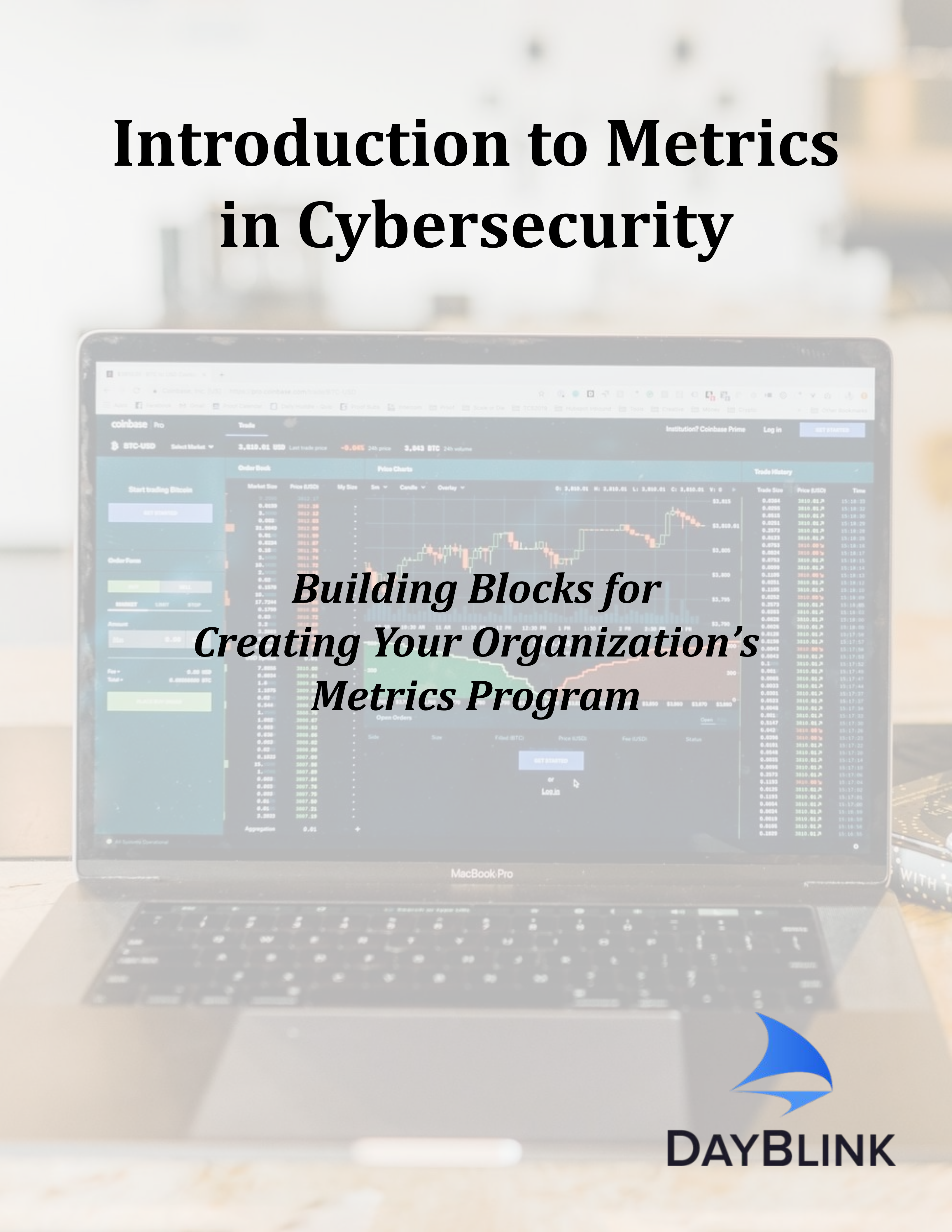
Introduction to Metrics in Cybersecurity



Building Blocks for Creating Your Organization's Metrics Program

DAYBLINK

Introduction

“We need metrics. What are our key performance indicators? How do we know if we’re doing okay?” These are questions that cyber leaders are often asking their security teams, often to no avail — or worse, to a labyrinth of spreadsheets, incongruent datasets, and a rudimentary business intelligence layer sitting over the top of everything.

