RAPID7

OVERVIEW

Cybersecurity Target Operating Model KPIs

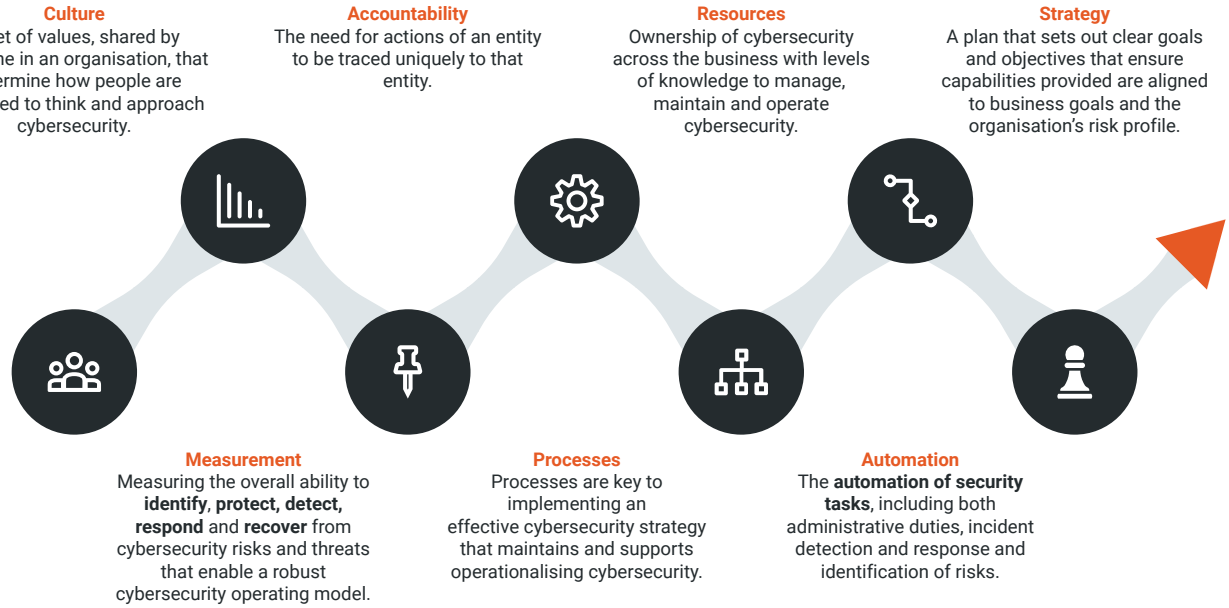
Contents

Cybersecurity Target Operating Model KPIs

1. Purpose, Maturity and Scope

1.1. Purpose

This document provides an overview of the baseline Key Performance Indicators (KPIs) required to implement a Cyber Target Operating Model (TOM). A TOM enables the application of a strategy or vision to a business or operation. It is a high level representation of how a company can be best organised to more efficiently & effectively deliver and execute the organisation's strategy. In order to support and measure the Target Operating Model, foundational components of cybersecurity are required to establish enablement and effectiveness. The foundational components of the Target Operating Model are:



The core focus of this document is to provide KPIs that are used across the life cycle of the Target Operating Model. The KPIs are categorised based on the level of maturity for each foundational component of cybersecurity and by persona. Core descriptions are identified for each KPI:

ITEM	DESCRIPTION
KPI name	The name of the KPI
KPIs description	A description clearly defines its objective
Measured by	How the KPI tracks and measures change
KPI target threshold	Suggested threshold for KPI effectiveness
Persona	Persona to which KPI is aligned
Foundational component	KPI required to support and enable the effectiveness of the foundational component
Maturity level	Required to achieve the level of maturity

1.2. What is a KPI

A KPI (Key Performance Indicator) intends to help you evaluate a metric's current value and status against a defined target. A KPI requires a base measure that evaluates to a value, a target measure or value, and a threshold or goal. A KPI dataset needs to contain goal values that focus towards outcomes.

