A SANS Survey

Improving the Bottom Line with Effective Security Metrics: A SANS Survey

Written by **Barbara Filkins**
Advisor: **John Pescatore**

August 2020

Sponsored by:
ThreatConnect

Analyst Program

Executive Summary

Meaningful security metrics are critical for both accurate insight into the status of an organization's security and persuasive communication to management to back needed changes and support the level of resources required. This year's SANS Security Metrics Survey reveals that much still needs to be done to fully realize the potential power that metrics bring to the security landscape.

Popular frameworks such as NIST and CIS provide the basis for generic metrics, but both survey respondents and the industry at large cite that useful security metrics are unique to an organization and its stakeholders. However, the survey results show that security programs still encounter obstacles to delivering business-meaningful security metrics and often fall back to focusing on compliance requirements or simple security event quantity reporting.

This survey reaffirms that security metrics development is an inexact science that is maturing. The emphasis is on what is easy to measure (performance), but there is quite a way to go to measure the impact security should have on an organization's mission. Maturing organizations need enhanced tools and industry success examples to help them overcome those obstacles.

Developing simple—but meaningful and useful—metrics is as much an art as a science. The steps organizations need to take to develop their own metrics are straightforward, but challenging:

- Define the requirements according to the critical business mission and services, and have a plan of action.
- Define the metrics to achieve the visibility you need.
- Implement metrics according to your infrastructure and any constraints.
- Establish context for your stakeholders to ensure effective communication.

Based on the information gathered from this survey, SANS has developed the following whitepaper with results and advice.

Key Findings

- Leading driver for metrics = audit and compliance—**55%**
- Most organizations are still maturing or are not mature in their use of metrics—**70%**
- Leading barriers to effective use of metrics = lack of automation and lack of requirements— **47%**
- Dissemination of metrics is mainly periodic, not continuous/real-time = **80%** weekly or longer between updates

Introduction

Three hundred seventy-one individuals took the 2020 SANS Metrics Survey, with general demographics shown in Figure 1.

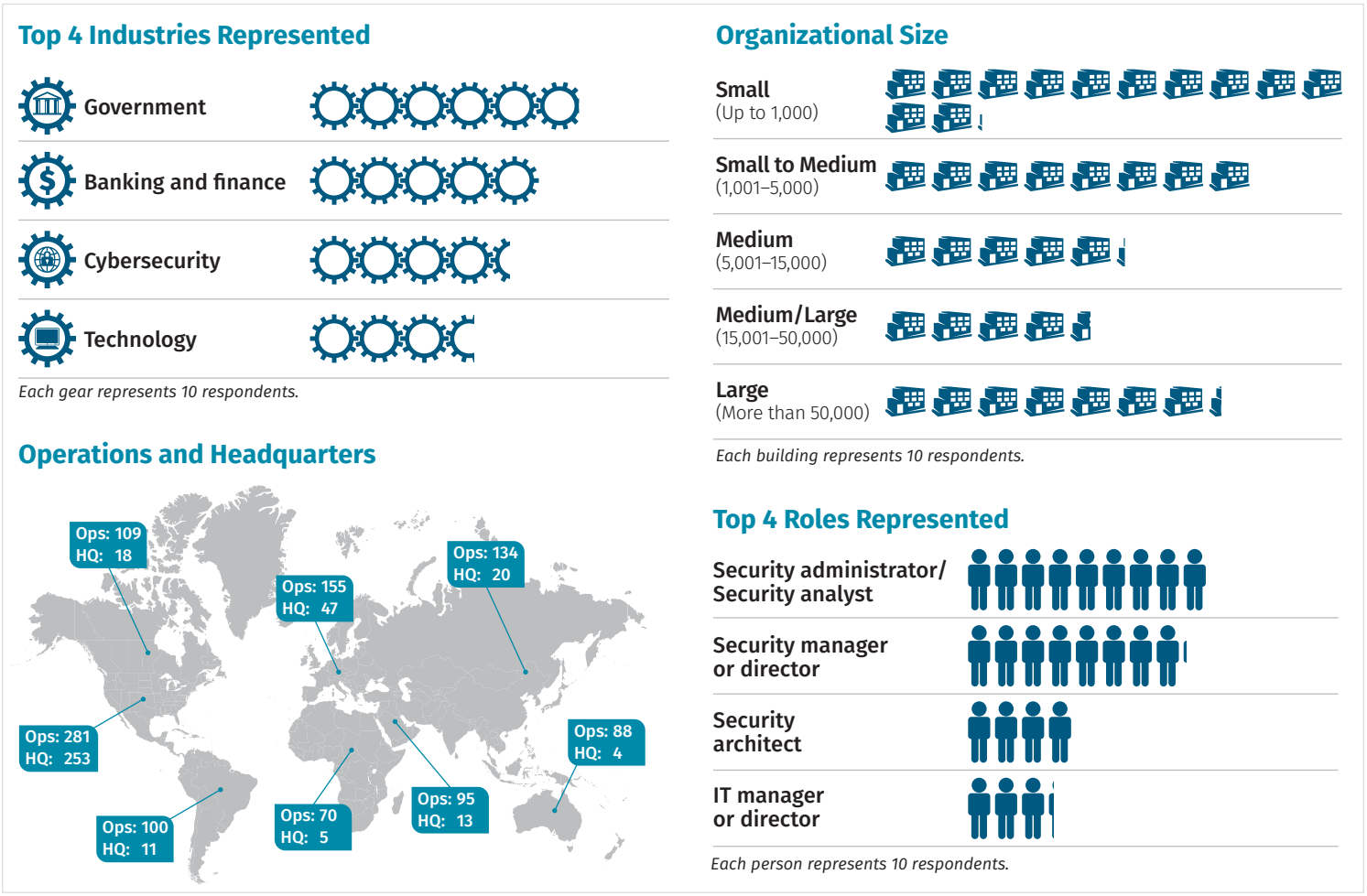

Figure 1. Survey Demographics

Normally, the demographic elements collected in a SANS survey provide a set of independent variables that can be used to evaluate survey results. However, evaluation against these variables doesn't always produce the results we might have expected—and that was certainly the case with this survey, because we had anticipated larger discrepancies in areas normally related to industry (a major driver for metrics) and roles. Management usually is not seeking the same metrics as, for example, an analyst.

Survey results, for the most part, reflect a fairly homogenous view across all respondents. Most respondents (69%) report that their organization has a set of security metrics, with slightly over 70% reporting that their use of security metrics is maturing or not mature. See Figure 2.