In order to avoid gaps in security, an information security team must advance both its coverage and its effectiveness as its overarching information technology infrastructure expands in scope. Metrics and data-driven analysis centered around improving business operations and team performance have been key points of discussion among business leaders for the past decade. However, these discussions often run up against other priorities within cybersecurity circles. In recent years, many new platforms have been advanced in the cybersecurity space to track metrics around intrusion detection, threat intelligence, and incident response. Unfortunately, many cybersecurity teams have still not implemented these types of metrics into their cybersecurity programs, and most still do not track all of the crucial, traditional metrics that measure operational effectiveness. This whitepaper focuses on establishing the foundation for effective metrics programs for cybersecurity teams.

Metrics: An Overview

At its core, a metric is a piece of information that fulfills three criteria: it is quantifiable, it is consistently measurable, and it answers a particular business question. Quantifiability simply means that a piece of information can be represented numerically. Consistently measurable requires that results must be the same when the same measurements are repeated. Answering a particular business question is the subjective part of a metric’s definition - it is what separates a *useful* metric from a *useless* metric.

Metrics create quantifiable baselines in order to assess progress against business goals, so determining which business questions are critical to the enterprise is the first step to developing an organizational metrics strategy. A cybersecurity metrics program should accomplish five key objectives:

1. Provide a **framework for assessment** of the organization’s cybersecurity posture
2. Prioritize **areas in the organization most susceptible** to security risks
3. Monitor **organizational change impacts on** people, process, and technology
4. Survey the **effectiveness** of the organization’s cybersecurity team
5. Promote a culture of **constant iteration** among teams

Cover Page Photo by Austin Distel on Unsplash

The five sections of this whitepaper will examine the key business questions that organizational leaders should address in order to create the building blocks of a cybersecurity metrics program.

Provide a Framework for the Assessment of the Organization’s Cybersecurity Posture

The cybersecurity posture of an organization can be quite broad and a sometimes nebulous concept. For the purposes of this analysis, a cybersecurity posture assessment should contemplate how well-equipped an organization is at handling a multitude of cybersecurity threats, including but not limited to: phishing, trojans, botnets, ransomware, DDoS attacks, intellectual property threats, financial crime, data leakage, spyware, malware, data manipulation and destruction, drive-by downloads, etc.

Of course, this exercise is no easy task. The above threats range across the cybersecurity spectrum, covering topics such as network security, data loss prevention, incident response, and identity and access management.

Providing structure to this discussion is the most important factor here: an enterprise must classify metrics and business questions across cybersecurity categories. Categorizing data, while challenging, allows for teams to drill-down evaluation and provides the level of granularity necessary to accurately assess an organization’s cybersecurity posture.

Frameworks exist to help with this. The Center for Internet Security (CIS), supported by SANS, has created one such cybersecurity category breakdown that has become an industry standard, the **CIS Twenty Critical Security Controls**.

Figure 1. CIS Twenty Critical Security Controls[1]

1	Inventory of Authorized & Unauthorized Devices	2	Inventory of Authorized & Unauthorized Software
3	Secure Configurations for Hardware and Software	4	Continuous Vulnerability Assessment & Remediation
5	Controlled Use of Administrative Privileges	6	Maintenance, Monitoring, and Analysis of Logs
7	Email and Web Browser Protection	8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols, & Services	10	Data Recovery Capability
11	Secure Configurations for Network Devices	12	Boundary Defense
13	Data Protection	14	Controlled Access Based on Need to Know
15	Wireless Access Control	16	Account Monitoring and Control
17	Security Skills Assessment	18	Application Software Security
19	Incident Response and Management	20	Penetration Tests and Red Team Exercises

[1] *https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf*

Each control in the CIS Twenty can have anywhere from dozens to thousands of relevant metrics. CIS provides a “Measurement Companion” with a few example metrics and thresholds for each of the above controls. Organizations should review these frameworks and begin to understand which measures are most important to them, based on their business goals. Some organizations, such as high-frequency trading hedge funds, put uptime and server redundancy at a premium. Others, such as health care providers, might prioritize personal data protection.

Prioritizing and categorizing which business questions are important to the organization within these controls is one of the most critical steps in developing the organization’s metrics program. An organization’s information security policy should clearly dictate the goals of the organization’s security strategy. This is the foundation from which a metrics program can be shaped.