KPIs in cybersecurity offer valuable insights that showcase and translate the success of security management and technical data into a format and language that all stakeholders can understand while helping make important decisions to improve an organisation's cybersecurity operating model. KPIs are crucial as they offer valuable insights into the health and effectiveness of an organisation's objectives. However, only a small percentage of organisations use or even consider the need and use of KPIs.

1.3. KPIs for Cybersecurity

Cybersecurity metrics and KPIs are crucial indicators that help security teams, and business stakeholders understand how their security controls function over time. KPIs offer a broader business context of how the security programme works, what has been implemented correctly, and which areas need attention, allowing security teams to validate the effectiveness continuously. As security threats constantly evolve, cybersecurity management is a continuous undertaking that relies on KPIs to measure performance and drive security decisions.

1.4. The Importance of KPIs

KPIs allow cybersecurity teams and businesses to measure security efforts, facilitating the Chief Information Security Officer (CISO) and business stakeholders to leverage these KPIs to demonstrate the returns on investment towards security spending. KPIs are also commonly used to raise security awareness across cross-functional teams and vendors. Including KPIs in cybersecurity awareness training results in a comprehensive understanding of security threats and the roles of various business units.

There are many reasons why KPIs are important, but here are four that stand out:

- KPIs strengthen employee morale
- KPIs support and influence business objectives
- KPIs foster personal growth
- KPIs are critical for performance management

1.5. Using KPIs to Enable Cybersecurity Maturity

To start operationalising cybersecurity using a Target Operating Model we first need to set the maturity of each foundational component of cybersecurity as defined in the purpose. Mature foundations will help ensure your business takes control of cybersecurity and can track the effectiveness of managing risks and threats. For each of the Target Operating Model foundational components, the requirement is to increase the level of maturity from Initial to Adaptive. The table below shows the levels of maturity that will be used to track the level of maturity for each foundational component.

STAGE	MATURITY LEVEL	DESCRIPTION
Initial	1	Cybersecurity is typically performed ad hoc/reactive, and activities are typically served with little to no prioritisation based on the degree of risk those activities address.
Risk-Informed	2	While risk management practices are not standardised, they directly inform the prioritisation of cybersecurity activities alongside organisational risk objectives, the threat environment, and business requirements.
Repeatable	3	Formally approved risk management practices are expressed as policy. These practices are regularly updated based on business requirements and the changing threat landscape.
Adaptive	4	Organisations adapt their cybersecurity practices based on previous and current activities, including lessons learned and predictive factors. Processes of continuous improvement - including incorporating advanced cybersecurity technologies.

1.6. Scope

- **Priority 1 "must have":** Foundational components that create and enable the "Initial" level of maturity to start the journey from the Current Operating Model to the Target Operating Model.
- **Priority 2 "should have":** Foundational components that enhance Priority 1 foundational components to start and underpin the level of maturity.
- **Priority 3 "target":** Foundational components that achieve and complete the six core foundations of the Target Operating Model, ensuring long term success of the Target Operating Model.

PRIORITY 1 FOUNDATIONS	PRIORITY 2 FOUNDATIONS	PRIORITY 3 FOUNDATIONS
Culture	Culture	Culture
Measurement	Measurement	Measurement
	Accountability	Accountability
	Process	Process
		Resources
		Automation

2. Personas and KPI Categories

2.1. Personas

It is important to note that KPIs need to be aligned to different personas within your business. The KPIs categorised will align and support different personas across your business. A set of example personas can be seen below:

- Board members
- Executives (CXO)
- CISO
- Head of Security
- SecOps
- DevOps
- Product management
- Development and Engineering teams
- General employees
- Human resources

2.2. KPI Categories

The first step in operationalising cybersecurity within a targeted area is setting the maturity of each foundation. A strong foundation will protect all systems from attacks and emerging threats. People play a critical role in providing protection and cyber resilience. They should be aware of potential risks so they can take appropriate actions to protect themselves and their business function.