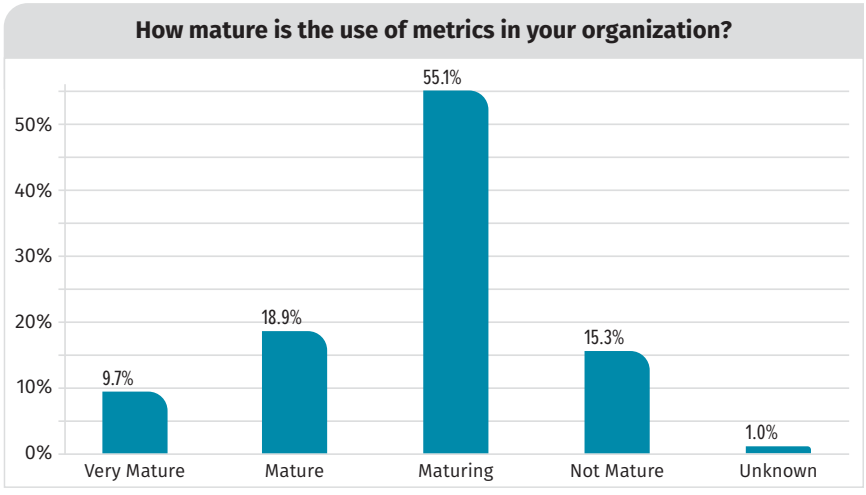

Figure 2. Maturity Related to the Use of Metrics

This perspective leads to the thought that, while the use of metrics is not new, the approach and skills needed to adequately measure security-related processes and performance are not especially mature. Making measures meaningful often requires an understanding of the nontechnical aspects of the business or mission and walking a fine line between the precision of scientific data collection and the magic of effective communication. Backed by our survey results, this paper explores how to approach the development of effective security metrics.

What's Holding Things Back?

> *"Most metrics either miss important context, measure the wrong things or are not combined with other metrics to tell a more complete story."*
>
> —Survey respondent

When designed appropriately, measured objectively and communicated effectively, metrics are an indispensable part of a mature security program. Solid metrics can help an organization measure and track risk and performance, make educated adjustments and decisions as required, and help convince management to back needed changes in processes and/or resources. While most security professionals recognize and understand this, in practice, the difficulties in selecting, collecting and operationalizing useful security metrics often limits organizations in their ability to realize significant benefits from security metrics.

There are many approaches to building an effective security metrics program, but some common activities stand out:

- Understanding the organizational mission
- Designing the metrics
- Implementing the metrics
- Communicating results (visibility)

Maturity of metrics use also does not equate to effectiveness. Mature processes that produce low impact metrics are common. Organizations that consider themselves mature or very mature identified the same barriers to effectiveness as those that are maturing or not mature. The barriers identified by respondents (see Figure 3) can be addressed in the four activities involved in building an effective program.

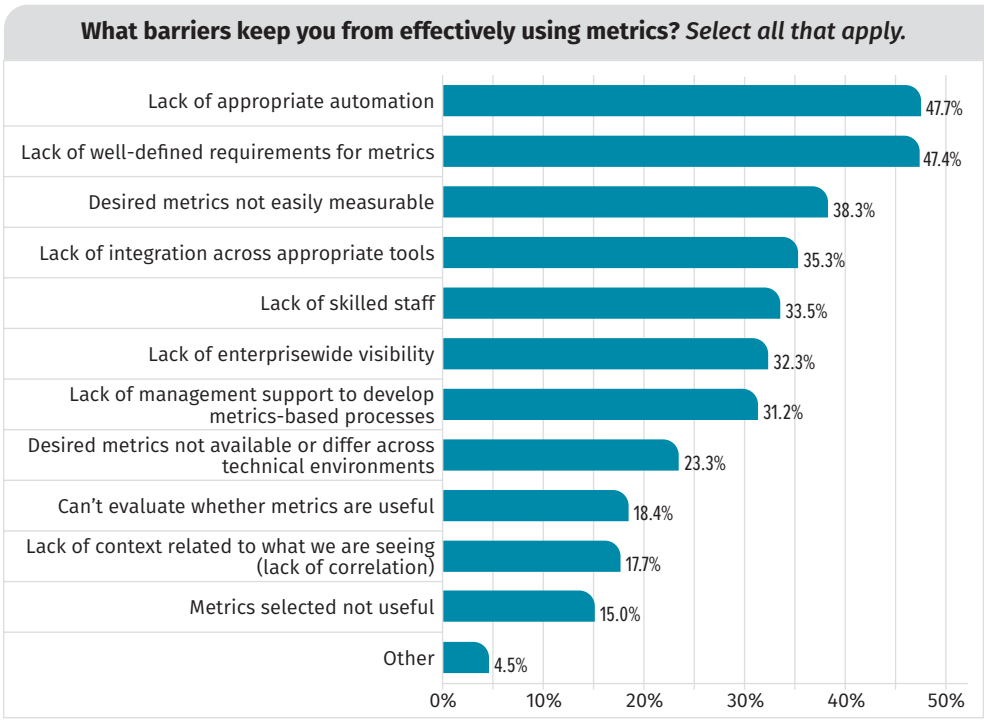

Figure 3. Barriers to Effectiveness of Security Metrics

Several SANS surveys across different areas have noted that automation is highly desired—but hard to implement—for many organizations. Essentially, to automate something, you must already be doing that process well! Organizations must overcome lack of automation altogether and other often-cited barriers (lack of defined requirements, staff skills and visibility) before they can implement automation, let alone show value.

An Open-Ended Question: Metrics in the Cloud

Respondents still overwhelmingly have their infrastructure predominantly on-premises (70%). Only 23% rely primarily on cloud services (IaaS or PaaS) for their infrastructure needs. See Figure 4.

Most organizations, especially large enterprises, actually do work with more than one cloud provider. In the upcoming 2020 SANS survey "Extending DevSecOps Security Controls into the Cloud,"[1] we found that most organizations (92% of those survey respondents) use at least one public cloud provider, with slightly over 60% having workloads running on three or more public cloud providers, including AWS, Azure and Google Cloud Platform (GCP), as well as a handful of others.

How is your infrastructure predominantly deployed?
Select the best response.

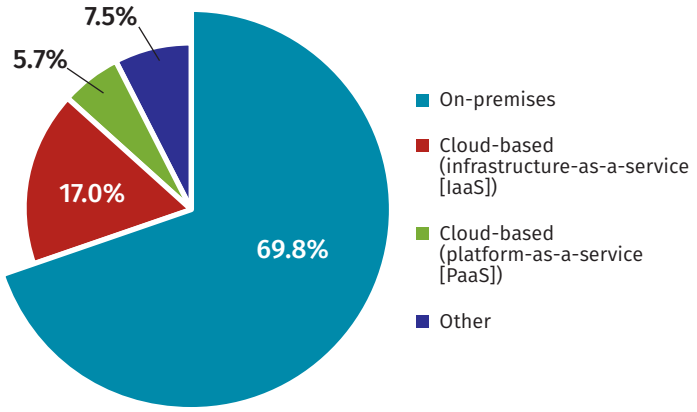

Figure 4. Primary Deployment of Infrastructure

Yet, we did see some unique considerations for those using cloud implementations. Automation is less of a concern, driven by the fact that the largest obstacle cited was "Desired metrics not easily measured." This may be due to the perception that, for cloud-based infrastructure models like IaaS and PaaS, automation in the cloud is easier to attain than dealing with managing a networked collection of hardware assets and endpoints.

