Four Steps to Develop Outcome-Driven Metrics for Cybersecurity

Published 27 September 2023 - ID G00787963 - 11 min read

By Analyst(s): Paul Proctor, Shruthi Shankel, Emily Tan, Richard Addiscott, Paul Furtado, Christopher Mixter

Initiatives: Technology Finance, Risk and Value Management; Procurement Functional Enablement

Outcome-driven metrics have a direct line of sight to the operational outcomes of investment and to the level of protection delivered in a business context. Using ODMs, CIOs can more effectively drive priorities and investments that balance the need to protect the business with the need to run it.

Additional Perspectives

- Summary Translation: Four Steps to Develop Outcome-Driven Metrics for Cybersecurity
  (19 December 2023)

Overview

Key Findings

- Senior business executives and boards of directors are increasingly seeking assurance that the organization's cybersecurity capabilities are appropriate and delivering the outcomes expected.
- Cybersecurity metrics are typically backward-looking, operational metrics that do not support decision making for priorities and investments.
- Quantifying protection levels represents a new approach for most organizations and will require investments in instrumenting systems and processes to gather new types of data.

Recommendations

CIOs focused on developing cybersecurity outcome-driven metrics (ODMs) should:

- Define protection-level outcomes by articulating the benefits of both operational performance and desired protection benefits against any control.
- Empower executive investment decision making by describing the trade-offs between cost and value for each control.
- Direct investment by defining the impact the control will have on business-related security threats or incidents.
- Articulate the benefits of cybersecurity investment by measuring ODMs against supporting technologies for discrete business units, operating functions or departments that create business outcomes for the organization.

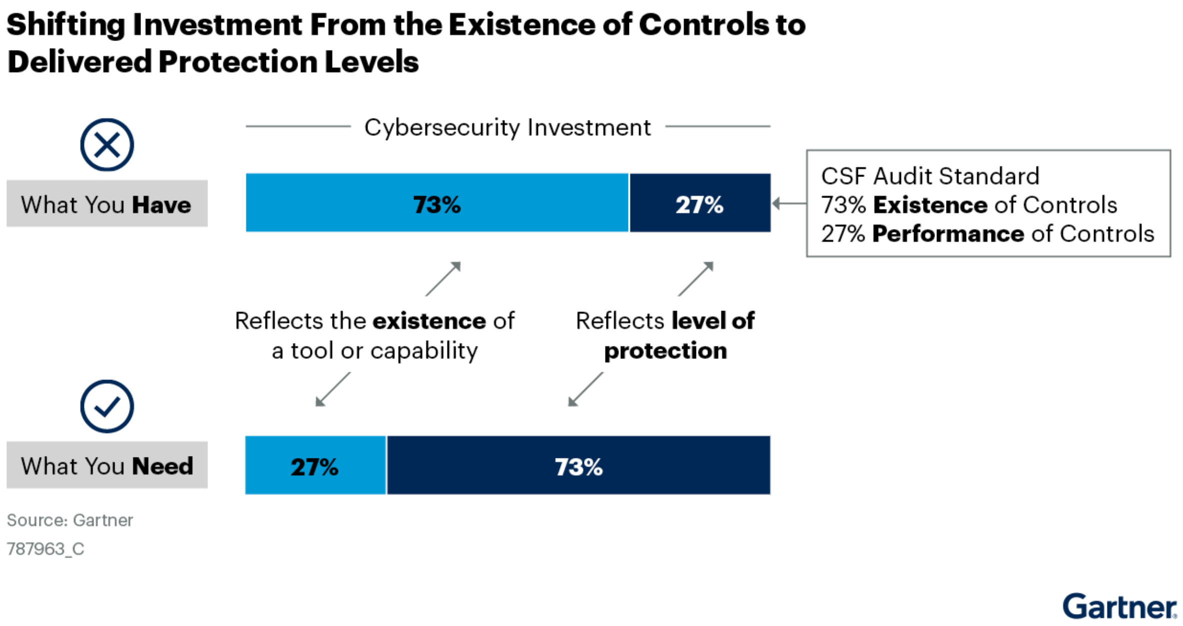
Introduction

A good metric should inform decision making, align with business outcomes, and guide priorities and investments. However, common limitations of typical cybersecurity metrics include:

- Spending metrics that do not guide investment, because spend does not reflect protection levels. Organizations with a very high spend in cybersecurity can deliver very poor protection and vice versa.
- Maturity metrics that lose effectiveness to guide investments at higher levels of maturity. For example, moving from a 3.4 to a 3.6 maturity level can be highly subjective.
- Backward-looking, operational metrics that are lagging indicators of risk and do not reflect protection levels and do not guide investments. For example, the number of emails that were blocked is not connected to how well the organization is protected, and we cannot make a direct investment to change it.

A 2019 analysis of audit standards for the National Institute of Standards and Technology (NIST) Cybersecurity Framework showed that 73% of the audit questions are related to the existence of controls, not their performance or levels of protection (see Figure 1).

Figure 1: Shifting Investment From the Existence of Controls to Delivered Protection Levels


Shifting Investment From the Existence of Controls to Delivered Protection Levels
Cybersecurity Investment
What You Have
73%
27%
CSF Audit Standard
73% Existence of Controls
27% Performance of Controls
Reflects the existence of a tool or capability
Reflects level of protection
What You Need
27%
73%
Gartner

Source: Gartner
787963_C

ODMs address these limitations. A cybersecurity ODM is a metric that acts as both a protection level and a value lever. This means the metric reflects how well an organization is protected, not how it is protected.

ODMs measure cybersecurity outcomes achieved by specific investments. They are constructed by aligning what is measured with the intended protection outcome of the investment. In this manner, ODMs simultaneously reflect protection levels and value for investment. Benchmarked ODMs create peer comparisons to guide defensible cyberinvestments.

For example, the time to patch vulnerabilities is an ODM because:

- It represents an outcome of an investment in threat and vulnerability management.
- It reflects a protection level, because patching faster reduces the time vulnerabilities are available for exploitation.
- It is a value lever, because it supports direct investment to achieve desired protection-level outcomes.

However, vulnerabilities patched in the past six months are not ODMs, as they are backward-looking and do not connect directly to business outcomes.

Gartner's Tool: Catalog of Business-Aligned Outcome-Driven Metrics for Risk and Security provides more than 130 examples of cybersecurity ODMs across 20 different control investments. Gartner's The Gartner Cybersecurity Business Value Benchmark, First Generation provides 16 fully defined ODMs that are being benchmarked.

This research will help CIOs develop an ODM program for cybersecurity that measures and reports how well their organizations are protected, rather than how they are protected. See Note 1: The Elements of an ODM Program for Cybersecurity.

Analysis

Follow These Four Steps to Develop an ODM for Any Cybersecurity Control Investment

Good ODMs have very specific properties to support new types of governance. They measure protection levels, they support direct investment to change protection levels and they are explainable to executives with no technical background. Follow these steps to ensure that new ODMs embody these properties. ODMs create the most value when organizations invest in instrumenting systems and processes to gather new types of data. The visibility and power to report and invest in protection levels in a business context make the investment worthwhile.

To develop an ODM, a control can be defined as any combination of people, processes and technologies that are supported by an investment to create a level of protection for the organization.

ODMs are most effective when they are aligned with investments in controls that you own and manage. Doing so supports using the business context and levels of readiness that you own and control to drive the decision making for priorities and investments.

Step 1: Define the Control's Protection-Level Outcome

A protection-level outcome is a simple description of the benefits that reflect both operational performance and desired protection benefits. It is important to define a measurable outcome that reflects higher and lower protection, and one that direct investment can be made in to change the outcome.

- **Phishing training:** Helps shape the behavior of people related to clicking on links that create security incidents. This protection level is measurable through the percentage of people who click on phishing training emails assessed over time as part of an organization's security. and behavior and culture program (see CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework).

- **Threat and vulnerability management (TVM):** Manages the continuous stream of vulnerabilities available for exploitation. The protection level is measured by the time it takes to deploy patches.