Figure 2. Example Metric for Data Recovery Capability[2]

Metric					
What percentage of the organization's systems have not recently had their operating system or application binaries backed up (by business unit)?					
Quantifiable	✓	**Consistently Measurable**	✓	**Business Question**	✓
Measured as a percentage		*No subjectivity in whether or not binaries have been backed up*		*Answers critical question: can data be recovered in case of an emergency?*	

Associated Risk Thresholds		
Low Risk	**Moderate Risk**	**High Risk**
Less than 1%	1-4%	5-10%

Risk thresholds will vary largely for each measure based on the particular organization’s needs. For example, some organizations need 100% uptime and others could successfully operate on one to two hours of uptime. Risk thresholds are defined by overall business strategy of the organization.

The example above also provides insight into the second key aspect of a cybersecurity metrics program – the target metrics should illuminate where the most security risk exists in the organization.

[2] https://www.cisecurity.org/wp-content/uploads/2017/03/A-Measurement-Companion-to-the-CIS-Critical-Security-Controls-VER-6.0-10.15.2015.pdf

Prioritize Areas in the Organization Most Susceptible to Security Risks

Risk management is a foundational pillar of cybersecurity because there are inherent security risks that accompany any information technology infrastructure. Risks may come in the form of weakened networks, servers not updated to the latest patches, data center temperature controls malfunctioning, or even employees unaware of the most recent phishing trends.

All of an organization's cybersecurity decisions should be derived from a thorough understanding of the risks that accompany them. Risk management involves constantly refining the organization's risk tolerance strategy, formally assessing security risks, and tracking these risks using a robust metrics program. When an organization begins to define its risk tolerance strategy, metrics provide both a baseline with which to measure risk and milestones with which to track risk mitigation.

The CIS controls and thresholds mentioned previously provide a great starting point. Imagine a hedge fund, ABC Capital Management, which trades thousands of equities on the stock market. For ABC, data protection, data recovery, and server uptime are key for profitability. ABC's senior management meets periodically with their information security leadership team to discuss tolerable risk thresholds for system downtime, how long trading data should be retained (for auditors such as FINRA), and similar issues.

This is where an effective metrics program comes in. ABC's information security team should identify several key metrics which evaluate the organization's posture in data protection, data recovery, and server uptime. Quantifying the answers to questions such as: “What percentage of the organization's backups have not recently been tested by the organization's personnel,” “How long, on average, does it take to notify system personnel that a backup has failed to properly take place on a system,” and “What percentage of the organization's systems do not currently have comprehensive logging enabled in accordance with the organization's standard?” is crucial to fully understanding the organization's risk points. If ABC requires 95% of its trading systems to have up to date backups, and 30% of its backup programs haven't been recently verified, it becomes clear that a potentially costly security risk exists.

Cybersecurity health checks are a practical representation of this concept. Health checks depict a consistent suite of metrics which executives and front-line management can view at a glance to understand the security risk of the organization. Producing metric health checks can alert the proper stakeholders if a risk approaches an intolerable level.

Figure 3. Sample Health Check for IT Executive[2]

Metric	Description	Current	Goal
Backup Coverage	What percentage of the organization's systems have not recently had their data sets backed up?	95%	20%
Backup Testing	What percentage of the organization's backups have not recently been tested by the organization's personnel?	92%	30%
Remote TFA	What percentage of the organization's remote access users are not required to use two-factor authentication to remotely access the organization's network?	90%	35%
Sensitive Data Logging	What percentage of sensitive data sets are not configured to require logging of access to the data set?	89%	50%
Logging Coverage	What percentage of the organization's systems do not currently have comprehensive logging enabled in accordance with the organization's standard?	65%	50%
Log Failure Alerts	If a system fails to log properly, how long does it take for an alert about the failure to be sent (time in minutes - by business unit)?	1 day	<1 hour
Anti-Malware Coverage	What percentage of systems have not been deployed with enabled and up-to-date anti-malware systems?	20%	10%
Secure Configuration Coverage	What is the percentage of business systems that are not currently configured with a security configuration that matches the organization's approved configuration standard?	15%	10%
DLP Coverage	What percentage of the organization's business systems are not utilizing host based Data Loss Prevention (DLP) software applications?	25%	20%
Plaintext Sensitive Data	How many plaintext instances of sensitive data have been detected recently by the organization's automated scanning software?	2	0
Phishing Failures	What percentage of the organization's users, on average, will inappropriately respond to an organization sponsored email phishing test?	15%	5%
Recent Events of Interest	How many anomalies / events of interest have been discovered in the organization's logs recently?	300	250
Agg. Vuln Rating	What is the aggregate vulnerability rating for all application and database system in the organization?	3	2.5
Unauthorized Wireless Devices	How many wireless access points or clients have been discovered using an unauthorized wireless configuration recently in the organization?	5	3
Wireless Device Alerts	How long does it take to generate alerts about unauthorized wireless devices that are detected (time in minutes - by business unit)?	<1 hour	Instant

The best health check matrices are presented with drill-down capabilities, so a manager who notices that backup coverage is lacking can "click-in" and reach out to the responsible team to see what the issue is. This practice encourages an adaptive, real-time response to security risk.

