The Gartner Cybersecurity Business Value Benchmark, First Generation

Published 5 September 2022 - ID G00775537 - 26 min read

By Analyst(s): Paul Proctor, Srinath Sampath, Paul Furtado, Patrick Long, Lisa Neubauer, Deepti Gopal

Initiatives: IT Cost Optimization, Finance, Risk and Value

> CIOs must drive cybersecurity investment through a business lens. These metric definitions are outcome-driven metrics used to create a peer comparison benchmark of cybersecurity business value across 16 value levers.

Analysis

When to Use

CIOs seeking to manage cybersecurity investment must use outcome-driven metrics. Gartner has defined 16 protection-level outcomes that create a foundation for effective collaboration with boards of directors, CISOs and CFOs.

These metrics serve as value levers to manage business-led cybersecurity investments. The goal is to achieve a desired level of cybersecurity readiness that aligns with the organization's willingness to pay for it (see Use Value and Cost to Treat Cybersecurity as a Business Decision).

The metrics establish a baseline for peer comparison that is very useful for guiding cybersecurity investments and board oversight.

Organizations should gather their operational execution data and establish a desired target goal of achievement for each metric.

Gartner will release a tool for collecting this benchmark data from clients and other participants. This data will be used in aggregate to create a first of its kind benchmark for organizations. Register your interest at the Gartner Cybersecurity Business Value Benchmark site. Gather these metrics for your organization now so you will be ready when the tool becomes available.

Directions for Use

- Use this guidance and metric definitions to facilitate gathering of the defined metrics.
- Instrument your systems and processes to gather these metrics for now and the future. That is because cybersecurity is always changing, and this benchmark will evolve year over year.
- Gather the defined metrics for both current operations results (“actual”) and desired levels of protection (“desired”).
- Periodically, once or twice a year, enter your data into the Gartner tool and receive custom peer benchmarking reports.
-

Context

A global benchmark has to accommodate organizations of every size, industry and region, and they all have to measure the same things. The definitions for these metrics accommodate a lot of variations with the intent to make peers comparable.

Any aspect that is not immediately clear should be based on the organization’s definition. For example, we do not address patch prioritization, and each organization should prioritize as it sees necessary. The metric still works across organizations that prioritize differently, and the assumption is that peer groups will prioritize roughly in a similar manner. This will be sharpened as the benchmark develops over different generations.

The FAQ and definitions below should provide additional context.

FAQ

Is it OK to estimate? Yes, credible and defensible estimates are OK. Although these are Gartner’s recommended calculations and definitions for these metrics, we understand that many organizations are not currently instrumented to gather the data exactly as we define it.

Do I need to answer every question? No, but you will receive data only for the questions you answer. Put a zero in any question you wish to skip. You can also answer for a “desired” value even if you do not have the data for the “actual” value.

Why does Gartner use average vs. median? Many of the benchmark questions are based on averages. We encourage organizations to calculate these averages in a credible and defensible manner. Medians can be submitted in lieu of averages if you can calculate them. Gartner reports results as medians and quartiles.

Why do many of the definitions rely on the definition that the organization uses? The benchmark has to balance a lot of variations across organizations of different sizes, industries and threat profiles. Because an organization will ultimately be compared with peers, an assumption is made that peers will have similar definitions. As the benchmark matures over time, we will add or modify questions to create more visibility into these definitions.

What is the difference between "actual" and "desired"? "Actual" is what you are operationally achieving, and "desired" is what you would like to achieve by prioritizing investment.

What is the appropriate way to determine what is "desired" for each metric? This is a choice that each organization must make for itself. The benchmark itself may help guide these decisions in the future by reflecting the most common achievements in your peer group.

How does Gartner address "gaming" these metrics and how that may impact the benchmark? Gartner is very experienced at benchmarking and synthesizing the data from thousands of organizations. We have tools and techniques to "clean" the data and ensure that the benchmark is a credible and defensible reflection of outcomes being achieved in our client base. We will be adding questions over time to confirm the credibility and defensibility of answers.

What are some examples of gaming these metrics? Any metric that is made to look good, while hiding actual issues may be considered as gaming the metrics. Especially because Gartner has integrated organizational choices into the metrics, it may be easy to make choices that just make the metrics look good. This is not recommended:

- Example: Define a common security incident as critical or high-risk that is typically remediated very quickly, and then flood your security operations center (SOC) with these incidents to drive down the average time to remediate incidents.
- Example: Define a very easy "standard" phishing campaign that will score very well to drive down your phishing scores.

- Example: Define a ransomware exercise as one that exercises only one system at a facility to drive up recovery testing percentages.

Why is gaming these metrics a bad idea for an organization? This is a self-correcting problem. The purpose of these metrics is to create a comparison of your organization with your peers for your board of directors and to guide investment. If the metrics are gamed, they will not be a credible and defensible comparison, and that will be made evident in any serious breach event that involves disclosure, legal, auditors, regulators or your cyberinsurance carrier. In addition to misleading your executives, you may create liability for yourself and your organization.

How is this information protected? Gathering sensitive information is central to Gartner's business. This information is protected using the same mechanisms that all client information is protected at Gartner. It will be shared with others only in aggregate.

Definitions

These definitions provide guidance in the absence of an internally defined criticality scale. They should be superseded by company-specific risk definitions, where such definitions have been developed and approved.

In all cases, the organization should default to measuring these outcome-driven metrics in the context of assets, alerts, vulnerabilities and incidents that the organization has deemed in its top tiers of risk.

Critical and high-risk assets: Assets for which a breach of confidentiality, integrity or availability would have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.