However, for SaaS, probably the dominant cloud service model, automation is really hard—likely because many SaaS applications provide little or no security visibility, nor do they provide the opportunity to directly monitor security-related events. Cloud-based concerns show a definite emphasis toward getting the right metrics and supporting measures, as opposed to getting the automation right. See Table 1.

Transitioning to a cloud-based infrastructure shifts the emphasis as to what IT and security metrics are most valuable. Rather than be shocked by these differences, the operations team must understand the variations to gain needed visibility into the cloud-based infrastructure. For example, organizations expect a high level of uptime as part of a cloud baseline, but the fundamental measure might now be application slowdown as opposed to complete loss of service, whether due to routine maintenance or DDoS.

Table 1. Barriers to Using Metrics Effectively

Barriers	Infrastructure		
	Overall	On-premises	Cloud
Lack of appropriate automation	34.2%	25.6%	6.5%
Lack of well-defined requirements for metrics	34.0%	24.8%	7.5%
Desired metrics not easily measurable	27.5%	18.3%	8.4%
Lack of integration across appropriate tools	25.3%	18.3%	4.9%
Lack of skilled staff	24.0%	18.6%	3.5%
Lack of enterprisewide visibility	23.2%	17.5%	4.6%
Lack of management support to develop metrics-based processes	22.4%	16.4%	4.9%
Desired metrics not available or differ across technical environments	16.7%	10.8%	4.3%
Can't evaluate whether metrics are useful	13.2%	9.7%	3.2%
Lack of context related to what we are seeing (lack of correlation)	12.7%	9.7%	1.9%
Metrics selected not useful	10.8%	6.7%	3.8%

[1] "Extending DevSecOps Security Controls into the Cloud," www.sans.org/reading-room/whitepapers/analyst/ [scheduled to be released September 2020; registration required.]

However, don't throw out the traditional, infrastructure-oriented metrics—they still have a lot of value. Take, for example, the Basic CIS Critical Controls.[2] These first six control families on the prioritized list of 20 are considered fundamental to cyber defense readiness and should be implemented by all organizations. These controls, however, are often used to provide guidance for securing software and on-premises hardware. However, in its "CIS Controls Cloud Companion Guide, Version 7," CIS has reviewed the control families and their applicability to cloud service models—specifically IaaS and PaaS—and determined that more than 60% of the CIS Sub-Controls in these families apply for IaaS and PaaS, the exception being family 5 for PaaS (see Table 2).

Table 2. Applicability Overview for Each Service Model[3]

Control	Control Title	Applicability of Service Model			
		IaaS	PaaS	SaaS	FaaS
1	Inventory and Control of Hardware Assets	●	●	◐	◐
2	Inventory and Control of Software Assets	●	●	◐	◐
3	Continuous Vulnerability Management	●	●	○	○
4	Controlled Use of Administrative Privileges	●	●	●	●
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	●	◐	◐	◐
6	Maintenance, Monitoring and Analysis of Audit Logs	●	●	●	●
7	Email and Web Browser Protections	●	●	◐	◐
8	Malware Defenses	●	●	○	○
9	Limitation and Control of Network Ports, Protocols, and Services	●	●	●	◐
10	Data Recovery Capabilities	●	●	●	●
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	●	◐	○	○
12	Boundary Defense	●	◐	○	○
13	Data Protection	●	◐	◐	◐
14	Controlled Access Based on the Need to Know	●	◐	◐	◐
15	Wireless Access Control	○	○	○	○
16	Account Monitoring and Control	●	●	●	●
17	Implement a Security Awareness and Training Program	●	●	●	●
18	Application Software Security	●	●	●	◐
19	Incident Response and Management	●	●	●	●
20	Penetration Tests and Red Team Exercises	●	●	●	●

Applicability Overview for Each Service Model

● More than 60% of CIS Sub-Controls Apply

◐ Between 60% and 0% of the CIS Sub-Controls Apply

○ 0%

Navigating Cloud Challenges

The main challenge now becomes more contractual, understanding and ensuring that the service-level agreements (SLAs) and legal arrangements with the cloud service provider (CSP) highlight those metrics not just related to user expectations, such as performance and availability, but also to liability, service levels, breach disclosure and incident response time frames. Cloud implementations bring into focus changes in who handles the security requirements and where the assumed security risk resides. Make sure your security tools capture the data needed and that there is overlap, rather than gaps, in coverage in the data being captured by the tools—both third-party and CSP native—that best fit your organization's security and management needs.

[2] https://www.cisecurity.org/controls/cis-controls-list/

[3] "CIS Controls Cloud Companion Guide," Version 7, www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/, p. 7

Understanding the Mission

Organizations are unique—and so are their specific needs for security metrics. In this year's survey, the leading reason for collecting security metrics was improved audit and compliance, most likely driven by the strong representation of respondents in government and highly regulated industries such as banking, education and healthcare. Metrics related to lowering costs of security or doing business did not gain much traction, possibly because of the complexity in developing such measures (see Figure 5).

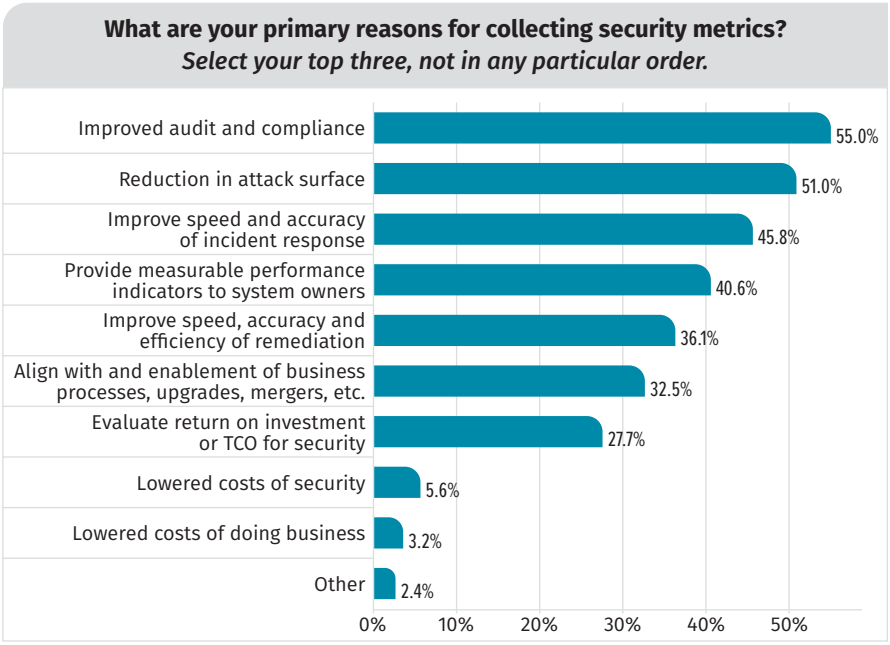

Figure 5. Reasons for Collecting Security Metrics

Interestingly, respondents in security management roles indicated that the leading reason for collecting security metrics was to provide measurable performance indicators to system owners, whereas security analysts took the view that improving audit and compliance was the significant driver. This likely shows a common disconnect: While upper levels of the organization talk about risk management, the operations team gets pressure to pass audits. This is similar to business management talking about value to the customer but relying on quarterly sales numbers to make business decisions.

