HotSoS 2017 Poster Abstract

Title:
A Value Model for Implementing Cyber Metrics and Best Practices

Authors:
Dr. Natalie Scala, Emil Manuel, Rachel Fredman, Jasmin Farahani - Towson University
Dr. Paul Goethals - United States Military Academy

Abstract:

Research in the Five Hard Problems has led to innovative and interdisciplinary advances in cybersecurity. However, a disconnect exists in transferring the research into implementable industry solutions. For example, as of October 2016, 110 papers in the metrics hard problem have been indexed by the Science of Security[1]. An organization looking to improve its cybersecurity posture may be overwhelmed by the sheer volume of options; organizations who lack cyber expertise may shy away from implementing metrics altogether by not knowing where to start.

This research promotes strengthening an organization's security posture by formulating a value model to identify the preferred metrics and best practices for defending against cyber attacks or intrusions. These practices may differ by organization, based on demographics and history such as size of firm and prior experiences of cyber attacks and/or breaches. To identify the preferred metrics and best practices, we employ multiple objective decision analysis (MODA), which is grounded in utility theory, to evaluate a set of candidate metrics and best practices against desired attributes in cyber defense.

This framework can be applied to any organization, customized by data applicable to that firm. We illustrate the model for the general supply chain. We identify six attributes that are valued in cybersecurity – data integrity, end to end security, cloud security, security policies, intrusion and threat detection, patch sets and hot fixes – and utilize IAD's Top 10 Information Assurance Mitigation Strategies as candidate metrics and best practices. We employ the combined standard of Parnell, et al.[2] for model data collection, interviewing subject matter experts and researching policy documents. Preliminary results identify controlling administrative privileges, limiting workstation-to-workstation communication, and using web domain name system recognition as the top three preferred metrics and best practices for supply chain organizations. Continuing research will evaluate the sensitivity of these results as well as index model attributes for other industries.

---

[1] Science of Security (2016). SoS documents: By topic. Retrieved from http://cps-vo.org

[2] Parnell, G. S., Bresnick, T. A., Tani, S. N., and Johnson, E. R. (2013). *Handbook of decision analysis*. Hoboken, New Jersey: Wiley.