Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures

Branko Bokan
The George Washington University
Washington, DC, USA
brankobokan@gwu.edu

Joost Santos
The George Washington University
Washington, DC, USA
joost@gwu.edu

2021 Systems and Information Engineering Design Symposium (SIEDS) | 978-1-6654-1250-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/SIEDS52267.2021.9483736

***Abstract*—To manage limited resources available to protect against cybersecurity threats, organizations must use risk management approach to prioritize investments in protection capabilities. Currently, there is no commonly accepted methodology for cybersecurity professionals that considers one of the key elements of risk function – threat landscape – to identify gaps (blinds spots) where cybersecurity protections do not exist and where future investments are needed. This paper discusses a new, threat-based approach for evaluation of cybersecurity architectures that allows organizations to look at their cybersecurity protections from the standpoint of an adversary. The approach is based on a methodology developed by the Department of Defense and further expanded by the Department of Homeland Security. The threat-based approach uses a cyber threat framework to enumerate all threat actions previously observed in the wild and scores protections (cybersecurity architectural capabilities) against each threat action for their ability to: a) detect; b) protect against; and c) help in recovery from the threat action. The answers form a matrix called capability coverage map – a visual representation of protections coverage, gaps, and overlaps against threats. To allow for prioritization, threat actions can be organized in a threat heat map – a visual representation of threat actions' prevalence and maneuverability that can be overlaid on top of a coverage map. The paper demonstrates a new threat modeling methodology and recommends future research to establish a decision-making framework for designing cybersecurity architectures (capability portfolios) that maximize protections (described as coverage in terms of protect, detect, and respond functions) against known cybersecurity threats.**

Keywords—threat modeling, cybersecurity architecture, cybersecurity capabilities, assessment, evaluation, cyber threat framework, risk, risk management

I. INTRODUCTION

A. Overview

Traditionally, organizations managed cybersecurity efforts and made decisions on which cybersecurity protections to deploy on their networks based on compliance standards, regulatory requirements, and by following the "best practices". This is frequently considered a "checklist approach" that does not result in cybersecurity architectures that protect against actual threats observed in the wild. Furthermore, no organization has unlimited resources to deploy every available technology, so they must resort to a risk-based prioritization approach. To date, no commonly accepted methodology exists to allow organizations to look at actual threats and determine what kind of protection their cybersecurity architectures provide and where gaps exist.

Anecdotally, decision makers, such as chief information security officers (CISOs), admit that most of their decisions on investments in cyber protections are driven by vendor recommendations and marketing pressure rather than by well-established risk management practices. The threat based approach to analysis of cybersecurity architectural protections allows organizations to incorporate the threat element in their risk management processes and make cybersecurity investment decisions informed by actual cybersecurity threats they are facing. Hence, there is an urgent need for a paradigm shift where organizations can look at their cybersecurity protections from the standpoint of an adversary to make threat informed risk decisions.

B. Problem Statement

The term "risk" is defined as a function of a security event or scenario (threat exploiting a vulnerability), the probability of the event taking place, and the consequence of the event taking place [1]. To fully exercise risk management practices, organizations need to factor in and consider all of these key risk factors. No well documented and accepted methodology previously existed to allow for proper consideration of the threat factor in making risk management decisions – specifically risk based decisions on investments in cybersecurity protections. This resulted in inadequate protections applied to organizational infrastructure, protection "blind spots", and wasted limited resources on protections that do not cover the actual threats organizations are facing or multiple protections covering the same limited threats.

The threat based approach to evaluation of cybersecurity protections – formally defined as architectural cybersecurity capabilities – allows us to determine the best protection coverage against the actual cybersecurity threats that exist in the wild. This is achieved by determining coverage of existing protections, identifying gaps (where threats without adequate protections exist), and overlaps (areas where multiple protections protect against the same types of threats thus unnecessarily multiplying costs).

C. Organization of the Paper

There are five sections in this paper. Section I discusses the problem organizations face when deciding which tools to select

XXX-X-XXXX-XXXX-X/XX/$XX.00©20XX IEEE
978-1-6654-1250-6/21/$31.00 ©2021 IEEE

for best protection against cybersecurity threats, and provides an overview of the paper. Section II discusses the concepts of risk and discusses the key factors in cyber risk management. Section III describes a novel approach to threat modeling – threat-based approach to evaluation of cybersecurity architectures and associated protections. Section IV demonstrates the use of the methodology in selection of the best cybersecurity protections for mobile infrastructure. Finally, Section V provides recommendations for future research.

