AXONIUS

Your framework for building cybersecurity program metrics

How to get started with identifying the right metrics and showcasing value

Metrics matter.

They're how all teams showcase value to the business. When it comes to cybersecurity, communicating metrics to both technical and non-technical audiences has become paramount in the age of evolving cyberthreats. In the past, the approach to cybersecurity was "don't let it get in the way of our work." Today, sophisticated threats have elevated cybersecurity to a strategic program within many companies, with heavy scrutiny on CISOs to prove the efficacy of the program and optimize costs. This means that generic approaches to cybersecurity measurement are no longer effective.

In this guide, we'll cover how security teams can build a risk-based approach to identifying the cybersecurity metrics that matter most to their business.

"Why should we track cybersecurity metrics?"

If you're a cybersecurity expert, the answer to the question is obvious - why *wouldn't* we track cybersecurity metrics? After all, we track metrics for every other business unit. That said, it can be challenging to communicate the ***why*** to non-security audiences.

Start with this	Instead of this
A stronger focus on meeting compliance regulations will help us limit future business disruption	Our policies and security documentation do not adhere to ____ compliance requirements
We can maintain our competitive edge by investing more in privacy	We want to implement _____ to help with customer data privacy
We've identified gaps in our policies that make us more susceptible to phishing and/or ransomware attacks	We require stronger email security and encryption technology
We don't have the right data insights to make accurate decisions on program spend	Our SIEM tool isn't working for us

53%

of organizations believe that cybersecurity is part of the core transformation team, indicating integration of cybersecurity in strategic business objectives.

Accenture, State of Cybersecurity Resilience 2023

Breaking down metrics

Where do you start in building a metrics-driven security program?
The goal is to identify outcome-driven metrics.

Least contextualized → **Most contextualized**

KPIs
(Key Performance Indicators)

a measure of whether or not a business unit has achieved its established goals at the highest level, and are therefore generally consistent in business units across companies

Metrics tied to strategic business objectives

- Security spending governance
- $$$ saved from blocked incidents
- % employees trained on security awareness
- Average SLAs for external and internal response

KRIs
(Key Risk Indicators)

skew towards measuring when something is headed in the wrong direction, and are typically associated with actions for getting things back in the right direction. As a result, KRIs start to become more contextualized to your company.

Metrics that signal potential risks

- Quarterly or semi-annual pass rate for audits
- # of Incidents/data breaches
- % of business units that fail to adhere to organizational security policies
- Vulnerabilities identified vs vulnerabilities patched in a given month/quarter

Internal reporting

KCIs
(Key Control Indicators)

a measure of the effectiveness of your company's security policies, process and systems. KRIs measure risk, KCIs measure the performance of the controls that you have in place used to mitigate those risks. This means KCIs are very business-specific, and will vary from company to company.

Effectiveness of an organization's policies, process and systems

Asset Inventory	• % of assets in policy
Patching	• % critical patches deployed in x hours
Endpoint Security	• % endpoints in policy
Identity Mgmt	• % of systems utilizing SSO and MFA • % of accounts not in SSO solution
Incident Response	• Mean time to detect • Mean time to recover • % incidents with critical business impact ($$$)
Key Asset (crown jewel) coverage	• % of critical assets covered by vuln scanning

Board reporting

Let's dig into this more.

Ultimately, historical trends in KCIs that are contextualized to your security org and business will give you the best sense of your security program efficacy. Here's a couple of examples of how to track targeted KCIs.

Do this	Instead of this
# of security incidents resolved within 48 hours each quarter → compare each incident to your MTTD	# of security incidents resolved each quarter
% of endpoints within policy each month and each quarter	# of critical vulnerabilities identified
% of critical assets covered by vulnerability scanner each week	Frequency of vulnerabilities identified each week
% of active users assigned to single sign-on and MFA	# of apps with SSO and MFA configured
Ratio of authorized to unauthorized logins (intrusion attempts) each quarter and % of successful vs blocked intrusion attempts	# of intrusion attempts per quarter

Pro tip

Think about KCIs in the context of a percentage or ratio, rather than a hard number. For example, don't just track the number of incidents that were resolved, track the % of all incidents that were resolved within 48 hours, and compare that number to your target MTTD.

Building a cybersecurity metrics framework

1. Identify metric categories (see the CIS Controls Measure and Metrics as an example)
2. Identify specific metrics within each category
3. Identify asset type
4. Identify the prioritization of each metric
5. Identify your current completion rate vs targets for each metric
6. Status

Example

Category	Metric	Asset Type	Priority	Current	Target	Status
Asset Discovery	# of critical assets not scanned by vulnerability tool	Endpoints, Infrastructure	P0	12%	5%	In Progress
Identity Mgmt	% of active users not secured with multi-factor auth	Users	P0	30%	15%	At Risk
Vulnerability Mgmt	% of assets with critical vulnerabilities not patched	Endpoints, Infrastructure	P0	15%	5%	In Progress
Incident Response	% of incidents with critical business impact (costs $x+ to remediate)	Any	P1	7%	5%	In Progress

The data you'll need to build out these dashboards can be sourced from platforms that support cyber asset management, vulnerability management, SaaS management, and more. Ideally, you'll utilize a unified platform that will enable you to pull the data for your reporting in a consistent manner to share across teams.