[2] https://www.cisecurity.org/wp-content/uploads/2017/03/A-Measurement-Companion-to-the-CIS-Critical-Security-Controls-VER-6.0-10.15.2015.pdf

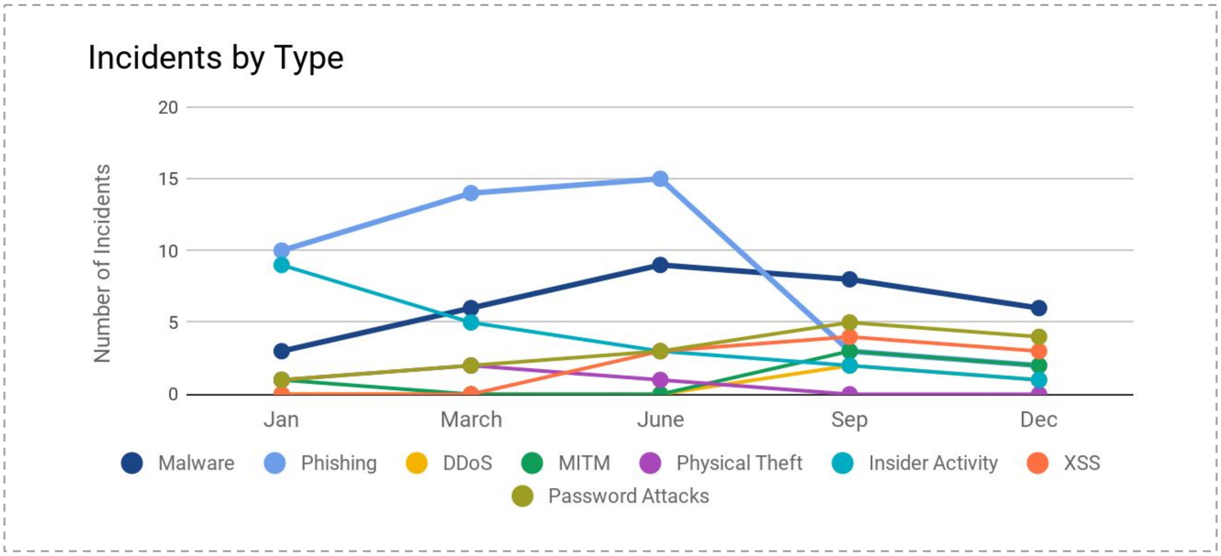
While a security risk metrics program does not explicitly tell an organization which risks need to be prioritized and how they can be managed, it does show the organizations where to look in order to track down risk and analyze it appropriately.

Monitor the Impact of Organizational People, Process, Technology, and Policy Changes

A clear benefit of an established metrics program is the ability to track the impacts of changes implemented in an organization's cybersecurity environment. Recording the same measurements before and after a policy, procedural, or technological change can provide insight about the efficacy of the change and any additional change management procedures that may be necessary.

Consider the example below. Imagine if ABC Capital Management implemented a phishing campaign and training program in June. After tracking the number of phishing incidents (alongside other types of incidents, for normalization), ABC can hypothesize that the phishing program successfully reduced the number of phishing incidents.

Figure 4. Annual Incident Report



Of course, other factors could actually be the root cause of this decrease in phishing incidents - other metrics that would be useful in this analysis could include the number of phishing attempts successfully reported by an ABC employee, as this metric can indicate if the number of phishing attempts went down as a whole from June to September. Using multiple angles of analysis can help guard an organization against the issue of "lurking variables."

