



MEASURING SECURITY:

Making Sense Out of a Modern-Day Tower of Babel

AFCEA Cyber Committee¹

March 2019



TABLE OF CONTENTS

3	INTRODUCTION
4	SECURITY METRICS SURVEYS
6	SECURITY METRICS TAXONOMIES
13	CONCLUSIONS
15	APPENDIX
20	BIBLIOGRAPHY




INTRODUCTION

Over the past decade, many organizations have suffered major security breaches leading to financial losses and damaged confidence in the eyes of their customers and the American public. In most cases, these breaches were a surprise to senior management staff members because they had been assured that their organizations' ability to identify and deter cyber attacks was solid. In other cases, the technical team had not been able to adequately describe the security risks an organization was facing in an objective way that would inform senior management of the risk of a security breach. Regardless of the reason, in the aftermath of every breach, outside experts found an organization's security posture was anything but solid. In fact, in many cases, its security posture was shockingly weak.

Senior executives are increasingly interested in having objective measures for determining the robustness of their organizations' cybersecurity protections. They also want to invest in security measures that are cost effective and therefore need to understand how much security is enough. Likewise, chief information officers (CIOs) and chief information security officers (CISOs) want measures to gauge if they are putting sufficient emphasis on security. They also want to know if their security is as good as that of their peers.

Despite these obvious and compelling needs for ways to measure security, AFCEA's Cyber Committee found that there is no consensus about how to measure security. To the contrary, its members found that the security metrics is all over the map with most organizations admitting in confidential discussions that they are not comfortable with the metrics they are using.



SECURITY METRICS SURVEYS

The Cyber Committee has been examining the area of security metrics for the past 24 months. During that time, the committee has attempted two surveys of AFCEA member organizations requesting input on security metrics in use. The results of the surveys were surprisingly poor, yielding no useful data. The committee members, comprising approximately 40 cybersecurity experts representing a mix of private sector, government and academic organizations, discussed the poor response from the surveys. These discussions highlighted that many organizations were struggling to define appropriate measures to assess their security posture. Moreover, it became clear that many organizations were reluctant to publicly acknowledge their relative immaturity in the area of security metrics.

The committee reviewed several publicly available compendiums of security metrics. Two of these reports were NIST's Special Publication 800-55 (rev 1) Performance Measurement Guide for Information Security² and The CIS Security Metrics³ published by the Center for Internet Security (CIS) in November 2010. It also reviewed published papers and held internal discussions on the topic. A few of key observations included:

- To be most helpful, security metrics need to be tied to specific objectives;
- Organizations typically wish to compare security metrics over time (i.e., using a dashboard that shows trends) or against peer organizations;
- For better or for worse, what gets measured, gets attention and hopefully improves;
- Ideally, security metrics should inform decisions; and
- Security metrics by themselves do not provide a good overall measure of the security of an organization at a point in time.

To try to get a better handle on what organizations were doing in the area of cyber metrics, the committee decided to reach out to a handful of organizations respected for their cybersecurity programs. This outreach included several companies represented within the Cyber Committee.



Specifically, the organizations that responded to the committee’s requests did not provide a list or book of security metrics. Rather, through in-person interviews with each organization, the committee was able to gain insight into their approach to measuring security and the type of security metrics they were using.

From these interviews, it became clear that the term “security metrics” has different meanings to different organizations. After analysis

of the interview results, it also became apparent that one of the fundamental problems in defining security metrics is the lack of a broadly accepted definition of what constitutes security metrics nor is there a model of the different types of measurements commonly equated to security metrics. Finally, it also became very clear that even organizations with relatively mature cybersecurity programs and robust security metrics were struggling to find the right measures to communicate their state of security to their boards of directors or senior executives.

This white paper provides an overview of different security metrics programs that the Cyber Committee found as well as a derived maturity model that permits the comparison of the different security metrics programs in an effort to provide some clarity in what the committee found is a modern-day Tower of Babel.



SECURITY METRICS TAXONOMIES

Several different structures or taxonomies are used by organizations as they implement security metrics. An overview of the various taxonomies Cyber Committee members found is provided in the appendix.

Interviews the Cyber Committee conducted led to the identification of what members determined was a particularly useful taxonomy for security metrics that also seemed to correlate well to what they assessed was an evolutionary path for most security metrics programs. This taxonomy focuses on the end uses of the metrics in which each use related to a target audience of the security metrics. Three common uses were the technical compliance indicator, the management indicator and the organization risk indicator. Each of these metrics usages and their target audiences are summarized briefly and in a bit more detail in the appendix.