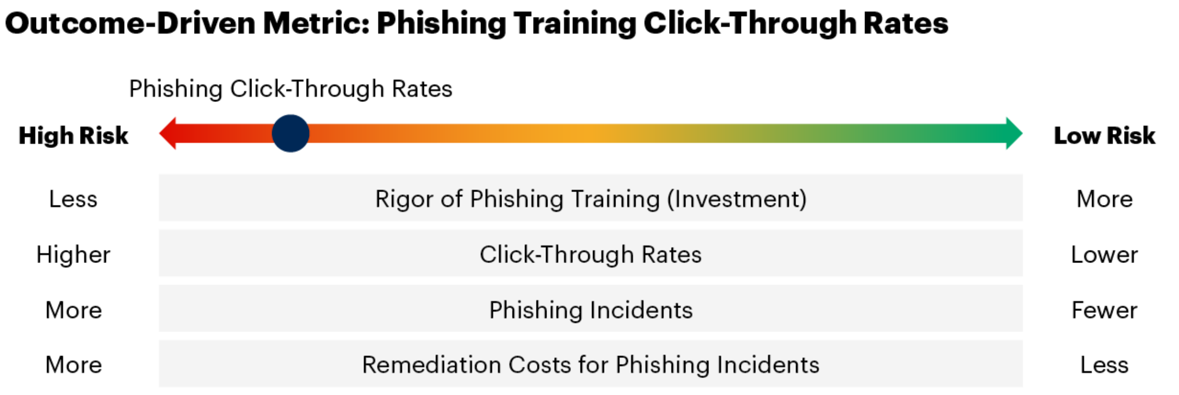
- **Third-party risk engagement:** Manages the assessment and governance of third parties to inform business decision making over which third parties the organization should engage. The protection level is measured as the percentage of engaged third parties that failed their assessments.

Step 2: Describe the Value Lever Trade-Offs

For each control, describe the relationship between cost (investment) and value (protection level). Generally, better protection (less risk) will be more costly and vice versa. Cost is not just a budget to implement and operate, but also business friction, such as employee and customer satisfaction, blocked business services, or other collateral costs to tighten a control.

Phishing training Higher phishing click-through rates reflect the propensity of employees to click on malware links in emails. Pushing phishing rates lower requires investment in anti-phishing tools and creates business friction (see Figure 2).

Figure 2: Outcome-Driven Metric: Phishing Training Click-Through Rates



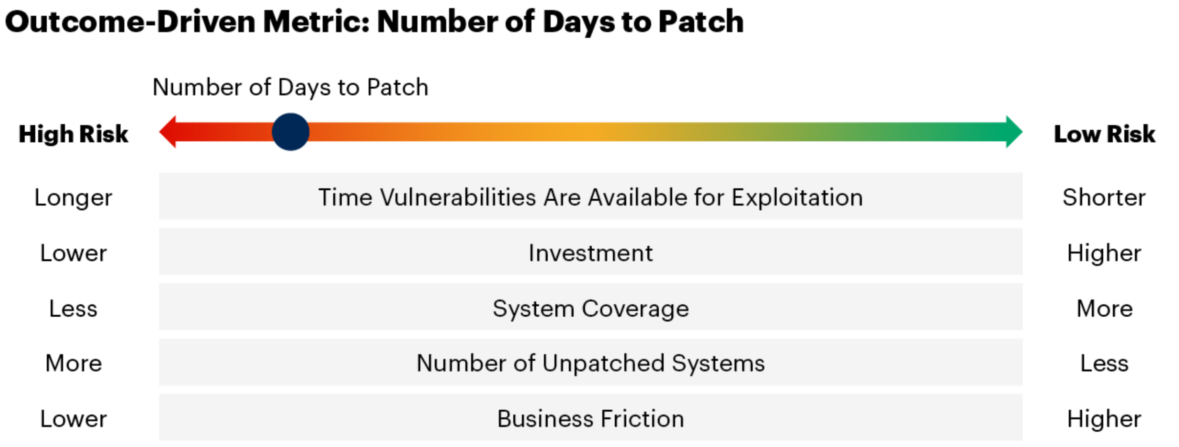
Outcome-Driven Metric: Phishing Training Click-Through Rates

High Risk		Low Risk
Less	Rigor of Phishing Training (Investment)	More
Higher	Click-Through Rates	Lower
More	Phishing Incidents	Fewer
More	Remediation Costs for Phishing Incidents	Less

Source: Gartner
787963_C

TVM: The faster known vulnerabilities are patched, the less time they are available to attack. Patching faster is typically more costly, not merely in direct spend, but also in disruption to business processes, patching slower is less costly (see Figure 3).

