Cyber Operations Rapid Assessment (CORA)

Examining the State of Cybersecurity Assessment Methodologies and Introducing a New Alternative

Dr. Lindsley Boiney
Julie Connolly
Dr. Clem Skorupka
Shelley Krueger
Dr. Alec Summers

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Department No.: J83D
Project No.: 25MSR615-BB
Bedford, MA

Approved for Public Release; Distribution Unlimited.
Case Number 15-2853

MITRE

This page intentionally left blank.

Table of Contents

Introduction 1
Background and Gap 1
Cyber Operations Rapid Assessment (CORA) 2
Structure of the Assessment 2
Organizational Context 4
Threat Awareness and Training 4
Tools and Data Collection 5
Internal Processes and Collaboration 6
Tracking and Analytics 6
External Engagement 7
Conclusion 8
Appendix 9
Mandiant RRA 9
Hewlett Packard SOMA 9
Booz Allen Hamilton COMF 9
Department of Homeland Security CRR 10
CERT OCTAVE Allegro 10
FFIEC CAT 11
ISACA COBIT 11
Other Assessments and Methodologies 11

List of Figures

Figure 1: Assessment Structure 2

This page intentionally left blank.

Introduction

Actionable threat intelligence plays a critical role in cyber defense in all respects, from helping to protect systems and data, to protecting organizations, industries, and even countries. A growing number of highly publicized breaches have led to tremendous activity in both the public and private sector to enhance capabilities to collect, utilize, and share cyber threat intelligence. Many organizations, however, are behind the curve in terms of threat intelligence, relying predominantly on static defensive measures and compliance-oriented processes. Transitioning to a threat-oriented posture is not easy, and change needs to occur across the triad of people, processes and technologies.

Some organizations have taken the important step of joining a formal industry-sector or regional cyber threat sharing collaborative such as an Information Sharing Analysis Center (ISAC). In such collaborative efforts, members' capability and resource levels often fall on a spectrum. It is important for the success of information sharing groups to understand the maturity levels of their respective memberships, and to identify ways to help improve the exchange of threat information for all parties.

In this paper we analyze modern cyber operations assessments and present an alternative to fill a gap in the current state of practice. MITRE has developed and piloted the Cyber Operations Rapid Assessment (CORA) methodology with the goal of helping organizations quickly identify areas in their cyber security defensive practices where improvements can be made in the collection, utilization, and sharing of threat information. CORA is not intended to be a complete review of an organization's entire security program, but rather focuses on those elements that are critical to the incorporation of threat information into defensive operations and risk management. We discuss the methodology in detail and the motivation behind each of its five main focus areas.

Background and Gap

A large number of highly-publicized breaches are causing executives and decision-makers to take a hard look at their own internal cybersecurity capabilities. In response, many assessment methodologies have been developed (e.g., by DHS, Mandiant, ISACA)[1] to evaluate an organization's current cybersecurity capabilities and make recommendations for raising its cybersecurity maturity. To provide an overview for the current state of the practice and market for these services, we scrutinized the offerings of a representative group in the vendor, consulting, and government sectors. A detailed overview of these methodologies and their defining characteristics can be found in the Appendix.

In the current market for cybersecurity assessment methodologies, we identified four distinguishing factors: cost, focus, objectivity, and support.

> **Cost**: Many assessments require a large investment of time and financial resources, which can be impractical for many organizations.
>
> **Focus**: Other assessments vary widely in terms of their focus on different aspects of cyber defense, including compliance with a particular standard, vulnerability penetration tests, or maximizing value for cybersecurity investment (a cost/benefit perspective). Even those aiming to be broad in scope typically do not assess engagement with external parties and sharing information about cyber threats.

[1] See Appendix.

Objectivity: There are also many tools or service options offered for sale by private companies in addition to their assessments, which may result in a lack of objectivity in their evaluation.

Support: Lastly, there are free or inexpensive methods that simply provide templates for self-directed use and do not offer support or engagement.

There is a need for a method that provides a threat-oriented approach, with lightweight but interactive engagement, that covers all elements of an organization's cyber operations (technical, non-technical, policy, external engagement, etc.) in an unbiased and objective manner. The Cyber Operations Rapid Assessment (CORA) methodology fills this niche in the cybersecurity assessment realm.

