The Future of Cybersecurity Assessments Is Here

Security assessments have traditionally relied on point-in-time snapshots of an organization's security program driven by the perceptions of information security and IT teams. The focus of today's security assessments is often achieving compliance with an alphabet soup of industry standards rather than determining the evolving nature and impact of potential threats to an organization. Traditional assessments may not provide a complete picture of an organization's risk profile, which could lead to a false sense of security. Thus, the need of the hour is to adopt a risk-prioritized, data-driven approach to conducting assessments that considers an organization's threat landscape and attack surface in near real time.

Data-driven security assessments (DSAs) are the next generation of cybersecurity assessments that organizations need to adopt to augment their traditional security assessments. There are various DSA approaches that organizations can adopt based on their size, operating industry, crown jewels and threat landscape. Information security leaders should employ step-by-step methodologies to aid their journeys in this new era of security assessments.

Traditional Security Assessments

Modern organizations grapple with the growing number and sophistication of threats, including the emergence of tactics based on artificial intelligence (AI) and swiftly evolving malicious software. Most enterprises perform security assessments to help qualitatively analyze their cybersecurity programs compared to leading industry standards and practices. Based on the results, an organization can remediate the loopholes in its cybersecurity program to prevent any financial, operational or reputational damage. However, even though these traditional assessments help organizations identify and resolve inherent security weaknesses, they do not necessarily identify dynamically evolving risk.

KARTHIK SRIDHARAN | AWS CERTIFIED CLOUD PRACTITIONER, ISO/IEC 27001:2013 LA

Is a cybersecurity consultant for the cyberstrategy and transformation practice at Optiv and has more than six years of experience in the cybersecurity industry. He has primarily worked on building cloud security strategies across industries and conducting cybersecurity assessments aligned with data privacy and protection standards and regulations. He has also provided cybersecurity support for divestitures for a global technology enterprise.

JYOTHSNA CHALASANI | CISA, CISSP

Is a cybersecurity leader delivering security strategy, transformation, and implementation advisory services and solutions to clients across a broad spectrum of industries. She is a manager at Optiv and has more than 10 years of experience providing strategy and advisory services to Fortune 500 and leading global organizations, helping them build security programs and enhance their security postures through tailored strategy solutions. Chalasani brings extensive industry experience in security areas such as risk management, strategy and program development, governance and operating model restructuring, policies and standard development, and metrics program build-outs.

PRADEEP SEKAR | AWS CERTIFIED SECURITY SPECIALTY, CCSP, CISSP, PMP

Is an experienced cybersecurity leader who has worked closely with Fortune 100 and Fortune 500 chief information security officers, chief information officers and their teams across various industries on developing and sustaining secure, adaptive and robust cybersecurity programs. His unique expertise includes the delivery of innovative cyberstrategy solutions and benchmarking insights for global organizations as they look to transform their cyber programs. As a managing director at Optiv, Sekar leads the cyberstrategy and transformation team in India and is the service-offering leader for portfolio assessments and security in mergers, acquisitions and divestitures.

Challenges With Traditional Assessments

Traditional security assessments make it difficult for organizations to keep pace with change in the modern business environment where new threats and vulnerabilities are constantly emerging. Challenges that limit an organization from conducting thorough and effective assessments using the traditional approach include:

- **Economy at the expense of accuracy**—Traditional assessments are the preferred form of assessment for most organizations because of their cost-effectiveness. Traditional assessments rely on documentation reviews and stakeholder interviews for the identification of gaps in an organization's security program. Despite this being an effective and economical method for evaluating an organization's security efforts and preventing the reoccurrence of incidents, the findings of these assessments may not always be current because they are conducted at a point in time and not in real time.
- **Proactive detection and prevention**—Traditional assessments are based on a singular premise and are typically static or unchanging, which makes it easy to measure the performance and security posture of an organization over a period by comparing the results of subsequent assessments. It helps to conduct an assessment immediately after the organization has faced an incident to gather and assess what went wrong and to remediate any gaps. However, this assessment does not provide meaningful insights that enable an organization to proactively detect and prevent incidents before they occur; nor does it consider the various situations under which risk could materialize into events or incidents.
- **Variability based on the assessor's judgment**—In traditional assessments, an assessor plays an integral part in developing the outline of the assessment, conducting interviews, and identifying and reporting findings and recommendations. The approach of the assessment may vary based on the assessor. Methods of observing and interpreting the findings are influenced by many situational and personal characteristics, which makes assessors susceptible to many types of conscious or unconscious biases.
- **Changes in business context**—Traditional assessments are generally driven by a hypothesis, which provides a methodology for organizations that have not determined where they want to begin assessing. Although this approach provides organizations with a basis for their assessments and identifying the scope, the same hypothesis may not be relevant to every industry and in every business context. Therefore, organizations must adapt to changes in their business context and tailor their assessment approaches and methodologies to fit their needs. Traditional assessments often lack this flexibility.

