# Zero Trust Metrics

September 16, 2022

Director, Community Ecosystem Engagement - Cybersecurity

Michael is a world-leading IT industry analyst. He has led North American and global initiatives focused on developing insights and strategies that connect technology solutions with business needs, combining data, knowledge, analysis and advanced content delivery to define options for IT and buy-side businesses.

Submitted by Michael O'Neil on 16, Sep 2022

Zero Trust Metrics


*Zero trust thought leadership group members: Geeta Kapoor (MSC Direct), Noah Davis (Trane Technologies), Leon Ravenna (KAR Global), Barney Baldwin (ex-MUFG, Columbia), Chase Cunningham (Ericom), Eve Maler (ForgeRock), Sean Frazier (Okta).*

Security leaders rely on metrics both for internal management of the security function, and for effective communication with business executives. Effective CISOs use meaningful metrics to build support for ZT across the organization, and to avoid the “precision without accuracy” trap.

## Executive summary:

Our research identified three stages for the effective use of metrics to assess and communicate security status and success.

1. **Establish context – ensure that the organization is ready to use metrics effectively and frame the metrics in ways that resonate with their target audiences.** The security team needs to have reached a reasonable level of achievement before metrics are helpful in driving attention rather than concern, and target audiences need to understand what the metrics represent before they can absorb and discuss their implications. Additionally, the metrics themselves must speak to objectives or concerns held by the target audiences. Organizational colleagues will tune out metrics that they view as too abstract, “in the weeds,” or esoteric.
2. **Identify a cohesive set of metrics that fill three key functions:**
    - *Strategic metrics* supporting communications with stakeholders (board of directors, senior business executives) who have responsibility for cyber risk management and for the budgets used to achieve both agility and compliance.
    - *Operational metrics* that help IT and security management identify cross-organizational security requirements and readiness.
    - *Tactical metrics* that are used to direct and assess security activities within the six ZT pillars (identity, devices, network, infrastructure, applications, and data).

    These metrics should be relevant to the top level (strategic, operational, tactical) objectives, quantitative and fact-based, measured in ways that are transparent and sound, and detailed/granular enough to make period-over-period comparison meaningful. Experience shows that the overall measurement framework will expand over time, so CISOs should not be too concerned with deploying a comprehensive set of metrics out of the gate: it’s better to start

with a refined set that track directly on key priorities.

3. **Implement processes for tracking progress against target objectives and over time.** CISOs can use metrics effectively by aligning them to targeted, high-value business objectives, identifying the technologies or practices that are intended to result in improved business or security outcomes, and then assessing the effectiveness of technology or process changes through the metrics. Tracking the degree of change over time will help the CISO to communicate consistently and effectively with the board of directors and business executives, to work with IT and security management colleagues to identify and address holistic issues requiring attention, and to guide and track progress within each of the six ZT pillars.

## Metrics: Force and alignment

Security leaders use metrics to set expectations, monitor progress, and identify problem areas, as well as to communicate with the senior leadership team (SLT) and board of directors, with business unit leaders, and with security team members.

Because metrics play such a central role in defining the parameters of analysis and action, CISOs take great care in analyzing how different kinds of inputs will be understood by key stakeholders. CISOs recognize the importance of defining the context for communication, selecting the most appropriate success measures – those which add to stakeholder understanding, rather than simply adding to the volume of information conveyed – and working with key parties, particularly executives and the board of directors, to use the metrics to build business momentum and resiliency. CISOs can use metrics as a guiding force in the development of security and business capabilities, but must also continually align the metrics with evolving internal and external requirements.

## Creating context

Metrics are used at multiple levels of the organization: by the board of directors and SLT to track the status of target protect levels, by IT and security leaders looking to balance budget across multiple requirements, and by security team managers and staff who are required to track the status of capabilities supporting ZT. CISOs can use metrics as the security *lingua franca* for the enterprise – but they must adapt

their metrics to the concerns/needs of each set of stakeholders.

CISOs need first to establish a security posture advanced enough to make metrics relevant. As one CISO contributing to this document observed, “what metrics can be used to evaluate zero trust impact and benefit?” is “a challenging question because there's a certain level of maturity that's needed. You need a baseline before you can even get started.” Below a threshold capability level, it’s more important to focus on building the foundation than measuring the thickness of its walls. Metrics are useful for assessing requirements and progress in a defined environment,[1] and superfluous when core capabilities have yet to be deployed.