D. Scope and Limitations

While the common language to describe adversarial activities through attack stages, objectives, and associated threat actions is well defined and accepted in the cybersecurity industry through the use of cyber threat frameworks (CTF), cybersecurity technology categories are not standardized and differ widely from one vendor to another. In an ever-growing industry with a large number of vendors and their portfolios of cybersecurity technologies, organizations have thousands of cybersecurity products to choose from. In 2018, there were more than 1,200 cybersecurity vendors with approximately 6,000 products and more than 20,000 features [2]. While ideally, we would like this research to cover all individual products, including different product models (e.g. Cisco ASA 5520 vs Cisco ASA 5550), a simple enumeration of the landscape would require tremendous resources and effort. To make the research manageable, this paper will focus on the major cybersecurity technology categories defined in Gartner's Magic Quadrant and Critical Capabilities [3].

II. REVIEW OF RELEVANT RISK CONCEPTS

This section provides an overview of the critical writings on cybersecurity risk and risk management, and discusses the lack of a common methodology to consider one of the key factors in risk function – threat, for mitigations using cybersecurity protections.

A. Risk

While the concept of risk and associated assessment and management activities in every-day life is seemingly easy to understand, the same does not translate to complex information systems and organizations. In everyday life, an average human makes hundreds of risk determinations and risk-based decisions on a daily basis. From the moment we wake up and check the weather forecast for the likelihood of precipitation to determine what to wear and whether or not to carry an umbrella, to the act of looking for oncoming traffic before crossing the street – we are constantly, although not always consciously, determining the risks of various actions and making appropriate risk decisions to mitigate possible negative outcomes.

Scholars traced the elements of risk analysis in the activities of the Asibu people who lived in the Tigris-Euphrates valley around 3200 B.C. [8]. The first reported use of the term risk in the English language dates back to early 1650 at which time it was defined as "the possibility of loss or injury". The word itself stems from the French *risque*, and Italian *risco*. [9]. Most scholarly articles on the topic date to the late 1960 onwards, and to this day, there is no commonly agreed-upon definition of the concept of risk. Definitions range from equating risk with uncertainty through the potential of loss, to a consequence of an activity associated with uncertainties [10]. In its widely used glossary, the Society for Risk Analysis provides seven qualitative definitions of the concept [7]. The definition provided by Kaplan and Garrick [1] more than 40 years ago, most closely aligns with the understanding of risk as it is understood in cybersecurity. It introduces the idea of the 'set of triples' that constitute risk: a scenario, the probability (or uncertainty to be more precise) of the scenario taking place, and the consequence of the scenario taking place. The risk is described by answers to the following three questions: a) what can happen, b) what is the likelihood that it will happen, and c) if it does happen, what are the consequences [1].

B. Risk in Cybersecurity

Applying the same principles at a higher level of abstraction, away from a single event toward the concept of risk in organizations and associated information systems, rapidly proves to be unattainable. This is mainly due to complexities associated with individual information systems that are forever multiplying as they become interconnected and interdependent as organizations grow. Uncertainty in computer software alone is known to be greater than in any other field [11]. One of the foundational articles that establishes the risk management process in federal organizations and is frequently used in other industries – Special Publication 800-39: Managing Information Security Risk - Organization, Mission, and Information System View [5] – recognizes the complexity of the problem in organizations of any size and recommends a tiered approach starting with the organization at the top. Unfortunately, it stops at the single information system level. Interestingly, this publication does not even attempt to define or explain the concept of risk and only provides a reference in the appendix (page B-7) to the Committee on National Security Systems Glossary [12] which in turn references the Federal Information Processing Standards Publication (FIPS) 200 [13]. FIPS defines risk as "[t]he level of impact on organizational operations […], organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring." Compared to Kaplan's definition [1], the scenario aligns with the occurrence of a specific threat, the probability aligns with likelihood, and the consequence is represented by the potential impact.