Lurking variables is essentially a statistical problem where other variables at play might have changed the measurements outside of an implemented policy change. For example, assessing the impact of a February policy change by measuring an organization's security breaches in January and March is problematic because it is possible that March simply had fewer or more attempted breaches, and the policy change was negligible. Comparing measurements over time in a vacuum can increase an organization's likelihood to fall victim to this trap, but if the proper metrics are measured for an organization's needs, this side effect is minimized.

Marrying up multiple data points available in metrics programs that provide a broader business perspective makes for more accurate conclusions. Analyzing the phishing campaign figures alongside the figures of ten other types of attack vectors can negate the seasonality of cyberattack frequency in an analysis and allow for a larger focus on the impact of a phishing program. Additionally, measuring the quantity of phishing attempts successfully reported by employees before and after the program using a ratio as opposed to an absolute number can minimize this issue.

Changes to an organization's policies, procedures and technology are often more easily identifiable in the associated metrics because they are more closely tied to material change in the data being reported. An often-overlooked aspect of a security metrics program is evaluating the effectiveness of the organization's cybersecurity team(s).

Survey the Effectiveness of the Cybersecurity Team

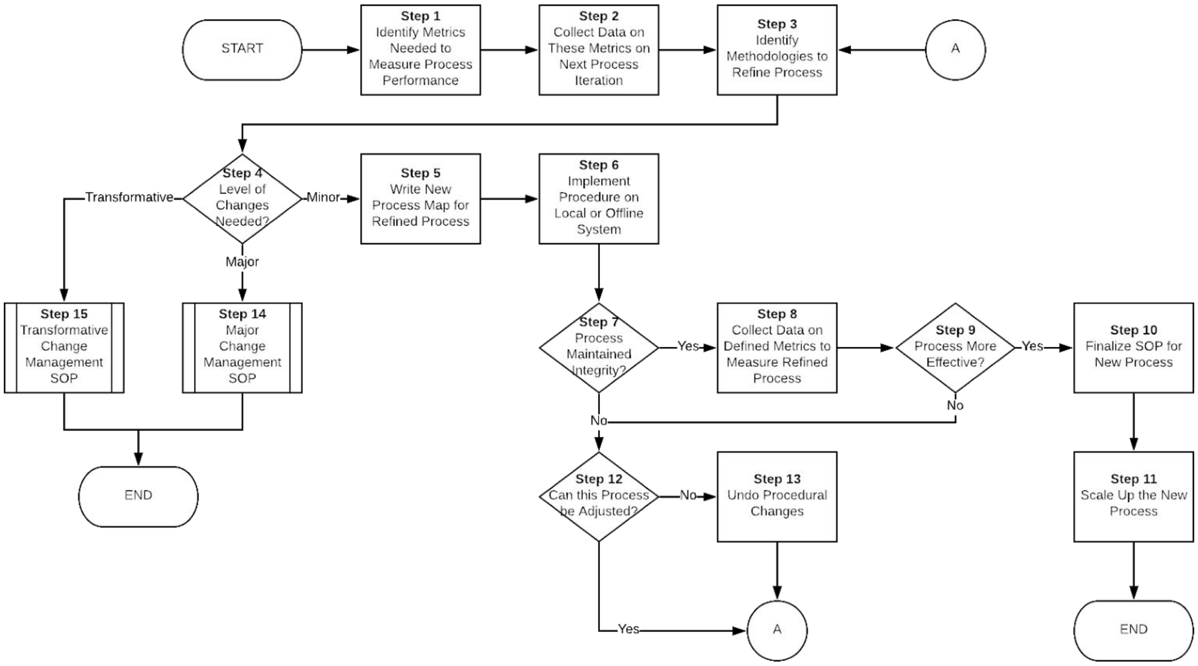
Business professionals across industries use program and portfolio management tools such as Jira and ServiceNow to track productivity and reallocate resources as necessary to bolster output, but these discussions rarely make headway in cybersecurity circles. This absence is especially risky as poor resource allocation in cybersecurity can lead to gaps in attack-surface coverage and pose additional risk to the organization.

Consider metrics such as the number of owned, open incidents per incident responder. This allows a front-line incident manager to analyze current resource allocation and drill-down into possible risks and gaps in coverage: Are there incidents that aren't being covered? Is one responder working on 70% of open incidents?. Team-based and process metrics are very easy to measure. There is minimal infrastructure required for data collection and analysis but capturing this data still provides a large benefit.

