Cybersecurity Measurement Science

Executive Summary

Cybersecurity departments across the United States all face a common problem: they spend loads of money and resources on implementing strong security controls with no standard way to measure the effectiveness of those controls. There are numerous frameworks that exist, including the Cybersecurity Framework from NIST. However, these frameworks typically are limited to identifying which controls to apply and do not include how to measure the effectiveness of the implemented controls. As a result, there is a great need for a standard set of metrics which can measure the effectiveness of security controls that have been implemented in a given environment/domain.

The goal of this project is:

1) Determine if it is possible to use the Cybersecurity Framework from NIST (NIST-CSF) as a tool to determine the controls that should be in place for a various security tools within the reference frame.
2) Determine a rating/metric scale to measure the effectiveness of the controls.
3) Determine how effectively the rating/metric scale can be applied to the test organization.

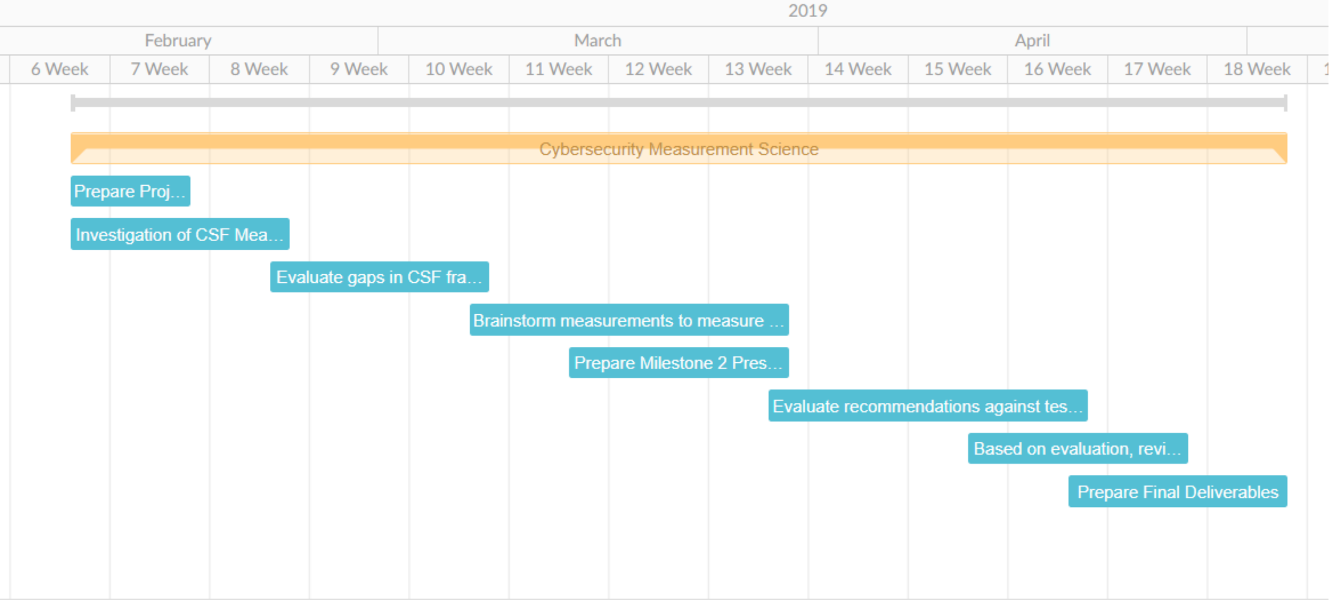
If this project is successful, the metrics will be able to provide a report card of a security environment or domain. The end goal would be used in an overall report card of a security program effectiveness if all tools could be evaluated with the same standards.