One way to describe the discipline of cybersecurity is through a series of well-defined core functions of cybersecurity: identify, protect, detect, respond, and recover [4]. The key to carrying out these functions is the ability for those who practice the discipline to understand risks to information systems on which organizations depend to deliver their mission; and to make appropriate decisions to respond and mitigate negative outcomes by carrying out risk management activities. The National Institute of Standards and Technology (NIST) identifies four components of a comprehensive process that constitute cybersecurity risk management: frame, assess, respond, and monitor [5]. The term risk management may have different meanings in different industries or in academia – as it is sometimes used to describe the entire set of activities associated with

understanding and responding to risk. At other times, it only captures the activities associated with responding to a specific scenario (e.g. what can be done to mitigate or remediate identified risk) [6]. The Society for Risk Analysis Glossary uses the term *risk analysis* to describe activities associated with risk assessment characterization, management and policy [7]. Some authors use the terms *risk analysis* and *risk assessment* interchangeably while others use them concurrently without defining their meaning.

To avoid these ambiguities, this paper will use the corresponding terms as follows:

Risk management will be used to capture all activities associated with identifying, responding to, and monitoring risk. This is in line with the terms used by NIST [5] and corresponds to the term *risk analysis* as defined by SRA [7]. This term has a different meaning in SRA [7] and Haimes [6], where it is used to describe activities limited to risk mitigation and remediation (see *managing risk* below).

Defining risk describes the set of activities aimed at understanding risk and related concepts, and how they apply to a particular organization or a system at hand. The term aligns with NIST's definition [5] of *framing risk*, and SRA's [7] terms – *risk framing*, *risk description*, and *pre-assessment*. This stage also aligns with *risk analysis* activities as defined by Kaplan [1].

Risk assessment is the most consistently used and understood term, and most authors seem to agree with its meaning. The only exception is when the term is used interchangeably with *risk analysis.*

Managing risk or *risk response* describes the mitigation and remediation activities captured under *respond to risk* and *monitor risk* in NIST terminology, and *risk management* as used by SRA [7] and Haimes [6].

C. Risk Assessment

The risk assessment method allows decisionmakers to enumerate and prioritize risks in order to make informed risk response decisions. The method identifies specific threat sources and threat events the sources could produce, identifies vulnerabilities that could be exploited by those sources, determines the likelihood of their exploitation, and determines potential adverse impact. In the final step, the risk is calculated as a function of likelihood of vulnerability being exploited by a threat (scenario) and the impact of the exploitation [14].

D. Risk Response (Managing Risk)

Haimes [6] follows up on the works for Kaplan and Garrick, and expands the original three questions used to assess the risk, and introduces three additional questions to help guide risk response: a) What can be done?; b) What options are available and what are their associated trade-offs in terms of all costs, benefits, and risks?; and c) What are the impacts of current management decisions on future options?

The options for *what can be done* generally fall into one of five major risk response strategies: accept, avoid, mitigate, share, and transfer [15]. Accepting the risk is frequently associated with not doing anything (i.e. inactivity) but is also the one used after other strategies are applied to deal with the residual risk. Risk avoidance strategy involves completely removing the scenario as an option and this usually translates to abandoning all activities associated with the risk in the first place (e.g. getting out of risky business). Risk mitigation involves activities that lead to the reduction of either the likelihood or the consequence of the scenario. In cybersecurity these activities may include implementation of countermeasures or controls such as deployment of cybersecurity protections, policies, or reduction of the attack vector (e.g. by applying patches to vulnerable software). Sharing and transfer of risk are usually associated with purchasing insurance or other ways where third party organizations get involved.

E. Cybersecurity Threats

To fully understand the previously provided definition of risk, it is important to define the meaning of the term *threat* in cybersecurity context. The Committee on National Security Systems Glossary defines *threat* as "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" [12].

F. Cybersecurity Vulnerabilities

Complementing threats is the concept of vulnerabilities – both are necessary for an event or a scenario to occur (a threat needs to exist for a vulnerability to be exploited). According to the same source, a vulnerability is defined as a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source" [12].

III. METHODOLOGY

Threat modeling is a structured process for enumeration, analysis, and prioritization of threats to, and vulnerabilities in, an information system [16]. The results of such a process can inform decisions on which threats and vulnerabilities are associated with the highest risk and need to be addressed first. Generally, this can be accomplished from two different perspectives: from the perspective of an asset (something we are trying to protect), which can include the information system and associated software itself; and from the perspective of an attacker (thinking like an adversary) [16].