Enhancing the Effectiveness of Security Assessments

In general, most organizations want to leverage assessments to answer questions to ensure that their efforts are effective and are expended in a way that is beneficial to them:

- What are the most significant cybersecurity threats right now?
- What kind of cybersecurity assessment would best suit this organization considering the evolving threat landscape?
- Should the assessment be focused on the enterprise as a whole or an specific business units that need special attention due to the nature of operations?
- Does the assessment include the elements of people, processes and technology related to both internal and external parties such as suppliers, partners or vendors?
- Should this organization perform a qualitative assessment or a quantitative assessment?

Answering these questions requires an approach that tailors security controls based on an organization's unique risk. To gather insights into their organization's security posture, security leaders must integrate today's qualitative maturity assessments with appropriate quantitative assessment methods. Although the data generated from an organization's security capabilities are some of the most valuable resources to achieve this goal, many enterprises cannot effectively manage these data because they lack formalized processes.[1]

Organizations typically deploy network monitoring, user access management and other infrastructure monitoring capabilities through solutions such as security information and event management (SIEM) systems and security operations centers (SOCs). The data these solutions collect can inform qualitative assessment findings and help establish a real-time understanding of prevalent threats and risk, driving objective security decisions. Of late, organizations are shifting the focus to DSAs because they provide greater confidence in making effectual business decisions and implementing intuitive solutions.[2]

> A DSA is a forward-looking exercise that leverages data points from multiple sources to provide a nearly real-time view of risk factors across an organization's crucial assets.

A DSA is a forward-looking exercise that leverages data points from multiple sources to provide a nearly real-time view of risk factors across an organization's crucial assets. Depending on the organization's size, security mechanisms and the amount of data it ingests daily, sources can include databases, network traffic flows, vulnerability scans, and log files from perimeter devices, access, changes, events, activity, proxies, errors and agents.[3]

Consider a healthcare organization that recently suffered a data breach and failed to safeguard its patients' protected health information (PHI), despite being compliant with the US Health Insurance Portability and Accountability Act (HIPAA). A root cause analysis showed that the email server was misconfigured, leaving sensitive data exposed. This incident could have been prevented had the organization leveraged a DSA technique, such as using a breach and attack simulation (BAS) to test its email server security and measuring the exposure factor on a continual basis.[4]

Types of DSAs

DSAs can be performed using various methodologies, but most of them align their results with industry frameworks that define adversary behavior. For instance, the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework is an open-source knowledge base that defines tactics, techniques and procedures (TTP) used by threat actors and is based on real-world observations.[5] By aligning the results of DSAs with the MITRE framework, organizations can prioritize and map individual threat techniques into a centralized view and better allocate resources to enhance their security posture.

Organizations can choose the type of DSA to perform based on the size of their business, risk appetite and attack surface. Prominent DSA types include:

- **Vulnerability assessment and penetration testing (VAPT)**—VAPT helps organizations identify any open ports and vulnerabilities (both internal and external) through the intervention of human experts. It highlights security weaknesses and provides guidance that can be used to address them.
- **BAS**—A BAS is used to perform advanced testing that analyzes security efforts by deploying agents within the environment to determine the effectiveness of security measures.
- **Attack surface management (ASM)**—An ASM DSA periodically tests an environment by simulating complex cyberattacks on demand and harvesting real-time data input to measure attack surface and risk appetite.
- **SIEM solution**—An SIEM solution collects logs from firewalls, intrusion detection systems (IDSs), web filtering systems and network sensors. These logs are combined for event correlation and analysis to issue alerts for potential events or incidents.
- **Security Orchestration, Automation, and Response (SOAR) tool**—This tool enables security data monitoring from various sources to manage vulnerabilities and threats. It is used to automate routine responses and helps to minimize human interventions.

Organizations must start conducting advanced security assessments involving real-time data from organizational assets in addition to traditional qualitative assessments to get more proactive insights into their attack surface. Adopting a DSA approach allows organizations to identify potential risk areas, evaluate the risk areas impartially, and highlight the critical risk indicators with a report that helps monitor emerging risk.

> The dynamic aggregation and correlation of real-time data into a single source of truth provides senior management with meaningful insights into the security of the organization's business and operations.

Benefits of a DSA

DSAs provide a more comprehensive view of an organization's security posture and help identify trends, patterns and relationships that may not be immediately apparent. The benefits highlight why organizations must implement DSAs and make more informed decisions on how to protect their assets and mitigate risk.