CORA is lightweight assessment that provides a snapshot of an organization's cybersecurity operations capabilities, including specific recommendations for improvement without specific marketing goals. It emphasizes threat analysis, incident prevention and response, and threat intelligence information sharing. CORA is an effective model for an organization seeking a quick review of its cybersecurity operations capability, and as a possible prelude to a more rigorous assessment.

Cyber Operations Rapid Assessment (CORA)

The CORA methodology is intended to

- Require minimal resources and time for the participant
- Focus on areas of cyber security practices critical to a threat-aware cyber defense
- Apply to organizations in different industry and government sectors
- Apply to organizations of varying cyber security capabilities and maturity levels
- Provide specific and tailored guidance about steps an organization could take to improve their capabilities

CORA is designed to be useful for both individual organizations and collaborative information sharing entities wishing to gain insight into their members' capabilities. The CORA approach does not impose requirements or address regulatory/compliance issues, nor does it recommend vendor-specific tools/services or include a technical vulnerability assessment.

Structure of the Assessment

CORA consists of a participant survey, a preparatory review of survey results, and an interview (either by phone or in person) to review the survey responses. A report of recommendations tailored to the participant is shared during a follow-up feedback session.

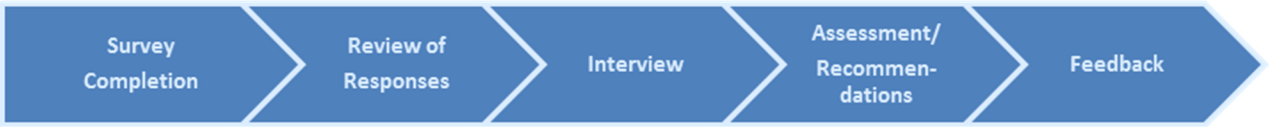

Figure 1: Assessment Structure

The survey is completed by one or more individuals familiar with the organization's cyber security operations and practices. Generally this is the manager of the cyber operations team or an experienced analyst, but this will vary depending on the size and structure of the organization.

The survey consists of multiple choice and multiple answer questions that address five core areas of cyber operations: Threat Awareness and Training, Tools and Data Collection, Internal Processes and

Collaboration, Tracking and Analytics, and External Engagement. There is a preliminary section to establish the organization's distinctive characteristics in terms of industry, size, and other aspects relevant to its threat environment.

Once the completed survey is returned, the organization's responses are reviewed. The purpose of this stage is to identify areas for in-depth follow up during the interview. Any additional comments the respondent has provided are also reviewed to identify any missing, ambiguous or particularly strong responses (good or bad) that may indicate a topic worth exploring more fully.

The follow-on interview typically takes one to two hours to complete. It should involve the primary survey respondent(s), but may include other organizational members as desired to flesh out responses. The interview phase is essential for eliciting the context surrounding responses and for correctly interpreting them.

The final survey responses are analyzed and incorporated into a report. The typical report is an eight-slide briefing that presents areas of strength, opportunities for improvement, a high-level graphical representation of the participant's capabilities in each of the five major areas, and specific recommendations as to how the organization can advance their capabilities in each of the five focus areas. The report is designed to be self-contained, immediately actionable, and succinct enough to share with senior decision makers.

Since the CORA assessment is lightweight and can be completed in a short amount of time, it can easily and effectively be used to compare organizational capabilities at different points in time. For example, assessments could be made both before and after implementation of new systems or procedures to reveal any changes in capabilities.

If multiple participating organizations are part of a collaborative information sharing group (such as an ISAC or other industry or regionally based threat sharing group), the CORA methodology can offer an aggregated and unattributed summary of the organizational profiles within the group. This highlights the variation in capabilities within a group, and can be used to identify potential peer mentoring relationships, or to help tailor training or services for group members. Aggregated information is shared exclusively for the purposes of awareness, learning, and improvement, and is never shared in an attributed or identifiable manner with others.

Assessment Areas

In order to collect and leverage threat intelligence towards building an effective, threat-oriented cyber defense program, an organization must consider many aspects of its cyber program. In this section we will discuss the motivation and thinking behind both the initial context questions as well as the five main sections of CORA: Threat Awareness and Training, Tools and Data Collection, Internal Process and Collaboration, Tracking and Analytics, and External Engagement.

