Module 8 Part 1

Component of a risk mitigation strategy and the challenges of implementation

Table of contents

1. Introduction

As organizations become more dependent on information technology, the risks related to these technologies increase. Module 1 emphasized the importance of accounting for cyber risk in an organization's overall risk strategy, and the modules that followed contributed to the most important aspects that need to be covered. These have included identifying the organization's most critical assets, potential threats, methods of attack, and protective technologies. They have also addressed considerations around effective leadership and governance structures, legal compliance, and preparing an incident response strategy.

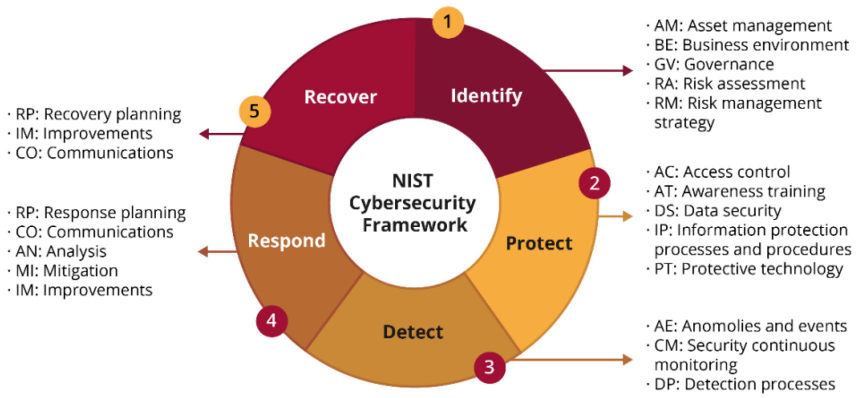
This set of notes provides input on integrating all the aspects addressed in the course thus far into a cyber risk mitigation strategy that guides an organization's overall approach to business operational, legal, and reputational risk. A risk mitigation strategy encourages an organization to prioritize its risks, so that it only devotes resources to significant threats. It also allows an organization to define action plans and to assign responsibility for the implementation of those plans to specific individuals. Creating a risk mitigation strategy that includes clear goals, objectives, and milestones, as well as metrics to measure whether goals have been met, will ensure that cybersecurity remains a top priority. These notes focus on the elements that should ideally be included in a risk mitigation strategy, the challenges that may arise during the implementation of the strategy, and the metrics that can be used to measure the successful implementation of the strategy.

2. Developing the cyber risk mitigation strategy

The structure and contents of each organization's risk management strategy will differ depending on the size and nature of the organization. The following process to develop the strategy, and the elements included, can be used as a guideline.

2.1 Identify the risks the organization is exposed to

Most organizations are exposed to some form of cyber risk. The NIST Cybersecurity Framework was developed to guide private-sector organizations in assessing their capacity to effectively mitigate these risks. The NIST framework, which was covered in Module 1, is depicted in Figure 1.



An organization can use tools, such as a self-assessment checklist, to identify the areas within the framework where it is at risk. To complete a risk assessment accurately, management must be familiar with the organization's risk environment. The following aspects of the risk environment were analyzed as part of the ongoing project completed in this course:

- Cyberthreats an organization is exposed to, and possible threat actors
- An organization's critical systems, networks, and data that are at risk of being attacked
- An organization's corporate governance structure
- Technologies used to protect an organization's systems, networks, and data
- Legal aspects relating to the cyber landscape an organization operates in
- An organization's ability to prepare for, respond to, and recover from a cyberattack

The risks an organization is exposed to and the actions that should be taken to mitigate these risks cannot be identified accurately unless an organization has gathered information and completed an analysis of the risk environment it operates in. It is, therefore, a critical part of developing a risk mitigation strategy.

2.2 Communicate the need for the strategy

One of the biggest challenges in creating a cyber risk mitigation strategy is communicating its importance to an organization's leadership, and ensuring organizational buy-in. In this regard, the introduction to the strategy should set out to convey a high-level overview of the organization's need for a risk mitigation strategy. It should provide enough context so that anyone reading the strategy will have a basic understanding of the purpose it aims to achieve.

2.3 Create a vision for the strategy

The vision should set out what the organization wants to achieve with the implementation of the risk mitigation strategy. It could also refer to how the vision of the strategy links to the mission and vision of the organization. The vision should be short and easy to understand and communicate. It should motivate the stakeholders involved, and should be a view shared by everyone involved in implementing the strategy.

2.4 Set strategic goals

Once the organization has identified its risks, it must identify its strategic goals. Strategic goals are the key goals the organization must achieve to reduce its risks to an acceptable level. These are high-level descriptions of the actions that the organization will take to address the risks it is exposed to. These goals will close the gap between the current state the organization finds itself in, and its desired state. Once these goals have been achieved, the organization will be in a better position to defend itself against and react to cyber threats successfully. An example of a strategic goal could be, for example, to create a culture of cybersecurity awareness in the organization.

After the strategic goals have been identified, they must be prioritized, as the organization will likely not have the time and resources available to achieve all goals. The aim is to identify the goals that are nonnegotiable and that must be achieved for the organization to remain resilient in the face of an attack.

2.5 Set objectives

Once the most important strategic goals have been identified, objectives should be set for each goal. The objectives are the specific items that must be accomplished to achieve the overarching strategic goals. For example, if one of the strategic goals of an organization is to protect its systems using technology, an objective could be to implement an intrusion detection tool.

2.6 Create action plans and set milestones

Each objective can then be developed into an action plan, with a specific person allocated responsibility for each task. The action plan should include milestones that state when certain actions should be accomplished. Referring to the example used before, milestones for the implementation of an intrusion detection tool could include the acquisition date, installation date, testing date, and date on which it will be fully operational.

