Drury University's NCSR Cyber Security Review

Table of Contents

5 NIST Sections Overview

Identify Sub Sections Averages

Protect Sub Sections Averages

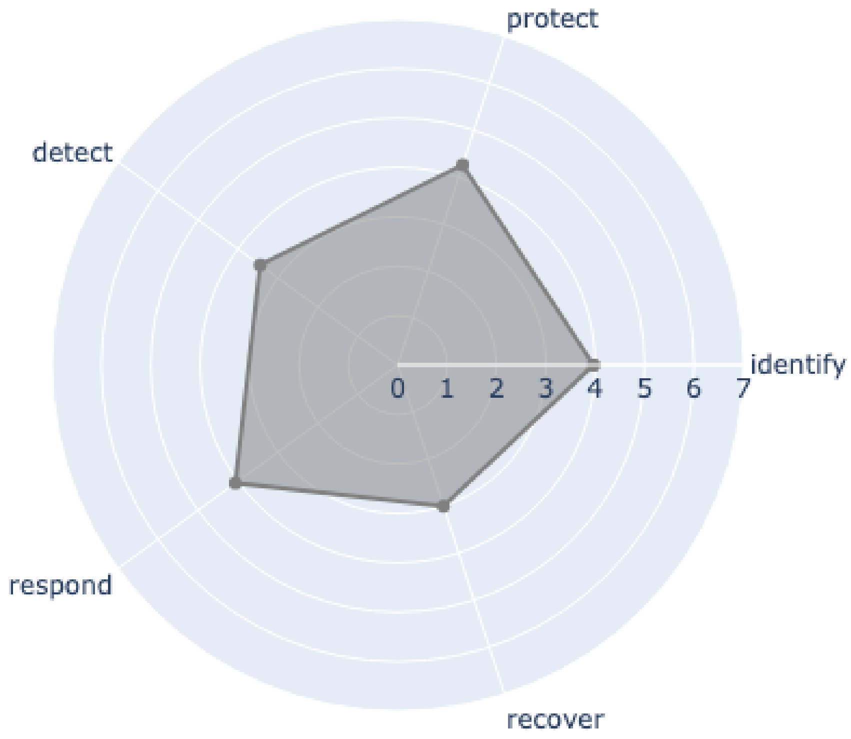
Detect Sub Sections Averages

Respond Sub Sections Averages

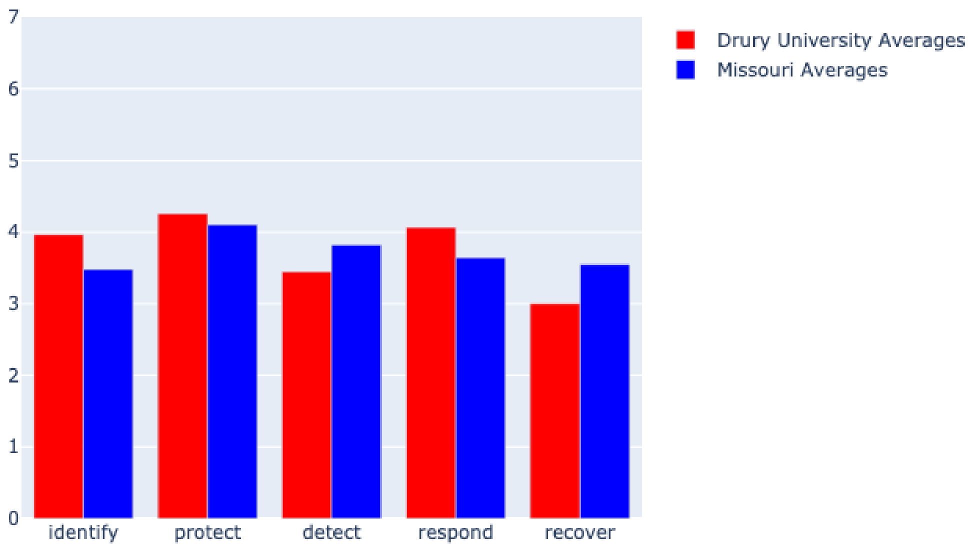
Recover Sub Sections Averages

Part 2 Overview

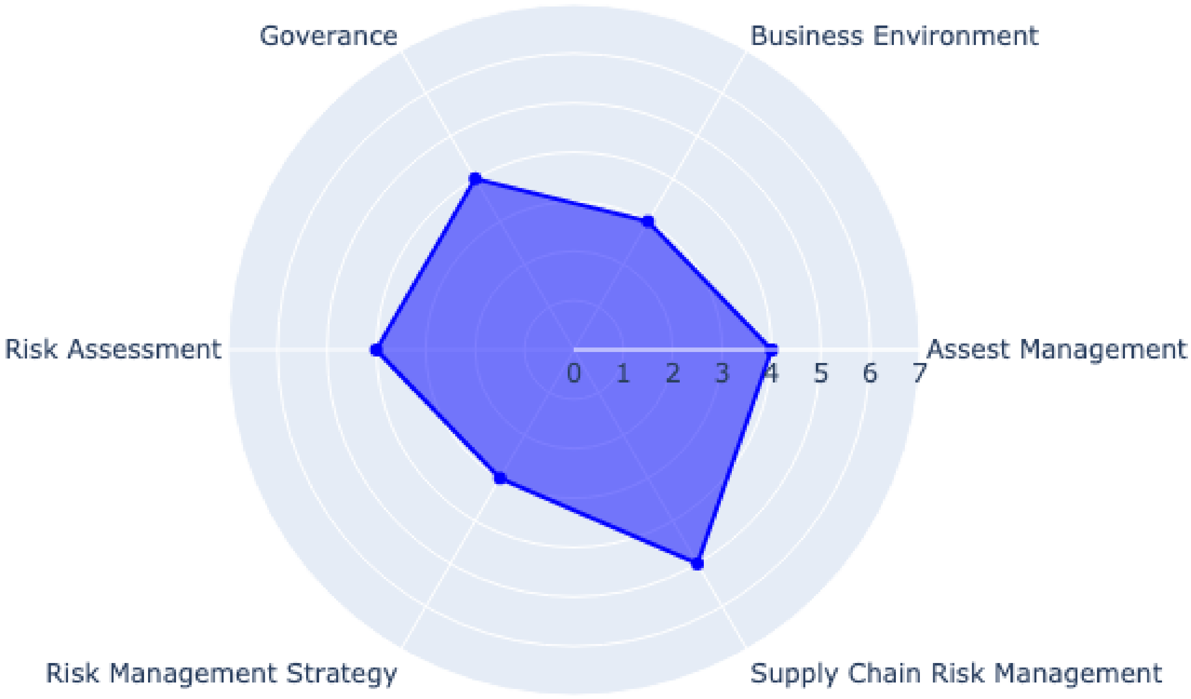
Section Average



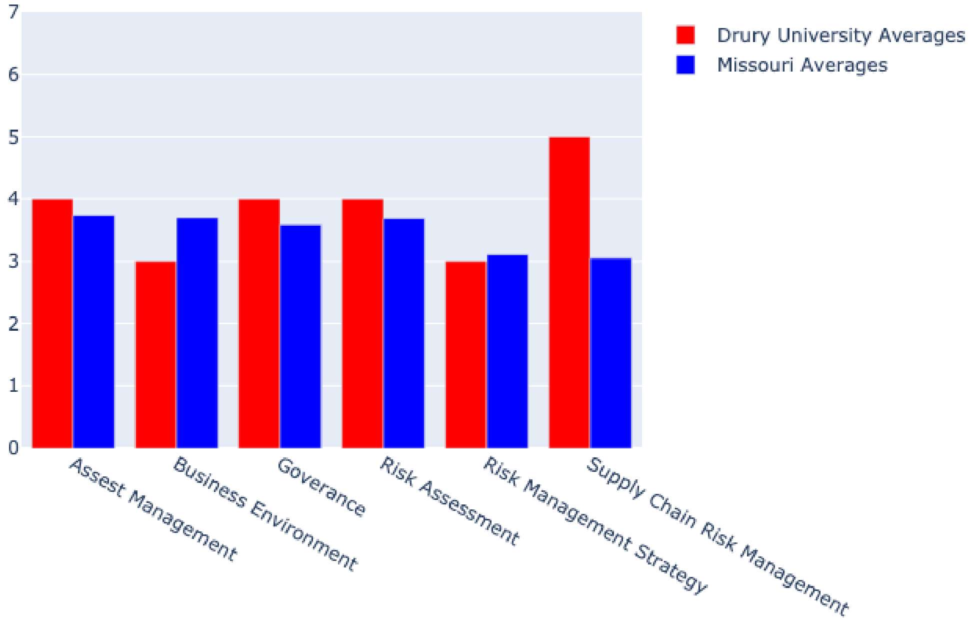
The graph above is the average of the all the sections within the NIST question set. The sections are scored 1 through 7. The numbers represent a maturity level in that particular section. 1 - Not Performed, 2 - Informally Performed, 3 - Documented, 4 - Partially Documented Strandards and/or Procedures, 5- Risk Formally Accepted/Implementation in Process, 6 - Tested and Vertifed, 7- Optimized. Throughout the rest of this readout will be a averages of each of the individual parts of the question set. Below is a graph with averages of the state of Missouri in the same sections compared to Drury University.