The first attempts to formalize the process for information systems can be traced back to the works of the Department of Defense in the late 1970s and early 1980s. One of the earliest dynamic threat analysis models was developed by ATT&T for the Strategic Defense Initiative as Security Vulnerability Analysis (SVA) for System Security Engineering (SSE) process. The process was designed to allow for a structured enumeration of system security requirements through a ten-step process. [17]. One of the "signatures" of this model is the use of "threat logic trees" for threat decomposition.

The next significant contribution to the development of threat modeling methodology was developed by a group of

authors led by Bruce Schneier and based on research sponsored by the National Security Agency [18]. The methodology introduced the way to enumerate and visually represent possible attacks (threat actions) and weigh them based on the risk, access, and cost to the adversary

The STRIDE threat modeling methodology was developed by Microsoft Corporation in 1999 and named after major categories of threats occurring in the wild [19]. The STRIDE methodology simplifies the task of enumerating possible threats and vulnerabilities in an information system and assists security engineers by grouping known threats into six categories and describing various products and services each category applies to [19]. The methodology is applied by deconstructing a system under consideration into components, analyzing each component for susceptibility to threats in each category to discover associated vulnerabilities and develop appropriate threat mitigation measures [20].

To date, STRIDE remains the most mature threat modeling methodology and is a part of Microsoft's security development lifecycle (SDL) [21]. It serves as a foundation for similar threat modeling methodology such as DESIST, developed by Gunnar Peterson and named for Dispute, Elevation of privileges, Spoofing, Information disclosure, Service denial, and Tempering [16].

The Process for Attack Simulation and Threat Analysis or PASTA for short, is a relatively new approach to threat modeling developed in the last 5-10 years. The major differentiator from other approaches is PASTA's focus on business objectives as drivers for both information system requirements and associated security responses. The premise behind the business objectives focus is that organizations in different industries face different types of threats and therefore only those impacting the organization should be mitigated [22].

A. *Cybersecurity Architecture Review*

In 2015, the Department of Defense (DOD) developed a methodology called NIPRNet SIPRNet Cyber Security Architecture Review (NSCSAR) (later renamed to DoDCAR) that allowed them to introduce the consideration of threat as a factor into their risk management process and, for the first time, look at the cybersecurity architectural capabilities and their ability to protect against the actual threats from the standpoint of an adversary. Today, the methodology is widely used by DoD to evaluate the threat landscape, identify gaps where protections do not exist but are necessary to inform the future investments into new protections, or to identify protection overlaps to inform decisions to retire redundant protections (e.g. two or more different products serving the same purpose and protecting against the same type of threat). The Department of Homeland Security later adopted and further expanded the methodology under the name .govCAR for use by the Federal Civilian Executive Branch agencies, other levels of government (state, local tribal, and territorial), and the public sector [23].

Stage	Engagement								
Objective	Delivery								
Threat action	Inject database command			Leverage device swapping			Send malicious email		
Function	Protect	Detect	Respond	Protect	Detect	Respond	Protect	Detect	Respond
Capabilities									
Features									
Firewall	M	M	M	L	None	L	L	L	L
GeoIP Blocking	L	None	L	L	None	L	L	L	L
Application Filtering	M	M	M	L	None	L	L	L	L
Protocol Port Enforcement	L	L	M	L	None	L	L	L	L

Fig. 1 - An excerpt from a sample scoring matrix showing scores for one capability (firewall) and its three features against three threat actions (Inject, Leverage, Send) in Delivery objective of the Engagement stage.

B. *Cyber Threat Framework*

The threat based approach to evaluation of cybersecurity architecture starts with a cyber threat framework (CTF), as a way to enumerate stages and objectives of an attack, and associated threat actions that have been actually observed in the wild as executed by adversaries. CTF allows cybersecurity engineers to enumerate all possible threat actions and create a common language to describe adversarial activities.

