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

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.

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.