STAGE	DESCRIPTION
Culture	A set of values and KPIs shared by everyone in an organisation determines how people think and approach cybersecurity. Cultural KPIs should emphasise, reinforce, and drive behaviour to create a resilient workforce.
Measurement	KPIs measure and track the ability to identify, protect, detect, respond, and recover from cybersecurity risks and threats, enabling a robust operating model. The best approach requires KPIs to understand your most significant risks.
Accountability	KPIs that generate traceable actions to a person or entity to support non-repudiation, deterrence, fault isolation, intrusion detection, prevention, after-action recovery, and legal action.
Process	Critical processes to implement an effective strategy, maintaining and supporting the process of operationalising cybersecurity.
Resources	Increased knowledge and ownership to manage, maintain and operate cybersecurity.
Automation	Automate security tasks to include administrative duties, incident detection, response, and identification of risk.

3. Priority 1 KPIs

3.1 KPIs That Support Culture and Measurement

3.1.1 Approach to Cybersecurity

KPI Name	Approach to Cybersecurity
Description	All stakeholders and employees acknowledge the importance of Cybersecurity and what is required from them.
KPI Category	Culture
Measurement	Acknowledging what is expected from them and adhering to policy
KPI Owner	Human Resources - Head of Security - CISO
KPI Target	100% of all board members 100% of all Executives (CxO) CISO and or Head of Security 80-90% of all employees
Personas accountable to KPI	All personas in a business

3.1.2 Security Policy Acknowledgement

KPI Name	Policy Acknowledgement
Description	At a minimum, every security awareness programme should communicate security policy requirements to staff. In addition, tracking employee policy acknowledgements will ensure your workforce is aware of the policy and helps the organisation meet compliance requirements.
KPI Category	Culture
Measurement	Acknowledging what is expected from them and adhering to policy
KPI Owner	Human Resources
KPI Target	100% of all board members 100% of all Executives (CxO) CISO and or Head of Security 100% of all employees
Personas accountable to KPI	All personas in a business

3.1.3 Self-Reporting

KPI Name	Self-reporting
Description	A quick response to a security incident can significantly reduce damages from an attack. Your security awareness training should teach your workforce what to do if they download a malicious file or click a phishing email. While the goal of your programme should be to help the workforce avoid attacks altogether, this KPI will prove you have safeguards in place in the event of a breach.
KPI Category	Culture - Measurement
Measurement	Monthly stats on self reported security incidents
KPI Owner	Head of Security - CISO - IT
KPI Target	No target; however, monthly stats showing the rate of reported incidents - The greater the number, highlights culture and awareness is changing
Personas accountable to KPI	All personas in a business

3.1.4 Security Awareness Training

KPI Name	Security Awareness Training
Description	Security awareness training that all employees have undertaken.
KPI Category	Culture - Measurement
Measurement	New joiners
KPI Owner	Human resources
KPI Target	No target; however, monthly stats showing the rate of reported incidents - The greater the number shows culture and awareness is changing
Personas accountable to KPI	All personas in a business

3.1.5 Number of Security Breaches

KPI Name	Number of Security Breaches
Description	Reducing breaches over time, especially those related to human error is a good indicator of program success.
KPI Category	Culture - Measurement
Measurement	Reported breaches and detected breaches
KPI Owner	Head of Security - CISO - IT
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	All personas in a business

3.1.6 Vulnerability Health

KPI Name	Vulnerability Health
Description	This KPI can be presented as overall user health to vulnerability management.
KPI Category	Measurement
Measurement	Monthly vulnerability reports cover key internal assets and all external assets. Track and monitor the number of vulnerabilities over time by level of Risk.
KPI Owner	Head of Security - CISO - IT
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	DevOps, SecOps, IT

3.1.7 Phish Rate

KPI Name	Phish Rate
Description	Measurement of phishing rates through phishing simulation programmes that track learners' abilities to detect and avoid phishing emails.
KPI Category	Measurement
Measurement	A reduction in phishing rate over time proves increased awareness of security threats.
KPI Owner	Head of Security - Human resources
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	All