Once they have established the foundational security posture and a baseline, CISOs work to create context for executive discussions of security as a function, before drilling down into ZT initiatives and objectives. As a member of the zero trust thought leadership team put it, “any new CISO knows that it's a dance the first time they get in front of the board of directors; there's a calibration process that takes place for a long time. High-level stuff is generally the most effective: pick a framework [e.g., ISO 27000 series, NIST CSF, CIS controls] and find a way to frame the conversation – develop a single pane of glass where you can demonstrate measured progress over time by using a CMMI model.”

This guidance came with a caution regarding the level of depth that is appropriate for executive level discussions. Security leaders, the contributor observed, “can get really granular. Often, qualitative analysis, a narrative that engages your stakeholders on the things that matter to them, works best. Can you dashboard the key issues around protecting IP for appropriate executives with a green/yellow/red approach?” This enables security leaders to “focus the conversation on the most important issues: current status with respect to protecting critical corporate information and intellectual property.”

One CISO explained that they have had success with a “GQM (goals, questions, metrics) approach: establish meaningful goals, identify and answer the questions that can and should be asked about ability to achieve those goals, and then establish metrics that demonstrate the efficacy of the ZT approach in protecting the business.”

When establishing context for a narrative that is based on metrics, CISOs should consider the following:

- Don’t go into the weeds. As one contributor said, “the math under the hood needs to be sound, but the presentation doesn’t need decimal points.” Another noted that a focus on often-abstract (to the audience) numbers can be detrimental: “If you say we're a 1.8, but we aspire to get to a 3.2 in terms of identify because we don't know where all our assets are, you need to be prepared to educate them” on what the numbers represent and why the current state is well below target.
    - Key implication: It’s better, the group agreed, to focus on why it is important to achieve a higher state of readiness, what is involved in building competence, and how long the journey will take.
- Take the time to consider different aspects of maturity and their relevance to metrics-based discussions. As an example, one contributor noted, “it will be difficult to speak to ZT initiatives and benefits in a business that relies on systems that haven’t been meaningfully updated in years” – but by the same token, “organizations that are progressive and which recognize that technology and change leads to greater efficiency and profitability” will likely be more aware of the need for ZT capabilities, and more proactive in understanding and applying metrics to evaluate priorities and progress.
    - Key implication: When using metrics to identify zero trust capabilities and progress, it’s important to understand that “maturity” isn’t strictly a property of the security function – it applies to the IT environment that is being secured, and (importantly) to the culture of the organization itself. The narrative described in this section needs to connect to relevant aspects of maturity.

## Business and technical measures of progress

After defining the context for metrics-driven discussion, CISOs need to develop and articulate the value of metrics that support the zero trust discussion – with the board of directors and SLT, as an IT security management tool, and as a means of organizing and evaluating progress within the six ZT pillars. These measures might be classified as:

- *Strategic* – focused on issues important to the board/SLT.
- *Operational* – focused on issues important to IT and security management.
- *Tactical* – focused on issues that are used to assess ZT maturity or progress within one of the six pillars.

There isn’t a one-size-fits-all set of metrics – what is strategic to one firm may be operational in another setting, operational measures might be used for tactical objectives – but generally speaking, CISOs will use a mix of these three types of measurements to assess their security posture and progress, and to communicate with other business stakeholders. Examples of different approaches used by contributors to this research include:

- “The business value we get out of zero trust is in time to repair or time to provision. It likely can be monetary because you are streamlining everything. It's likely going to be monetary from a resource capacity perspective. Those are quantifiable measures.”
- “We measure reduction of spend across IT – for example, savings gained by rationalizing multiple redundant tools against ZT objectives and principles.”
- “We use third party security ratings, CRQ measurement, cyber risk metrics, and security benchmarks. I run those numbers because they are 100% objective.”
- “We have a listing of critical apps. How many of those are covered by MFA?”
- “How many times does MFA need to happen? How many times did we actually get assurance through conditional access?”
- “We track accounts automatically created through our IGA platform: How many are provisioned, how many are decommissioned, how many had errors? Progress is defined in terms of reducing error rates.”

The business and technical measures listed above represent only a subset of metrics used by CISOs. Collectively, they shed light on how specific metrics inform strategy-level discussions about zero trust.

The first quote, referring to value, illustrates the importance of measuring outcomes that are important to SLT members as business objectives. Such a metric would be strategic in most contexts. These measures may not always be precise, but they represent points at which ZT contributes to overall business success.

The second quote is specific to IT cost savings obtained by rationalizing the controls, tools, and vendors used to protect the enterprise. This would be operational in most organizations, as it is of keen interest to people who manage IT expenditures, but probably more important at an aggregate than detailed level to business leaders.

The third quote refers to how metrics are assembled, and reflects the contributor’s belief that independent measurement sources are important to positioning the

metrics themselves as impartial and independent, allowing discussion to focus on implications of the current state and advantages that can be gained from improvement. Third party sources might be valuable for any type of metric – strategic, operational, or tactical.