Critical and high-risk third parties: Third parties for which a breach of confidentiality, integrity or availability would have a severe or catastrophic adverse effect on organizational operations, organizational assets, regulatory action, organizational reputation, or other material business outcomes or impacts.

Critical and high-risk alerts: Alerts that are related to an asset with a critical or high-risk classification *and* result from high-fidelity alerting and correlation (endpoint detection, IDS and highly tuned SIEM use cases).

Critical and high-risk vulnerabilities: To determine the vulnerability risk level, apply the Common Vulnerability Scoring System (CVSS) to the findings in your environment. Most commercial vulnerability scanners will calculate CVSS automatically as they report findings, but it is important to apply environmental context to the findings, such as network position and impact rating, to ensure scores are properly applied.

Critical and high-risk incidents: Incidents or conditions that must be addressed to avoid severe or catastrophic adverse effects on organizational operations, organizational assets or individuals. An incident that is addressed before adverse effects are experienced, is still an incident. These metrics are measuring the investments to avoid such effects, not only investments made in dealing with such effects.

Critical and high-risk policy exceptions: Formally tracked policy exceptions with expiration times or dates that must be addressed to avoid severe or catastrophic adverse effects on organizational operations, organizational assets or individuals.

Systems: Systems are all IT assets and applications that support business and mission outcomes. Systems are defined by each organization and are used largely to calculate percentages of systems for different metrics — for example, the percentage of systems with required build and security controls.

Business or mission outcomes: Business and mission outcomes are measurable goals that support a business — for example, a manufacturing plant that produces 5,000 widgets a day. Business outcomes can be defined at different levels, such as all manufacturing production for a business, the production for a single plant, or the production across a product line that may be split across several manufacturing plants. Outcomes are defined by each organization.

Alignment of systems to business or mission outcomes: A system is aligned to a business outcome when it has a direct line of sight to the support of that outcome — for example, the systems that support a manufacturing plant are aligned to the business outcome of producing 5,000 widgets a day. If the systems aligned to a business outcome fail, then it harms the business outcome. Organizations determine which systems are aligned by their defined outcomes. This relationship is a critical concept in this benchmark to support concepts like percentage of systems that are aligned to an outcome and have key controls deployed.

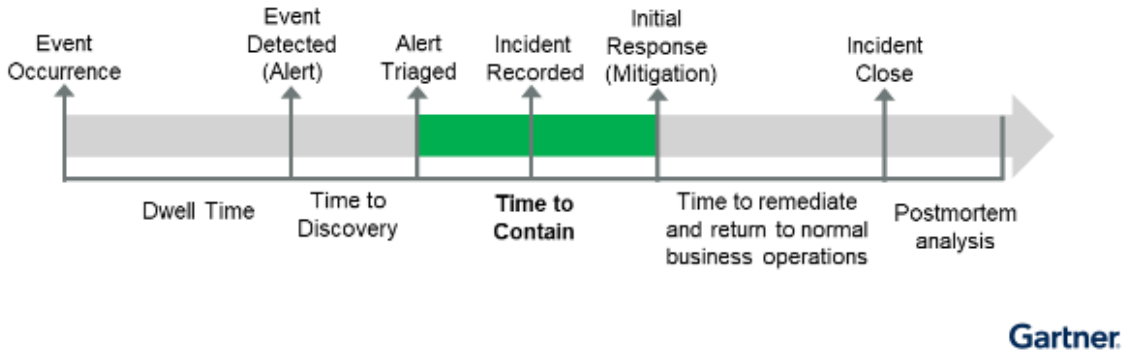
The Outcome-Driven Metrics

Outcome-Driven Metric 1: Incident Containment (Minutes)

MTTC

Mean time to contain (MTTC) is typically an SOC metric. If you outsource your SOC, your provider will have this information. Containment is the time from when an incident is determined to be in a priority class for remediation (triaged) to when it is contained from creating further damage or risk. How fast you contain incidents is a protection level against security incidents damaging your business outcomes and a value measure for your investment in incident response (see Figure 1 and Table 1).

Figure 1: Outcome-Driven Metric 1 — Incident Containment (Minutes)



Source: Gartner Cybersecurity Value Benchmark

Table 1: Outcome-Driven Metric 1 — Incident Containment (Minutes)

Target Question	**For critical and high-risk security incidents, what is your average time (in minutes) between the alert being allocated (triage starts) and the initial containment response (mitigation) of that issue?**
In-scope incidents	In-scope incidents are all categories of incidents or conditions that must be addressed to avoid severe or catastrophic adverse effects on organizational operations, organizational assets or individuals. This excludes: ■ Incidents where a false positive was recorded. ■ Incidents that were automatically remediated and closed.
Clock	The clock starts when alert is triaged, which means it is determined to be in a priority class for remediation. The clock stops when an incident is contained, which means security has taken the action necessary to prevent further damage and it is handed over to internal nonsecurity operational teams to bring systems back to normal operations.
Calculation	MTTC = For the most recent 12-month period, average of the time difference between when the alert is triaged (or allocated) and when an initial response for that alert is executed for each in-scope incident.