Technical Compliance Indicator

Most organizations measure security activities by tracking their technical activities such as currency of software patches, number of vulnerabilities discovered during a vulnerability scan and existence of specific security controls such as hardware/software asset identification and application white listing. The committee found that some organizations track a large number of technical compliance metrics. However, it was clear in many cases that organizations did not have organizationwide standards for technical compliance security metrics, and suborganizations were free to select the technical compliance metrics they chose to implement.

The audience for technical metrics is the IT team—the IT managers, CIO and CISO in particular—that is interested in having measures that relate to the technical activities involved with providing security. A comprehensive set of technical controls, such as the CIS Controls, can be a very positive foundation for an effective cybersecurity program. However, technical compliance indicators by themselves do not provide a solid basis for senior leadership to assess the overall quality of the security program or whether it is cost effective to implement additional security measures.



Management Indicator

A number of organizations have developed a set of security metrics that track security-related activities and are specifically visible to and endorsed by senior management. In short, these management indicators reveal to the organization's personnel that management is interested in good security. Following the principle of what gets measured improves, management indicators typically show improvement over time. Examples of management indicators include counting the number of systems with current security accreditation, the percentage of systems using a particular software version or the number of personnel who have completed security awareness training.

The Cyber Committee found that security management indicators were a positive way to convey management interest in security and to ensure that senior management had visibility into what is typically a small set of important metrics. In the words of one of the organizations, "We needed to start with something simple to get the attention of the [many component] organizations." Committee members determined that the management indicator or scorecard approach was valuable in bringing organizationwide attention to security. However, they also found that management indicators, while visible to senior management, are a weak proxy for determining the actual state of cybersecurity across the entire organization.

Organization Risk Indicator

Several organizations interviewed described their security metrics effort as aligning their security metrics with their risk management efforts, specifically risks-to-mission accomplishment. These organizations typically had implemented a set of technical compliance security measures and, in some cases, the technical measures were quite extensive. However, senior management could not conclude from the technical metrics if the security posture was sufficiently robust to meet their overall objectives, or if the return on investment of additional investments in cybersecurity was appropriate. Therefore, in addition to the use of technical controls and metrics, organizations evaluated the goodness of their security programs from a top-down perspective. Specifically, they identified the major mission risks because of security issues and assessed whether the technical controls were adequate to mitigate the risks. If not, senior leadership could make informed decisions to invest in additional controls or to accept the residual risks.



The use of organization risk indicators is perhaps best seen by comparing two organizations that were interviewed.



Organization A has a very mature process for defining and assessing organizational risks across its enterprise that includes identifying potential risks from cyber events. It also has a very extensive and standard set of companywide technical compliance security metrics and employs external auditors to determine if the

technical security controls are being properly implemented. This organization identifies key organizational risks using a top-down assessment methodology. The objective is to reduce the potential consequence of any risk—in this case it is measured in potential dollars loss—to an acceptable level as defined by the board of directors. For each security risk area, appropriate metrics identify and assess the security controls, which are mostly technical, that have been implemented and are expected to mitigate the identified risk. Organization A uses analysis and modeling to help document if the security risk can be mitigated with high confidence. If the risk cannot be adequately measured and mitigated below a board of directors-defined dollar threshold, the acceptance of this risk must be approved by the organization's board of directors.

Organization B also has a robust enterprise risk management framework that matured over a number of years and helped it identify risks to its business operations. It has implemented a significant set of technical controls, although the implementation is not uniform across the organization. Recently, it added a new risk area titled cybersecurity, but the organization had been struggling to define how to assess this risk area. Organization B acknowledged it had a difficult time communicating the potential mission benefits of additional investments in technical security controls to its board of directors. Specifically, the organization noted that the board of directors was not able to assess



whether the current technical metrics indicated an acceptable security posture or additional investment was warranted. In attempting to assist the board in evaluating the adequacy of current security measures, the company's security team had done extensive modeling of expected losses as a result of inadvertent or hostile cyber events. Unfortunately, the models illustrated minimal losses because they were only based on historical patterns and could not show the potential consequences of future attacks or events.

A Security Metrics Maturity Model

After analyzing the results of the interviews with selected organizations that had very different security metrics programs, the committee observed there was more order in the security metrics "Tower of Babel" than had been initially apparent. The committee found that, regardless of the taxonomy adopted, all organizations were ultimately striving to be in a position to assess the risk of accomplishing the overall mission of the organization. This was their common goal, and each organization was trying to mature its security processes and measures toward this objective. It became apparent to committee members that there was a logical maturing process for organizations as they strove to define the security metrics that could accurately portray an organization's overall security posture.