This raises another important point about the use of metrics—their value is not restricted to demonstrating regulatory compliance. Metrics provide visibility into how an enterprise is performing and how it is meeting its strategic business goals—whether related to its mission, its earnings or the maturity of its security culture. The key is to ensure that the metrics have been designed to measure the objective.

Metrics 101: Have a Plan

How do you go about designing a successful metric or metric framework? The answer is straightforward but not always easy to accomplish: Have a plan of action and the dedicated resources to execute it.

An organization needs a well-defined action plan to achieve its goals (such as meeting growth objectives in its strategic business plan), measure its processes (such as maintaining SOC performance objectives) or demonstrate regulatory compliance. Metrics or a metric framework are a means to gauge your organization's progress in meeting and maintaining these goals and objectives.

Metrics, no matter how well-accepted, have limited use to an organization if its action plan is weak and lacks clear and achievable objectives with coherent, practical and actionable implementation steps. Successful metrics help assess whether committed resources match the plan; whether activities are truly focused on accomplishing organizational goals and objectives; and where plan efforts might need to be refocused with time.

Development of a solid metric framework requires an organization to commit the necessary resources and skills. This goes hand-in-hand with the organizational vision of security—and leadership commitment at the appropriate level(s): board of directors, C-suite (including CISO), business system owner, SOC director or other management, thus establishing a solid security culture.

One survey respondent summed up the situation nicely: "We are [finally] getting prioritization, which includes implementing metrics. The struggle has been having appropriate support to implement projects and having available resources beyond moving limited security projects forward."

In terms of formally developing metrics requirements, most respondents (20%) cited the use of an existing framework as their primary method, followed (not surprisingly) by regulations/compliance requirements, as illustrated in Figure 6.

> *"The biggest problem I see is that the organization is not defining the requirements for metrics and therefore [is] not able to make decisions based [on] them."*
>
> —Survey respondent

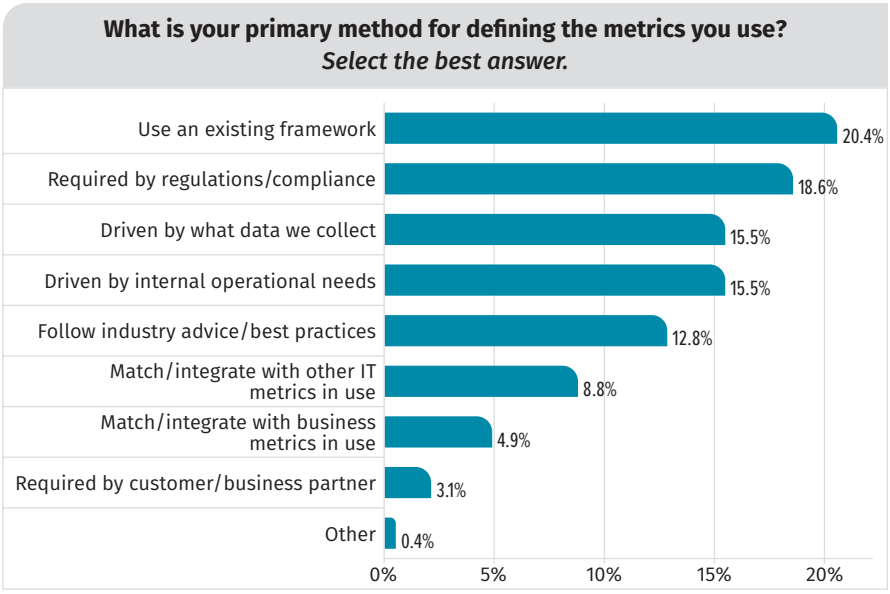

Figure 6. Primary Method to Define Metrics

Both NIST SP 800-53[4] and the CIS Security Controls have formal guides to metrics that can help organizations establish metrics that gauge security performance. The NIST CSF,[5] on the other hand, encourages an organization to develop its own metrics through a gap assessment process, identifying controls that can close the gap between the organization's present and desired states of security. The frameworks in general use are provided in Figure 7.

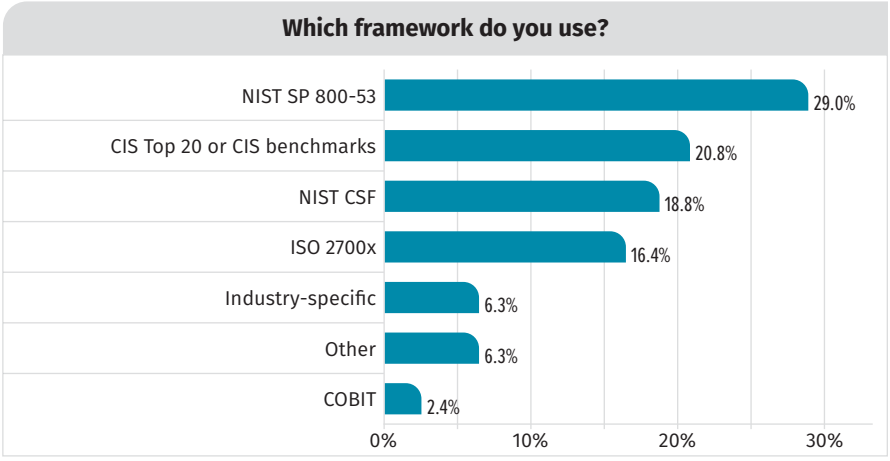

Figure 7. Frameworks in Use

Map Your Metrics to Your Security Controls

Industrywide frameworks are an excellent starting point for security metrics. A good metric ultimately helps an organization assess whether or not a security control is effective at reducing risk, helping security teams gain an understanding of where gaps may exist or uncovering where controls may need to be either designed or implemented differently.

Using a formal framework can help, because many offer predefined, industry-accepted metrics. For example, taking the two frameworks most commonly used by respondents, we have the following resources available:

- SP 800-55 Rev. 1: Performance Measurement Guide for Information Security[6] that supports NIST SP 800-53
- CIS Controls V7 Measures & Metrics[7] that supports the CIS Top 20 or CIS benchmarks

[4] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

[5] https://www.nist.gov/cyberframework

[6] "SP 800-55 Rev. 1: Performance Measurement Guide for Information Security," July 2008, https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final

[7] "CIS Controls V7 Measures & Metrics," www.cisecurity.org/white-papers/cis-controls-v7-measures-metrics/

"We have assessed ourselves utilizing NIST-based controls and have done maturity assessments to drive where we need to be. Ultimately, we need to understand whether we are in a defensible position. Metrics [requirements should] include:

- *Maturity and where security needs to be in the 15 areas of NIST.*
- *Showing how security projects are successful in moving security and addressing gaps.*
- *Operational metrics to understand how things are working (i.e., patching, vulnerability assessment, preventing x infections, etc.).*
- *Awareness activities such as education, phishing exercises, etc. to understand whether the people aspect is successful."*

—Survey respondent

When we look at the top methods for developing metrics across the top six industries in this survey, grouped by vertical—government, banking and finance, cybersecurity, technology, education and healthcare—we find that the verticals are driven by following industry best practices as opposed to merely complying with an existing (formal) framework and regulatory compliance demands. This implies that these verticals depend not only on the regulatory elements, but also have adopted the regulatory compliance demands to meet the needs of the industry—as it probably should be.