Figure 3: Outcome-Driven Metric: Number of Days to Patch



Outcome-Driven Metric: Number of Days to Patch

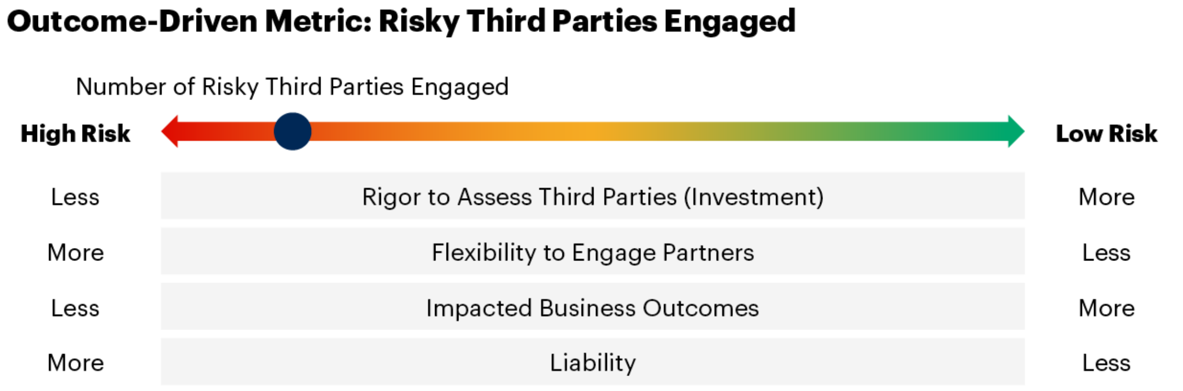
High Risk		Low Risk
Longer	Time Vulnerabilities Are Available for Exploitation	Shorter
Lower	Investment	Higher
Less	System Coverage	More
More	Number of Unpatched Systems	Less
Lower	Business Friction	Higher

Source: Gartner
787963_C

Third-party risk engagement

Higher percentages of vendors you engage with that have failed their security assessment creates more opportunities for a third party to have a security incident that impacts your business. Reducing third-party risk engagement creates business cost and business friction by reducing the opportunity for the business to work with whoever it wants/needs (see Figure 4).

Figure 4: Outcome-Driven Metric: Risky Third Parties Engaged


Outcome-Driven Metric: Risky Third Parties Engaged
Number of Risky Third Parties Engaged
High Risk
Low Risk

Less	Rigor to Assess Third Parties (Investment)	More
More	Flexibility to Engage Partners	Less
Less	Impacted Business Outcomes	More
More	Liability	Less

Source: Gartner
787963_C

The primary goal of this consideration and analysis in Step 2 is to understand the protection levels and costs across the organization as you tighten or loosen a control. These benefits and costs become the key influences in decisions related to priorities and investments for adding or changing a control. They also create the "direct line of sight" to the level of protection when put into a business context in Step 4.

Step 3: Define Benefit Outcomes

Benefits are measures of impact. In a business context for security, that generally means the impact to the business related to security threats or incidents. These outcomes should be defined as sharply as possible to direct the relationship to the intended benefits of the control defined in Step 1. Many times, these are categorizations of incidents and costs related to incidents:

- **Phishing training:** Number of incidents related to phishing emails, costs related to business interruption, regulatory fines and remediation
- **TVM:** Number of incidents related to unpatched vulnerabilities
- **Third-party risk:** Number of incidents where third parties created a liability

Security incidents should not always be thought of as the failure of a control. For example, if an organization has invested in 20-day patching, and a vulnerability is exploited within 15 days of a patch being made available, this is the result of a business decision to accept any hacks that occur within 20 days. It is not the failure of a control. See Use Value and Cost to Treat Cybersecurity as a Business Decision.