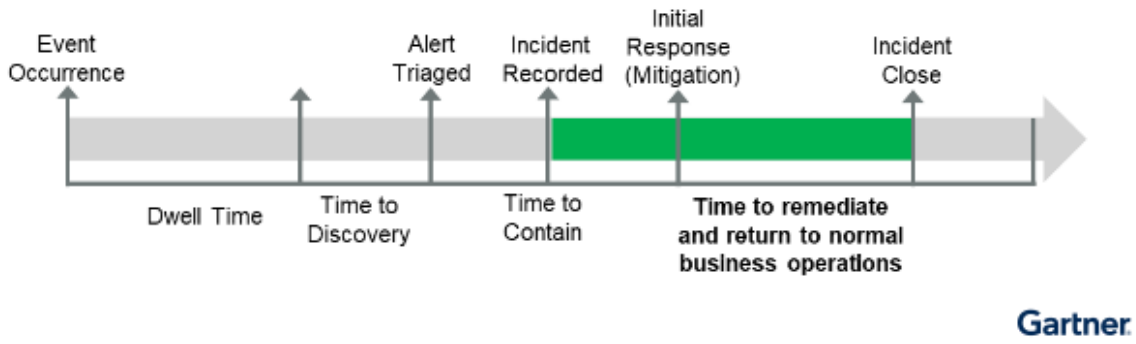
Source: Gartner (September 2022)

Outcome-Driven Metric 2: Incident Remediation (Hours)

MTTR

Mean time to remediate (MTTR) is typically an SOC metric. If you outsource your SOC, your provider will have this information. Remediation is the time from when an incident ticket is opened to start remediation activities to when the ticket is closed, which means that all systems have been brought back to normal operations. How fast you remediate incidents is a protection level against security incidents damaging your business outcomes and a value measure for your investment in incident response (see Figure 2 and Table 2).

Figure 2: Outcome-Driven Metric 2 — Incident Remediation (Hours)



Source: Gartner Cybersecurity Value Benchmark

Table 2: Outcome-Driven Metric 2 — Incident Remediation (Hours)

Target Question	**For critical and high-risk security incidents, what is your average time (in hours) between incident detection (ticket generation) and incident closure (ticket close)?**
In-scope incidents	In-scope incidents are all categories of incidents or conditions that must be addressed to avoid severe or catastrophic adverse effects on organizational operations, organizational assets or individuals. This excludes: ■ Incidents where a false positive was recorded. ■ Incidents that were automatically remediated and closed. ■ Incidents that result in breach response events that involve forensics and may drag out for days, weeks or months.
Clock	The clock starts when an incident is recorded, which means a ticket is opened to start remediation actions. The clock stops when an incident is closed, which means all systems have been brought back to normal operations.
Calculation	MTTR = For the most recent 12-month period, average time (in hours) between incident ticket generation and ticket close for all in-scope incidents.

Source: Gartner (September 2022)

Outcome-Driven Metric 3: OS Patching Cadence (Standard)

Average Days of System Exposure

This measures standard OS patching that requires no special handling. How fast you deploy patches is a protection level that reduces the time that vulnerabilities are available for exploitation and a value measure for your investment in threat and vulnerability management (see Table 3).

Table 3: Outcome-Driven Metric 3 — OS Patching Cadence (Standard)

Target Question	What is your average time (in days) to apply critical operating system patches within your standard patch process?
In-scope patches and systems	In-scope patches are all operating system patches that address critical and high-risk vulnerabilities on systems that support business outcomes.
Definitions	"Patch deployment time": Number of days from in-scope patch availability to patch deployment (including testing) on 100% of critical and high-risk assets. Organizations may substitute 90% of all in-scope assets. "Standard patch process": Operating system patches that are prioritized, tested and deployed with no special handling or treatment required.
Calculation	OS patching time = For the most recent 12-month period, average patch deployment time (see the definition above) for all in-scope patches.

Source: Gartner (September 2022)

Outcome-Driven Metric 4: Third-Party Cybersecurity Risk Engagement

The metric reflects your executives' decision to accept a known risk and work with vendors and partners that scored poorly on the organization's cybersecurity risk assessment. This would include any indication that the third party is a bad risk or a recommendation to avoid engagement. This data is the cross-section of vendors and partners that have a working relationship with your organization (typically found in procurement) and the record of cybersecurity assessment. Third-party cybersecurity risk engagement is a protection level for business decisions that create cybersecurity risk and a value measure for your investment in overall third-party risk management (see Table 4).

Table 4: Outcome-Driven Metric 4 — Third-Party Cybersecurity Risk Engagement

(Enlarged table in Appendix)

Target Question	What percentage of known critical and high-risk third parties with poor (noncompliant) cybersecurity assessment results have been engaged by the organization?
In-scope third parties	In-scope third parties are: ■ Known third parties have gone through normal procurement processes. ■ Unknown third parties (those that have a business relationship that have not gone through procurement) are excluded. ■ Unassessed third parties or third parties with expired or out-of-date assessments are also excluded and measured in a separate, benchmarked metric. Organizations should consider assessments older than three years as out of date for the purposes of this benchmark.
Definitions	"Poor security assessment results" are defined as the most recent security assessment indicating that the third party is a bad risk or a recommendation to avoid engagement. This is a determination made by each organization, based on its own scoring and risk tolerance. "Engaged": The third party has a working relationship with the organization and presents a critical and high risk. That means a breach of confidentiality, integrity or availability would have a severe or catastrophic adverse effect on organizational operations, organizational assets, regulatory action, organizational reputation, or other material business outcomes or impacts.
Calculation	Third-party risk engagement = For the most recent 12-month period, total number of known critical and high-risk third parties with poor security assessment results divided by the total number of in-scope third parties.

Source: Gartner (September 2022)

Outcome-Driven Metric 5: Unassessed Third Parties

Poor Visibility Into Third-Party Cybersecurity Risk

This metric reflects poor visibility into third-party risk for vendors and partners that have no current cybersecurity assessment. Currency and required assessment levels are defined by the organization. Unassessed third-party metric is a protection level for visibility into cybersecurity risk and a value measure for your investment in third-party risk management (see Table 5).