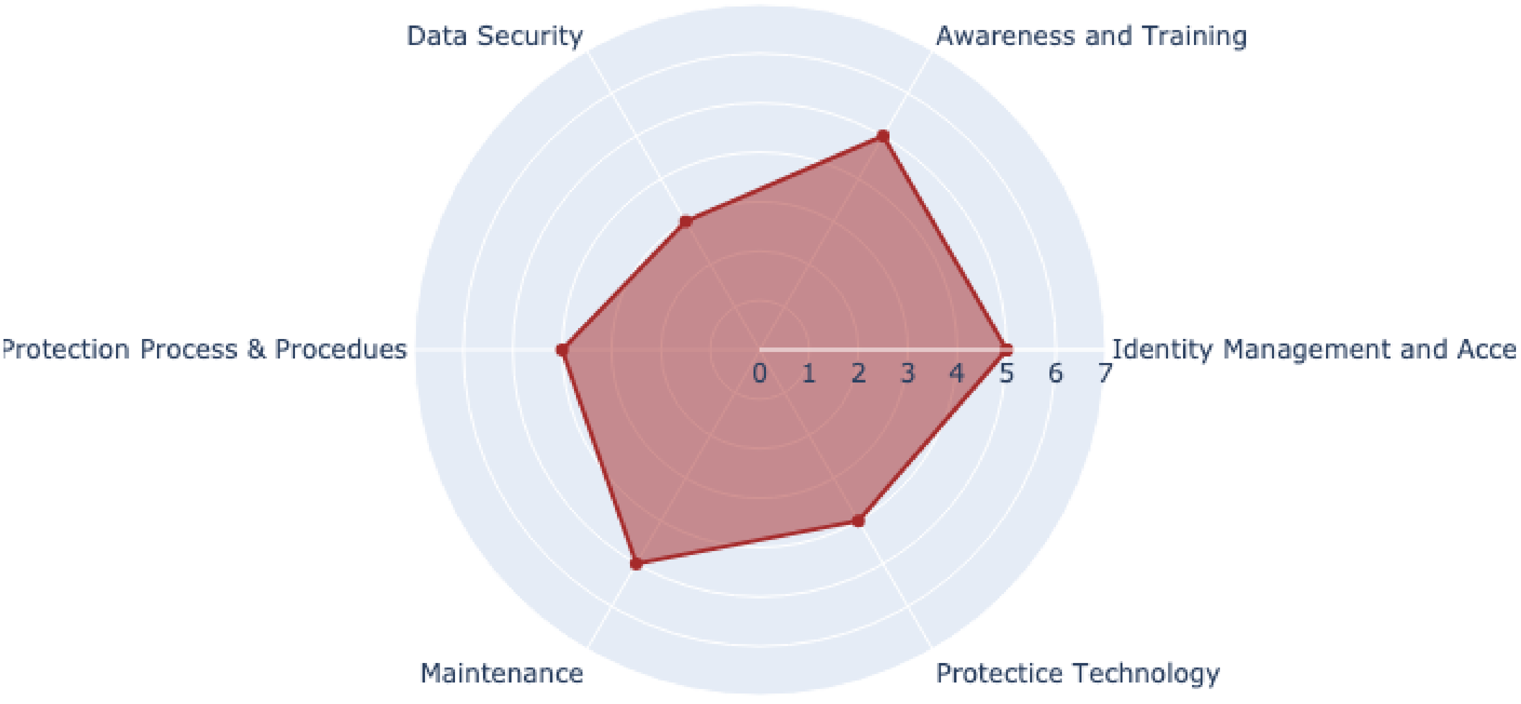
Identify Sub Sections Averages



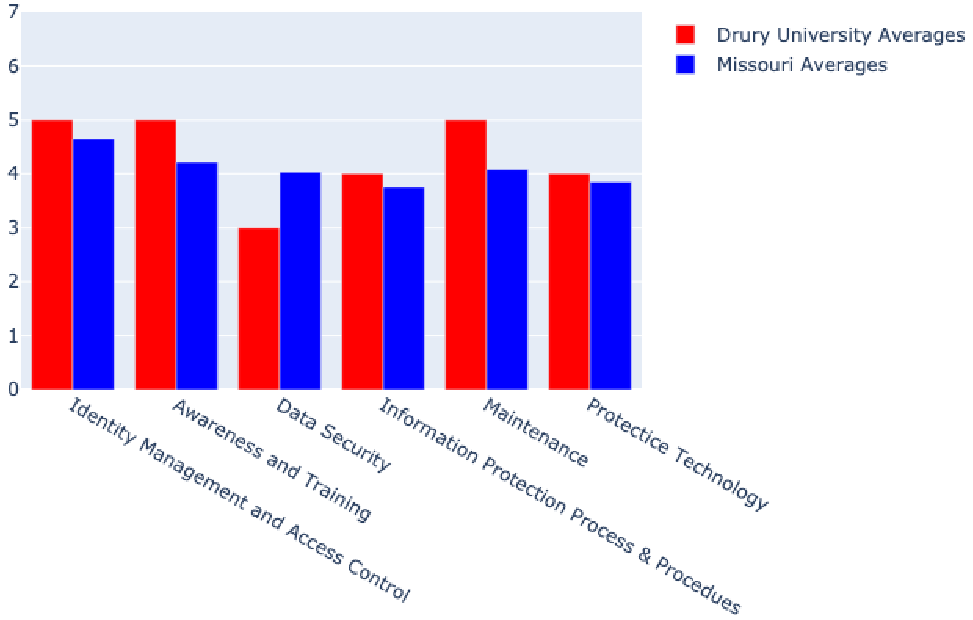
The activities under this functional area are key for an organizations understanding of their current internal culture, infrastructure, and risk tolerance. This functional area tends to be one of the lowest-rated functions for many organizations. Immature capabilities in the Identify function may hinder an organizations ability to effectively apply risk management principles for cybersecurity. By incorporating sound risk management principles into cybersecurity programs, organizations will be able to continuously align their efforts towards protecting their most valuable assets against the most relevant risks.