Cyber Committee Three Stages of the Maturity Progression

Stage 1: The Initial Maturity Level is characterized by an ad hoc security metrics program. Organizations at an Initial Maturity Level implement security metrics in a non-uniform way across the organization, and the metrics are not related or they are inconsistently related to the organizations' security policies or mission goals. Moreover, at the Initial Maturity Level, senior managers have little or no visibility into the security metrics and little insight into the state of security of their organizations. Most often, the board assess the security of their organizations based on personal assurances by the CIO and CISO. At this maturity level, technical compliance indicator metrics are most commonly being implemented.

Initial Maturity
defined by non-uniform implementation of metrics and metrics not related to organization security policies or mission goals.



Stage 2: The Defined Maturity Level reflects a more mature security metrics program. At this level, technical security metrics are implemented based on approved organization security goals or policies. These metrics, or at least a subset of them, are visible to and overseen by senior management through organizationwide dashboards or scorecards. While security metrics at a Defined Maturity Level reflect important security-related input or output, they are not directly linked to an organization's outcomes or objectives such as the ability of the organization to perform its primary mission. In many cases, management indicator-type metrics, for example the deployment of tools or implementation of security processes, are used to convey the priority that senior management is placing on the importance of a robust cybersecurity program. At the Defined Maturity Level, while management has visibility into security measures, it cannot answer objectively the questions: "Is our security adequate?" or "Should we invest more in security measures?" Specifically, it is not possible for management to assess the residual risks to mission accomplishment or the incremental value of additional investment in security countermeasures.

Defined Maturity reflected by security metrics based on organization's security goals or policies and security measures are visible and overseen by senior management.

Stage 3: Linked Maturity Level is the goal of mature security programs. At this level, organizations address security risks at both the technical level as well as the organization mission level. At the technical level, Cyber Committee members found that organizations at a Linked Maturity Level have a well-defined set of technical controls consistently implemented across the organization that target the most common cyber threat patterns that can be mitigated by cyber controls. Most often these controls focus on good cyber hygiene.



An example of the type of controls implemented is the CIS Controls that align with the most common security threats to all organizations. In addition, however, organizations at a Linked Maturity Level analyze and specifically identify organization-unique security risk areas that might jeopardize achievement of organizational missions. This risk analysis is done as a part of an overall organizationwide risk identification and risk management effort. In short, these organizations address security risk from both the bottom up—a technical focus on the most common cyber threats—as well as the top down, identifying unique risks to accomplishing their missions. Specifically, as a part of defining and analyzing risks to achieving the mission, risk scenarios are detailed that will help identify risks that partially or completely arise from potential cyber-related events. These organization-level security risks are then specifically linked to the applicable technical security controls the organizations have implemented.

Linked Maturity is defined by top-down identification of cyber risks to accomplishment of organization’s mission, linking of these risks to the mitigating (mostly technical) security controls, and analytical assessment of residual risk exposure.

In some of the risk scenarios, analysis will likely determine technical security controls are not adequate to fully mitigate the identified cyber risks. This will necessitate further analysis to determine if additional investments in technical controls or other security countermeasures are warranted. This might result in recommending the purchase of more hardware or software security measures or recommending enhanced monitoring by expert security personnel. Organizations at a Linked Maturity Level also may determine that additional investment to mitigate a specific risk is not appropriate because of the low probability of occurrence or the high cost of the appropriate countermeasures. This set of recommendations and the supporting analysis tied to organization mission risks can be brought to the organization’s board for approval.

In short, by objectively identifying and analyzing risks to mission accomplishment and linking these risks to the largely technical security measures that have been implemented, organizations at a Linked Maturity Level are able to show with analytical rigor the reduction in their risk exposure as a



result of the technical security controls and to highlight residual risk. In this way, they can provide senior managers and board members with objective measures regarding the organizations' state of security, specifically with regard to achievement of the their primary mission objectives. Decisions regarding security investments, including return on investment calculations, for these organizations can be based on objective business-based analysis rather than subjective arguments.



CONCLUSIONS

While the Cyber Committee found that most organizations are struggling with regard to implementing the right security metrics, there does appear to be a reasonable maturity path that organizations can follow. Specifically, in order for an organization to achieve a Defined Maturity Level, it must implement a set of security controls that relate to defined organizational policies or organization security objectives. At this level, management indicators such as scorecards are useful to convey to the workforce that security is important and to overcome cultural resistance to a more disciplined security regime.

Moreover, the committee concluded it is not possible for an organization to move from an Initial Maturity Level directly to the Linked Maturity Level without a culture of awareness of the importance of security and a foundational security metrics program consisting of mostly technical metrics that aligns with defined organization policies or objectives. As such, most organizations must progress from an Initial Maturity Level posture to a Defined Maturity Level as they progress toward a Linked Maturity Level.