Several slightly different CTFs currently exist and are in use by various organizations. The most common ones include MITRE ATT&CK [24], Lockheed Martin's Kill Chain [25], and National Security Agency's (NSA/CSS Technical Cyber Threat Framework – NTCTF) v2.0 [26]. What all these frameworks have in common is that they identify all different threat actions (sometimes called tactics, techniques, and protocols or TTPs) carried out by the adversaries in known cyber-attacks and incidents observed in the wild. In NTCTF 2.0, threat actions are grouped by objectives (what is the adversary trying to achieve), and stages of attack at the top level. The resulting inventory is presented as a matrix – with stages at the very top, objectives under each stage, and threat actions under each objective at the bottom. For example, *Using Social Media* to find information about a target is a threat action, under the *Reconnaissance* objective, that takes place during the attack *Preparation* phase. NTCTF v2.0 breaks down into six phases: Administration, Preparation, Engagement, Presence, Effect, and Ongoing process. Each phase breaks down into two to five objectives – 21 in total. Each objective can contain between two and twenty-one threat actions resulting in 186 individual threat actions.

C. *Cybersecurity Capabilities, Flows, and Topologies*

In the next step of threat modeling, we identify target cybersecurity architectures for review. This step includes identifying the building blocks of the architecture: cybersecurity capabilities (generally referred to as protections in this paper), their topologies (e.g. positions on the network), and network flows that are routed through those capabilities. The capabilities are representations of vendor-agnostic cybersecurity tools at an architectural level (e.g. the methodology uses generic capabilities such as firewall instead of a particular implementation such as CISCO ASA 5550).

NIST defines capability as a "combination of mutually reinforcing controls implemented by technical means, physical means, and procedural means […] typically selected to achieve a common information security or privacy purpose" [15]. Most frequently, capabilities represent technologies such as firewall or antivirus software, but they can also represent non-materiel capabilities such as policies or other management controls.

D. *Coverage Scoring and Analysis*

Once the threat actions are enumerated and cybersecurity architectures are defined, they are arranged into a matrix, with

actions listed at the top as column headers and architectural capabilities on the left as row titles (Fig. 1). If desired, capabilities can be further broken down into features (e.g. firewall capability can be broken down into GeoIP blocking, application filtering, protocol port enforcement, etc.) [23].

Each architectural capability is scored for its ability to protect, detect, and respond to each threat action by answering the following questions at intersections of threat actions and corresponding capabilities (or features): a) can this capability (or feature) detect this threat action?; b) can this capability protect against this threat action?; and c) can this capability help in recovery against this threat action? The answers can be binary (e.g. yes or no) or they can be ranked on a scale (e.g. some, moderate, or significant coverage). The questions are aligned with three out of five functions of NIST cybersecurity framework (CSF – not to be confused with CTF) developed to provide a common language for describing cybersecurity risk among stakeholders. At the highest level, CSF is organized into five functions – Identify, Protect, Detect, Respond, and Recover – that also align with methodologies for incident management [4].

DHS tailored the NIST CSF definitions further to avoid ambiguity between functions and currently only uses Protect, Detect, and Respond in .govCAR analysis [23]: The *Protect function* represents active measures with or without detection abilities that support the ability to limit or contain the impact of a threat action in cyber relevant time. The *Detect function* enables discovery of threat actions in cyber relevant time and require at least one sensor and an analytic function that operates on that sensor produced data. The *Respond function* provides data that support activities that occur after the threat actions have executed, including mitigation of the threat action or triggering further sensor data collection and analysis.

The three functions are not mutually exclusive – a capability may be able to protect against a particular threat action but may not be able to detect or respond to the same threat action at the same time. For example, a firewall that is configured to block (drop) all incoming traffic on port TCP/UDP:53 (a port typically reserved for standard DNS protocol) will mitigate (protect) against a threat action coming through this port, but will no longer be able to detect nor log the malicious activity associated with that threat action due to the traffic being dropped before any action is taken. Similarly, an intrusion detection system (IDS) configured to alert on a particular activity on the same port may be able to detect and respond, but not protect against the associated threat action in cyber-relevant time.

The answers to scoring questions are entered into the matrix and the results form a capability coverage map – a visual representation of capability coverage, gaps, and overlaps against the threats. Coverage maps for multiple capabilities can then be combined by overlaying them on top of each other to demonstrate the coverage of the entire organizational defense in depth architecture.