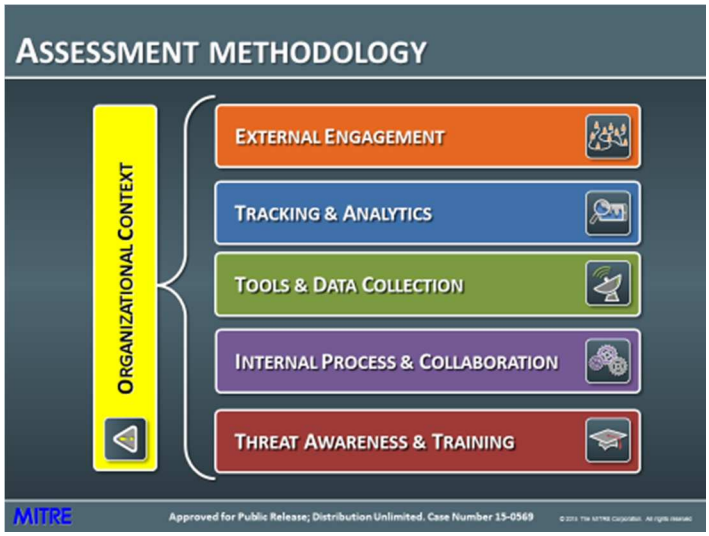

Figure 2. CORA Model Visualization

Organizational Context

It is important to capture basic contextual facts to help generate recommendations that will be feasible and appropriate for the participating organization across the five CORA assessment areas. Organizations vary widely in terms of their mission or industry sector, and which threats are of primary concern. Different industries face specific challenges in addition to more general threats. For example, financial service companies may be concerned about sophisticated cyber criminals, defense contractors may be concerned about APT and espionage, and hospitals may be concerned about breaches of personally identifiable information.

The size and relative maturity of each organization must also be considered with respect to their cyber defense operations. Cyber defense of any kind requires resources, and a small to mid-sized company cannot be expected to support an operational capability as robust as that of a large defense contractor or financial institution. Newer defense operations can experience a range of deployment challenges such as lack of experienced staff, incomplete sensor coverage, or inefficient communication channels with IT or business units.

CORA may be used for individual companies as well as for ISACs (sharing organizations). These two examples have different needs: unlike an individual organization, an ISAC has almost no assets to protect; alternatively, a company's role in sharing information is different from that of an ISAC's.

International and geographically dispersed operations also present unique challenges such as distributed groups that may span time zones and languages, different standard operating procedures, or NDAs that prevent full information disclosure. Remote workers may bring their systems to environments that are much less secure than they would be at a central office. BYOD (Bring Your Own Device) policies may reduce some IT costs, but can introduce new maintenance, configuration and security problems. CORA discovers the qualities of an organization that can be leveraged to promote cyber security, and also those that hinder these efforts.

Threat Awareness and Training

Cyber defense requires more than just technical defenses. It requires awareness of the threats an organization faces across the entire organization, from the entry-level up to the corporate officers.

Awareness of threats and risks at the leadership level is vital to garnering sufficient resources for technical defense and supporting policies. CORA measures the organization's current effort to instill a culture of security among all employees. Ideally, an organization identifies the importance of cyber defense and reinforces this culture with regular training, awareness campaigns, and a well-constructed and enforced policy.

User populations can vary in degree of sophistication. Policies and controls on user behavior can vary widely depending on industry or corporate culture.[2] [3] Employee awareness training programs for cyber threats are now commonplace in organizations of all kinds, whether through in-house efforts or consultancy. Studies have shown that threat education and security training for employees improves individual and enterprise security efforts.[4]

For cyber defenders, training is an important attribute of successful operations. Analysts are frequently trained to use a particular tool or technology but may not receive training about making the many judgments required to categorize, analyze and take action on a specific attack. This is a challenge often faced by organizations with a high turnover rate, where expertise may not be passed on to new analysts. In many organizations, jobs or functions can become stove-piped, with little understanding or visibility between processes. Business units and individuals under attack are not always informed of the nature of the threat or its impact, even when an incident has occurred.

Tools and Data Collection

CORA's second focus is on the technologies employed in defense, and in particular the cyber defender's ease in accessing, searching and processing relevant threat information.