- **Facilitates proactive risk management**—DSAs help identify emerging risk and potential vulnerabilities that could increase the likelihood of data leakage or a breach. This approach helps organizations proactively patch the loopholes in their environment before they can cause operational or reputational damage to the organization.
- **Enables decision-making through real-time dashboarding**—A risk-prioritized dashboard displaying key risk indicators (KRIs) and potential threat vectors empowers organizations by providing a single-pane-of-glass view for identifying security violations across complex infrastructure and multiple environments. The insights gathered from the dashboard can inform business decisions because the findings are backed by accurate, real-time data.
- **Fosters collaboration between data and risk management functions**—The data management team can help identify and share relevant data to determine potential risk areas. The risk management team can then assess the likelihood of the risk scenarios occurring and develop strategies to mitigate risk. By synergizing these two functions, risk managers can gain insight into the factors that contribute to the risk within their organizations.
- **Enables concurrent evaluation of compliance posture and correlation of patterns**—The dynamic aggregation and correlation of real-time data into a single source of truth provides senior management with meaningful insights into the security of the organization's business and operations. This makes it easier to view and analyze real-time performance, identify anomalous patterns, assess compliance and apply relevant controls to mitigate potential risk.

How to Implement a DSA

For the successful implementation of the DSA methodology, organizations should follow a step-by-step approach **(figure 1**) to ensure a streamlined and structured way of determining the qualitative and quantitative risk impacting them and thereby make it feasible to identify and align appropriate resources for the mitigation.

Step One: Identify and Define

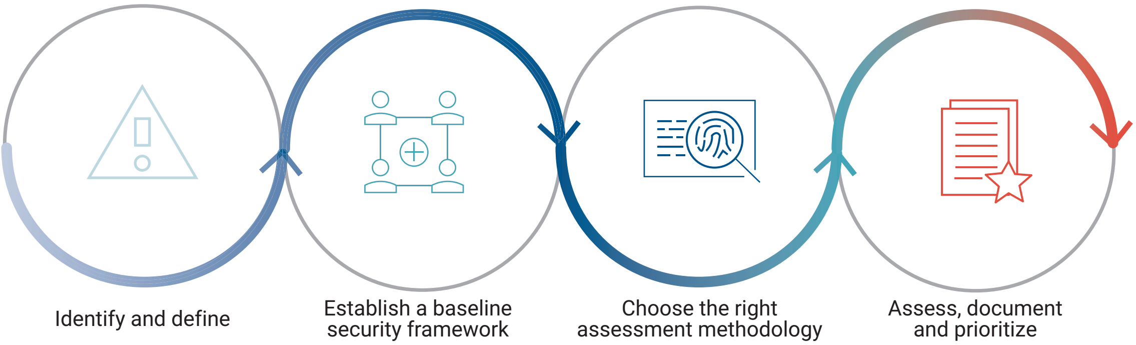
As a first step, organizations must identify the critical assets and processes within their environment that need to be protected. They should define their attack surface through continuous scanning to discover, inventory and classify known and unknown assets. They should also identify and understand their threat landscapes based on the industry and geographical locations in which they operate. For example, if a healthcare organization's highest risk lies in securing its patients' personal health information (PHI), then the systems that store and process such data constitute the organization's attack surface. Adequate knowledge about prevalent threats plus a comprehensive view of the attack surface informs and guides efforts toward risk identification and mitigation. A data discovery or a network scanning tool can help identify various data stores and systems within an enterprise network.

Step Two: Establish a Security Framework

Next, organizations must establish a baseline cybersecurity framework of their choice based on various standards, best practices and regulations across their industries, such as the International Organization for Standardization (ISO) standard ISO 27001 and the US National Institute of

FIGURE 1

Steps for Enhancing the Effectiveness of Security Assessments



Identify and define

- Identify the critical assets and processes to define an attack surface for the organization.
- Determine the threat landscape based on the industry and region.

Establish a baseline security framework

- Develop a baseline security framework that the organization wishes to align with.
- Map the baseline framework with MITRE ATT&CK framework's TTPs.

Choose the right assessment methodology

- Select an appropriate data-driven risk assessment methodology.
- Develop an in-house capability or opt for a retainer service for conducting periodic assessments.

Assess, document and prioritize

- Conduct the assessment and document the observations.
- Classify and prioritize identified risk, catalog a remediation plan and develop an actionable road map.

Standards and Technology (NIST) Cybersecurity Framework (CSF).

The established framework should then be mapped to the MITRE ATT&CK TTPs to align common threat actor methods with the qualitative elements of the security program. This provides a comprehensive and multidimensional view to identify and treat any underlying defects in foundational security capabilities while fixing the operational deficiencies discovered through DSAs.[6] For example, an organization that chooses NIST CSF as its baseline framework can map the privilege escalation technique from the MITRE ATT&CK framework to the subcategory PR.AC-4 within the Protect function and Access Control category of the NIST CSF (access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties). So, if the DSA results in a privilege escalation-related risk, such mapping enables the organization to identify the underlying qualitative aspects that need to be worked on in addition to fixing the one threat instance identified by the DSA.