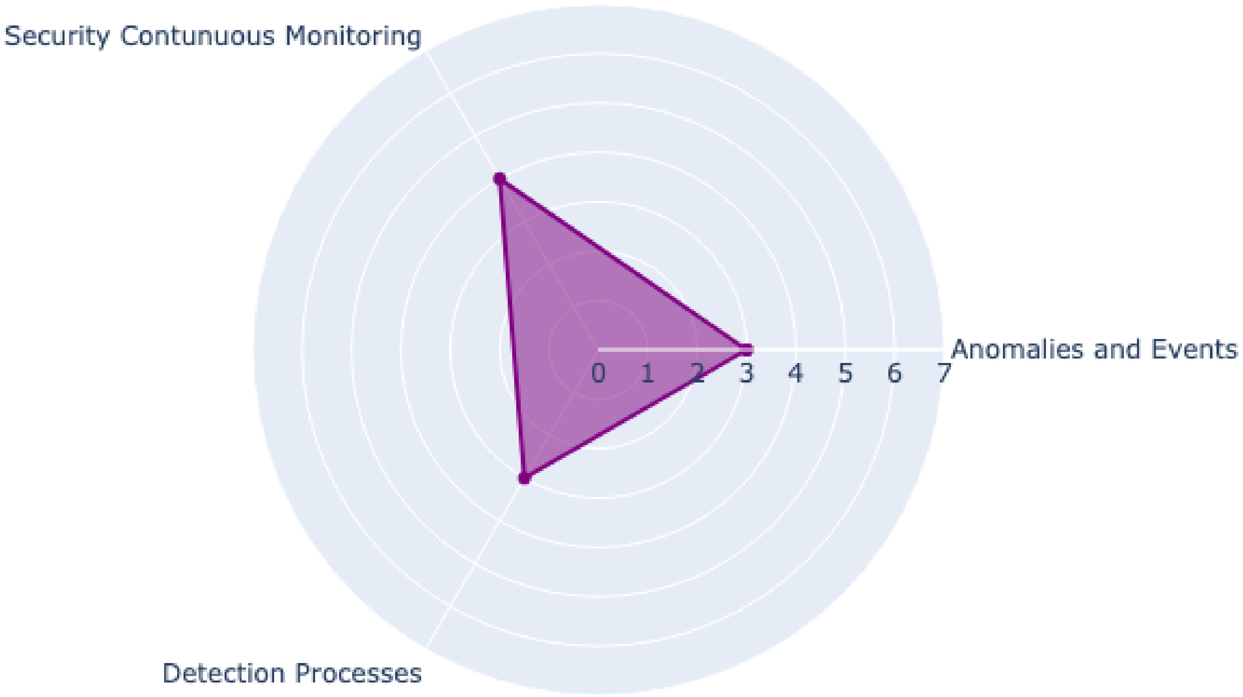
Protect Sub Sections Averages



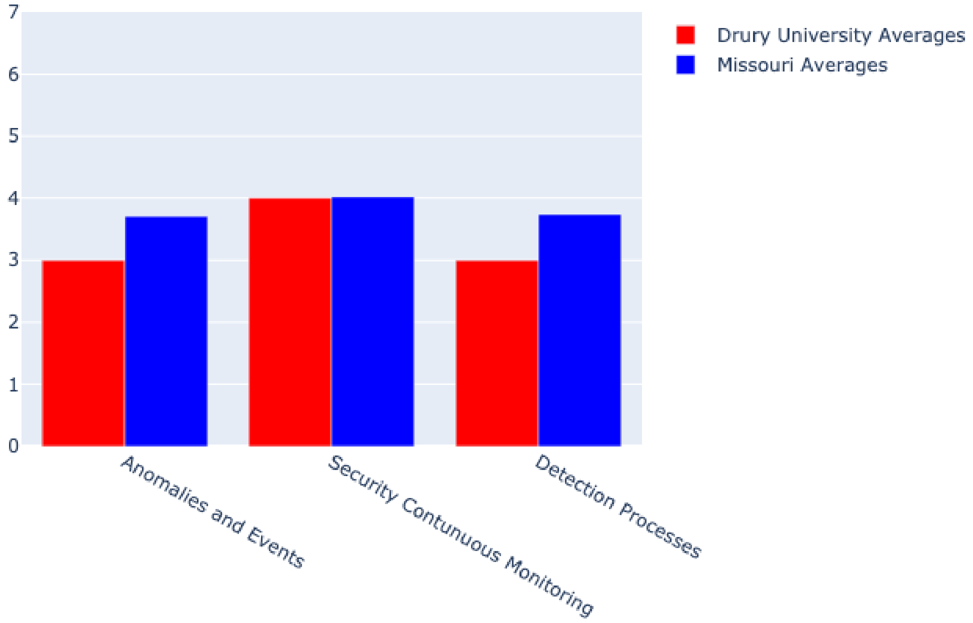
The activities under the Protect function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services. These controls are focused on preventing cybersecurity events from occurring through common attack vectors, including attacks targeting users and attacks leveraging inherent weakness in applications and network communication.