To allow for prioritization and better understanding of threat actions, they can be examined based on their prevalence (frequency of occurrence in the wild) and maneuverability (the number of different threat actions that can be used to achieve the same objective) to develop a threat heat map – a visual representation of threat actions based on their priority. The heat map can be overlaid on top of any coverage map to prioritize future protections focus.

IV. Proof of Concept

A. Mobile Protections

In this section, we look at the analysis of the three most common mobile cybersecurity capabilities and their coverage visually represented through a series of coverage maps for protect, detect, and respond cybersecurity functions derived using the methodology described in Section III METHODOLOGY. The scores mapped to a visual representation of CTF were provided in .govCAR Recommendations for Mobile Cybersecurity [27].

In this example three mobile capabilities are considered:

Enterprise Mobility Management (EMM), with three core functions: Mobile Device Management (MDM) for management of policy and configuration of mobile devices; Mobile Application Management (MAM) for management of application configuration on mobile devices; and Mobile Identity Management (MIM) for management of authentication and access to devices.

Mobile Threat Defense (MTD): signature based anti-malware, anomaly detection, and device and application monitoring.

Mobile Application Vetting (MAV): detects anomalies in mobile applications and prevents deployment; requires analysis of mobile applications prior to deployment.

Finally, scores for all three capabilities were stacked up on a single visual coverage map to show combined overlay coverage (capturing the highest score for each protect, detect, and respond function). Fig. 1 shows two coverage maps – on the right is a coverage map for standalone EMM and on the left is a coverage map for EMM, MTD, and MAV integrated together. Each cell represents an individual mobile threat action organized by columns that represent threat *Objectives* and *Stages* of an attack the threat actions belong to (Objectives and Stages not applicable to mobile architecture were omitted). The coverage levels were color coded and range from gray (for no coverage at all – none and n/a), red for limited, yellow for moderate, to green for significant coverage. Narrative descriptions were intentionally omitted to highlight the visual impact of coverage maps.

The same method could be used to combine any number of capabilities and demonstrate how additions and removals of those capabilities to and from an architecture affect overall coverage.

B. Analysis

A visual inspection of coverage maps (Fig. 2), indicates limited ability to protect from, detect, or respond to threat actions for each individual mobile cybersecurity capability on the left. But when three capabilities are integrated together (overlaid on top of each other on the right coverage map) we see significant impact of defense in depth strategy where three capabilities with relatively small individual coverage increase

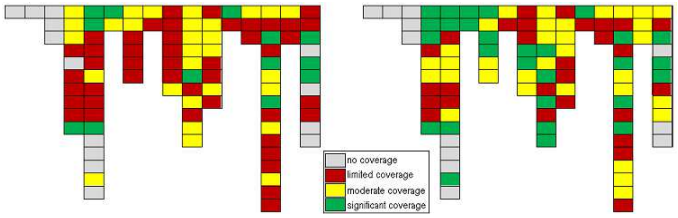

Fig. 2 – Coverage maps for standalone EMM capability (left) vs. integrated EMM, MTD, and MAC capabilities (right) show how coverage of threat actions improves with integration of multiple capabilities.

the overall coverage across all but few stages of the attack. In Fig 2., the coverage map on the right shows a number of red boxes representing threat actions with limited protection coverage for mobile architecture with only EMM deployed. However, when EMM is integrated with MTD and MAV, the overall colors change to green indicating significant increase in protection against known mobile threats.

It is also interesting to note that none of the sample cybersecurity capabilities have coverage in the first three stages.

Using this approach, additional capabilities can be added or removed from coverage maps to determine how modifications of an enterprise architectural capabilities affect overall coverage.

V. AREAS FOR FUTURE RESEARCH

The threat-based methodology discussed in this paper provides a powerful tool for senior executives to inform risk management decisions and align cybersecurity protections with real threats facing organizations. Future research is necessary in order to develop a decision-making framework for enhancing cybersecurity capability portfolios to maximize protect, detect, and respond coverage against the current cybersecurity threat actions.

Additional research is also recommended to determine the following: how common cybersecurity capabilities cover protect, detect, and respond functions against known cybersecurity threats; identify if organizations are using the most efficient portfolio of cybersecurity capabilities to provide the highest protect/detect/respond coverage against actual cybersecurity threats; how different demographics or industries perceive capability coverage in their organizations; and to what extend capabilities deployed in organizations overlap.

