Chapter 12: Organizational Management Tasks Applied at Competitions

12.1 Background of Organization Management Tasks

This section discusses, in detail, concepts related to organizational management which are commonly needed at cyber defense competitions.

12.1.1 Creating a Comprehensive Information Classification Program

Organizations today deal with so much data. Often, it can be difficult to determine what data is important, what data is not important, and what data is considered sensitive. To ensure that sensitive data is not released to unauthorized individuals, creating a comprehensive information classification program can be helpful. Andrew McCreath notes the following in a Computer Weekly article [80]:

> *"Data classification best practices enable organisations to store their data in line with compliance controls, thereby reducing any risk to the business in the event of an audit or legal discovery."*

The legal issue is just one of many reasons to implement a data classification program. Additionally, data classification can be useful in ensuring that the concept of least privilege is achieved, that is, that only individuals with a need to know have access to designated information. A comedic, yet relevant example of this exists in the children's television show, "SpongeBob SquarePants" [81]. In the show, the owner of a restaurant has a secret formula for creating their signature item, the *Krabby Patty*. Throughout the series, various individuals attempt to gain access to the formula, though the owner ensures that information is protected. Even his own employees don't know the secret formula because they do not need to in order to perform their function. Similarly, organizations should ensure that privileged information is limited to only those individuals who require access.

This further begs the following two questions:

- What levels of information classification should an organization have?

- How does an organization determine what access level an individual should have to information?

The answer to the first question is very subjective. Every organization will handle information differently, and different types of information. Depending on the type of information, different classification levels will be needed. For example, in healthcare organizations, protected health information (PHI) are present whereas at a automobile production company, engine design details exist. This leads one to need to go through a full process to determine how to set up an appropriate information classification program. Generically, there are three high level categories of classification according to an article in Strong DM relating to SOC 2 Compliance [79]. Author Brian Johnson presents these three high level categories in descending order of sensitivity. These levels are Confidential, Internal, and Public. Public data is information with no protection. This data is available openly to the public and may include items such as what products the company is producing. Internal data is protected within the organization. These data should not be discussed publicly but may freely be discussed internally. These data may include employee salaries. Lastly, confidential data is confined to select individuals with a strict need to know. These information may include employee and client information including social security numbers.

In a Sirius Edge article, authors Thomas Eck and Anne Grahn outline seven steps to creating an effective information classification program [78]. These steps are as follows:

1. **Complete a Risk Assessment**: Determine what regulatory and contractual requirements the organization has related to data confidentiality.

2. **Develop a Formal Classification Policy**: Determine the categories of data classification. Limit to three to five categories to avoid unnecessary confusion over high level of granularity.

3. **Categorize Data Types**: Determine what protected data the organization manages. This means identifying what data the organization maintains, creates, or handles. Knowing the data and assets allows the organization to determine classification levels.

4. **Discover Location of Data**: Now that the types of data have been identified, the organization needs to identify where the data are located. This may be physical location of data (storage room in the room 104 of the east wing) or digital (credit cards folder on the private share).

5. **Identify and Classify Data**: Formally classify the data. Make it known to the organization that a policy is in place and must be followed.

6. **Enable Security Controls**: Implement the program. This may require limiting access to data digitally using group policy type software or physically by granting access to specific areas. Additionally, the organization can implement encryption for digital data as well as air gaps for physical data.

7. **Monitor and Maintain**: Having implemented the program, it is critical that the program is maintained. Regularly monitor both digital and physical accesses to high sensitivity documents and ensure that the access was from an authorized individual. Be sure to regularly reevaluate the classification level of data as well as the level of access an individual within the organization has.

Following the seven step process, an organization should be able to implement a fairly comprehensive information classification program.

12.1.2 Selecting the Appropriate Organizational Structure

An effective organization requires an appropriate organizational structure. Organizational structures refer to the configuration of relationships between positions and teams within an organization. According to articles from Smart Draw and Point Park University, four common organizational structures include [90, 89]:

- Functional Top-Down
- Divisional
- Matrix

- Flat

The functional top-down structure is hierarchical and very much based on chain of authority. In this structure executives rest at the top of the structures, with senior management below, followed by junior management, team leads, etc. This organizational structure excels in it's ability to group similarly skilled individuals in teams which allow a focused approach to problems. However, this structure leads to a lack of communication between groups and poor transparency up the structure.

The divisional structure has the organization split into various divisions which operate as sub organizations in some sense. In this structure, the individual divisions have a high level of independence and may not require higher level authority to make decisions. However, in this structure, individuals working in similar capacities in different divisions may have little collaboration.

The matrix structure has its teams split based on projects or products. Individuals may work as part of a project with a project lead, but will typically also have a function manager they report to. This structure excels in its ability to facilitate communication and provide a dynamically shifting work environment. This structure struggles in coordination at times. Individuals may belong to multiple projects and thereby report to separate project leads, between whom their may be little communication.

The flat structure has very little to no hierarchy. All individuals report equally to a single authority. This structure enables a very individually managed team where individuals work independent of others and provide autonomy for each employee. This structure does struggle in that by providing each employee autonomy, there can be disagreements on how to proceed with a task without intervention of the single higher authority.

Which organizational structure should be implemented is entirely dependent upon the needs of the organization, what type of products/services it offers, and the size of the organization, among other things.

12.1.3 Choosing an Effective Team

An organization is only as successful as its staff. Ensuring that an effective team of staff members has been chosen can be the difference between a successful organization and failed organization. Articles from BrightWork [92] and AboutLeaders [91] outline tips for selecting an effective team. They suggest hiring individuals who are able to communicate effectively. Individuals who can listen to others in a meaningful manner but also respond eloquently are invaluable. These individuals can help facilitate cooperation internally but also interact with sponsors and prospective clients.

Additionally, skilled project managers should be hired. The organization will need an individual(s) who possess strong leadership skills and can manage small to large teams to lighten the burden on any single individual within the organization.

Another suggestion is to remain strictly objective in the hiring process. It can be tempting to hire an individual who is family friends with a project lead, but if a better candidate applies for the role, ensure that the best candidate is hired.

It is important to be mindful of the budget your organization has as well as what needs it has. Select the team accordingly to ensure the most effective team.