"Metrics are difficult to define, especially desired metrics. My company is very much a 'Well, what is industry best practice?' architecture type, and we rely on what other companies are doing to be able to build our program. Currently, we're not aware of excellent metrics with defined action items to hit higher maturity levels, so we try to do what we can with what we have."

—Survey respondent

Designing Your Metrics

The metrics that respondents use to track, measure and report on the status of their security efforts are shown in Figure 8. The focus is on those metrics that measure quantities—alerts and their severity, as well as the number of incidents handled.

There was a big drop in use from quantity metrics to quality/efficiency metrics, such as time to detect, time to assess, impact to business, ticket closures per shift, etc., which are key to managing security operations. These are the key areas of focus needed to improve the usefulness of your organization's security metrics.

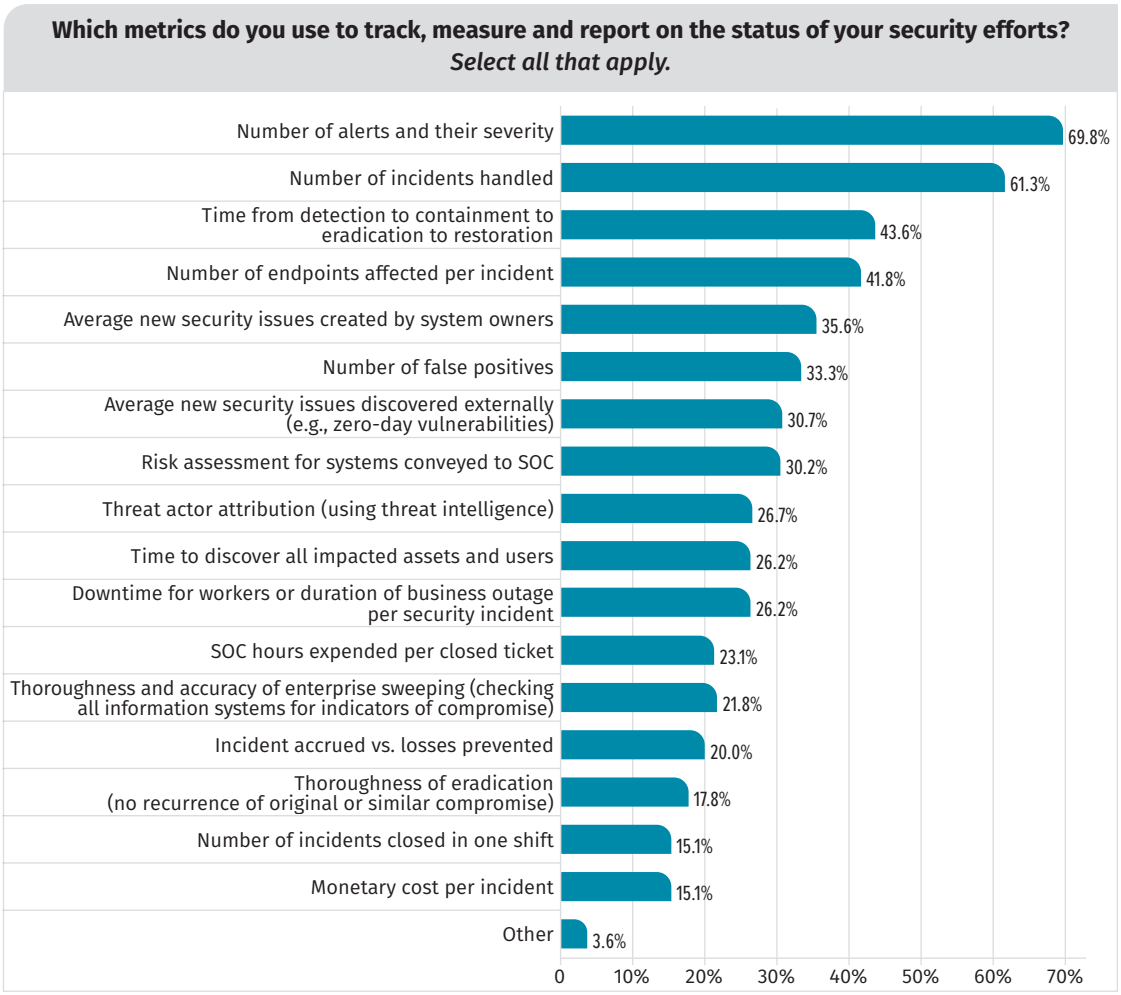

Figure 8. Metrics Used for Tracking, Measuring and Reporting Security Efforts

It takes resources in people, process and technology to increase the effectiveness and maturity of day-to-day security operations practices. Senior management will invariably ask security managers to demonstrate how their budget and activities improve the organization's security posture in some business-meaningful way. Metrics are an essential tool for security pros to both understand and demonstrate how their systems and processes support the business. Well-designed metrics support data-driven decisions.

Tracking Management-Oriented Metrics

Management-oriented metrics are complex, one possible reason that many are not tracked. Items such as "time to complete standard and custom tasks (e.g., average and mean time for each of the phases of the IR process)," require understanding the workflow involved to determine the actual measure.

To actually collect data to support using these management metrics, organizations and staff need to spend more time discretely tracking the phases of an incident, as well as devise methods to actually track incidents as they are resolved. Given that tracking time detracts from actual incident handling, it is logical that respondents would prioritize solving for an incident over meticulously tracking time expended in discrete phases.

The results of this survey didn't show a high divergence between the metrics used by analyst staff versus management. However, in areas such as "Monetary cost per incident" there were some differences. See Table 3.

Table 3. Metrics Used by Security Management vs. Security Analysts

Metrics	Total	Security Management	Security Analyst
Number of alerts and their severity	140	53	61
Number of incidents handled	126	58	51
Time from detection to containment to eradication to restoration	86	33	36
Number of endpoints affected per incident	82	30	37
Average new security issues created by system owners	72	30	30
Number of false positives	66	26	27
Average new security issues discovered externally (e.g., zero-day vulnerabilities)	61	27	24
Risk assessment for systems conveyed to SOC	59	19	30
Downtime for workers or duration of business outage per security incident	51	20	18
Threat actor attribution (using threat intelligence)	50	16	26
Time to discover all impacted assets and users	50	16	20
SOC hours expended per closed ticket	44	20	18
Thoroughness and accuracy of enterprise sweeping (checking all information systems for indicators of compromise)	41	16	17
Incident accrued vs. losses prevented	40	11	21
Number of incidents closed in one shift	31	12	15
Thoroughness of eradication (no recurrence of original or similar compromise)	30	9	14
Monetary cost per incident	26	14	7
Other	7	4	3
Total Count	**326**	**133**	**128**

Building Your Metrics

Let's take a brief time-out to discuss how to build metrics. Figure 9 shows a generic approach. Assuming the basic organizational metric requirements have been established, building metrics usually starts from the bottom up, with a goal of providing summarized metrics that allow a high level of visibility into issues for evaluation and decision making.

