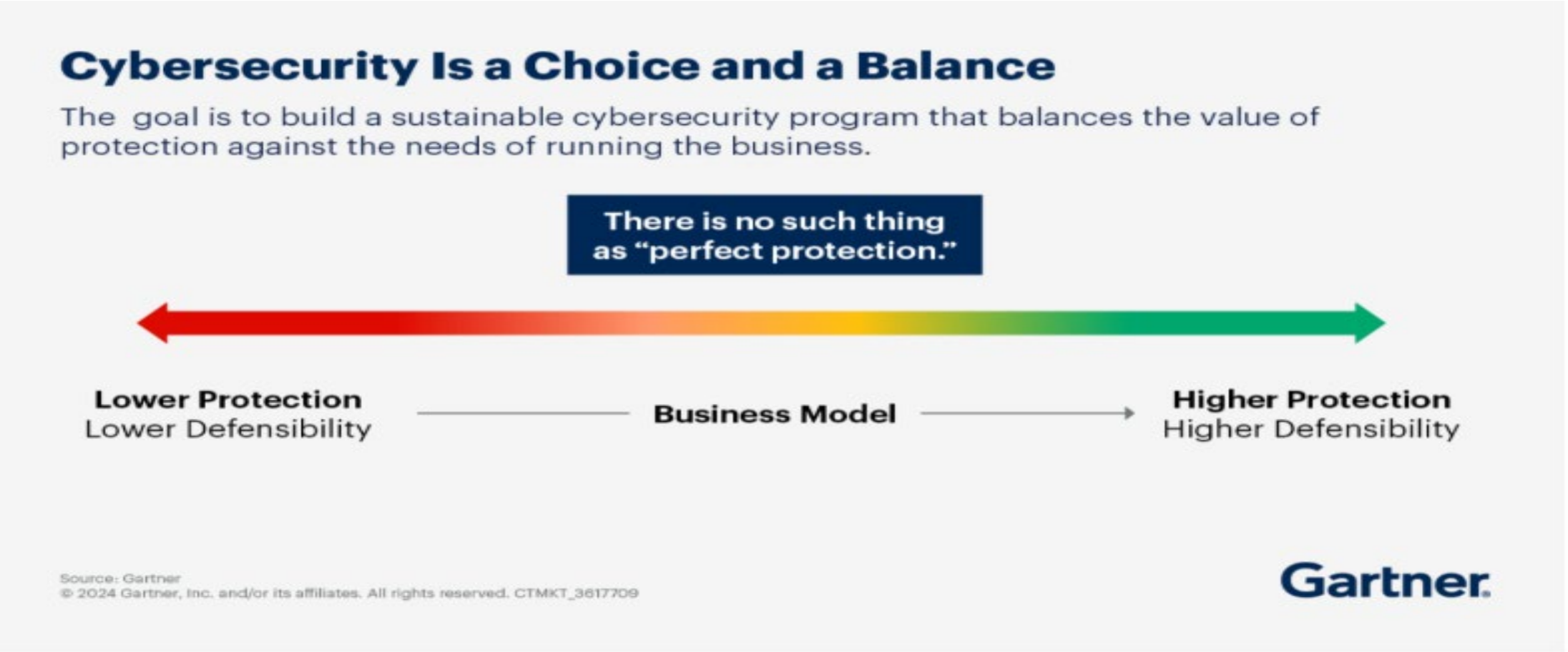
The Essential Building Blocks of Mainframe Vulnerability Management

