Secureworks®

WHITE PAPER

What You Need to Know About Measuring Cybersecurity Progress and Success

Cybersecurity is a must-have competency for organizations across every industry. However, faced with an ever-evolving threat landscape that requires constant upgrades and attention, executive leaders are increasingly asking their cybersecurity teams to provide performance updates and reports in order to justify their budgets and expenditures.

The Current Cybersecurity KPI Landscape

Robust performance measurement can deliver security teams the proof to show they are meeting their goals, and in the process, their leaders can gain a better understanding of their security posture and the risks that their organization faces. Yet all too often, organizations do not have any type of measurement system in place, or if they do, varying compliance rules and a decentralized leadership structure have forced them to report against a wide, disconnected variety of key performance indicators (KPIs) that fail to tell a holistic story. This haphazard approach to measurement is harmful to cybersecurity teams within their organizations, particularly those that do not have a CISO or C-suite level leader advocating for them.

According to the EY Global Information Security Survey 2020[1], less than half of respondents (48%) say that their board does not yet have a full understanding of cybersecurity risk, while 43% say that the board does not fully understand the value and needs of the cybersecurity team. Even more tellingly, six in ten organizations say that they cannot quantify the effectiveness of their cybersecurity spending to their boards.

Ongoing changes to the global economy have tightened already strained security budgets and created unknowns that must be addressed with a well-defined strategy. Understanding the important role of cybersecurity KPIs and defining the right goals for your organization can help make the case for security teams as a necessary resource by clearly demonstrating security performance value.

This paper will explore the benefits of having security KPIs and the considerations you should address before developing them.

48%

of EY Global Information Security Survey 2020 respondents say their board does not yet have a full understanding of cybersecurity risk.

6 in 10

organizations say that they cannot quantify the effectiveness of their cybersecurity spending to their boards.

[1] EY, How does security evolve from bolted on to built-in?

Availability varies by region. ©2022 SecureWorks, Inc. All rights reserved.

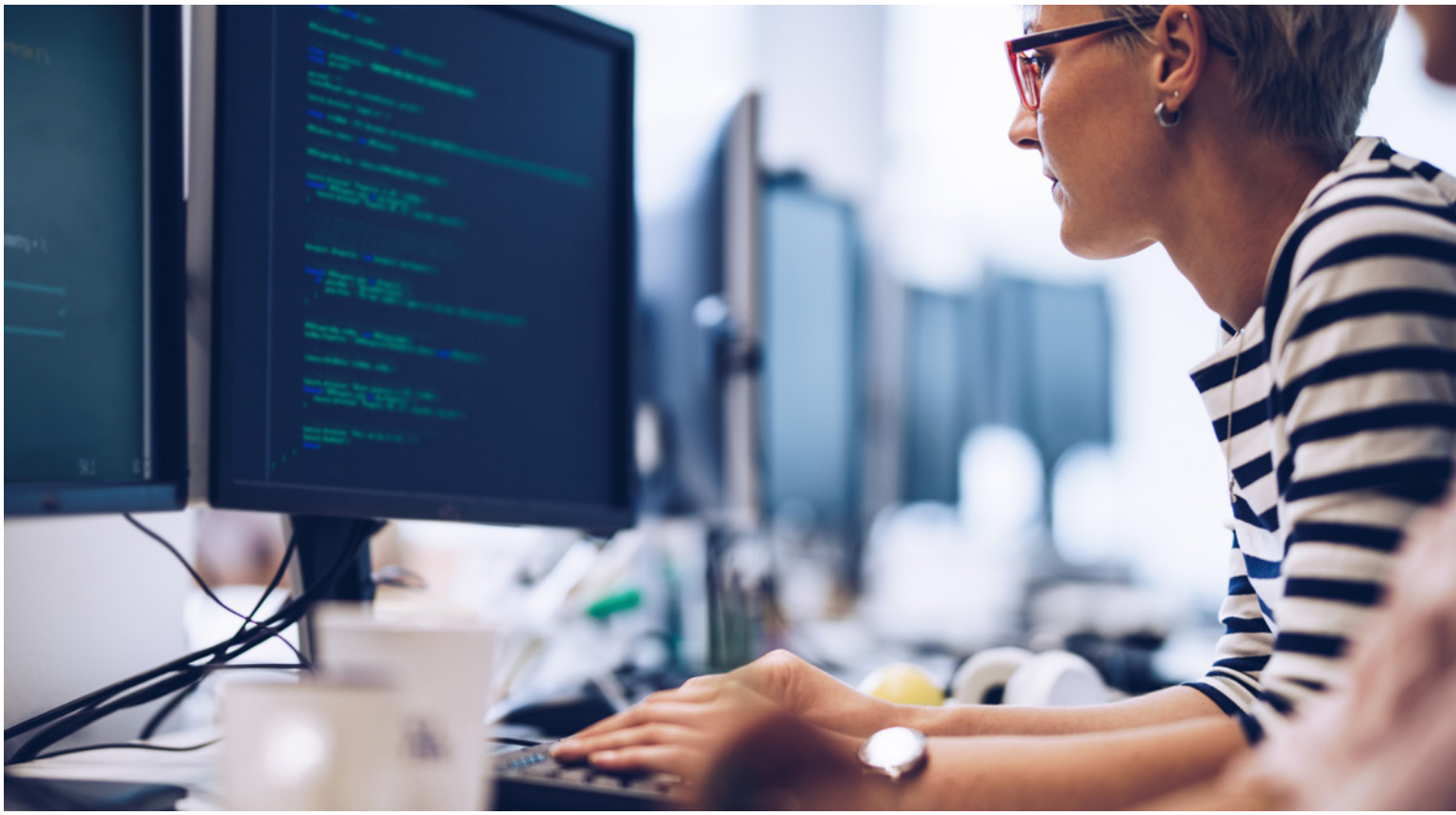
Where Does Your Organization Stand?