It is worth noting that cost is present in both operational and benefit outcome metrics. Costs in operational outcomes (Step 3) are the costs related to operating the control. Costs in benefit outcomes (Step 4) are related to the security impacts of the threats and incidents the control is intended to address.

Step 4: Sharpen Outcomes in a Business Context

ODMs should be measured against the supporting technologies for discrete business units, operating functions or departments that create business outcomes for the organization — for example, ODMs for the infrastructure and application portfolio that support claims processing in an insurance company. See Optimize Risk, Value and Cost in Cybersecurity and Technology Risk.

- **Phishing training:** Click-through rates by job role or business unit
- **TVM:** Speed to patch by technology stacks supporting each business unit (or business process)
- **Third-party risk:** Percentage of revenue dependent on risky third parties by business unit

Moving Forward, Use ODMs as the Foundation for Protection-Level Agreements

Metrics are more powerful and useful if they support decision making in a formal governance process. This can best be managed via protection-level agreement (PLAs) — contracts between executives and CIOs/CISOs to achieve a desired level of protection for a planned cybersecurity investment.

A PLA is typically constructed from an ODM that supports the identification of a desired/target protection level and a projected cost to achieve the protection level. Engaging executives through the dimensions of cost and value (protection levels) creates highly productive exchanges that ultimately settle on the protection executives say they want, within their willingness to pay for it. (See Six Steps to Manage Cybersecurity Risk Appetite Through Protection-Level Agreements).

Benchmarks provide peer comparisons that help executives make informed PLA decisions. Gartner is benchmarking 16 ODMs as part of the Gartner cybersecurity business value benchmark (see The Gartner Cybersecurity Business Value Benchmark, First Generation).

Evidence

This research is drawn from numerous client interactions and the results of the pilot study for The Gartner Cybersecurity Business Value Benchmark, First Generation.

Note 1: The Elements of an ODM Program for Cybersecurity

An ODM program is intended to support a governance process for measuring and executive reporting that guides priorities and investments in cybersecurity. The following components and concepts are necessary:

- Define the cybersecurity protection-level outcomes: ODMs measure cybersecurity protection-level outcomes achieved by specific investments. They are constructed by aligning what is measured with the intended protection outcome of the investment. ODMs reflect protection levels. When an ODM improves, the organization is measurably better protected. When the ODM is worse, the organization is measurably less protected.

- Value levers: ODMs act as value levers for cybersecurity investment. ODMs support direct investment to achieve different outcomes. Organizations can increase their investment to improve protection levels, or save money and accept lower protection levels.

- Benefit outcomes: These outcomes are measurable results that reflect successfully producing a desired benefit or goal — for example, the number of incidents related to unpatched systems, the number of incidents related to phishing or the number of incidents related to third-party risk. Benefits can also be cost savings, such as reducing the cost of recovering from ransomware.

- Business context: ODMs should be measured against technology stacks directly supporting discrete business units, operating functions or departments that create business outcomes for the organization. Putting ODMs in a business context creates opportunities to measure and report delivered levels of protections against business outcomes. This changes the conversation with executives to the relative value of investments that protect business outcomes, rather than decisions like buying a firewall.

- Cost to deliver outcomes: Reflecting cost is a vital component of choosing levels of protection. Cost is not just a budget to implement and operate, but also business friction, such as customer satisfaction, impacted business outcomes or other collateral costs to improve protection levels. See Measure the Real Cost of Cybersecurity Protection.

- PLAs: A PLA is an agreement between executives and CIOs/CISOs to achieve a desired level of protection for a planned cybersecurity investment. A PLA is typically constructed from an ODM that supports the identification of a desired/target protection level and a projected cost to achieve the protection level. (See Quick Answer: What Is a Cybersecurity Protection-Level Agreement?)

Document Revision History

Outcome-Driven Metrics for Cybersecurity in the Digital Era - 12 February 2020

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Use Value and Cost to Treat Cybersecurity as a Business Decision

Metrics to Prove You CARE About Cybersecurity

Measure the Real Cost of Cybersecurity Protection

Cyber-Risk Appetite: How to Put the ‘Business’ in ‘Managing Cybersecurity as a Business Decision’

Kick-Start Your IT Value Story With Business Metrics That Matter