Table 5: Outcome-Driven Metric 5 — Unassessed Third Parties

Target Question	**What percentage of known critical and high-risk third parties have no current cybersecurity risk assessment?**
In-scope third parties	In-scope third parties are known — and have gone through normal procurement processes. Excluded third parties are: ■ Unknown third parties (those that have a business relationship that have not gone through procurement) are excluded. ■ Unassessed third parties or third parties with expired or out-of-date assessments. Organizations should consider assessments older than three years as out of date for the purposes of this benchmark, unless the organization has defined a time of less than three years.
Definitions	"Currency and required level of assessment" is defined by policy in each organization. "Engaged": The third party has a working relationship with the organization and presents a critical and high risk. This means a breach of confidentiality, integrity or availability would have a severe or catastrophic adverse effect on organizational operations, organizational assets, regulatory action, organizational reputation, or other material business outcomes or impacts.
Calculation	Unassessed third parties = For the most recent 12-month period, total number of known critical and high-risk third parties with no cybersecurity risk assessment divided by the total number of in-scope third parties.

Source: Gartner (September 2022)

Outcome-Driven Metric 6: Expired Policy Exceptions

Expired and Unremediated Policy Exceptions

This metric requires a formalized policy exception process. The organization chooses its own management of expirations and required remediations. If everything is an exception, and exceptions have no time limit, then the organization may have poor visibility into material levels of risk. Percentage of expired policy exceptions is a protection level for addressing risky policy violations and a value measure for your investment in governance, risk and compliance (see Table 6).

Table 6: Outcome-Driven Metric 6 — Expired Policy Exceptions

Target Question	What is your percentage of critical security policy exceptions that have expired and are unremediated?
In-scope policy exceptions	In-scope policy exceptions are formally tracked critical policy exceptions with expiration times and dates that have expired and are not addressed.
Calculation	Expired policy exceptions = For the most recent 12-month period, the number of in-scope policy exceptions that have expired and are unremediated, which is then divided by the total number of in-scope policy exceptions.

Source: Gartner (September 2022)

Outcome-Driven Metric 7: Endpoint Protection Coverage

Endpoints With Approved Build and Controls

Endpoints are better protected when they are known to have the approved build and security controls. Percentage of endpoints with approved controls is a protection level for addressing poorly protected systems and a value measure for your investment in endpoint protection (see Table 7).

Table 7: Outcome-Driven Metric 7 — Endpoint Protection Coverage

Target Question	**What is your percentage of known endpoints with company-approved or company-required build and security controls?**
In-scope endpoints	In-scope endpoints are known endpoints that are managed, tracked and identifiable that also have a defined build and set of security controls. Exclusions are: ■ Endpoints that are not managed, tracked and identifiable are excluded. ■ Endpoints that do not have a defined build and security controls are excluded. For example, IoT devices that do not support a controllable build or set of security controls and configurations.
Definitions	"Build and security controls": Identified security tools installed, appropriate OS and applications, ports, and protocols appropriately limited per imaging standard.
Calculation	Endpoint protection coverage = For the most recent 12-month period, number of in-scope endpoints with approved or required build and security controls divided by the total number of in-scope endpoints.

Source: Gartner (September 2022)

Outcome-Driven Metric 8: Ransomware Recovery (Mission-Critical)

Mission-Critical Systems With Ransomware Recovery Exercise

Recovery exercising is a critical control to manage ransomware threats. It supports visibility and capability to recover, estimate loss expectancy, and inform negotiations with ransomware criminals. Percentage of mission-critical systems with ransomware readiness exercising is a protection level against ransomware and a value measure for your investment in ransomware readiness (see Table 8).

Table 8: Outcome-Driven Metric 8 — Ransomware Recovery (Mission-Critical)

Target Question	**What is your percentage of mission-critical systems supporting critical business or mission functions that have successfully completed ransomware recovery exercising in the past 12 months?**
In-scope systems	In-scope systems are: ■ Systems that would materially damage critical business or mission functions if they are down. ■ Critical business or mission functions that are defined by each organization.
Definitions	"Ransomware recovery exercising": An in-scope system was successfully restored in exercise mode in a simulated ransomware attack to an acceptable level of operation. The level of exercise should provide confidence that an acceptable level of business operations can be restored after a loss of supporting systems. "Successfully completed": The systems were restored, and the functions brought back to an acceptable level of operations, including procedures to recreate any lost data and backlog procedures to enter business transacted manually while the systems were down due to the ransomware attack.
Calculation	Ransomware recovery = For the most recent 12-month period, number of in-scope mission systems that have successfully completed ransomware recovery exercising divided by the total number of in-scope systems.

Source: Gartner (September 2022)

Outcome-Driven Metric 9: Ransomware Downtime and Workaround Procedures

Critical Business or Mission Functions That Can Operate During a Ransomware Event Without IT Systems

During a ransomware event, downtime and workaround procedure is a set of tasks and workflow to be taken — often manually — to ensure critical business or mission functions can continue in the absence of the IT resources normally used. The procedure should be crafted such that it can be used for business operations for a period of time appropriate for the outage — for example, 45 days for ransomware. The procedure should be developed with consideration given to the viability of the procedure (for example, is it really going to work?) and that it doesn't create more problems than it solves. Percentage of critical business- or mission-critical functions that have downtime and workaround procedures is a protection level against ransomware and a value measure for your investment in ransomware readiness (see Table 9).