Before determining how your organization can measure success, it's important to first understand the current maturity of your program by undertaking a business impact analysis of your organization's systems and processes. By benchmarking your current status, you can set the standard of measurement for future progress.

In some cases, if the program has grown reactively in response to incidents, measurement can't begin without first building a central strategy. This is a key element, since once the strategy is in place, measurement naturally follows to ensure progress on key milestones and adherence to the timeline for delivery. The most successful organizations not only demonstrate buy-in on their strategy from executive leadership, but also a clearly articulated roadmap, which defines the roles that their processes, people, and technology will play.

For organizations looking to build or expand their strategies, there are several robust frameworks to serve as guides. For example, the National Institute of Standards and Technology's (NIST) Cybersecurity Framework is commonly used by all types of organizations.

It's important to first understand the current maturity of your program by undertaking a business impact analysis of your organization's systems and processes.



Availability varies by region. ©2022 SecureWorks, Inc. All rights reserved.

How to Build an Effective Measurement Action Plan

Once you've established your strategy, it's time to build a measurement plan. When determining what to evaluate, be sure to consider the different audiences involved. For example, the information delivered to a CISO will be very different than what's given to an executive leadership team, since the latter will have a bigger focus on the risk facing an organization, rather than pure metrics.

Once again, a good cybersecurity framework is a helpful tool in clarifying performance to business leaders. The NIST Cybersecurity Framework, for example, provides clarity by breaking the information into five key pillars to measure against when discussing cybersecurity threats: Identify, Protect, Detect, Response Rate, and Recovery. Let's explore these areas further.

A good cybersecurity framework is a helpful tool in clarifying performance to business leaders.

Identify: Identify is about providing foundational understanding to how an organization is managing cybersecurity risk to systems, people, assets, data, and capabilities. This process is about identifying the business context, critical function resources, and the related cybersecurity risks that help an organization to focus and prioritize its efforts. Examples include identifying an organization's physical and software assets or identifying the legal and regulatory requirements associated with a particular industry and how the organization's policies stack up.

Protect: Protect is about defining the appropriate safeguards to ensure consistent delivery of critical infrastructure services and working to limit or contain the impact of a potential cybersecurity event. Examples include rolling out physical and remote access controls within the organization and providing staff trainings.

Detect: Detect is about defining the appropriate activities to identify that a breach or cybersecurity event has occurred. Examples include continuous monitoring or tracking to ensure events and incidents are detected, and their potential impact is understood.

Respond: Respond is about undertaking the appropriate activities to take action following a detected cybersecurity incident. Examples include the execution of response planning process following an event and managing communications to different stakeholder groups.

Recover: Recover is about identifying ongoing activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. Examples include ensuring the organization implements recovery processes in a timely manner and restoring systems and assets that were affected.

Availability varies by region. ©2022 SecureWorks, Inc. All rights reserved.

Understanding your organization's performance with regard to these five pillars can help determine where weaknesses lie. For example, if you do not yet have a response plan in place to address a breach, your future goals should be centered around the timeline and deliverables associated with this pillar.

While every organization's specific KPIs will be different depending on where they are in their journey, key categories every organization should consider include:

Risk Score – What is the risk score from a cybersecurity perspective and a business point of view? Has your risk score changed in light of recent changes to the business landscape?

Human Capital – How are your people putting your organization at risk? Phishing is one of the most common ways for incidents to happen, and that occurs through human error.

Asset Management – What are the key assets that your organization has, and how are they being protected? You can only control/trace what you know.

Incidents – How effective is your team at catching incidents? What is your response to recovery time ratio?

Availability varies by region. ©2022 SecureWorks, Inc. All rights reserved.

The Importance of Measuring Progress

With other business priorities and a focus on maintaining daily operations, measuring cybersecurity progress or maturity is all too easy to ignore. However, in our constantly evolving corporate environment, business leaders are increasingly looking for security teams to justify their budgets and value to the organization. Goal setting within the context of a larger framework and strategy provides a clear demonstration of how security leaders are helping to meet organizational goals and protect assets within an uncertain and unpredictable world.

For CISOs and security leaders, this is an opportunity to rethink your approach to enterprise risk and build an integrated strategy that will protect your organizations now and well into the future.

Goal setting within the context of a larger framework and strategy provides a clear demonstration of how security leaders are helping to meet organizational goals and protect assets within an uncertain and unpredictable world.

Availability varies by region. ©2022 SecureWorks, Inc. All rights reserved.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Otemachi One Tower 17F
2-1 Otemachi 1-chome, Chiyoda-ku
Tokyo 100-8159
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region. ©2022 SecureWorks, Inc. All rights reserved.