Logs from firewalls, intrusion detection systems, and other common security technologies are important in analysis of attacks. Other logs, such as mail, DNS (Domain Name Service), and DHCP (Dynamic Host Control Protocol) are necessary for identifying targets of phishing attacks and accesses to known malicious sites. Not all organizations have the capability or need to collect all types of logs; CORA is designed to determine whether the right information is getting to the right people at the right time based on the organization's mission, threat profile, and resources.

Availability of logs can be a critical issue during incident response. Some organizations may outsource their email. The provider may not grant access to logs, or will do so only at additional expense. Even when an organization internally collects logs, accessibility may still be an issue if the logs are owned by an organizational unit under different leadership or with operating with different incentives. Moreover, incident discovery often takes significant time after an initial breach, and long-term storage of log data can become a strain on budget and resources.

Whatever logs are available for review, their level of searchability can present an additional challenge. Logs that are poorly indexed or scattered across a large number of servers can greatly delay response efforts. Ideally, logs are readily accessible to defenders, well-organized, collected in a timely fashion, and retained for sufficient time to enable historical review.

---

[2] United States Army. "Threat Awareness and Reporting Program." Army Regulation 381-12. October 4, 2010. http://www.apd.army.mil/pdffiles/r381_12.pdf (Accessed August 21, 2015).

[3] PCI Security Standards Council. "Information Supplement: Best Practices for Implementing a Security Awareness Program." October 2014. https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf (Accessed August 21, 2015).

[4] McCrohan, Kevin, Kathyrn Engel, and James Harvey. "Influence of Awareness and Training on Cyber Security." Journal of Internet Commerce, 9, 1, 2010. http://www.tandfonline.com/doi/abs/10.1080/15332861.2010.487415#.VdcgCrRhgfE (Accessed August 21, 2015).

Understanding and prioritizing security alerts can be difficult without proper context. This can include the type of attack, the vulnerability of the system to the attack, the business function and criticality of the system, or the role or job function of users associated with the attack.

User reporting can also be an important source of intelligence about attacks, particularly if the users have been trained to identify certain types of attacks (e.g., spear phishing) and are provided with a simple way to report the activity for further validation and investigation. User reported information can be entered into a database for storage and analysis by security staff.

Internal Processes and Collaboration

Cyber defensive operations include such elements as incident response, malware analysis, monitoring, intelligence analysis, as well as IT functions (e.g., patch management and network operations). Some functions have a tendency to be stove-piped or slower-moving than others, but it is critical for these elements to work well together. In the event of an attack, actions like the deployment of security patches may need to be accelerated. If an organization outsources certain functions, such as malware analysis or log collection, it can potentially lead to issues with communication, coordination, and availability of data.

Relationships between different functions or stakeholders can be inconsistent. Despite their related nature, IT and security departments prioritize differently and have their own budgetary and management concerns. It is not uncommon that the relationship between the two can become adversarial: IT may view security requests for logs or other actions as a burden, and cyber security may view IT as unresponsive to their requests.

Coordinating planning and scheduling is important within an organization. IT or business units can roll-out systems that tax resources for cyber defenders; security requirements can drive up costs for system development and maintenance.

CORA helps cyber defensive operations understand how to prioritize response activities as well as communicate effectively to management, user populations, and different business units.

Tracking and Analytics

Fusing both local and external knowledge can provide insight into which groups are targeting or actively attacking an organization. In addition, details of how cyber adversaries gain access, maintain a foothold, and which individuals or projects may be targeted can help to mitigate the threat these adversaries pose. Organizations use a variety of methods to track indicators and incidents, from ticketing systems and file-shares to wikis and dedicated intelligence databases.

Well-organized threat intelligence can aid and assist incident response by allowing responders to have a more complete understanding of the tactics, techniques, and procedures (TTPs) used by an attacker. Intelligence may be collected from different sources, some under the constraints of an NDA, so it is necessary to track the source of a given indicator to allow for appropriate sharing or restrictions on sharing. There has been a rise in organizations offering threat intelligence services for hire. It is not enough to simply subscribe to a feed and take its information as truth. Periodic assessment of the accuracy, relevance, and value for an organization of different intelligence sources is critical.

Analytics require staff with appropriate skills to identify exploit techniques, perform trending and analysis, tune sensors, attribute attacks to given groups, or to mine data for signs of new types of attacks. CORA points to an organization’s abilities to collect and leverage information towards defensive efforts. Reviewing sensors and tools, their use and maintenance, and the information they retain identifies potential room for growth in threat-oriented cyber defense.