REFERENCES

[1] S. Kaplan and B. J. Garrick, "On the Quantitative Definition of Risk," Society for Risk Analysis, pp. 11-27, 1981.
[2] N. Miller, "With More Than 1,200 Cybersecurity Vendors in the Industry, How Do You Stand Out?," 8 May 2018. [Online]. Available: https://www.mcafee.com/blogs/enterprise/with-more-than-1200-cybersecurity-vendors-in-the-industry-how-do-you-stand-out/.
[3] Gartner, "Gartner Magic Quadrant & Critical Capabilities," 13 May 2020. [Online]. Available: https://www.gartner.com/en/research/magic-quadrant.
[4] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," Gaithersburg, 2018.
[5] National Institute of Standards and Technology, "Special Publication 800-39: Managing Information Security Risk - Organization, Mission, and Information System View," Gaithersburg, 2011.
[6] Y. Y. Haimes, "Total Risk Management," Risk Analysis, pp. 169-171, 1991.
[7] T. Aven, "Society for Risk Analysis Glossary," August 2018. [Online]. Available: https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf.
[8] V. T. Covello and J. Mumpower, "Risk Analysis and Risk Management: An Historical Perspective," Risk Analysis, pp. 103-120, 1985.
[9] "Merriam Webster," 11 November 2020. [Online]. Available: merriam-webster.com/dictionary/risk.
[10] T. Aven, "The risk concept—historical and recent development trends," Reliability Engineering & System Safety, pp. 33-34, 2012.
[11] Y. Y. Haimes, Risk Modeling, Assessment, and Management, John Wiley & Sons, Incorporated, 2004.
[12] Committee on National Security Systems Glossary, "CNSSI-4009 Committee on National Security Systems Glossary," Ft. Meade, 2015.
[13] National Institute of Standards and Technology, "Federal Information Processing Standards Publication (FIPS 200): Minimum Security Requirements for Federal Information and Information Systems," Gaithersburg, 2006.
[14] National Institute of Standards and Technology, "Special Publication 800-30: Guide for Conducting Risk Assessments Revision 1," Gaithersburg, 2012.
[15] National Institute of Standards and Technology, "Risk Management Framework for Information Systems and Organizations - A system Life Cycle Approach for Security and Privacy NIST SP 800-37 Revision 2," Gaithersburg, 2018.
[16] A. Shostack, Threat Modeling: Designing for Security, Germany: Wiley, 2014.
[17] J. D. Weiss, "A System Security Engineering Process," in 14th National Computer Security Conference - Information Systems Security: Requirements and Practices , Washington, DC, 1991.
[18] B. Schneier, C. Salter, S. Saydjari and J. Wallner, "Toward a secure system engineering methodology," in 7th New Security Paradigms Workshop Proceedings, CHARLOTTESVILLE, VA, 1999.
[19] L. Kohnfelder and P. Garg , "The threats to our products," April 1999. [Online]. Available: https://cloudblogs.microsoft.com/microsoftsecure/2009/08/27/the-threats-to-our-products/.
[20] S. Hernan, S. Lambert, T. Ostwald and A. Shostack, "Uncover Security Design Flaws Using The STRIDE Approach," MSDN Magazine - The Microsoft Journal for Developers, 2006.
[21] N. Shevchenko, "Threat Modeling: 12 Available Methods," 3 December 2018. [Online]. Available: https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html.
[22] Versprite, "PASTA Threat Modeling," 1 December 2020. [Online]. Available: https://versprite.com/tag/pasta-threat-modeling/.
[23] The Department of Homeland Security, ".gov Cybersecurity Architecture Review (.govCAR) Methodology," Washington, 2018.
[24] The MITRE Corporation, "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)," 17 February 2019. [Online]. Available: https://attack.mitre.org/.
[25] Lockheed Martin Corporation, "The Cyber Kill Chain," 17 February 2020. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html .
[26] National Security Agency, "NSA/CSS Technical Cyber Threat Framework v2," National Security Agency, Washington, 2018.
[27] The Department of Homeland Security, ".govCAR Recommendations: MOBILE SECURITY," The Department of Homeland Security, Washington, DC, 2019.
[28] DigitalGuiardian, "Information Security Industryscape," 17 July 2017. [Online]. Available: https://digitalguardian.com/blog/information-security-industryscape.