Committee members believe organizations must get to a Linked Maturity Level before they are able to objectively answer questions from senior management or boards of directors such as “How good is our security?” or “What is the return on specific investments in additional security controls or countermeasures?”

From the committee’s research, it is clear that some organizations are approaching or have achieved a Linked Maturity Level. There are two essential requirements for organizations at this level. First, they must implement an enterprisewide risk assessment and management process that specifically addresses potential cyber risks in the context of their mission.



Although many organizations are moving in this direction, most are learning that expanding enterprise risk assessment efforts to specifically include cybersecurity is new and somewhat difficult given their lack of experience in understanding potential cyber risks that can impact the mission. A second requirement for achieving a Linked Maturity Level is that documented specific security risks in the enterprisewide risk assessment processes are linked or mapped to the security controls or other countermeasures that have been or will be implemented to mitigate these mission-impacting cyber-related risks.

It is important that organizations have a thorough assessment of mission risks involving cyber threats. A narrow mission risk assessment is dangerous. Equifax is one example of an organization that had an enterprisewide cyber risk assessment process that was too narrowly focused. In the aftermath of the company's massive security breach in 2017, it became clear that while Equifax was focused on enterprise risks from cyber, it did not identify one of the essential elements of its mission: the highly sensitive personal data used to calculate financial risk scores.

The Equifax example illustrates that just having an enterprise risk focus is not enough; risk assessment must be robust, comprehensive and truly objective. The Cyber Committee found several organizations that were struggling in objectively identifying security risks as a part of their corporate risk management process. Committee members believe it will likely take several cycles of risk evaluation for most organizations to have confidence that they have adequately identified security-related risks in their corporate risk identification and analysis process. Tabletop exercises focusing on cyber threats and risks as well as outside cyber consultants can be used to help organizations identify mission risks from cyber threats.



APPENDIX

The AFCEA Cyber Committee identified these security metrics taxonomies during the course of this study:

One taxonomy identifies metrics as relating to one or more types of measures, specifically input metrics, output metrics and outcome metrics. An example of an input metric is measuring the installation of a cyber defense tool. In some organizations, these metrics also are called activity metrics as they reflect accomplishment of activities. By contrast, an output metric might measure the reduction in cyber incidents resulting from use of a cyber defense tool or installation of security controls. Finally, an outcome metric might measure the reduced financial loss or an increased ability to operate in a cyber environment through a cyber attack as a result of additional security controls.

Outcome-based metrics often involve external factors such as the level and sophistication of an attack, factors that are determined by the threat actor or the operating environment and largely beyond the securing organization's ability to control.

It is recognized that each of these metrics has validity. However, as can be seen through the examples, what is being measured and the value of the metric to different audiences—a director of IT or CIO versus a CEO—are quite different.

The NIST Cybersecurity Framework provides another taxonomy adopted by many organizations to guide their security metrics efforts.⁵ The committee found that some organizations align their cyber metrics with the five functions of the framework: identify, protect, detect, respond and recover. Within the NIST framework, specific activities defined as categories and subcategories relate to each of the five functions. Explicit references within the framework have been used as the basis for some organizations' security metrics.



Technical Compliance Indicator

Many organizations measure security activities by tracking their technical activities such as the number of vulnerabilities discovered during a scan, currency of software patches and the existence of specific security controls such as hardware/software asset identification and application white listing. These metrics typically measure the technical activities involved with security. In many instances, they are compared to established policies such as a policy requiring software patches to be installed within a certain number of days after a vendor issues a new patch.

The committee found that some organizations track a large number of technical compliance metrics. In many cases, however, it was clear that organizations do not have organizationwide standards for technical compliance security metrics, and suborganizations are free to select which technical compliance metrics they will implement. One company interviewed indicated it had a 60-page book of the technical compliance metrics—or security controls—that it tracks across the entire company. In this case, the company also required its key supply chain partners to implement the same technical security controls. The audience for technical metrics is the IT team—the IT managers, CIO and CISO in particular—who are interested in having some measures that relate to the technical activities involved with providing security.

As noted, the Center for Internet Security (CIS) has compiled a good compendium of primarily technical security metrics developed through a consensus process. The compendium has become a popular resource for organizations that are interested in implementing a security metrics program. While technical metrics are valuable, the committee found that each organization decides which metrics it will track and what is determined to be good or adequate for a particular organization.