External Engagement

There is great potential for collective benefit when organizations exchange threat intelligence. One company may observe an attack and notify other potential victims ahead of time. Another organization may have advanced malware or other analysis capabilities and can share new indicators that others may have missed. Companies likely employ different anti-malware or intrusion detection technology, thereby increasing the likelihood that an attacker will be detected by at least one of the complementary defenses. Collections of information about attacks against an industry can provide useful trending data or give insight into the motivations or even the identities of the attacking groups. These concepts were given credence recently in February 2015, when President Obama issued an executive order stressing the critical nature of cyber intelligence sharing as a component of national security.[5]

The increase of threat intelligence sharing among a variety of defender communities has shown to benefit many. Informal sharing has been a common practice via mailing lists and private communications. Formal arrangements, such as the Information Sharing and Analysis Centers (ISACs) that are organized by industry sector, and regional collaboratives, such as the Advanced Cyber Security Center (ACSC) and the Western Cyber Exchange, provide useful, trusted forums to exchange both threat intelligence and best practices.

Examples of actionable threat intelligence to share include, but are not limited to, IP addresses, URLs or malicious hosts, sender accounts of phishing emails, samples of malware used in attacks, and intrusion detection signatures. Such information, when it includes the necessary context, can be used to review logs for signs of attacks, place blocks in firewalls, or instrument sensors.

For these collaboratives to be effective, frequent and timely sharing of threat indicators by as many members as possible is desirable. The capabilities of information sharing entities varies widely within a threat sharing group. Larger, more mature member organizations often contribute the bulk of intelligence and smaller, less-mature member organizations are often more passive group participants. One of the goals of CORA is to identify ways for organizations to improve their participation in threat collaboratives, realizing that not all will have the resources necessary to be primary sources of information within the group. Five sharing roles are defined within the CORA methodology:

- Member: may develop situational awareness, but otherwise does not act on intel provided
- Checker: collects intel shared with the group, and checks their own systems, but does not report sightings / findings
- Reporter: checks their own networks, and reports back on sightings / findings
- Contributor: checks their own networks, but also contributes new threat indicators developed from their own analysis
- Leader: contributes new intelligence and advanced analysis, and mentors less mature organizations by providing best practices guidance

Given an organization's available resources, CORA helps to identify ways to promote engagement level, perhaps from Member to Checker, or Checker to Reporter. The interviews and feedback sessions can help identify impediments to this process. For example, Members may not have the resources for appropriate cyber defense, or may consider their intelligence not actionable, relevant, or valuable enough to be of a benefit to the group. Checkers may be unwilling to share information due to policy or legal concerns, lack of trust in the other members of the collective, find the reporting mechanism cumbersome, or perhaps lack an approved sharing process. Reporters may not have sufficiently trained staff or technical capabilities to generate new intelligence. Increasing participants' roles in collaborative groups could yield improved

[5] The White House. "Executive Order – Promoting Private Sector Cybersecurity Information Sharing." February 13, 2015. https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (Accessed August 21, 2015).

cyber defense throughout the group, and ultimately create more robust cyber defense across all sectors of the economy.

Conclusion

Transitioning from a cycle of incident detection/response towards a more preventative and threat-oriented posture requires transforming an organization's cyber defense efforts. This is not an easy task. Assessment methodologies are a good way to identify how the triad of people, processes and technologies can be improved towards this end. We have shown the benefits of CORA, an objective, rapid assessment methodology supported by interactive engagement with MITRE that emphasizes threat intelligence and information sharing.

Appendix

Mandiant RRA

Mandiant, a part of FireEye, Inc., has been a significant player in the IT security community for over a decade. Drawing upon this experience and expertise, Mandiant sells its "Response Readiness Assessment" (RRA) to organizations seeking metrics of their Security Operations Center (SOC) and incident response capabilities against known best practices. Through a combination of workshops (discussions and interviews), document review, and a table-top exercise to gather information, the approach gathers insights into six areas: regulatory compliance, organization, training of incident responders, incident detection, processes, and technology. This data is charted according to Mandiant's "Core Capability Model" of governance, communications, visibility, intelligence, response, and metrics. The client organization ultimately receives an assessment document, an incident response best practices overview, a briefing outlining the latest threats, another tabletop exercise, and list of key recommendations.