Cynthia Overby

Director, Strategic Security Solutions

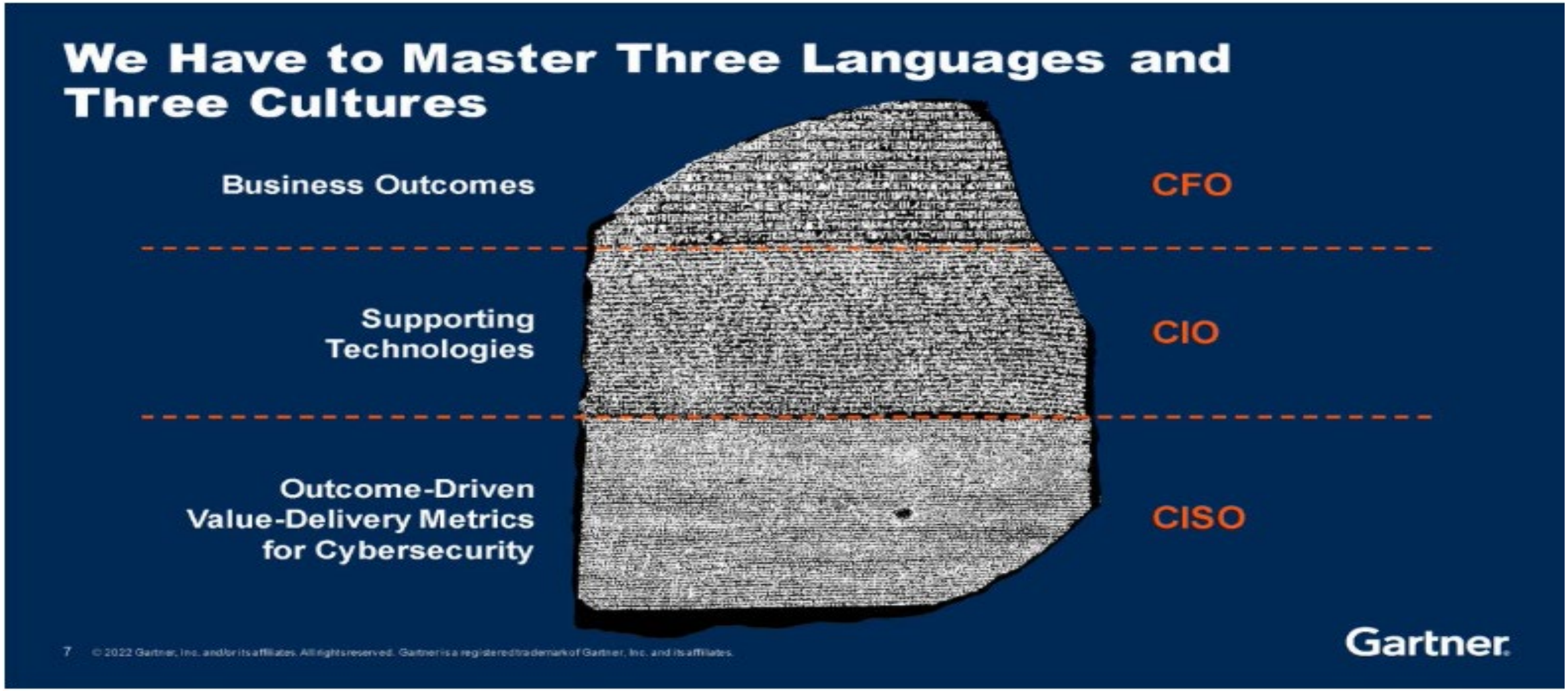
Rocket® software

Cybersecurity: A Strategic Choice



https://emt.gartnerweb.com/ngw/globalassets/en/cybersecurity/images/infographics/cybersecurity-is-a-choice-and-a-balance.png

Three Languages and 3 Different Expected Outcomes



https://pbs.twimg.com/media/FfcHd8bXwAAFeNg.jpg

vare

Mainframe Security: What are the Components

Code & Configuration Based Vulnerability Mgmt.

At the operating system layer

- SVC's
- PC Routines
- APF Libraries
- Home-grown exits that make SAF calls

- Security parameters in 3rd party products
- ESM's (RACF, CA ACF2, CA Top Secret)
- Hardware configurations
- IPL parameters
- Over privileging
- Excessive access
- APF Libraries

- Security Policy Mgmt.
- Change Mgmt.
- Patch Mgmt.
- Backup & Recovery

Example: Evolving Regulation's: PCI 4.0 DSS

3. Protect Card Holder Data

- Storing payment account data should only be done if it is essential for business purposes.
- Sensitive authentication data must never be retained post-authorization.

5. Maintain a Vulnerability Management Program

- Vulnerability management entails the systematic and ongoing process of identifying and addressing weaknesses within an organization's payment card ecosystem. This involves:
  - tackling threats posed by malicious software,
  - regularly identifying and fixing vulnerabilities,
  - and guaranteeing that software is developed securely, free from known coding vulnerabilities.