The CIS also has published a focused set of 20 technical security measures, called the CIS Controls, intended to address the most frequent cyber attack patterns. Although many organizations implement these controls and subcontrols, an initial measurement standard for the controls has only recently been published with Version 7.



Through the original surveys and subsequent interviews, the Cyber Committee found that most organizations track some technical security metrics. However, as noted, there is little commonality of technical metrics among organizations, and there is no objective basis for comparing technical security metrics between companies.

Management Indicator

A number of organizations have developed a set of security metrics to track security-related activities and make them available to senior management. In short, management indicators demonstrate to an organization's personnel that its leaders are interested in good security. Following the principle that what gets measured improves, management indicators typically show improvement over time.

Examples of management indicators include counting the number of systems



that have current security accreditation; determining the percentage of systems that have a particular software version; and/or tracking the number of personnel who have completed security awareness training. While management indicators are valuable to emphasize security, they typically do a poor job of reflecting an organization's state of

security because they focus only on selected subsets of a comprehensive cybersecurity program.

One example of a management indicator effort is the security metrics associated with the Federal Information Security Management Act (FISMA), initially passed in 2002 and updated in later years. FISMA outlines responsibilities for ensuring the security of federal IT systems and requires



reporting of security metrics by federal agencies. Over the years, different sets of security metrics have been defined by the Office of Management and Budget for federal agencies to report. These metrics have become more robust and focus on a subset of security measures that are deemed to be particularly relevant to assessing the security of federal systems.

The metrics roll up to an agency level and are typically stated in terms of percentages—of systems, of users or of activities—across the agency. The FISMA metrics are useful. Because they focus on a subset of important security areas and are at an aggregate level, they serve to provide an indication of whether management of the agency is focusing on security or providing a solid overall measure of the an agency’s state of security.

Similarly, the Department of Defense (DoD) has recently implemented the Cybersecurity Scorecard, which measures the highest priority items from the DoD Cybersecurity Discipline Implementation Plan.⁷ Like the FISMA reporting, the DoD Cybersecurity Scorecard is collecting metrics tied to specific security initiatives, such as the DoD’s deployment of Windows 10, the implementation of a host-based security system (HBSS), and the move of Internet-facing servers to a protected area called a DMZ.

The Cyber Committee found that security management indicators were a positive way to convey management interest in security and to ensure that senior management could see a small set of important metrics. In the words of one of the DoD CIO team, “We needed to start with something simple to get the attention of the DoD component organizations.” The committee determined that the management indicator or scorecard approach was valuable in bringing organizationwide attention to security. However, it also found that management indicators are a weak proxy for determining the actual state of an organization’s cybersecurity.

Organization Risk Indicator

Several organizations interviewed described their security metrics effort as aligning their security metrics with organizational (i.e., mission) risks. These organizations typically had implemented a set of technical compliance security measures and, in some cases, the technical measures were quite extensive. However, senior management could not conclude from the technical metrics



if their organizations' security posture was sufficiently robust to meet the organizations' overall objectives, or if the return on investment of additional resources in cybersecurity was appropriate. The goal for these organizations then became to identify those security metrics that were most important to understanding and evaluating risks to their ability to perform their missions or their strategic objectives. In most cases, these security metrics would be specifically aligned with risks that could disrupt an organization's fundamental operations. Once defined, these risk-based metrics were tracked and regularly reported to senior management. The Department of Defense stated its eventual goal is to define a set of security metrics that relate to measuring the risk to executing warfighting and humanitarian missions in an environment of increasing cyber attacks. For other organizations, the potential for significant financial loss (such as a loss of more than \$X million), the inability to meet customer expectations, or the consequence of reputational damage from a major cyber incident were being used to help identify the acceptable amount of risk to their organizations.



BIBLIOGRAPHY

- 1 John Gilligan is the principal author of the paper with contributions from Michael Basla, John Bruton, Robert Carey, Glenn Hernandez, James Richberg and Gregory Touhill.
- 2 Performance Measurement Guide for Information Security, NIST, Information Technology Laboratory, July 2008.
- 3 The CIS Security Metrics V1.1.0, The Center for Internet Security, November 1, 2010.
- 4 CIS Controls, Version 7, the Center for Internet Security, March 19, 2018.
- 5 Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST Information Technology Laboratory, April 16, 2018.
- 6 CIS Controls, Version 7, the Center for Internet Security, March 19, 2018.
- 7 DoD Cybersecurity Discipline Implementation Plan, DoD CIO, October 2015 amended February 2016.

The AFCEA International Cyber Committee White Paper Series

www.afcea.org/committees/cyber

Copyright 2019 AFCEA International. All rights reserved.

All distribution must include www.afcea.org.