Table 9: Outcome-Driven Metric 9 — Ransomware Downtime and Workaround Procedure

Target Question	**What is your percentage of critical business or mission functions that have exercised downtime and workaround procedures in the past 12 months?**
In-scope business functions	In-scope critical business or mission functions are those that have downtime and workaround procedures to operate without IT systems in the event of a ransomware attack.
Definitions	"Downtime and workaround procedures" are defined as written plans to achieve business and mission outcomes after a ransomware event when systems are offline. "Exercised downtime and workaround procedures" are defined as exercises or other training to ensure that different roles supporting a critical business or mission function know how to operate without IT. Critical business and mission functions are defined by each organization.
Calculation	Ransomware downtime and workarounds = For the most recent 12-month period, the number of in-scope functions or outcomes that have successfully exercised downtime and workaround procedures, or that have a written downtime and workaround procedure, divided by the total number of in-scope functions or outcomes.

Source: Gartner (September 2022)

Outcome-Driven Metric 10: Cloud Security Coverage

Cloud Workloads Aligned to the Security Baseline

Cloud workloads must be aligned to a defined security baseline to support appropriate protection levels. Percentage of cloud workloads aligned to the required security baseline is a protection level for addressing poorly protected cloud instances and a value measure for your investment in cloud protection (see Table 10).

Table 10: Outcome-Driven Metric 10 — Cloud Security Coverage

Target Question	**What is your percentage of production cloud workloads aligned with the defined and approved security baseline?**
In-scope cloud workloads	In-scope cloud workloads are cloud workloads supporting business or mission outcomes that require a defined security baseline of controls.
Definitions	"Production cloud workloads" are defined by each organization. "Security baseline" is defined by each organization.
Calculation	Cloud security coverage = For the most recent 12-month period, the number of in-scope cloud workloads aligned with the approved security baseline, divided by the total number of in-scope cloud workloads.

Source: Gartner (September 2022)

Outcome-Driven Metric 11: Multifactor Authentication Coverage

Multifactor authentication is one of the most effective ways to protect access. Percentage of critical and high-risk systems with multifactor authentication protection is a protection level for addressing unauthorized system access and a value measure for your investment in access control (see Table 11).

Table 11: Outcome-Driven Metric 11 — Multifactor Authentication Coverage

Target Question	What percentage of critical and high-risk applications are protected by multifactor authentication?
In-scope systems	In-scope systems are critical and high-risk systems that are determined to need multifactor authentication protection either by policy, criticality or designation.
Definitions	"Multifactor authentication protection" is defined as the inability to access the system without passing through a multifactor authentication control within the company policy.
Calculation	Multifactor authentication coverage = For the most recent 12-month period, the number of in-scope systems with multifactor authentication protection divided by the total number of in-scope systems.

Source: Gartner (September 2022)

Outcome-Driven Metric 12: Access Removal Time

Time to Deprovision Critical Access After an (Employee) Termination Request

The more time it takes to deprovision access, the longer unauthorized individuals have access to data that they are no longer entitled to access. Termination and deprovisioning protection varies widely across different organizations, so it is based on the organization's definition of terminating access that would be considered a threat. Access removal time is a protection level for addressing unauthorized system and data access and a value measure for your investment in access control (see Table 12).

Table 12: Outcome-Driven Metric 12 — Access Removal Time

Target Question	**What is your average number of hours from the request for termination of access to sensitive or high-risk systems or information to deprovisioning of all access?**
In-scope access changes	In-scope access change requests are any changes that require removal of access to sensitive or high-risk systems or information.
Definitions	"All access": This includes directory, application and all authentication channels that provide sensitive data and resource access. "Access termination time": Time from receipt of original request to terminate employee access to time that all access is deprovisioned.
Calculation	Access removal time = For the most recent 12-month period, the sum of all access termination times for all in-scope access change requests divided by the total number of in-scope access termination requests.

Source: Gartner (September 2022)

Outcome-Driven Metric 13: Privileged Access Management

Controlling "Always On" Personal Privileged Accounts

Privileged access should ideally be just in time — that is, authorized users will gain privileged access for a short duration, and then lose it (until they require it again). However, some exceptions will need to be granted and this number should be kept as low as possible. The ratio of always-on accounts to individuals who may use them is a protection level for unauthorized access to sensitive, powerful accounts and a value measure for your investment in privileged access management (see Table 13).

Table 13: Outcome-Driven Metric 13 — Privileged Access Management

Target Question	**What is your ratio of always-on personal privileged accounts to the number of individuals in roles who should have access to these accounts?**
In-scope individuals and accounts	In-scope individuals are system administrators who need access to privileged accounts. In-scope accounts are owned by in-scope individuals and have privileged access.
Definitions	"Privileged accounts" have privileged access that can negatively impact production systems or other business outcomes, including access to sensitive information.
Calculation	Privileged access management = For the most recent 12-month period, the number of privileged accounts divided by the number of in-scope individuals. Note: This ratio may be above 1 if the number of accounts exceeds the number of individuals.

Source: Gartner (September 2022)

Outcome-Driven Metric 14: Security Awareness Training

Employee Security Training Coverage

Trained employees are more likely to understand and execute proper security behavior in their roles. Trained employees are a protection measure for people understanding secure behaviors and a value measure of your investment in people to behave in a secure manner (see Table 14).

Table 14: Outcome-Driven Metric 14 — Security Awareness Training

Target Question	What percentage of your employees and contractors have completed mandatory security training?
In-scope individuals	In-scope individuals are defined by each organization and usually include employees, contractors, and others who have access to critical and high-risk systems.
Definitions	Mandatory security training is defined by each organization.
Calculation	Security awareness training coverage = For the most recent 12-month period, the total number of in-scope individuals who have completed mandatory security training divided by the total number of in-scope individuals.