Good metrics are relatively simple but, as with many aspects of life, achieving simplicity is hard. Designers can get lost in the granular details of the actual data underlying the metric, losing sight of what that specific metric is intended to measure. This is why it is key that the organization can conceptually define a metric and ensure that it is understood and accepted at the beginning by the

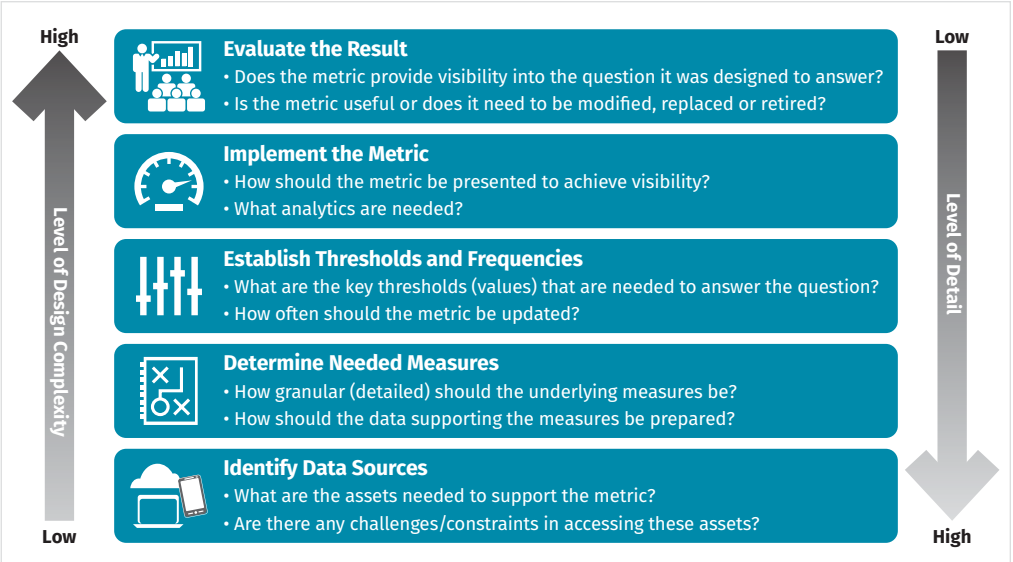

Figure 9. Building Metrics

intended stakeholder audience. This helps keep the design focused as one moves from the granular data to increasingly abstract measures and, finally, the presentation of a metric that—although it depends on actual data and measurements—has been abstracted from the elements that comprise it.

The level of detail is highest at the lowest level of design complexity, where the greatest number of data elements will be collected from various endpoints. The level of detail decreases as design complexity increases, where this data ultimately will be aggregated, rolled up into chunks of information for presentation to stakeholders.

> *"Metrics will need both abstract and granular measures, where granular measures contribute to abstract metrics. Most times, problems arise where the metrics defined by a department (e.g., DLP) doesn't align and contribute to metrics and measures that the CISO needs [to present] to the exec.*
>
> *"There seems to always be two or more types of metrics. Management seems to believe that everything can be rolled up into one nice little pie chart, and there are companies out there that sell those types of solutions [that] can give a false sense of security."*
>
> —Survey respondent

Gathering the Measures

The measures (and therefore the metrics) will be influenced by what is available within the organization. This includes the business systems (both on-premises and cloud-based) that produce and store mission-critical data related to the mission and services of the organization, the infrastructure assets that log events and actions, and the security tools and services used for collection, correlation and analysis.

Based on the data sources used, our respondents definitely still see endpoint events as the major source of truth, as opposed to network-based traffic. The information being gathered is mostly infrastructure-based. To have this information relate to broader business objectives, it would have to be correlated with workflows, project management and tracking information (scope, schedule and cost), financial data and HR statistics. See Figure 10.

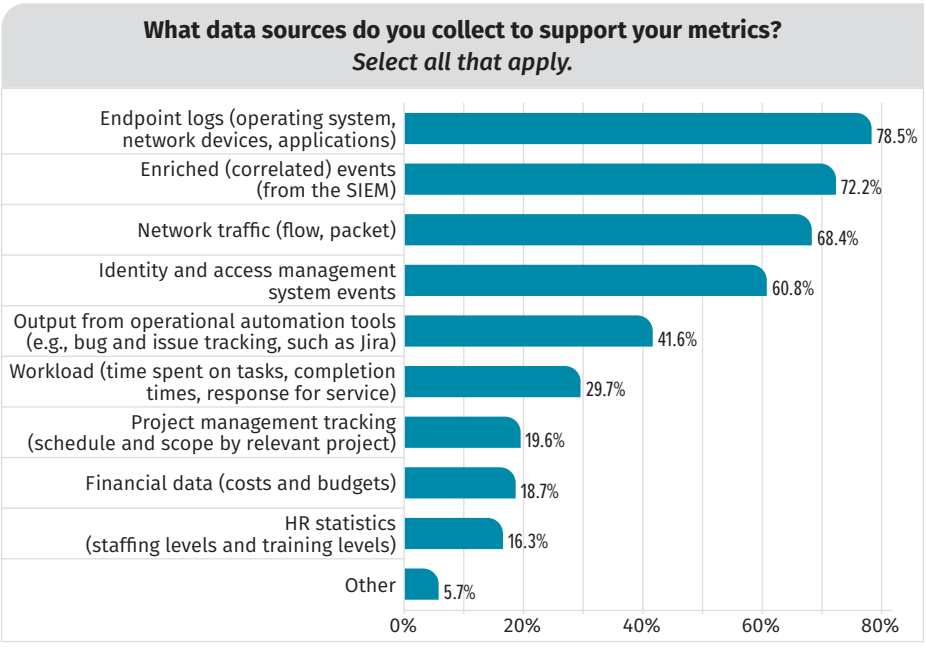

Figure 10. Supporting Data Sources

One thing to consider in developing metrics is making sure that the data being captured is not so broad (or so restrictive) that it fails to apply to the specific metric. Segmentation can support this strategic aggregation, allowing the organization of data upon which a specific measure and metric are based.

Segmentation can range from very simplistic (separating information by date/time or source) to more complex methods (such as data provenance that evaluates how data is acted on and how it moves over time). Figure 11 illustrates the types of segmentation used by respondents. Also known as *data lineage*, data provenance increases visibility while greatly simplifying the ability to trace errors back to the root cause in a data analysis process.