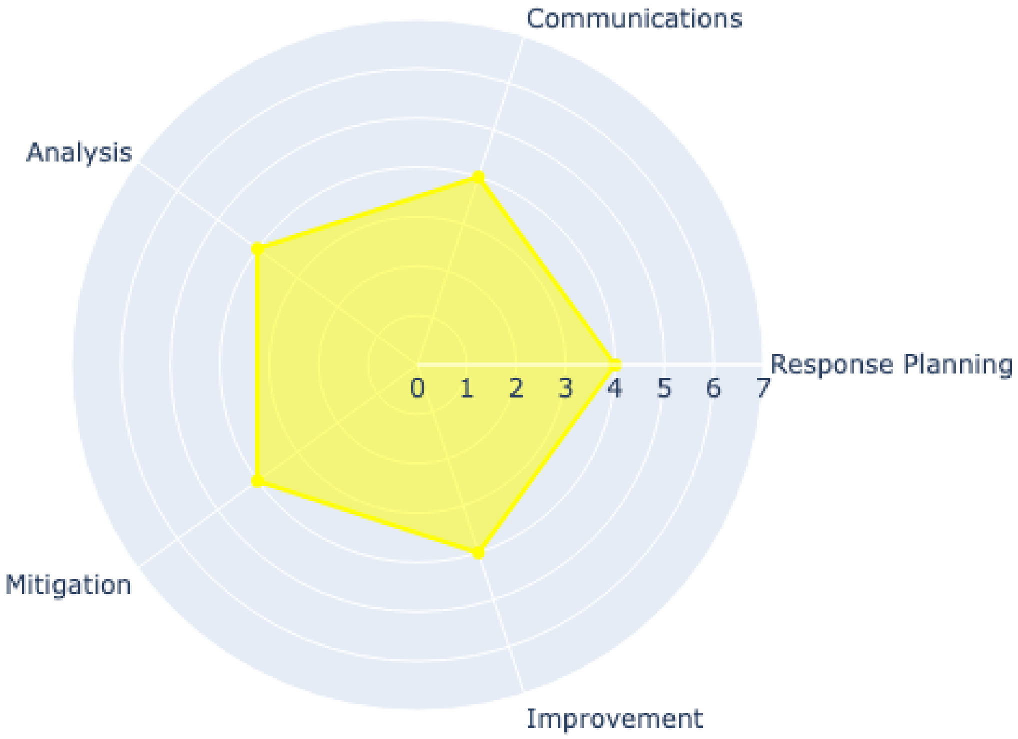
Detect Sub Sections Averages



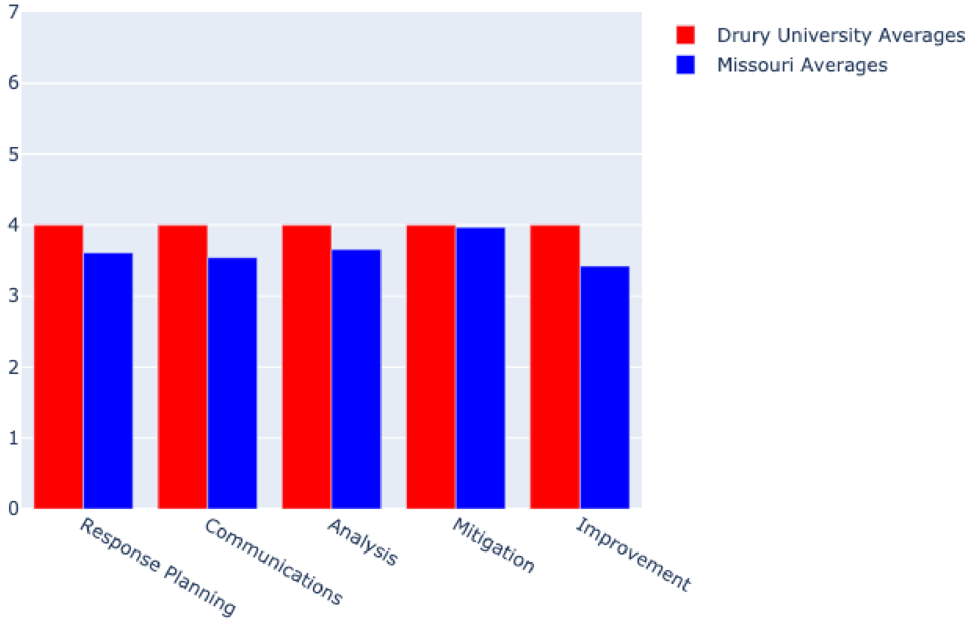
The quicker an organization can detect a cybersecurity incident, the better positioned it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the Detect function pertain to an organizations ability to identify incidents. These controls are becoming more important, as growing numbers of logs and events within an environment can be overwhelming to handle and make it difficult to identify key concerns.