The fourth, fifth, and sixth quotes reference specific issues tracked by contributors to this research. These quotes are included to provide a sense as to how these kinds of issues are tracked, evaluated, and used within an organization. The fourth quote, regarding MFA and applications, refers to a metric that would be operational in some firms, and tactical (as part of the application pillar) in others. The fifth quote references a measurement that might be tactical in a mature organization – used to evaluate the identity pillar – but which might be strategic in others, helping the CISO to provide quantitative evidence of how more effective authentication contributes to "frictionless security," and as a result, to better productivity and less temptation to use work-arounds or shadow IT.

## The dog that didn't bark

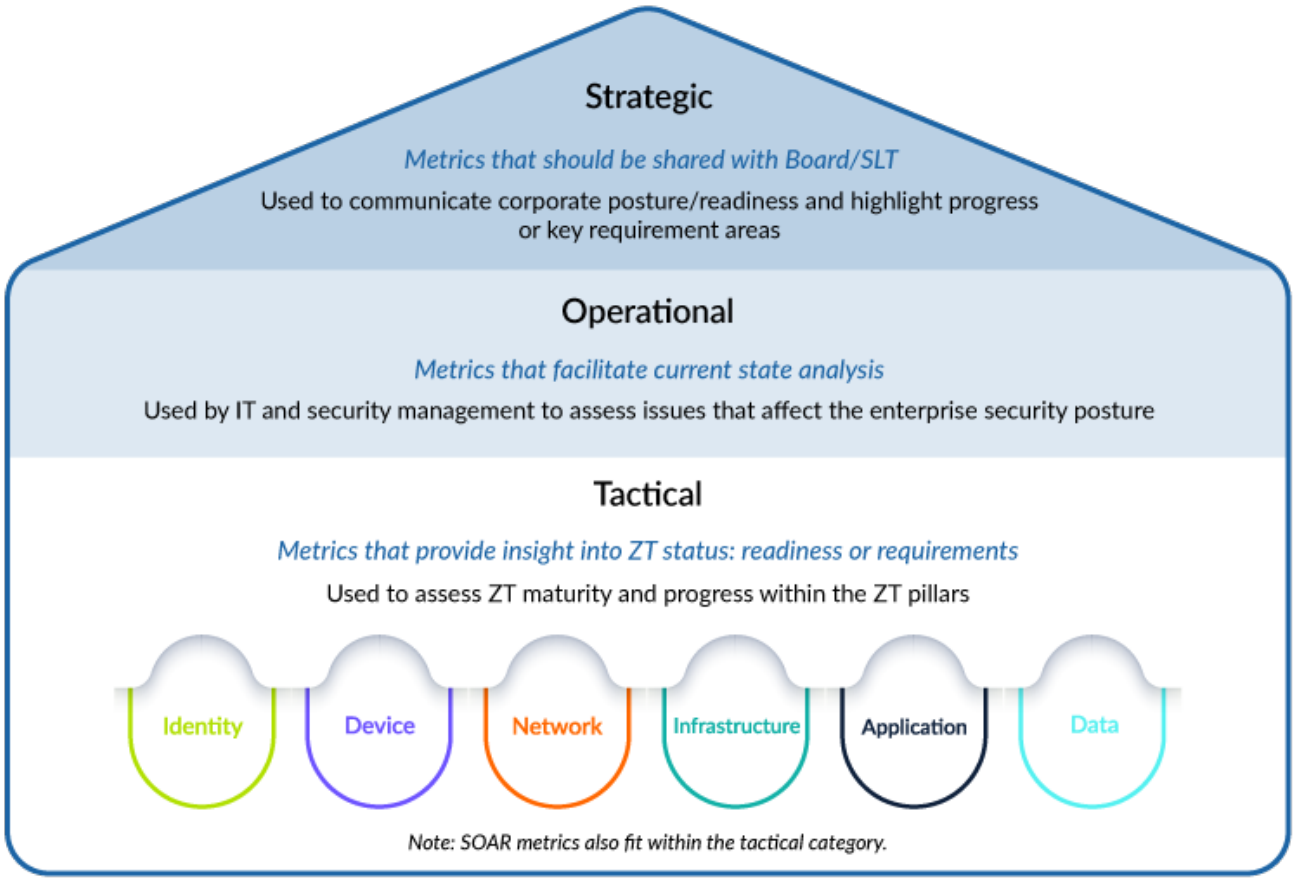
- "It's a constant struggle for cybersecurity. The better the job you're doing, the harder it is to show it."