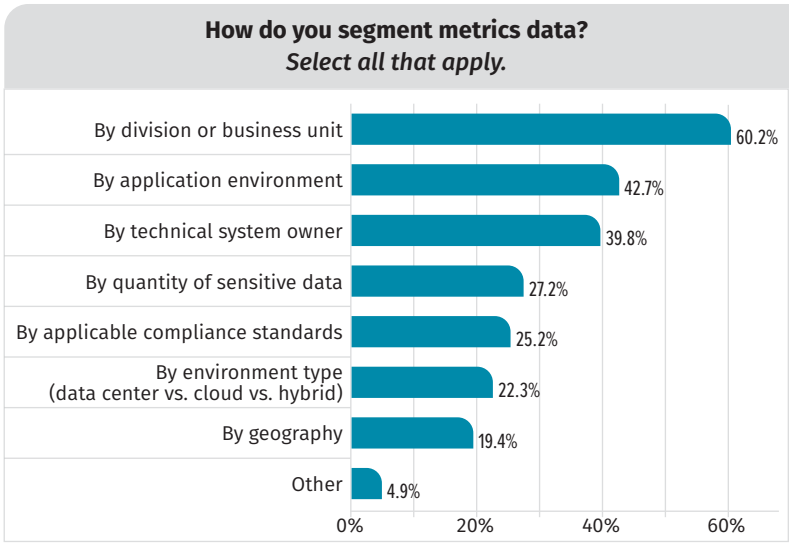

Figure 11. Methods of Data Segmentation

Unfortunately, methods such as data provenance can add to the overhead associated with capturing, storing and processing data. One survey respondent commented that the volume and size of datasets makes the data hard to analyze and derive meaningful statistics. An analyst might need to know how to use powerful but general analytical and statistical tools (such as R Analytics) to wrangle the data into a beneficial structure.

Tools for the Job

Respondents reported using a variety of tools for analyzing data. The majority (64%) still depend on spreadsheets. Spreadsheets are easy to use and customize, but often result in silos of information that are a major obstacle to more continuous monitoring and assessment. See Figure 12.

Results do not indicate, however, whether these are standalone spreadsheets or spreadsheets that provide an analytical front end to a larger data store such as a SIEM. One respondent reported using SharePoint lists that connect to an Excel document, which then imports the data. So the use of spreadsheets does not necessarily imply a completely manual process for analysis. However, the forms of collaboration and integration across spreadsheets is usually fragile.

Building Your Metrics

Consider arranging information in levels or tiers, where each layer builds upon the one beneath it—rolling up more granular measures into broader, more strategic metrics as you move up the tiers. As you build, evaluate the numbers you will likely encounter across each tier to establish acceptable values, appropriate thresholds and objective ranges.

The end result will be well-understood metrics together with confidence in what they represent, whether qualitative or quantitative, allowing stakeholders the visibility to make the objective decisions needed to improve security decisions in the organization.

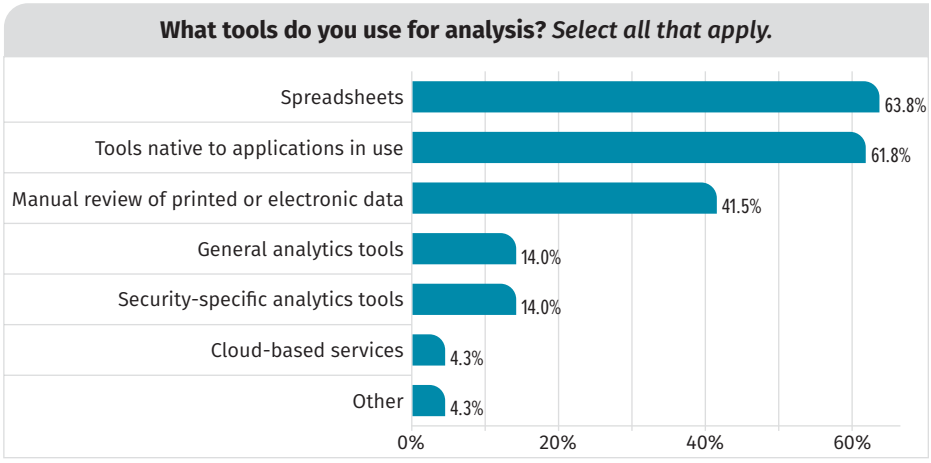

Figure 12. Analysis Tools in Use

Results led to a few interesting notes about the other tools:

- Splunk led as the leading security-specific analysis tool.
- Industry giants PowerBI and Tableau dominated use of general analysis tools.
- Cloud-based analysis tools still lag in adoption.
- In-house-developed and customized tools are still in use. One respondent described how metrics are parsed from their native format via Python scripts into a common schema with fields specific to all logs as well as unique products. The results are then loaded into a commercial tool that provides the dashboards and reports that drive further analysis.

Communicating the Results

Appropriate metrics can provide visibility into real-time events, as has been powerfully proven in the current coronavirus pandemic. Yet the delivery of security metrics remains a stilted process. The primary method of disseminating results for 37% of respondents is holding meetings with stakeholders and using prepared reports (PowerPoint, spreadsheets), with another 26% relying on email attachments. Only 28% use dashboards, which allow direct access to results. See Figure 13.

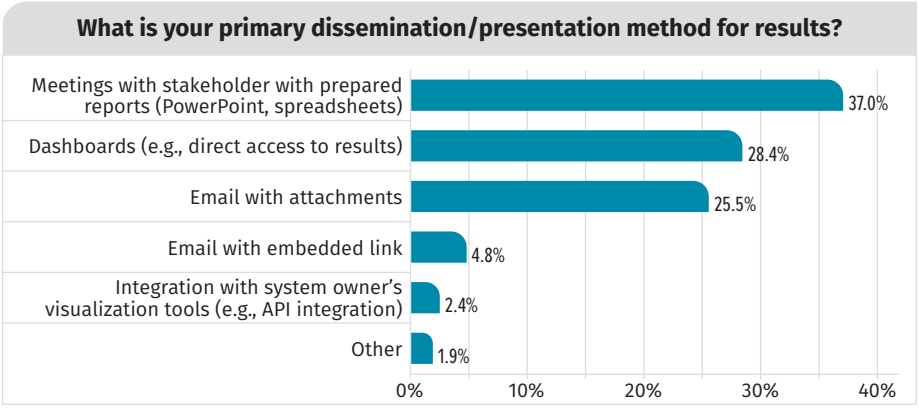

Figure 13. Methods for Sharing Metrics

> *"The metrics that I would create are metrics that could be leveraged [in] real time to make realistic business information changes in real time. This would help prevent time loss and funding loss."*
>
> —Survey respondent

Metrics delivery must be timely, accurate and regular. Metrics should be living and dynamic to inform risk decisions, rather than static snapshots. The value of a given metric represents an accurate measurement only in the moment in which it is measured. Reporting metrics frequently and regularly allows visualization of trends over time, early identification of abnormalities early on and prevention of unnecessary risk.