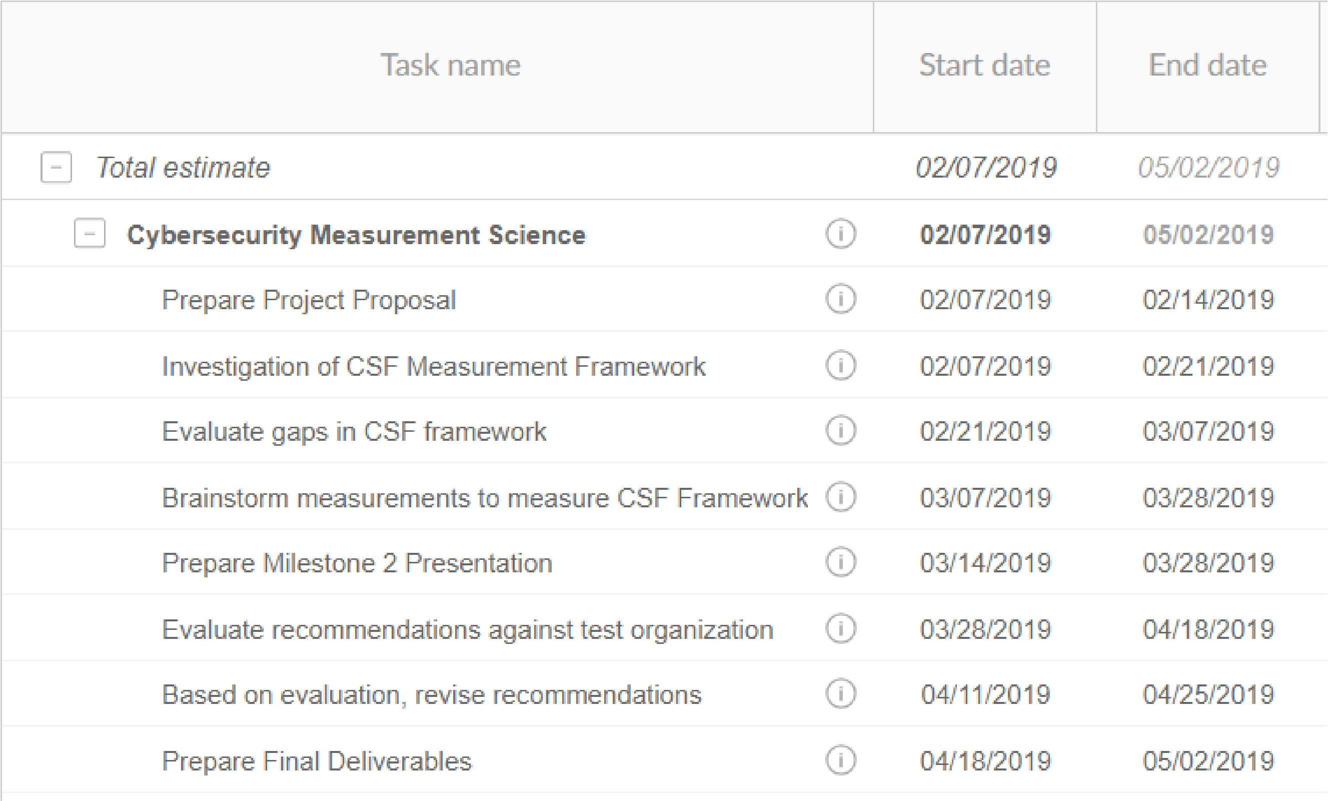
Team members that will be executing this project are:

1. Lisa Bazis
2. Sarah Noles
3. Collin Daily
4. Lyle Reinholz
5. Sanjar Hamidi

Project Timeline

The proposed timeline for this project is shown below. Additionally, a more detailed view with estimated start and end dates is provided.





Task name	Start date	End date
⊟ *Total estimate*	*02/07/2019*	*05/02/2019*
⊟ **Cybersecurity Measurement Science**	**02/07/2019**	**05/02/2019**
Prepare Project Proposal	02/07/2019	02/14/2019
Investigation of CSF Measurement Framework	02/07/2019	02/21/2019
Evaluate gaps in CSF framework	02/21/2019	03/07/2019
Brainstorm measurements to measure CSF Framework	03/07/2019	03/28/2019
Prepare Milestone 2 Presentation	03/14/2019	03/28/2019
Evaluate recommendations against test organization	03/28/2019	04/18/2019
Based on evaluation, revise recommendations	04/11/2019	04/25/2019
Prepare Final Deliverables	04/18/2019	05/02/2019

Risk List

Risk name (value)	Impact	Likelihood	Description
Resource restrictions (48)	8	6	Having limited resources can affect the testing phase of new measurements techniques/tools, which could affect the

Risk name (value)	Impact	Likelihood	Description
			final outcome of this project.
Time restrictions (42)	7	6	One risk that could arise is running out of time to complete a task setting us back and endangering the completion of the project
Identified measurements are not effective (32)	8	4	One risk that affects us is that the metrics that we identify for measuring the effectiveness of a cybersecurity program could be ineffective.
Identified measurements are too effective (18)	9	2	One risk that could arise is that the current measurements for effectiveness are very effective leaving our work to be in vain.
The methodology is not universal (10)	5	2	It is possible that the identified methodology cannot be applied evenly to all systems in the evaluated domain. This has the potential to skew certain aspects of the methodology.

