Chapter 99
The Next Generation of Scientific-Based Risk Metrics:
Measuring Cyber Maturity

Lanier Watkins
Johns Hopkins University Information Security Institution, Baltimore, USA

John S. Hurley
National Defense University, Washington D.C., USA

ABSTRACT

One of the major challenges to an organization achieving a certain level of preparedness to "effectively" combat existing and future cyber threats and vulnerabilities is its ability to ensure the security and reliability of its networks. Most of the existing efforts are quantitative, by nature, and limited solely to the networks and systems of the organization. It would be unfair to not acknowledge that for sure some progress has been achieved in the way that organizations, as a whole, are now positioning themselves to address the threats (GAO 2012). Unfortunately, so have the skill sets and resource levels improved for attackers--they are increasingly getting better at achieving the unwanted access to organizations' information assets. In large part the authors believe that some of this is due to the failure by methods to assess the overall vulnerability of the networks. In addition, significant levels of threats and vulnerabilities beyond organizations' networks and systems are not being given the level of attention that is warranted. In this paper, the authors propose a more comprehensive approach that enables an organization to more realistically assess its "cyber maturity" level in hope of better positioning itself to address existing and new cyber threats. The authors also propose the need to better understand another missing critical piece to the puzzle--the reliability and security of networks in terms of scientific risk-based metrics (e.g., the severity of individual vulnerabilities and overall vulnerability of the network). Their risk-based metrics focus on the probability of compromise due to a given vulnerability; employee non-adherence to company cyber-based policies; insider threats. They are: (1) built on the CVSS Base Score which is modified by developing weights derived from the Analytic Hierarchy Process (AHP) to make the overall score more representative of the impact the vulnerability has on the global infrastructure, and (2) rooted in repeatable quantitative characteristics (i.e., vulnerabilities) such as the sum of the probabilities that

DOI: 10.4018/978-1-7998-2466-4.ch099

devices will be compromised via client-side or server-side attacks stemming from software or hardware vulnerabilities. The authors will demonstrate the feasibility of their method by applying their approach to a case study and highlighting the benefits and impediments which result.

INTRODUCTION

One of the major challenges for federal agencies is preparedness to address present and future cyber threats and vulnerabilities. Cybersecurity practices, especially within the Department of Defense (DoD), have been focused exclusively on securing and protecting the networks. What is needed is a more comprehensive view of cybersecurity that, to date, has been largely missing. It is important to address this issue because existing efforts take very narrow approaches that tend to reveal results that can lead to inaccurate conclusions. This possibility is anything but trivial because it can potentially cause organizations to develop a false sense of security that actually places them at even higher risk.

Much of the difficulty lies in the fact that within these agencies threats and vulnerabilities are treated as IT security issues-- i.e., ("technical" problems that can be linked primarily to the agency's network) instead of cybersecurity issues, which should be treated much more broadly. The absence in thought of some of the more relevant organizational elements is also revealed in the metrics that are used to assess how organizations position themselves against cybersecurity threats and vulnerabilities. A lot of reasoning is based on culture and training in terms of traditional views on IT security that have been over-extended to cybersecurity. Previous approaches have rarely examined the severity of individual vulnerabilities or the overall vulnerability of the network. Less work even still has been done on both of the two, simultaneously. In addition, traditional approaches are still pretty network-centric and have largely ignored other elements of the organization that can have an immense impact on the vulnerabilities and threats.

In this paper, we propose quantifiable, scientific risk-based metrics to gain a better understanding of the overall cyber vulnerability as it relates to global network infrastructures. In addition, our approach recognizes the need to prioritize vulnerabilities in terms of severity. Lastly, we extend the factors that can contribute to cyber threats and vulnerabilities beyond the traditional network-centric approach. We propose future work that will look to quantify the factors, which will here-to-fore be viewed as elements of the organization (beyond networks) to provide a more comprehensive and accurate reflection of cyber threats and vulnerabilities.

THE TRIAD: CITIZENS, DEFENSE AND INTELLIGENCE

The 2003 World Summit on the Information Society (WSIS 2003) was a major driver in the significant shift in the view of the oversight of information within an "information society". It called for a new, radical stakeholder-centric view, in which information was seen as a foundation of an evolving society in which decision making needed to be shared by all. Of course, this represented a significant deviation from the traditional government-driven view in which decisions regarding information should be made by various segments of the government, especially within the defense and intelligence sectors. Unfortunately, recent differences in perspective have led to an unprecedented level (at least, post- September 11th) of mistrust between the three communities: citizens, defense, and intelligence. The differences,