With 70% percent of respondents reporting that their SOC provides metrics that can be used in reports and dashboards, it seems evident that real-time visibility should be considered as a necessary requirement. Yet for the majority of respondents, the distribution of metrics is weekly or monthly. See Figure 14.

To build a strong metrics framework, you need to understand for whom you're building it—especially if there are multiple audiences with different needs, such as security analysts and management. The metrics you want to report

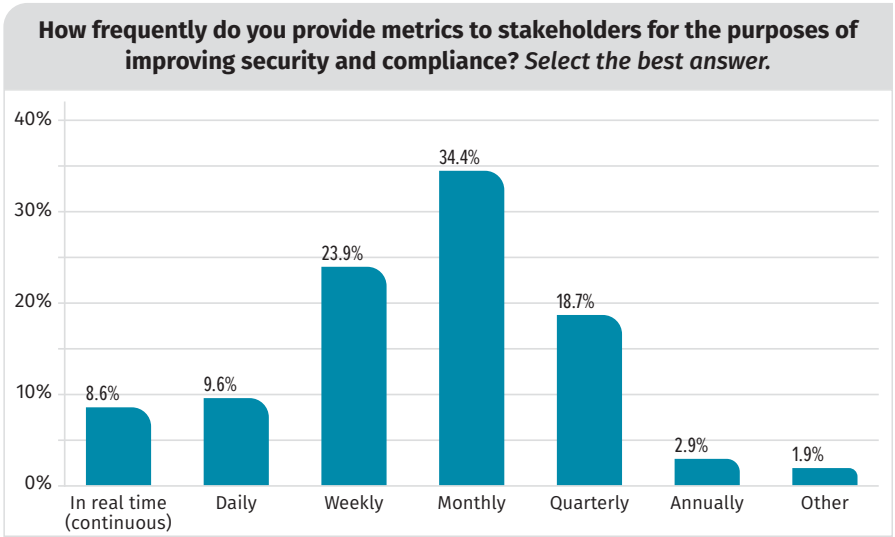

Figure 14. Frequency of Sharing Metrics

to the board and executives are different from the ones you use to make operational improvements and tactical adjustments. The metrics provided to customers showing that their data is protected are different from the metrics that security management needs to make well-informed decisions. A good metrics framework provides the right metrics to the appropriate audiences, even when there are multiple audiences.

Depending on the complexity of the metrics being collected, developing the right metrics and training stakeholders on how to interpret them takes time and effort. This is a common theme with survey respondents, as expressed by several quotes:

> *"Differing sets of metrics for different levels of management. For example, frontline technology/security managers want to be able to access details behind the metrics and need [a] lower level of metrics related to effectiveness of technology and process number of malware infections not blocked/cleaned, number of phishing emails reported (not blocked), coverage/installation of toolsets, anything anomalous from the baseline. At an executive level, the metrics need to be higher and more tied to risk outcomes. I like to use trendlines over several months here."*
>
> —Survey respondent

> *"We use metrics for a variety of reasons, such as stakeholder engagement to encourage remediation, audit visibility, and to show the value of our security organization. There are many challenges to our metrics program—and one that I struggle with is the so what of executive metrics."*
>
> —Survey respondent

> *"I collect a lot of metrics for my team that are ultimately not important to leadership (ex. availability/uptime for the SIEM). It is important but not something that will resonate with the board or SR leadership. Finding executive-friendly metrics is a challenge."*
>
> —Survey respondent

> *"Our biggest struggle [is] how do you make the work being done relevant and understandable to a sales group vs. an application development group."*
>
> —Survey respondent

As with everything else, management must be committed to the time and resources security teams need to make the metrics process viable and its results visible to the appropriate stakeholder role.

Thoughts on Automation

Metrics capture and presentation is an appealing candidate for automation. But automation is not a silver bullet. Fifty percent of respondents depend on partial automation, with another 18% using completely manual processes (see Figure 15).

One survey respondent summed up some of the challenges nicely:

> *"Compliance-required security metrics are not all measurable by automation, for example a list of your defined networks—hard to count up air-gapped networks from a central location. [It's] also hard to incorporate external defenses in system risk scoring. Context is important, exploitability as well as impact, not just vulnerability."*
>
> —Survey respondent

How are metrics tracked, analyzed and reported?
Select the one that best applies.

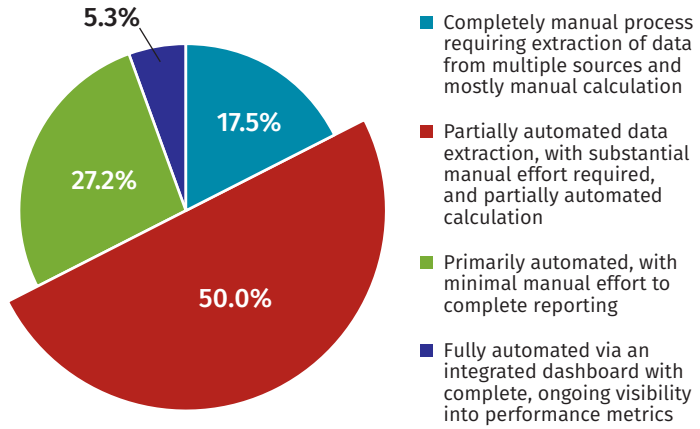

Figure 15. Tracking, Analysis and Reporting of Metrics

> *"My emphasis, with every metric, is to show the value and return of the total security investment, specifically the people investment, so I try to segregate the automated functions from the human functions."*
>
> —Survey respondent

Collecting automation-related metrics is critical to determining the impact of an organization's investment—how effective automation really is, whether the technology performs as expected, and how satisfied management is with the outcomes. Developing a new strategy for metrics will take time and investment in skills and tools. It is key to convince management of the business value of more meaningful security metrics. Make a plan and stick to it.

Conclusion

One of the largest struggles today is trying to convince organizations to adopt a culture of security, much as how aviation has adopted a culture of safety. Metrics can help measure that adoption. Collecting metrics blindly is not productive and wastes resources.

Think of metrics, their meaning and visualization, as a way of communicating the state of the organization's security culture to its stakeholders. Metrics can also provide insight into the need for change, whether in regard to the organization's mission or the effectiveness of the process being measured.

> *"I'm frankly tired of the 'What's everyone else doing?' arguments I see over and over again in this area. [...] While there are common minimal measurements, [a successful metrics framework] quickly gets to the [heart] of your organization's culture. What you are about should be somewhat different from others."*
>
> —Survey respondent

The emphasis on metrics development is neither on the analytics nor the data science (although they are important), but on educating and training organizations about how to implement a metric framework, taking into account how organizations must differ in achieving their goals and objectives for security.

About the Authoring Team

Barbara Filkins, SANS Analyst Program Research Director, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, plus the legal aspects of enforcing information security in today's mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this survey's sponsor:

ThreatConnect™