****

**NORTHCENTRAL UNIVERSITY**

**ASSIGNMENT COVER SHEET**

# Student: Joshua Campbell

|  |  |
| --- | --- |
|  |  |
| **TIM-6302** | **Unknown** |
|  |  |
| **Changing Times: Trends & Topics in Cybersecurity** | **3 Protecting Employees and Identifying Dangers** |
|  |  |

**I have not comments to add, but if I did, this where they should go.**

**Faculty Use Only**

<Faculty comments here>

Protecting Employees and Identifying Dangers

Joshua Campbell

NorthCentral University

Protecting Employees and Identifying Dangers

The Cybersecurity Framework is a tool for guidance in the approach to improve IT Infrastructure cybersecurity risk by assisting with the understanding, communicating, and acting on cybersecurity risks in an IT infrastructure environment. The framework core consists of 5 activities “Identify, Protect, Detect, Respond, and Recover” (Framework for Improving Critical Infrastructure Cybersecurity). The components of One aspect of the framework provides multiple steps to approach and identify different aspects to be considered when attempting to improve cybersecurity risk. The “identification” portion of this framework is critical to all additional aspects of the framework, by “identifying cybersecurity risk to systems, assets, data, and capabilities” (Framework for Improving Critical Infrastructure Cybersecurity).

The uses for the information derived from the identification process will be used to assist in understanding business context of Cybersecurity risk in the environment. This portion is to identify systems and resources that are critical to the operation of the business as well as being compliant with any requirements of the specific line of business. Some outputs of this process can be categorized as;

* Asset Management
* Business Environment
* Governance
* Risk Assessment
* Risk Management

These are example categorizations, but an environment could include more, combine or separate differing groupings. These are a good start and can typically be used as a guide for an approach in the identification process.

The asset management aspect is the process of identifying systems and resources that are critical in the support of the line of business and maintaining cybersecurity in all areas required. The successful outcome of the “identify” portion of the framework would assist in;

* Define the current state of their enterprise
* Define mitigation priorities
* Define processes that are reliable and reproducible
* Meet the needs of all stakeholders
* Make managing complex systems easier
* Have methods for communicating with all critical parties

These are some examples, but additional information can and should be defined as needed by environments, but the above are a good baseline for this process (Framework for Improving Critical Infrastructure Cybersecurity, Symantec).

In the definition of the current state of an enterprise, it is important to formally identify all systems, resources, interconnected and dependent systems. Additionally, this is the phase that gaps are identified and critical paths are defined to address resolution. This phase is often presented at the beginning of the identification process and again at the end. This allow additional requirements or dependencies to be defined and then re-associated with assets discovered. The assets are then again reclassified based of the interdependency list.

During the mitigation phase, known security risks should be identified and potential methods for resolving, mitigating, or removing the risk should be identified. This would be a phase that each asset, service, and resource would be defined and the estimated risk vs value would be identified and a cost would then be associated with the potential risk. Then an evaluation based on potential loss and the cost to remediate or mitigate the risk would be compared.

In identifying and defining the processes phase, the processes that will assist in ensuring due diligence, prove to be reliable, and are easily reproducible will be evaluated and defined. These processes are typically considered due diligence (Conrad), but are often required by other requirements that are identified by either a company’s data governance philosophy or any industry standards that apply to the line of business. Examples of these processes are;

* User in processing and out processing
* Change management and disaster recovery
* Security event and incident response handling
* System baselines for servers and clients
* Internal/external access
* Defining and handling data classification

These are just a few examples of potential of processes that could apply to an organization, but should provide a good set of examples for the types of outputs of this phase.

Identifying and evaluating the needs of stakeholders. In this phase, it is to ensure that currently identified policies and procedures account for the requirements put forth by all stake holders. In this phase, all policies would be reviewed and reflected on by all stake holders and shortcomings in requirements would be identified and resolved.

There are many principles and IT methodologies in use in the industry today that define logical reasons to maintain simplicity in an environment. One such principle defines this pretty well, in the KISS principle (KISS) In the phase of identifying complex systems and easing the complexity, there are several reasons for this activity. In the realm of cybersecurity, it is important to ensure transparency so that ensuring security is less ambiguous and easier to understand and mitigate.

Disseminating pertinent information to stakeholders and additional resources is another integral part of identification in the framework. It is when formal methods for communicating incident, outages, and potential risks are communicated to affected parties and system stakeholders. This identification and definition is typically added to an incident response policy that was defined previously in the process.

All previously mentioned aspects of the identification process can and usually are changed to suite the business and are sometimes combined and segregated into different components all together, but this has been a brief overview and generalization of the identification phase of the Cybersecurity Framework.

References

# Conrad, E., Misenar, S., & Feldman, J. (2017). Eleventh hour CISSP: Study guide (3rd ed.). Snyngress Publishing. 9780128112489

# Framework for Improving Critical Infrastructure Cybersecurity. www.symantec.com. Retrieved 19:45, Dec 4, 2018, from

# <https://www.symantec.com/connect/blogs/breaking-down-identify-function-nist-cybersecurity-framework>

# Framework for Improving Critical Infrastructure Cybersecurity. www.nist.gov. Retrieved 19:45, November 14, 2017, from

# <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

What does KISS stand for. *people.apache.org.* Retrieved 19:50, February 4, 2018, from

<https://people.apache.org/~fhanik/kiss.html>