Source: Gartner (September 2022)

Outcome-Driven Metric 15: Phishing Training on Click-Throughs

Recognizing and Avoiding Phishing Emails

Measuring click-throughs is not a perfect measure. However, it is very common, and it is already socialized with your board and executives. Phishing training on click-throughs are a protection level against employees clicking on dangerous links and a value measure of your investment in phishing training (see Table 15).

Table 15: Outcome-Driven Metric 15 — Phishing Training on Click-Throughs

Target Question	**What is your percentage of click-throughs for your standard organizationwide phishing campaigns in the past 12 months?**
In-scope individuals	In-scope individuals are all employees or other required individuals who are subject to phishing campaigns.
Definitions	"Standard campaign" is defined by each organization. It is neither the strongest, most aggressive campaigns, nor the weakest, least aggressive campaigns. "Click-through" is defined as clicking on a link in a phishing email. If an individual clicked on any phishing training link through a standard phishing campaign in the past 12 months, it is counted as a click-through. Any click-through of a real phishing email should also be counted as part of this metric.
Calculation	Phishing training on click-throughs = For the most recent 12-month period, the number of employees who have clicked on a phishing training link in a standard phishing campaign (or real phishing email) divided by the total number of in-scope individuals.Note: The number of times that an employee clicks on a phishing link does not impact this metric. An employee is only counted as 1 in the numerator of this calculation if the employee clicked on a phishing link in the past 12 months.

Source: Gartner (September 2022)

Outcome-Driven Metric 16: Phishing Reporting Rates

Employees Reporting Suspected Phishing

Employees who report suspected phishing emails help the organization improve defenses and limit damage from phishing. Phishing training on click-throughs is a protection level against employees clicking on dangerous links and a value measure of your investment in phishing training (see Table 16).

Table 16: Outcome-Driven Metric 16 — Phishing Reporting Rates

Target Question	**What is the percentage of employees who report suspicious emails for your standard organizationwide phishing campaigns?**
In-scope individuals	In-scope individuals are all employees or other required individuals who are subject to phishing campaigns.
Definitions	"Standard campaign" is defined by each organization. It is neither the strongest, most aggressive campaigns, nor the weakest, least aggressive campaigns. "Reporting suspicious emails" is defined as reporting a phishing attempt through normal channels. If an individual reports any attempted phishing in the past 12 months, it is counted as a report for this metric.
Calculation	Phishing reporting rates = For the most recent 12-month period, the number of in-scope individuals who reported the receipt of a suspicious email (training or real email) divided by the total number of employees. Note: The number of times an employee reports suspected phishing does not impact this metric. An employee is counted as 1 in the numerator of this calculation if the employee has reported a phishing link in the past 12 months.

Source: Gartner (September 2022)

Recommended by the Authors

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

Tool: Catalog of Business-Aligned Outcome-Driven Metrics for Risk and Security

Measure the Real Cost of Cybersecurity Protection

How Much You Should Spend on Cybersecurity in Three Steps

Tool: Downtime/Workaround Procedures To Operate Your Business When Recovery Times Can't Be Met

Restore vs. Rebuild — Strategies for Recovering Applications After a Ransomware Attack

---

Table 1: Outcome-Driven Metric 1 — Incident Containment (Minutes)

Target Question	**For critical and high-risk security incidents, what is your average time (in minutes) between the alert being allocated (triage starts) and the initial containment response (mitigation) of that issue?**
In-scope incidents	In-scope incidents are all categories of incidents or conditions that must be addressed to avoid severe or catastrophic adverse effects on organizational operations, organizational assets or individuals. This excludes: ■ Incidents where a false positive was recorded. ■ Incidents that were automatically remediated and closed.
Clock	The clock starts when alert is triaged, which means it is determined to be in a priority class for remediation. The clock stops when an incident is contained, which means security has taken the action necessary to prevent further damage and it is handed over to internal nonsecurity operational teams to bring systems back to normal operations.
Calculation	MTTC = For the most recent 12-month period, average of the time difference between when the alert is triaged (or allocated) and when an initial response for that alert is executed for each in-scope incident.

Source: Gartner (September 2022)

Table 2: Outcome-Driven Metric 2 — Incident Remediation (Hours)

Target Question	**For critical and high-risk security incidents, what is your average time (in hours) between incident detection (ticket generation) and incident closure (ticket close)?**
In-scope incidents	In-scope incidents are all categories of incidents or conditions that must be addressed to avoid severe or catastrophic adverse effects on organizational operations, organizational assets or individuals. This excludes: ■ Incidents where a false positive was recorded. ■ Incidents that were automatically remediated and closed. ■ Incidents that result in breach response events that involve forensics and may drag out for days, weeks or months.
Clock	The clock starts when an incident is recorded, which means a ticket is opened to start remediation actions. The clock stops when an incident is closed, which means all systems have been brought back to normal operations.
Calculation	MTTR = For the most recent 12-month period, average time (in hours) between incident ticket generation and ticket close for all in-scope incidents.

Source: Gartner (September 2022)

Table 3: Outcome-Driven Metric 3 — OS Patching Cadence (Standard)

Target Question	What is your average time (in days) to apply critical operating system patches within your standard patch process?
In-scope patches and systems	In-scope patches are all operating system patches that address critical and high-risk vulnerabilities on systems that support business outcomes.
Definitions	“Patch deployment time”: Number of days from in-scope patch availability to patch deployment (including testing) on 100% of critical and high-risk assets. Organizations may substitute 90% of all in-scope assets. “Standard patch process”: Operating system patches that are prioritized, tested and deployed with no special handling or treatment required.
Calculation	OS patching time = For the most recent 12-month period, average patch deployment time (see the definition above) for all in-scope patches.