A prime example in team based-metrics is reviewing the efficiency of the organization's Security Operations Center (SOC), the group that watches the perimeter for potential breaches. Team-based metrics enable a manager to evaluate if the SOC is properly resolving and escalating events. Key questions include: Is there a gap in coverage on certain devices/subnets? Is the SOC properly escalating events? Are they resolving too many events prior to escalation? Not enough events? Metrics like these can inform a security manager if the current event notification schema is either too hands-on or too hands-off. Plus, resolving basic issues like these both save costs and mitigate risk. Moreover, the SOC is one of the most manually-run programs in current cybersecurity organizations and because the SOC is the front line of cybersecurity defense, measuring its effectiveness is all the more important.

As an added benefit, process evaluation and process reengineering are more straightforward with consistent process measurements. Consider the below process map for process reengineering. Metrics identification and conducting consistent process measurements are cornerstones of effective process improvement as they provide a lens to identify the areas where changes would yield the best value.

Figure 5. Process Reengineering Flow


START
Step 1 Identify Metrics Needed to Measure Process Performance
Step 2 Collect Data on These Metrics on Next Process Iteration
Step 3 Identify Methodologies to Refine Process
A
Step 4 Level of Changes Needed?
Transformative
Minor
Major
Step 5 Write New Process Map for Refined Process
Step 6 Implement Procedure on Local or Offline System
Step 15 Transformative Change Management SOP
Step 14 Major Change Management SOP
END
Step 7 Process Maintained Integrity?
Yes
Step 8 Collect Data on Defined Metrics to Measure Refined Process
Step 9 Process More Effective?
Yes
Step 10 Finalize SOP for New Process
No
No
Step 12 Can this Process be Adjusted?
No
Step 13 Undo Procedural Changes
Step 11 Scale Up the New Process
Yes
A
END

Promote a Culture of Constant Iteration

Creating a metrics program from scratch can seem daunting, particularly when we consider the number of strategic questions that can be answered when the appropriate data is available to decision-makers. Add to that the infinite number of ways it is possible to create the answer to those questions using measurable metrics, and the effort ahead can become unruly very quickly.

The key to overcoming this hesitation is to start small. By providing a metrics team and the relevant stakeholders grace and time to figure things out, the pressure subsides and creativity can blossom. As the team starts to gather data, they will quickly delineate what is important and what is not important - ultimately spawning new ideas that leadership would prefer to focus on in the long run.

Rather than taking a waterfall approach to planning out every detail in advance, utilize Agile practices to create manageable pieces of the overall puzzle. This culture promotes learning how to complete the work as a team, effective and frequent stakeholder engagement, flexibility to adapt to changing circumstances, and perhaps most importantly - provides the foundation for constant iteration. As cybersecurity threats change, so too should the ways we track and tackle them.

Conclusion

These five components – a common assessment framework, prioritization of information, change monitoring, measuring team effectiveness, and embracing constant iteration – build the foundation for a comprehensive metrics program. As with all transformational efforts, engaging leadership in a transparent conversation with front-line managers and those who “live in the day-to-day” brings to light the appropriate data points to track and share with relevant stakeholders.

Ultimately, a well-rounded metrics program that is customized to an organization’s specific business needs will not only answer the question, “What data do we need?”, but provide actionable insights that answer “What can we learn from these conclusions?”. There are plenty of platforms that track metrics and provide actionable insights on what to do with the information. Which metrics are most important to track for your organization’s success?

ABOUT THE AUTHORS

Shelby Balius is a Manager within DayBlink's Organization & People Center of Excellence

Aditya Krishnamurthi is a Senior Consultant within DayBlink's Cybersecurity and Digital Centers of Excellence.

Michael Morgenstern is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence

Justin Whitaker is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence

ABOUT DAYBLINK

In today's cybersecurity environment, the threat landscape is rapidly evolving. It's outpacing the current defensive resources and skill sets of most corporations – meaning many companies are falling victim to attacks by malicious agents. The way we do business is also changing – with more data stored, living in the cloud, and constantly demand on the go. Breaches can mean losing clients and customers overnight.

DayBlink works with clients to improve their security posture. We assess threats and vulnerabilities, identify organizational risk, prioritize remediation efforts, and implement solutions to secure IT environments and critical assets from sophisticated cyber-attacks.

DAYBLINK

For more information:
Visit: www.dayblink.com/services/technology/cybersecurity
Email: cybersecurity@dayblink.com
Call: 1 (866) 281-4403