As important as reliable, relevant, objective metrics are, cybersecurity success is ultimately reflected in the *absence* of events, rather than in the cadence and completeness of actions taken to safeguard users, data, and other assets. As one contributor stated, "a majority of ZT benefits are qualitative – the proactive measures that you put it place. It's almost like proving a negative – you didn't get impacted by a new vulnerability. How do you prove the impact of not having to do something?"[2]

CISOs use metrics to demonstrate risk and the measures taken to address risk. But all CISOs know that a single significant breach will weigh more heavily than hundreds of proactive actions. This is ultimately the driving force behind zero trust: the understanding that by using ZT principles and technologies, and ensuring that these controls are optimally aligned with risk, CISOs improve their ability to prevent breaches from negatively affecting corporate operations, reputation, and shareholder value.

# Metrics as a guiding force: *Stratascale ZT-MICA*

As a final step in creating *The Executive Guide to Zero Trust,* Stratascale SMEs assembled an Excel-based tool: the Stratascale Zero Trust Metrics in Context and Action, or *Stratascale ZT-MICA*. *Stratascale ZT-MICA* contains an extensive set of metrics that may be important to CISOs who are looking to build foundations for board, executive, peer, and team discussions around zero trust.




Source: Stratascale 2022

The metrics are organized into the three major categories discussed earlier in this document: strategic, operational, and tactical. Some issues may be important in multiple areas, or may be (as discussed above) positioned differently across businesses, based on organizational maturity or other factors.

The strategic metrics are those that are used in board and SLT discussions. Dashboards prepared for executives can use metrics from this category to support

dialogue around risk and resilience.

The operational metrics function across pillars and are used by IT and security management to obtain a holistic view of the organizational security posture and to identify top-level areas requiring attention or remedial action.

The tactical metrics are specific to pillars. These are used by line management to understand current state and progress in areas that are important to the overall security capabilities of the organization.

Each security leadership team will select metrics that are relevant to their specific business context. To help support this process, *Stratascale ZT-MICA* gives CISOs an ability to prioritize across a large set of prospective metrics – to assess current achievement in each area, using either default or company-specific achievement measures – and to use either built-in or user-generated Excel charts to plot current state and changes over time.

If you would like a copy of *Stratascale ZT-MICA*, please click here. Please note that while the tool is provided at no cost, you will need to enter basic registration information. You will also have the option of enrolling in a ZT Metrics Benchmark Comparisons initiative, which will provide you with a comparison of your results compared with five or ten anonymized peer organizations.

## Working with this content

CISOs looking to integrate this perspective on zero trust within executive-level strategy discussion or as a management tool can use the following challenges/constraints and takeaways to inform their approach.

### Key challenges/constraints to use of metrics in assessing and communicating ZT strategy:

- Internal maturity acts as a gate on the use and impact of metrics. In particular, firms that rely heavily on aging systems may not be candidates for metrics-based explanations of ZT benefits.
- Data granularity needs to map to the audience for the metrics. Detailed metrics are appropriate at a tactical level, but not for executives, who will look for fact-based perspectives that establish a foundation for discussion.

- In many cases, specificity and accuracy have an inverse relationship to metric value: the most strategic metrics are difficult to quantify, while the most rigidly-quantified metrics tend to apply to tactical areas.

## Takeaways from “Metrics”:

- Metrics support discussions at strategic, operational, and tactical levels. Well chosen and well-supported metrics provide a foundation for dialogue – but they aren’t a *substitute* for dialogue. CISO discussions of strategy, readiness, and connections with business objectives expand from a fact base rooted in metrics.
- Use of third-party services and frameworks can help enhance executive confidence in strategic-level metric quantification.
- There is a rich set of metrics available to the CISO, which can be used to support strategic, operational, and tactical discussion. CISOs who can use these metrics to demonstrate the efficacy of ZT controls build trust within the organization, and potentially, with external stakeholders such as customers and regulators.

## Accessing the *Stratascale ZT-MICA tool*

To access the Stratascale Zero Trust Metrics in Context and Action (*Stratascale ZT-MICA*) tool – either as a template for measuring and tracking ZT within your organization, or as a source of ideas that can inform your own ZT metrics – please fill out the form below.

---

[1] “Defined” used here as it appears in the CMMI framework: processes that are characterized for the organization (as opposed to discrete projects) and which are proactive.

[2] This quote is also discussed in The Zero Trust Rollout Notebook, in the section on Setting Expectations.

*This is the eighth of eight source documents included in Stratascale's "An Executive Guide to Zero Trust" research series. We will also publish a capstone report connecting these eight pieces, plus a six-part companion series ("The Technical Manager's Guide to Zero Trust") and several compilations and ancillary documents and tools.*