Figure 2 shows the relationship between the vision, strategic goals, and objectives included in
a risk mitigation strategy. The vision sets the scene for the strategy, while the strategic goals
are the high-level aspects the organization will focus on. The objectives provide more detailed information about the steps that will be taken to achieve the strategic goals, while the action plans allocate time and resources toward the achievement of the objectives. By including these elements, the organization moves from planning what to do to mitigate its risks, to executing practical plans to address the risks.

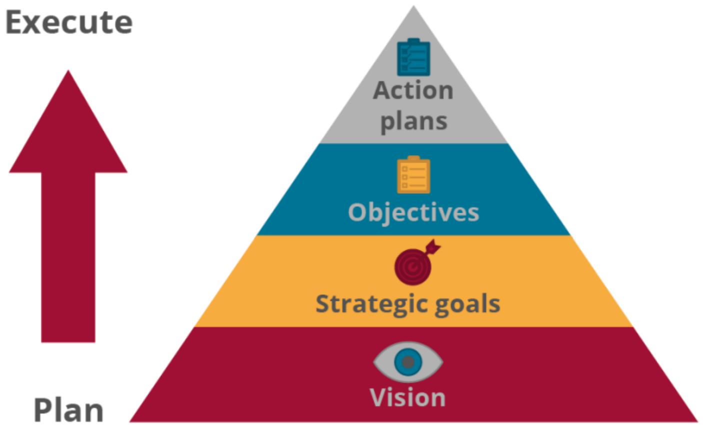


Figure 2: The relationship between the vision, strategic goals, and objectives.

2.7 Use metrics to measure progress

Metrics are used to measure whether goals and objectives have been achieved successfully. It provides management with the information necessary to make decisions, and aids in holding stakeholders accountable. Metrics can range from impact measures (such as return on investment), to effectiveness and efficiency measures (such as the number of system-level controls that are implemented according to the cybersecurity policy). It is important that the metrics used by the organization are specific to the nature of its goals and objectives.

For example, if the objective is for all staff members in the organization to partake in cybersecurity awareness training during a specific period, the metric could be the number of staff members who successfully completed the training at the end of the period. If the objective is to have strong passwords on all computers to prevent unauthorized access, the metric could be the number of weak passwords identified during an audit.

Refer to the notes in Module 4 Unit 2, where the use of metrics was identified as part of a good governance plan.
Selecting the best metrics to measure the achievements of goals and objectives can be difficult, as it might become quite technical. Engage in the class-wide discussion forum in this unit to discuss the metrics you would use to measure the achievement of your organization's cybersecurity goals.

2.8 Make improvements

Management should regularly check on the progress made on the achievement of objectives, as there is no purpose in compiling a strategy if it is not implemented. Mechanisms should be in place to improve metrics that are not being met. This might require updates to the action plans, or the allocation of more resources to meet the objectives. Regular feedback should be given to relevant stakeholders on the progress made. Lastly, the risk mitigation strategy should be reviewed and updated on a regular basis to ensure that it remains current and relevant to the organization's operations.

3. Challenges when implementing a risk mitigation strategy

Depending on the requirements of an organization's cyber risk mitigation strategy, leaders may face several pitfalls during implementation. Management should be aware of the challenges associated with implementation, including the following:

- **Compliance:** Ensure that the strategy complies with the legal and regulatory requirements of the country in which the organization operates. Most of these measures should proactively account for cyber risk in the strategy itself. It's important to keep in mind, however, that laws and regulations change, particularly as the cyber risk landscape evolves. The strategy should change accordingly, if necessary.

- **Collaboration:** Collaboration between different departments within an organization is often required when implementing a cyber risk mitigation strategy. Roles and responsibilities must be allocated to each task, and a common methodology should be established. The completion of tasks across departments should be tracked, especially if one department's tasks are dependent on the completion of another department's tasks. The interdepartmental nature of a cyber risk mitigation strategy might also result in tension between the different managers when it comes to the allocation of resources and the timeframes allocated to tasks. Keep in mind the leadership and governance structures dealt with in Module 4, which provides principles on ensuring the holistic integration of a cyber risk culture.

- **Allocating financial resources:** It might be difficult to obtain the necessary financial resources to implement the plan successfully, as there are usually competing needs within an organization. Refer to the notes in Module 4 Unit 2, where budget requirements were discussed in more detail.

- **Allocating human resources:** The implementation of some of the goals included in the strategy might require skills and expertise that the organization does not have. This will require the recruitment of additional human resources, which will have operational and financial implications.

- **Appropriate metrics:** There might be differences in opinion as to which metrics should be used to measure the successful implementation of the plan.

- **Adaptability:** The cyber landscape is constantly changing, and new threats regularly arise. Therefore, the risk mitigation strategy should be agile and reviewed on a regular basis, as some of the strategic goals might have to be updated/

Due to the complexities involved in the implementation of a cyber risk mitigation strategy, an organization should appoint a leader who is responsible for the development and implementation of the strategy. This person should have the necessary skills and expertise to address the challenges that arise, and should have the authority to ensure that the strategy becomes a practical reality instead of just a paper exercise.

4. Conclusion

Various aspects that should be taken into consideration when it comes to cybersecurity have been discussed in this course. A cyber risk mitigation strategy is the culmination of all these aspects, as it focuses management's attention on the areas in their organization that need improvement. The strategy document not only serves as a guideline for all stakeholders, but also provides management with the means to measure the progress made in preparing the organization for a cyberattack. Without this document, an organization will have trouble allocating time, money, and effort to the actions that will have the greatest impact on the organization's ability to remain resilient in the ever-changing cyber landscape.

.