Source: Gartner (September 2022)

Table 4: Outcome-Driven Metric 4 — Third-Party Cybersecurity Risk Engagement

Target Question	**What percentage of known critical and high-risk third parties with poor (noncompliant) cybersecurity assessment results have been engaged by the organization?**
In-scope third parties	In-scope third parties are: ■ Known third parties have gone through normal procurement processes. ■ Unknown third parties (those that have a business relationship that have not gone through procurement) are excluded. ■ Unassessed third parties or third parties with expired or out-of-date assessments are also excluded and measured in a separate, benchmarked metric. Organizations should consider assessments older than three years as out of date for the purposes of this benchmark.
Definitions	“Poor security assessment results” are defined as the most recent security assessment indicating that the third party is a bad risk or a recommendation to avoid engagement. This is a determination made by each organization, based on its own scoring and risk tolerance. “Engaged”: The third party has a working relationship with the organization and presents a critical and high risk. That means a breach of confidentiality, integrity or availability would have a severe or catastrophic adverse effect on organizational operations, organizational assets, regulatory action, organizational reputation, or other material business outcomes or impacts.
Calculation	Third-party risk engagement = For the most recent 12-month period, total

	number of known critical and high-risk third parties with poor security assessment results divided by the total number of in-scope third parties.

Source: Gartner (September 2022)

Table 5: Outcome-Driven Metric 5 — Unassessed Third Parties

Target Question	What percentage of known critical and high-risk third parties have no current cybersecurity risk assessment?
In-scope third parties	In-scope third parties are known — and have gone through normal procurement processes. Excluded third parties are: ■ Unknown third parties (those that have a business relationship that have not gone through procurement) are excluded. ■ Unassessed third parties or third parties with expired or out-of-date assessments. Organizations should consider assessments older than three years as out of date for the purposes of this benchmark, unless the organization has defined a time of less than three years.
Definitions	“Currency and required level of assessment” is defined by policy in each organization. “Engaged”: The third party has a working relationship with the organization and presents a critical and high risk. This means a breach of confidentiality, integrity or availability would have a severe or catastrophic adverse effect on organizational operations, organizational assets, regulatory action, organizational reputation, or other material business outcomes or impacts.
Calculation	Unassessed third parties = For the most recent 12-month period, total number of known critical and high-risk third parties with no cybersecurity risk assessment divided by the total number of in-scope third parties.

Source: Gartner (September 2022)

Table 6: Outcome-Driven Metric 6 — Expired Policy Exceptions

Target Question	What is your percentage of critical security policy exceptions that have expired and are unremediated?
In-scope policy exceptions	In-scope policy exceptions are formally tracked critical policy exceptions with expiration times and dates that have expired and are not addressed.
Calculation	Expired policy exceptions = For the most recent 12-month period, the number of in-scope policy exceptions that have expired and are unremediated, which is then divided by the total number of in-scope policy exceptions.

Source: Gartner (September 2022)

Table 7: Outcome-Driven Metric 7 — Endpoint Protection Coverage

Target Question	What is your percentage of known endpoints with company-approved or company-required build and security controls?
In-scope endpoints	In-scope endpoints are known endpoints that are managed, tracked and identifiable that also have a defined build and set of security controls. Exclusions are: ■ Endpoints that are not managed, tracked and identifiable are excluded. ■ Endpoints that do not have a defined build and security controls are excluded. For example, IoT devices that do not support a controllable build or set of security controls and configurations.
Definitions	"Build and security controls": Identified security tools installed, appropriate OS and applications, ports, and protocols appropriately limited per imaging standard.
Calculation	Endpoint protection coverage = For the most recent 12-month period, number of in-scope endpoints with approved or required build and security controls divided by the total number of in-scope endpoints.

Source: Gartner (September 2022)

Table 8: Outcome-Driven Metric 8 — Ransomware Recovery (Mission-Critical)

Target Question	**What is your percentage of mission-critical systems supporting critical business or mission functions that have successfully completed ransomware recovery exercising in the past 12 months?**
In-scope systems	In-scope systems are: ■ Systems that would materially damage critical business or mission functions if they are down. ■ Critical business or mission functions that are defined by each organization.
Definitions	“Ransomware recovery exercising”: An in-scope system was successfully restored in exercise mode in a simulated ransomware attack to an acceptable level of operation. The level of exercise should provide confidence that an acceptable level of business operations can be restored after a loss of supporting systems. “Successfully completed”: The systems were restored, and the functions brought back to an acceptable level of operations, including procedures to recreate any lost data and backlog procedures to enter business transacted manually while the systems were down due to the ransomware attack.
Calculation	Ransomware recovery = For the most recent 12-month period, number of in-scope mission systems that have successfully completed ransomware recovery exercising divided by the total number of in-scope systems.

Source: Gartner (September 2022)

Table 9: Outcome-Driven Metric 9 — Ransomware Downtime and Workaround Procedure

Target Question	What is your percentage of critical business or mission functions that have exercised downtime and workaround procedures in the past 12 months?
In-scope business functions	In-scope critical business or mission functions are those that have downtime and workaround procedures to operate without IT systems in the event of a ransomware attack.
Definitions	“Downtime and workaround procedures” are defined as written plans to achieve business and mission outcomes after a ransomware event when systems are offline. “Exercised downtime and workaround procedures” are defined as exercises or other training to ensure that different roles supporting a critical business or mission function know how to operate without IT. Critical business and mission functions are defined by each organization.
Calculation	Ransomware downtime and workarounds = For the most recent 12-month period, the number of in-scope functions or outcomes that have successfully exercised downtime and workaround procedures, or that have a written downtime and workaround procedure, divided by the total number of in-scope functions or outcomes.