Step Three: Choose the Right Assessment Methodology

The selection of an appropriate DSA model is one of the most crucial decisions for an organization and can be accomplished by considering the factors present in steps one and two. Once the assessment type is chosen, an organization should decide on frequency (e.g., weekly, monthly, quarterly, annually, continuous) based on its unique operations and the identified critical assets. Choosing the right solution provider to perform an assessment is equally important. Organizations can choose to develop an in-house capability for some assessment models such as SIEM, SOAR and BAS, or they can opt to retain the service from a cybersecurity service provider.

> Because each risk identified may affect each organization differently, risk must be further prioritized based on industry, threat profile and potential impact.

Step Four: Assess, Document and Prioritize

After finalizing the assessment methodology, organizations should establish a structured documentation process to quickly recognize anomalous behavior. After conducting assessments per the defined frequency, they should document observations and identify and categorize deficiencies and vulnerabilities. Because each risk identified may affect each organization differently, risk must be further prioritized based on industry, threat profile and potential impact.

Documenting and prioritizing risk is incomplete without a remediation plan. Depending on the level of risk and an organization's appetite for it, a risk may be accepted, transferred, avoided or treated. This plan should be cataloged and further consolidated into an actionable road map to minimize the impact of the identified risk.

Case Study

A global financial and insurance enterprise intended to gain insights into its cybersecurity and data privacy risk across its organizations located in multiple geographies to gain a holistic view of the cyberrisk impacting its investments.

The differentiated DSA approach for this engagement included a comprehensive qualitative and quantitative assessment leveraging the NIST CSF as the baseline. The qualitative assessment comprised a detailed crown jewel analysis that included identifying the threat, risk and impact on the enterprise's investments, along with a review of the current security controls including documentation (policies, procedures and standards) and stakeholder interviews on the categories of the NIST CSF. The quantitative assessment comprised an external and internal VAPT and a BAS in alignment with the MITRE ATT&CK framework.

The findings across the different assessments performed (e.g., crown jewel analysis, VAPT, and BAS) were mapped to the baseline framework and provided the insurance enterprise with organization-specific findings and recommendations, along with an executive summary.

The enterprise obtained an understanding of the risk across its organizations, empowering it to gain insights into its broader enterprisewide risk and to realign its security investment decisions to enhance the overall cybermaturity of its organizations.

Conclusion

To gather truly insightful information about their security posture and adopt a data-driven model of performing security assessments, organizations should follow a four-step approach. This holistic, risk-based approach allows organizations of all sizes to overcome the intrinsic limits of traditional security assessments to identify and prioritize the threats and risk that would impact them the most, and to appropriately remediate them. The dual nature of such an approach helps organizations maintain compliance with relevant laws and regulations and, at the same time, implements a threat-focused security program with actionable controls to mitigate the specific tactics and techniques that impact critical assets.

Authors' Note

The authors wish to acknowledge and thank Srishti Ahuja, Srinivas Teppa, Esha Rastogi and Abhishek Pandey for providing their support and assistance throughout all aspects of the development and completion of this article. The views expressed in this article by the authors are personal.

Endnotes

[1] IBM Security, "Implementing MITRE ATT&CK: How to Successfully Deploy the Leading Cybersecurity Framework in Five Steps," *Forbes*, 19 March 2021, *https://www.forbes.com/sites/ibmsecurity/2021/03/19/implementing-mitre-attck-how-to-successfully-deploy-the-leading-cybersecurity-framework-in-5-steps/*

[2] Rosenberg, D.; "Data-Driven Cyber Risk Assessment Can Bolster Business Continuity," *Security Magazine*, 24 December 2020, *https://www.securitymagazine.com/articles/93884-data-driven-cyber-risk-assessment-can-bolster-business-continuity*

[3] SecurityScorecard, "Guide to Performing a Data Risk Assessment," 24 November 2021, *https://securityscorecard.com/blog/guide-to-performing-a-data-risk-assessment*

[4] Elgan, M.; "Breach and Attack Simulation: Hack Yourself to a More Secure Future," *Security Intelligence*, 10 November 2021, *https://securityintelligence.com/articles/breach-attack-simulation/*

[5] Watson, D; "How MITRE's ATT&CK Framework Helps Security Teams Map Adversary Behavior," *SC Media*, 6 October 2021, *https://www.scmagazine.com/perspective/threat-intelligence/how-mitres-attck-framework-helps-security-teams-map-adversary-behavior*

[6] Thuraisingham, B. *et al*.; "A Data Driven Approach for the Science of Cyber Security: Challenges and Directions," IEEE 17th International Conference on Information Reuse and Integration, 2016, *https://ieeexplore.ieee.org/document/7785719*