Project Methodology

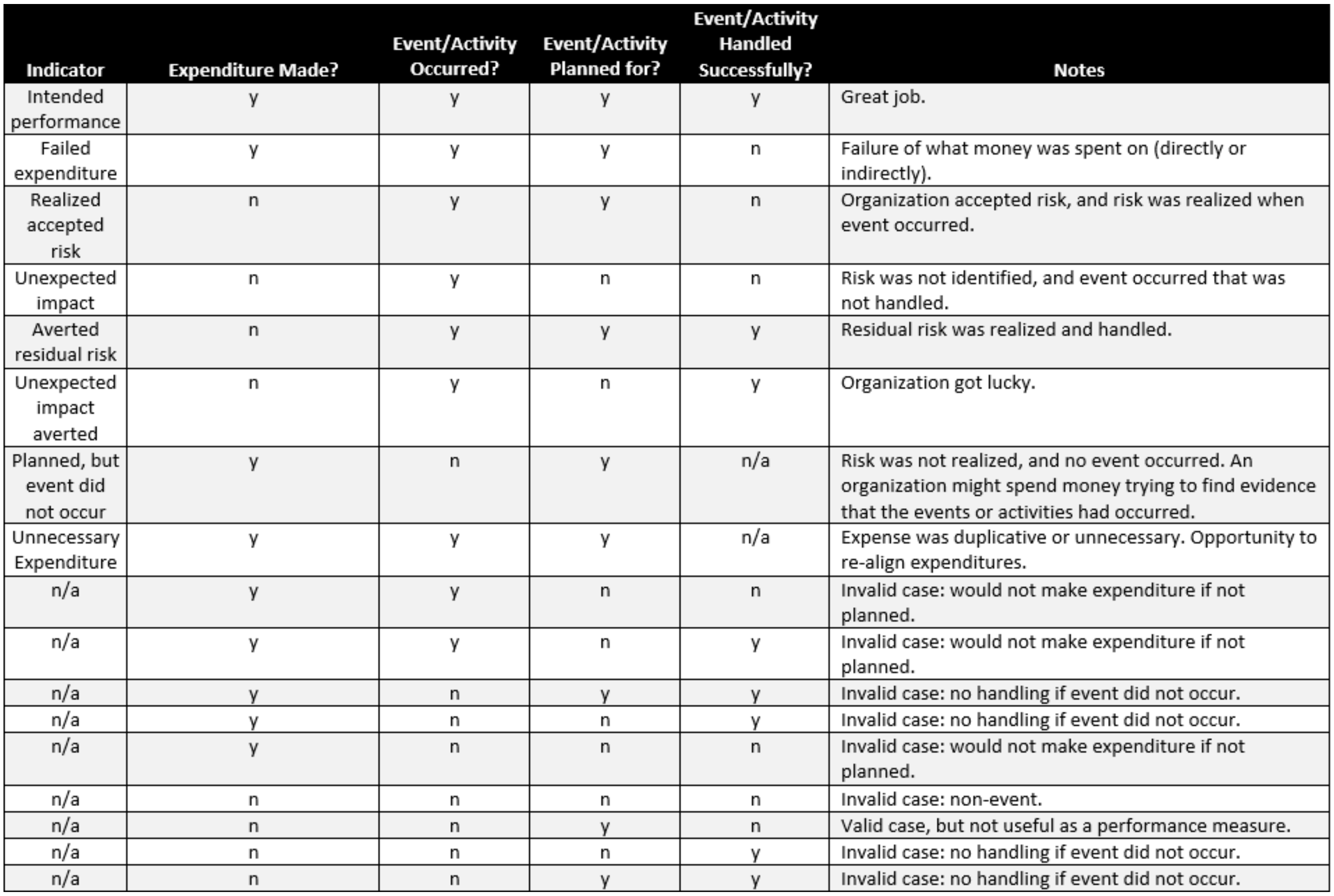
Literature Review:

Measuring Cybersecurity Effectiveness: A Critical Review of the Literature

In order to improve cybersecurity, it first must have a metric to be measured against. This literature review serves as a look into the current way cybersecurity effectiveness is measured. This review will not focus on the current ways cybersecurity effectiveness can be measured in its individual parts (e.g. Data Centers, Internal Networks, Endpoints, Users, Perimeter) but rather the effectiveness of the system as a whole. The review was successful in finding mentions of different metrics for analyzing the effectiveness of a cybersecurity system.

