Establishing clear and consistent security policies is crucial, as these will serve as the foundation for the training content. Once these policies are established, the organization must focus on educating its members about these policies and the best practices for mitigating security risks. To ensure the training remains relevant, ongoing monitoring and evaluation are necessary. This can be achieved by implementing specific metrics to assess the effectiveness of the security training and to evaluate the return on investment. By following these steps, an organization can create a robust security training program that prepares its members to handle security risks effectively.

Link to ISO 31000

ISO 31000 Risk management principles: Human and culture factors.



1. Introduction

Security training encompasses a range of practices aimed at enhancing the knowledge and skills necessary to protect sensitive information and physical assets.

The design of security training programs is a critical aspect that ensures the training is effective and relevant to the needs of the organization. It includes the development of a curriculum that covers essential topics such as data and record management, password safety, fire safety, evacuation and other crisis procedures. Security training design also involves creating a governance model to drive accountability during development and after the program is rolled out, ensuring that the training objectives align with the organization's security policies and regulatory requirements.

Moreover, it is not just about the content but also about the delivery methods, which can range from workshops, crisis scenarios and cosplay to online courses, and the evaluation of training effectiveness through assessments and feedback mechanisms. Effective security training design is a proactive approach to safeguarding an organization, emphasizing the importance of continuous learning and adaptation in the face of evolving threats. It is a strategic investment in the human element of security risk management, equipping individuals with the tools and understanding necessary to act as the first line of defense against potential breaches and incidents.

2. Case

Latvijas Finieris is the leading plywood and its products' manufacturer in Baltic States and Finland. The company is also active in forest management, logging and the production of synthetic resins and phenol films.

In 2014 “Latvijas finieris” had a huge fire in one of Rīga-based factories. After this event, the holding company decided to implement security culture and develop it. As part of its efforts was the creation of Safety management service (SMS) that managed security risks in such areas as – fire safety, occupational health and work safety, environmental protection and physical security. Before the fires there was a high amount of work related accidents which led to losses of working power, insurance costs and a decrease in feelings of safety among workers.

The efforts of SMS allowed to develop such a security culture that drastically lowered work related incidents, increase the ROI from security and safety investment and increase the overall organization culture. One of the core aspects of the security culture and risk management, was the development of training programs.

3. Best practices

Good security training design relies upon 3 basic pillars - 1) Panic (self) control 2) Preparedness for unknown 3) Overcoming of fear. For this to be achieved, creating a security training design for universal security risk readiness involves several key steps:

3.1. Assessment of Security Risks: Begin by identifying and assessing potential security threats and vulnerabilities within the organization or environment. This includes analyzing past incidents, current security measures, and potential future risks. A good security training design relies on relevant Security risk analysis.

3.2. Defining Training Objectives: Clearly outline what the security training program aims to achieve. Objectives may include enhancing awareness, improving response strategies, and ensuring compliance with security policies. Also it might include refreshing knowledge.

3.3. Developing a Curriculum: Design a comprehensive curriculum that covers all necessary topics, such as risk identification, prevention strategies, emergency response, and recovery plans. With the curriculum - a scenario also has to be created or put forward.

3.4. Incorporating Diverse Learning Methods: Utilize a mix of learning methods including lectures, interactive workshops, simulations, and e-learning modules to cater to different learning styles and ensure better retention of information. For the best practical training, it is recommended to use simulations of diversified scenarios of the same risk - people should not get accustomed to the expectable, but rather be trained to be prepared for unexpectable.

3.5. Customization for Different Roles: Tailor training modules for various roles within the organization, ensuring that each employee receives relevant information according to their responsibilities and level of access. Remember about specific training for essential workers - they will also be outlined during the security risk analysis.

3.6. Regular Updates and Revisions: Keep the training material up-to-date with the latest security trends, technologies, and practices. Regularly review and revise the content to maintain its relevance and effectiveness.

3.7. Evaluation and Feedback: Establish metrics to evaluate the effectiveness of the training program. Collect feedback from participants to identify areas for improvement and adjust the training accordingly. It’s good to include focus groups for employees in high risk environments and talk about their fears in workplace.

References

UNSMS Security Policy Manual – Security Training and Certification
https://policy.un.org/sites/policy.un.org/files/files/documents/2024/Apr/spm_-_chapter_v_section_c_-_learning_and_training.pdf

Designing a Successful Security Awareness Training Program
https://www.infosecinstitute.com/resources/security-awareness/designing-security-awareness-training-program/

https://www.finieris.com/en/home

https://www.tvnet.lv/4765017/latvijas-finiera-rupnica-liels-ugunsgreks