Funded by the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

HOW TO DEVELOP AND IMPLEMENT A SECURITY CULTURE IN YOUR ORGANIZATION

Kārlis Apalups / Turiba University, Latvia / 2023

ABSTRACT

The development of a security culture in an organization can be a challenge, but there are some steps for success that should be considered once a decision is made to develop a culture of security. Such a decision should come from the top management, since without such support no significant development of organizational culture can take place. Likewise, it is important to establish clear and consistent security policies to be followed as a standard throughout the organization. Once support and policies are set in place, the next step should be training your organization on the policies and best practices for security. In order to maintain an up-to-date security culture, there also need to be monitoring and measurement of the security culture and this may be achieved by setting in place specific metrics to measure the success of the security culture as well as establishing an ROI.

Link to ISO 31000

ISO 31000:2018 Risk management principles: Human and culture factors.

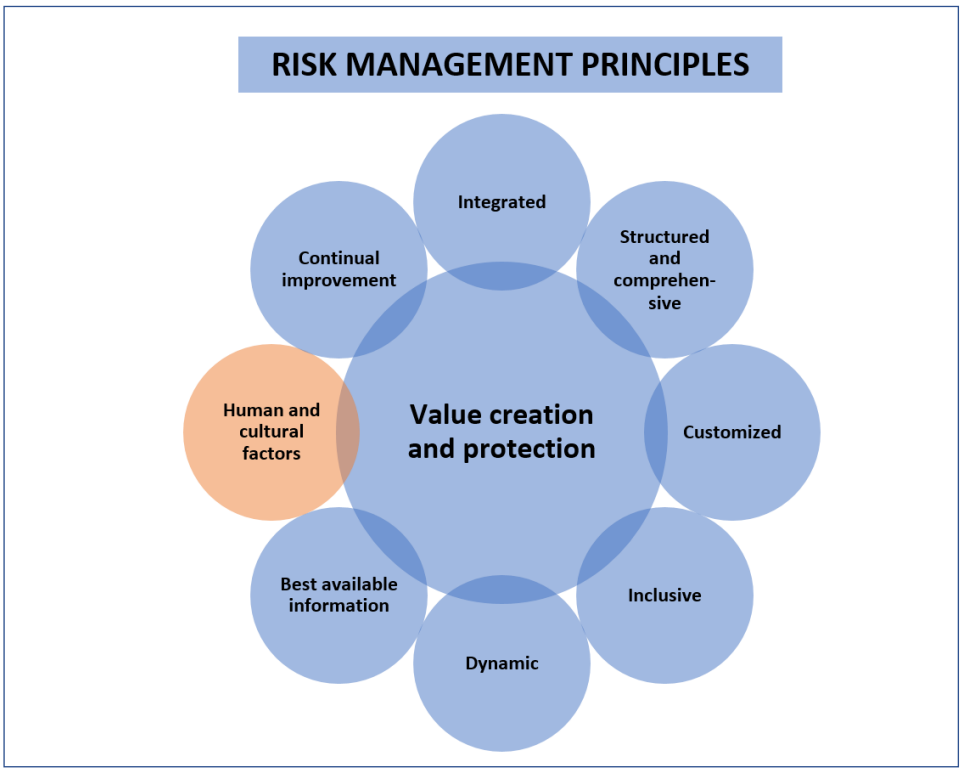

Figure 1. Risk management principles (adapted from ISO 31000:2018)

1. Introduction

Security culture is the set of ideas, customs and social behaviors that influence the security of an organization. It is the most important element in an organization's security strategy, as it affects how employees perceive and respond to security threats and incidents. A strong security culture can reduce risk and save money by preventing data breaches, complying with regulations, and protecting the reputation of the organization.

However, developing and implementing a security culture is not a simple task. It requires a strategic, long-term approach that involves top management support, clear and consistent security policies, effective awareness and training programmes, and continuous measurement and improvement. In this article, we will discuss some best practices for creating and maintaining a security culture in your organization. For the purpose of this article, we will be studying the case of “Latvijas finieris” which works in an international environment and has security as one of its core values.

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 a security culture and develop it. A part of its efforts was the creation of a 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 had been a high amount of work related accidents which had led to losses of working power, insurance costs and a decrease in feelings of safety among workers.

The efforts of SMS enabled developing a security culture that drastically lowered work related incidents, increased the ROI from security and safety investment and improved the overall organization culture.

3. Best practices

3.1. Get top management support. Obtaining the support of senior leaders is the first step in building a security culture. It is important that they communicate the significance and value of security and safety to all employees, allocate sufficient resources and budget for security initiatives, and hold themselves and others accountable for security performance. This support can also help create a positive tone at the top, where security is seen as a strategic priority and a shared responsibility, not just another budget expenditure.

3.2. Establish clear and consistent security policies. Security policy is like a standard for the organization. It’s the rules that define the expected behaviour and actions of employees regarding security. The policy should cover topics such as access control, password management, data protection, incident response and compliance requirements. Security policies should be aligned with the organization's goals and values, as well as with the relevant laws and regulations. They should also

be written in simple and understandable language, communicated to all employees, and enforced consistently.

3.3. Provide effective awareness and training programmes. Awareness and training programmes are essential for educating employees about the security risks they face, the policies they need to follow, and the best practices they need to adopt. They should be tailored to the specific needs and roles of different groups of employees, such as IT staff, managers, or end users. Awareness and training programmes should be delivered regularly and updated frequently to keep up with the changing threat landscape.

3.4. Measure and improve security culture. Security culture is not a static state, but a dynamic process that needs to be monitored and evaluated over time (just like risk management). There are various tools and methods that can be used to measure security culture, such as questionnaires, surveys, interviews, or audits. These can help to assess the current state of security culture, identify strengths and weaknesses, and track progress and changes. Based on the results of these measurements, security culture can be improved by addressing gaps, reinforcing positive behaviours, rewarding good performance, or correcting bad habits.

3.5. **Get an ROI of security culture.** Security culture is not only a cost centre, but also a value driver for an organization. By developing and implementing a security culture, an organization can achieve various benefits such as:

- Reducing the likelihood and impact of security incidents
- Enhancing customer trust and loyalty
- Improving employee engagement and retention
- Increasing operational efficiency and productivity
- Complying with legal and regulatory obligations
- Gaining competitive advantage in the market

To quantify these benefits, an organization could use metrics such as:
- Number of security incidents prevented or detected
- Amount of money saved or recovered from security incidents
- Customer satisfaction or retention rate
- Employee satisfaction or turnover rate
- Time or resources saved or optimized by security measures
- Compliance status or audit results
- Market share or revenue growth

By measuring these metrics before and after implementing a security culture programme, an organization can calculate the return on investment (ROI) of its security culture efforts.

By following these best practices, an organization can build and maintain a strong security culture.

References

The Importance Of A Strong Security Culture And How To Build One - Forbes https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/

Building a Culture of Security - ISACA https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security

Developing a cyber security culture: Current practices and future directions - ScienceDirect https://www.sciencedirect.com/science/article/pii/S016740482100211X

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

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