In doing this literature review it became clear that there was no one determined way to measure the effectiveness of cybersecurity systems. That being said, there were some interesting ways to find metrics including using economic-returns as a way to assess the effectiveness. This method, introduced by Dr. Paul Garvey and Dr. Susmit Patel at the 2014 IEEE Military Communications Conference, discussed three potential frameworks for measuring the effectiveness of cybersecurity investments. The first of the frameworks is "designed for conducting an economic-benefit return analysis of risk reduction investments in cybersecurity" [1]. This framework, which can be used as a matrix or a graph, shows the mission areas by the capabilities they depend on and the assets those capabilities depend on to accomplish mission objectives. The entries in the matrix are scores that reflect the cyber risk each asset poses to its dependent capabilities, if the asset's vulnerabilities are exploited [1]. The second of these frameworks chose to do a return analysis from an organizational view. This framework "models the impact of a cyber threat event on the security of systems an organization's missions and business process depend on to achieve its outcome objectives."[1]. This framework is also created in part from the NIST Special Publications SP 800-30 Rev. 1,2012. The last framework they discussed is a return analysis on cyber event impact on mission effectiveness. This was "designed for conducting mission level analyses by modeling deep-dives into the impacts of cyber events on the effectiveness of missions at their lower level mission elements." [1]. In order to accomplish this, they first needed to split missions into mission trees, then assess the potential vulnerabilities and then evaluate the economic-benefit return on threat reducing or mission strengthening investments that improve overall mission effectiveness.

Carnegie Mellon University also came up with a way to measure cybersecurity effectiveness using the Earned Value Management (EVM) method. EVM calculates actual performance against planned performance across the scope, schedule, budget, and expenses of a project. It uses three different metrics, Planned Value (PV) which is the amount of work, in monetary value, expected to be completed, Earned Value (EV) which is the monetary value of work completed to date, and the Actual Cost (AC) which is the amount of money spent to date. In order to use EVM to calculate effectiveness of a cybersecurity system, they used 4 different dimensions as a way to calculate the performance over a given time frame. The first of these dimensions was Cybersecurity expenditures. This is a comprehensive list of how much money was invested and where it was invested in including the technical (e.g. hardware, software) and non-technical (e.g., personnel, policy development) expenses [2]. They also needed to use actual events and activities that occurred during that time frame, both planned and unplanned. Planned scope of cybersecurity events and activities that the expenditures were intended to address. This covers all events, malicious or unintended attacks, and activities like policy development and execution or monitoring of third-party performance. Lastly, they needed to use the successful handling of these events or activities. Using these 4 dimensions, they were able to come up with a chart that showed indicators of performance. (see fig. 1)



Indicator	Expenditure Made?	Event/Activity Occurred?	Event/Activity Planned for?	Event/Activity Handled Successfully?	Notes
Intended performance	y	y	y	y	Great job.
Failed expenditure	y	y	y	n	Failure of what money was spent on (directly or indirectly).
Realized accepted risk	n	y	y	n	Organization accepted risk, and risk was realized when event occurred.
Unexpected impact	n	y	n	n	Risk was not identified, and event occurred that was not handled.
Averted residual risk	n	y	y	y	Residual risk was realized and handled.
Unexpected impact averted	n	y	n	y	Organization got lucky.
Planned, but event did not occur	y	n	y	n/a	Risk was not realized, and no event occurred. An organization might spend money trying to find evidence that the events or activities had occurred.
Unnecessary Expenditure	y	y	y	n/a	Expense was duplicative or unnecessary. Opportunity to re-align expenditures.
n/a	y	y	n	n	Invalid case: would not make expenditure if not planned.
n/a	y	y	n	y	Invalid case: would not make expenditure if not planned.
n/a	y	n	y	y	Invalid case: no handling if event did not occur.
n/a	y	n	n	y	Invalid case: no handling if event did not occur.
n/a	y	n	n	n	Invalid case: would not make expenditure if not planned.
n/a	n	n	n	n	Invalid case: non-event.
n/a	n	n	y	n	Valid case, but not useful as a performance measure.
n/a	n	n	n	y	Invalid case: no handling if event did not occur.
n/a	n	n	y	y	Invalid case: no handling if event did not occur.