Source: Gartner (September 2022)

Table 10: Outcome-Driven Metric 10 — Cloud Security Coverage

Target Question	What is your percentage of production cloud workloads aligned with the defined and approved security baseline?
In-scope cloud workloads	In-scope cloud workloads are cloud workloads supporting business or mission outcomes that require a defined security baseline of controls.
Definitions	“Production cloud workloads” are defined by each organization. “Security baseline” is defined by each organization.
Calculation	Cloud security coverage = For the most recent 12-month period, the number of in-scope cloud workloads aligned with the approved security baseline, divided by the total number of in-scope cloud workloads.

Source: Gartner (September 2022)

Table 11: Outcome-Driven Metric 11 — Multifactor Authentication Coverage

Target Question	What percentage of critical and high-risk applications are protected by multifactor authentication?
In-scope systems	In-scope systems are critical and high-risk systems that are determined to need multifactor authentication protection either by policy, criticality or designation.
Definitions	“Multifactor authentication protection” is defined as the inability to access the system without passing through a multifactor authentication control within the company policy.
Calculation	Multifactor authentication coverage = For the most recent 12-month period, the number of in-scope systems with multifactor authentication protection divided by the total number of in-scope systems.

Source: Gartner (September 2022)

Table 12: Outcome-Driven Metric 12 — Access Removal Time

Target Question	**What is your average number of hours from the request for termination of access to sensitive or high-risk systems or information to deprovisioning of all access?**
In-scope access changes	In-scope access change requests are any changes that require removal of access to sensitive or high-risk systems or information.
Definitions	“All access”: This includes directory, application and all authentication channels that provide sensitive data and resource access. “Access termination time”: Time from receipt of original request to terminate employee access to time that all access is deprovisioned.
Calculation	Access removal time = For the most recent 12-month period, the sum of all access termination times for all in-scope access change requests divided by the total number of in-scope access termination requests.

Source: Gartner (September 2022)

Table 13: Outcome-Driven Metric 13 — Privileged Access Management

Target Question	**What is your ratio of always-on personal privileged accounts to the number of individuals in roles who should have access to these accounts?**
In-scope individuals and accounts	In-scope individuals are system administrators who need access to privileged accounts. In-scope accounts are owned by in-scope individuals and have privileged access.
Definitions	“Privileged accounts” have privileged access that can negatively impact production systems or other business outcomes, including access to sensitive information.
Calculation	Privileged access management = For the most recent 12-month period, the number of privileged accounts divided by the number of in-scope individuals. Note: This ratio may be above 1 if the number of accounts exceeds the number of individuals.

Source: Gartner (September 2022)

Table 14: Outcome-Driven Metric 14 — Security Awareness Training

Target Question	What percentage of your employees and contractors have completed mandatory security training?
In-scope individuals	In-scope individuals are defined by each organization and usually include employees, contractors, and others who have access to critical and high-risk systems.
Definitions	Mandatory security training is defined by each organization.
Calculation	Security awareness training coverage = For the most recent 12-month period, the total number of in-scope individuals who have completed mandatory security training divided by the total number of in-scope individuals.

Source: Gartner (September 2022)

Table 15: Outcome-Driven Metric 15 — Phishing Training on Click-Throughs

Target Question	What is your percentage of click-throughs for your standard organizationwide phishing campaigns in the past 12 months?
In-scope individuals	In-scope individuals are all employees or other required individuals who are subject to phishing campaigns.
Definitions	“Standard campaign” is defined by each organization. It is neither the strongest, most aggressive campaigns, nor the weakest, least aggressive campaigns. “Click-through” is defined as clicking on a link in a phishing email. If an individual clicked on any phishing training link through a standard phishing campaign in the past 12 months, it is counted as a click-through. Any click-through of a real phishing email should also be counted as part of this metric.
Calculation	Phishing training on click-throughs = For the most recent 12-month period, the number of employees who have clicked on a phishing training link in a standard phishing campaign (or real phishing email) divided by the total number of in-scope individuals.Note: The number of times that an employee clicks on a phishing link does not impact this metric. An employee is only counted as 1 in the numerator of this calculation if the employee clicked on a phishing link in the past 12 months.

Source: Gartner (September 2022)

Table 16: Outcome-Driven Metric 16 — Phishing Reporting Rates

Target Question	**What is the percentage of employees who report suspicious emails for your standard organizationwide phishing campaigns?**
In-scope individuals	In-scope individuals are all employees or other required individuals who are subject to phishing campaigns.
Definitions	“Standard campaign” is defined by each organization. It is neither the strongest, most aggressive campaigns, nor the weakest, least aggressive campaigns. “Reporting suspicious emails” is defined as reporting a phishing attempt through normal channels. If an individual reports any attempted phishing in the past 12 months, it is counted as a report for this metric.
Calculation	Phishing reporting rates = For the most recent 12-month period, the number of in-scope individuals who reported the receipt of a suspicious email (training or real email) divided by the total number of employees. Note: The number of times an employee reports suspected phishing does not impact this metric. An employee is counted as 1 in the numerator of this calculation if the employee has reported a phishing link in the past 12 months.

Source: Gartner (September 2022)