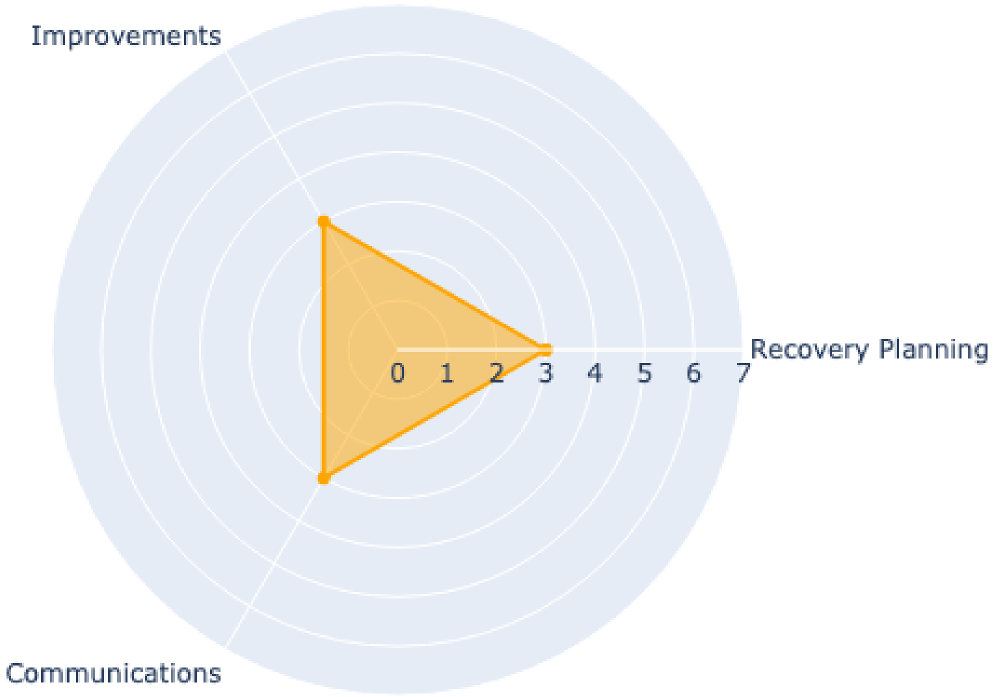
Respond Sub Sections Averages



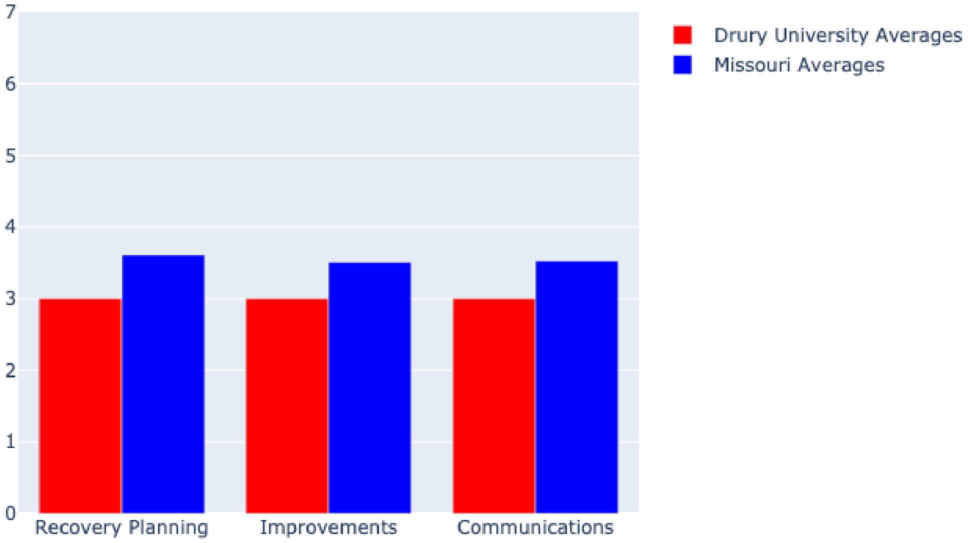
An organizations ability to quickly and appropriately respond to an incident plays a large role in reducing the incidents consequences. As such, the activities within the Respond function examine how an organization plans, analyzes, communicates, mitigates, and improves its response capabilities. For many organizations, integration and cooperation with other entities is key. Many organizations do not have the internal resources to handle all components of incident response. One example is the ability to conduct forensics after an incident, which helps organizations to identify and remediate the original attack vector. This gap can be addressed through resource-sharing within the SLTT community and leveraging organizations such as MS-ISAC and CISA, which have dedicated resources to provide incident response at no cost to the victim.



Recover Sub Sections Averages



Activities within the Recover function pertain to an organizations ability to return to its baseline after an incident has occurred. Such controls are focused not only on activities to recover from the incident, but also on many of the components dedicated to managing response plans throughout their lifecycle.


Recovery Planning
Improvements
Communications
Drury University Averages
Missouri Averages