McGill | School of Continuing Studies

Using the NIST Cyber Security Framework:

The Respond Function

Celia Fuentes

CCCS 453 – Security Risk Management and Governance

Introduction

The following is a revised version of an assignment I did for the Security Risk Management and Governance course in the Certificate in Applied Cybersecurity at McGill's School of Continuing Studies. The purpose is to apply the NIST Cybersecurity Framework (CSF), specifically the Respond function, to a given scenario. This document has been updated to map to the NIST Cybersecurity Framework (CSF) 2.0[1] released in February 2024.

In the provided scenario, there was a recent incident at a financial institution and the following issues were identified:

- There was confusion as to who should be contacted at the cybersecurity service provider
- The were problems obtaining and analyzing the data from the in-house detection system at the financial institution

Despite a shaky initial response, the financial institution identified, analyzed and mitigated the incident, and eventually fully recovered. During the post-mortem, the CEO requested three concise recommendations to improve the institution's Respond Function, that is "Actions regarding a detected cybersecurity incident are taken."[2] The recommendations made must refer to a specific category or subcategory of the framework.

[1] "The NIST Cybersecurity Framework (CSF) 2.0." NIST (National Institute of Standards and Technology), February 24, 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] *Ibid*, p. 22

Recommendation #1: Clear categorization of incidents

Category: RS.MA

Incident Management: Responses to detected cybersecurity incidents are managed

Subcategory:

RS.MA-03: Incidents are categorized and prioritized

Explanation: Incidents must be clearly categorized before internal and external resources can be designated. Prioritization ensures the proper response is quickly enacted while considering the incident's severity. This would have avoided the initial confusion during the incident at the financial institution.

Recommendation #2: Clarify relevant internal and external stakeholders

Category: RS.CO

Incident Response Reporting and Communication: Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies

Subcategory:

RS.CO-2: Internal and external stakeholders are notified of incidents

Explanation: The confusion as to who to contact at the service provider suggests the processes are unclear on the resource person or department to contact. It is recommended that designated internal/external stakeholders be clearly defined so that both the financial institution and the service provider can quickly coordinate further response activities.

Recommendation #3: Investigate and rectify detection system difficulties

Category: RS.AN

Incident Analysis: Investigations are conducted to ensure effective response and support forensics and recovery activities

Subcategory

RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident

Explanation: Determine whether the difficulties with the data from the detection systems were due to the incident, misconfigurations, or lack of personnel training/expertise. If multiple reasons are identified, put them in order of priority accompanied by proposed solutions with their associated cost to present to decision makers.