3.1.8 Time to Detect

KPI Name	Time to Detect
Description	This KPI is the average time that passes between the creation and detection of a vulnerability.
KPI Category	Measurement
Measurement	Example, an attack happened on Tuesday, but it was discovered only three days later by the system or IT people. The lesser this time gap is, the more efficient your vulnerability management program is
KPI Owner	Head of Security -CISCO
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	All

3.1.9 Vulnerability Time to Resolution

KPI Name	Vulnerability Time to Resolution
Description	This KPI determines the average time it takes to find a resolution to a vulnerability.
KPI Category	Measurement
Measurement	From the time of identifying the vulnerability to the time of resolution
KPI Owner	Head of Security -CISCO
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	All

3.1.10 Time to Mitigation

KPI Name	Time to Mitigation
Description	Determines the average time it takes to alleviate the attack. For example, while Time to Resolution is about finding a resolution, Time to Mitigation relates to the deployment of resolution to contain the vulnerability from further worsening the situation.
KPI Category	Measurement
Measurement	From the time of identifying the vulnerability to the time of mitigation
KPI Owner	Head of Security -CISCO
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	All

3.1.11 Number or Open Critical and High-risk Vulnerabilities

KPI Name	Number or Open Critical and High-risk Vulnerabilities
Description	Tracking of vulnerabilities based on risk level.
KPI Category	Measurement
Measurement	Number of vulnerabilities based on asset and or scope
KPI Owner	Head of Security -CISCO
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	Owners of assets or scope

3.1.12 Number of Exceptions

KPI Name	Number of Exceptions
Description	Determines and tracks the number of vulnerabilities that are pending resolution. These vulnerabilities may not be old or high risk, but still need to be regularly tracked to mitigate future risks.
KPI Category	Measurement
Measurement	Number based on asset and or scope and dates
KPI Owner	Head of Security -CISCO
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	Owners of assets or scope

3.1.13 Vulnerability Re-open Rate

KPI Name	Vulnerability Re-open Rate
Description	The requirement to track recurring vulnerabilities that continue to be the same.
KPI Category	Measurement
Measurement	Repeating occurrence of the same vulnerability
KPI Owner	Head of Security -CISCO
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	Owners of assets or scope

3.1.14 System Hardening Rate

KPI Name	System Hardening Rate
Description	Determines whether your organisation's applications, network infrastructure devices, and operating system are properly configured.
KPI Category	Measurement
Measurement	CIS Benchmarks
KPI Owner	Head of Security -CISCO
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	Owners of assets or scope

3.1.15 Risk by Business Unit or Asset Group

KPI Name	Risk by Business Unit or Asset Group
Description	Determines the risk level that each business unit or asset group of your organisation faces due to vulnerabilities. This will help you to focus your vulnerability management programme priorities accordingly.
KPI Category	Measurement
Measurement	The number of risks relative to the business function
KPI Owner	Head of Security -CISCO
KPI Target	To be defined by the KPI owner
Personas accountable to KPI	All

Next steps

While you're never going to guarantee 100% that you'll be able to stop attacks from happening, being prepared will decide the extent to which an attack could damage your organisation. Attackers will always try to remain one step ahead of any measures you may have in place, so consider how a partner can help you further your cyber resilience, particularly in light of the current lack of skills and resources.

As a partner to many organisations globally, we guide them through the myriad of cybersecurity challenges, providing that vital level of expertise and support to your team.

To watch the cybersecurity webcast series 'Hackers're Gonna Hack' on-demand click here

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organisations strengthen their security programmes in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web.

We foster open source communities and cutting-edge research–using these insights to optimise our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

Contact Rapid7 to see how we can help you.

North America:
+866.7.RAPID7 | sales@rapid7.com

EMEA:
+44.1183.703500 | emeasales@rapid7.com

APAC:
+65.3159.0080 | apacsales@rapid7.com

@rapid7 | rapid7.com