The RRA is tailored to organizations with significant financial resources and time. The process can take several months and can cost hundreds of thousands of dollars. It focuses on cyber incident detection and response efforts as opposed to prioritizing prevention. Since Mandiant is part of FireEye, a publically-traded company that sells cybersecurity goods and services, its recommendations come with significant bias.

See more at: https://dl.mandiant.com/EE/library/Mandiant_SecurityDefenseAssessment.pdf

Hewlett Packard SOMA

Since 2008, Hewlett Packard has worked with over 100 organizations with its "Security Operations Maturity Assessment" (SOMA). This sample set provides strong baseline data with which to compare new clients. Each assessment categorizes organization's operational processes from Level 1 ("Initial") to Level 5 ("Optimizing") and recommends that clients perform a SOMA regularly over the course of a few years to capture progress and identify any corrections. The assessment consists of a series of interviews, documentation review, discussions, and observations. Clients' analytical (e.g., incident management, intrusion analysis), technological (e.g., configuration management, system administration), operational (e.g., event management, training), and business processes (e.g., compliance, business continuity) across the security operations domain are scrutinized and reported on in the form of a report. This document includes key findings, recommendations, the maturity score, best practices, and a roadmap for maturity improvement.

SOMA's degree of rigor and investment is considerable (multiple days and significant cost). HP is heavily invested in various security operations tools (e.g., ArcSight, Fortify, TippingPoint, etc.), so it is in their interest to promote these as solutions. It does not emphasize threat analysis nor evaluate external engagement or information sharing.

See more at: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA4-4144ENW.pdf

Booz Allen Hamilton COMF

Booz Allen Hamilton has developed "Cyber Operations Maturity Framework" (COMF), a self-assessment, to help characterize an organization's cyber operational maturity. It builds upon key characteristics observed in successful operational responses to disasters in other domains, such as wildfires and infectious disease. The framework includes both a functional and a maturity model. Both record data against a set of eleven technical process areas before compiling them into two respective scores. Each level enumerates an expected set of capabilities for each process area. The overall

framework is intended as a starting point for self-assessment and improvement with the data gathering, analysis, and output is entirely left to the client organization itself.

COMF does not include a true methodology nor many detailed recommendations, but it does collect data on external collaboration. It is best characterized and used as a guidance document on which to generally critique organizations' cybersecurity posture.

See more at: http://www.boozallen.com/consulting/view-our-work/48383297/Collaborative-Cybersecurity-in-a-Connected-World

Department of Homeland Security CRR

The U.S. Department of Homeland Security (DHS) has adapted the Cyber Resilience Evaluation Method and the CERT Resilience Management Model (CERT-RMM) – developed by Carnegie Mellon's Software Engineering Institute – into a shorter, more focused cybersecurity assessment called the Cyber Resilience Review (CRR). The CRR reviews the protection and sustainment practices within ten domains and across four asset types:

> **Domains**: asset management, configuration and change management, risk management, controls management, vulnerability management, incident management, service continuity management, external dependencies management, training and awareness, and situational awareness
> **Assets**: people, information, technology, facilities

DHS characterizes the CRR as "designed to start a constructive dialogue…with the goal of cooperative improvement." DHS also notes that CRR is "NOT a control-based audit or technical evaluation of an organization's cyber security posture." The CRR is offered at no-cost to organizations within the 18 critical infrastructure sectors and to State, Local, Tribal, and Territorial governments (participation is voluntary). It is typically performed during a one-day, on-site structured facilitation and interview of key cyber security personnel. A questionnaire is the main tool used to capture results and insights. The CRR questionnaire asks detailed questions within each of the ten domains, and the responses – Yes, Incomplete, or No -- are answered for each of the four asset types, as applicable. Interviewees are also asked to cite evidence of cybersecurity practice execution and how these practices continue during an incident. The questionnaire answers are reviewed by DHS, and a maturity level is assigned for each domain and the organization as a whole. The report contains a summary of the effectiveness of the organization's cyber security management capabilities. Suggested actions and/or activities to raise the organization's and each domain's maturity are included. Participants receive a draft report within 45 calendar days, and then DHS then issues a final CRR Report. The CRR results are for organization use only; DHS does not share the results.