Figure 1

The last piece we wanted to examine in this review was some of the keywords included in these pieces of literature. Below is a short table of some of the important keywords and how often they appeared.

Keyword	Number of Occurrences
Cybersecurity	72
Risk	20
Effectiveness	60
Economic(s)	61
Security	14

Keyword	Number of Occurrences
Measure(ment)	32
Investment	60

While we did find some frameworks to measure the effectiveness of cybersecurity controls, nothing stood out as being the best form of measurement. We believe that there is a better way to measure the effectiveness of the controls and intend to create a new framework that helps reach this goal.

Cyber Security Metrics and Measures

In 2008, Paul E. Black, Karen Scarfone, and Murugiah Souppaya from NIST published a paper on Cyber Security Metrics and Measures. In this paper the authors discuss the contrast between Metrics and Measures, selecting measures to support metrics, problems regarding selection, accuracy, and use of measures, and the Common Vulnerability Scoring System (CVSS) [3].

The authors describe metric as “measurement of performance”, and measure as “a concrete, objective, or attribute.” After identifying its metrics, an organization then determines what measures can be collected to support the identified metrics. A main problem with accuracy of measures is the dependency of metric accuracy on measure accuracy; measures are often defined imprecisely, which causes the problem. There are many tools used for measurement which can problems with selection of measures within an organization. The CVSS is comprised of three sets of measures, (i) base measures, (ii) temporal measures, and (iii) environmental measures [3].

Furthermore, the authors explain the benefits of metrics and measures within an organization. Using metrics and measures can verify that an organization’s security controls are in compliance with required policies or procedures, reveal their strengths and weaknesses, and identify security trends which can help an organization monitor its security performance using the past trends. These benefits can help an organization improve performance of its security controls, and answer sophisticated questions regarding its security which helps with strategic decision making [3].

References

[2] Fowler, S. (2018, March 15). *Insider Threat Blog: Cybersecurity Performance 8 Indicators*. Retrieved from Cornegie Mellon University - Software Engineering Institute:

https://insights.sei.cmu.edu/insider-threat/2018/03/cybersecurity-performance-8-indicators.html

[1] Garvey, P., & Patel, S. (2014). Analytical Frameworks to Assess the Effectiveness and Economic-Returns of Cybersecurity Investments. *IEEE Military Communications Conference.* Baltimore: IEEE.

[3] Black, Paul E, et al. “Cyber Security Metrics and Measures.” NIST, NIST, https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51292.

Technical Plan:

First, we will review the NIST Cybersecurity Framework within the context of various technology domains associated with the cybersecurity field, including endpoint, network, and user technologies to name a few. After reviewing the framework with respect to these domains, we will evaluate any potential gaps and brainstorm a way to measure the effectiveness of these controls, using a combination of the resources identified in the literature review.

The next step is to collect data, and that data would be from open source sites, UNO databases, and perhaps from UNO and the test organization. The data we are able to collect will determine the analysis technique we use on the data. However, the analysis will test the controls and measurements identified in the previous step.

This evaluation will first be done on collected data, the measurements that we will use if data is collected will be used to assess its framework whether it was successful or not since the data sets will most likely not be comparable to other datasets. Second, We will be doing qualitative measurements for this evaluation where we compare different frameworks and depending on how they are set up and what implementations they have or do not have. The comparisons of the identified measurements will show us where some of the measurements lack and where some go too far. This will be done based off of experience and reasoning through what is needed for a measurement. The evaluation of the measurements could lead to potential gaps that we plan to discover and formulate different possible solutions to these gaps by altering our proposed solution and retesting these changes. The resources used are our personal computers and campus computers and the test organization.

Requirements

Resource	Dr. Hale	Investigating Team	Description

Resource	Dr. Hale needed?	Investigating Team member	Description
Test Organization	No	Lisa	We need an organization that we can test our measures and recommendations against.