The CARR approach is process-oriented and does not delve deeply into the technical mechanics of cybersecurity capability execution. It is built around long-term organizational change over time. The CRR is not threat-oriented, focusing more on "incidents" (i.e., declaring them, responding to them, tracking them, etc.), as opposed to prevention efforts focusing on much smaller "indicators." It emphasizes the oversight of external dependencies but not the value of interactive engagement / information sharing.

See more at: https://www.us-cert.gov/ccubedvp/self-service-crr

CERT OCTAVE Allegro

CERT developed the "Operationally Critical Threat, Asset and Vulnerability Evaluation" (OCTAVE) approach. The most recently developed and actively supported version of the method is called OCTAVE Allegro, which is a self-directed way for organizations to assess their information security needs according to their own risk appetite, environment, and objectives. OCTAVE Allegro focuses on information assets, what security requirements they need, where they "live," and who "owns" them. The

overall process consists of four phases: developing risk criteria according to the unique profile of the organization, developing a profile of each information asset and its requirements/containers, identifying threats/risks to each asset in the context of its requirements/containers, and making decisions about risk management response to them (e.g., accept, transfer, mitigate, etc.). Ultimately, an organization will create a file of templates that can be continually added to as information assets are acquired, retired, etc. OCTAVE Allegro lacks any evaluation of information sharing or external engagement.

See more at: http://www.cert.org/resilience/products-services/octave/

FFIEC CAT

In response to the growing number and sophistication of cyber attacks against the financial sector, the Federal Financial Institutions Examination Council (FFIEC), which includes representatives from the Federal Reserve, FDIC, National Credit Union Administration, and other national groups with sector interest, developed the "Cybersecurity Assessment Tool" for its members as a means to strengthen their existing risk management processes and cybersecurity programs. Consistent with the NIST Cybersecurity Framework, the tool is meant to be used recurrently to inform decision makers about their organization's cyber risk and defensive posture on a continual basis. The assessment is made up of two parts: the first focuses on inherent risk before deploying controls/policies, and the second evaluates an organization's maturity level pertaining to cyber risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resilience. A score is assigned for each of these domains, but not for the organization as a whole. The assessment is overseen by management and the template is populated by employees so that managers can then interpret and evaluate the results.

The Cybersecurity Assessment Tool comes with no service or support from the FFIEC. It is not meant exclusively for financial sector firms but those that created it exclusively represent that sector.

See more at: https://www.ffiec.gov/cyberassessmenttool.htm

ISACA COBIT

ISACA's "Control Objectives for Information and related Technology" (COBIT) is an information technology (IT) governance product. It is an overarching framework designed to align IT with business goals, implement best practices, improve risk/resource management, and measure performance. It was originally influenced by Carnegie Mellon University Software Engineering Institute's Capability Maturity Model. Fundamentally, COBIT's purpose is to improve IT efficiency for business purposes and reduce operational risk. It is divided up into many purchasable products that range from $40-$120, with additional education/training available in online courses approximately $500. Once purchased, the framework is a self-directed assessment model, as organizations are expected to tailor it to their specific needs.

COBIT stresses IT risk from a business (i.e., cost) management perspective, as opposed to addressing it via a threat-oriented approach emphasizing security and information/intelligence sharing.

See more at: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

Other Assessments and Methodologies

Kroll Cyber Risk Assessment, http://www.kroll.com/en-us/cyber-security/data-breach-prevention/cyber-risk-assessments

Coalfire Cyber Risk and Controls Assessments, http://www.coalfire.com/Solutions/Cyber-Risk-Management/Risk-and-Controls-Assessment

DHS Cyber Security Evaluation Tool, https://ics-cert.us-cert.gov/Assessments

DHS Cybersecurity Assessment and Risk Management Approach, http://www.dhs.gov/sites/default/files/publications/DHS%20Industry%20Resources_0.pdf

CANSO Cyber Security and Risk Assessment Guide, https://www.canso.org/canso-cyber-security-and-risk-assessment-guide

SANS Baseline, Audit and Assess, Secure, Evaluate and Educate Assessment Methodology, http://www.sans.org/reading-room/whitepapers/auditing/base-security-assessment-methodology-1587

NetDiligence QuietAudit Cyber Risk Assessment, http://www.netdiligence.com/services.php

Quantitative Evaluation of Risk for Investment Efficient Strategies, http://www.securitymetrics.org/attachments/Metricon-3-Cybenko-Article.pdf