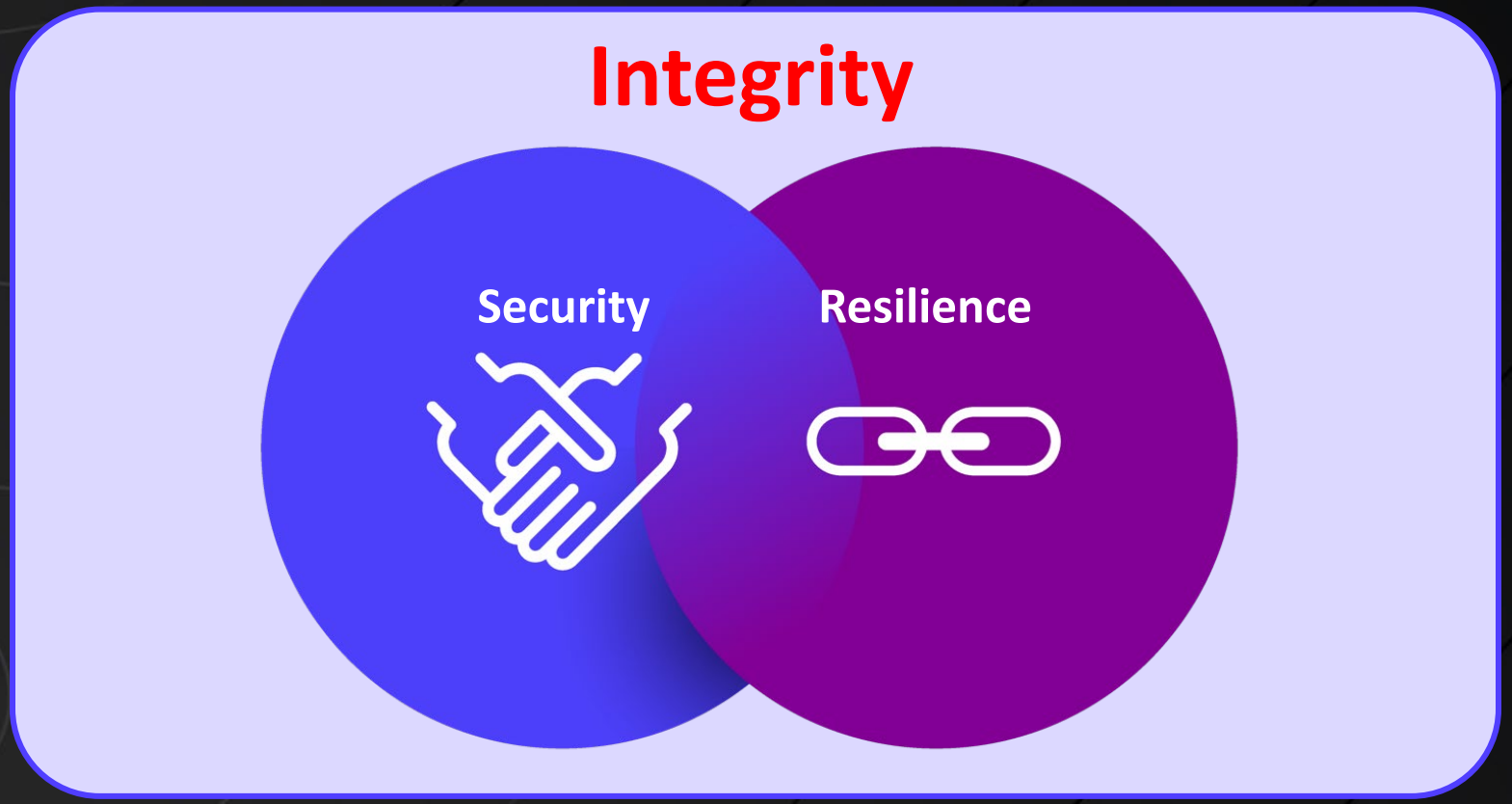
Note: PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. This applies to data that is printed, stored locally, or transmitted over internal or public networks to remote servers or service providers. If you accept or process payment cards, PCI DSS applies to you.

Let’s Talk Mainframe Vulnerability Mgmt.

What is different and Why

“Without Integrity There Can be No Security”

Integrity means the inability of the end user to bypass the controls put in place by you and the operating system.



Mainframe Integrity Customer Responsibilities

WHAT DOES THIS MEAN?

- IBM does **not** state that z/OS will not have any system integrity problems
- It is the installation's responsibility that all authorized code (vendor and internal) conforms to the same high-level standards that z/OS uses to maintain its integrity

The IBM MVS Authorized Assembler Services Guide states:

"… to ensure that system integrity is effective and to avoid compromising any integrity controls provided in the system, the installation must assume responsibility … that its own modifications and additions to the system do not introduce any integrity exposures. That is, all installation-written authorized code (for example, an installation SVC) must perform the same or equivalent type of validity checking and control that the system uses to maintain its integrity."

Where to Begin?

Key Components to Building Effective Mainframe Vulnerability Management, Challenges, and Best Practices

The first phase of developing the capability TO DO mainframe vulnerability mgmt. is to define/refine a strategy for achieving the organization's business goals. This means understanding what your business leaders are trying to achieve and mapping that to risk metrics. Asking the hard questions to business leaders.

Identify the Assets

Identify the programs, security configurations to be assessed and monitored. The DISA Stigs are a good place to start.

Determine the operational environment comprising the areas of concern to include LPARs, systems programmers, security personnel, mgmt. team).

Identify Stakeholders

Identify a list of stakeholders and include internal and external entities. Potential candidates include:

Executive and Senior Mgmt.
Heads of Business Lines
IT Operations
Mainframe Security
Board of Directors
Vendors
Regulators and Auditors
Compliance Officers
Risk Officers

Create a Scoping Statement

Create a scoping statement that includes all assets and stakeholders to be assessed and monitored.

Determine who is responsible for each area, who is read in on vulnerabilities, who reports out to risk, how are metrics reported out.

Key Components to Building Effective Mainframe Vulnerability Management, Challenges, and Best Practices

Understand What you Need to Protect and Recover

Define/Modify the digital operational resilience governance strategy with risk tolerances.

Identify and **Assess** the Important Business Services and consequential impact from the loss of a core service.

Identify the Gaps

Assess the current Risk posture for the Important Business Services to identify gaps.

Determine the full scope of your mainframe vulnerability management.

Define your Roadmap

Create a transition roadmap to address the identified gaps.

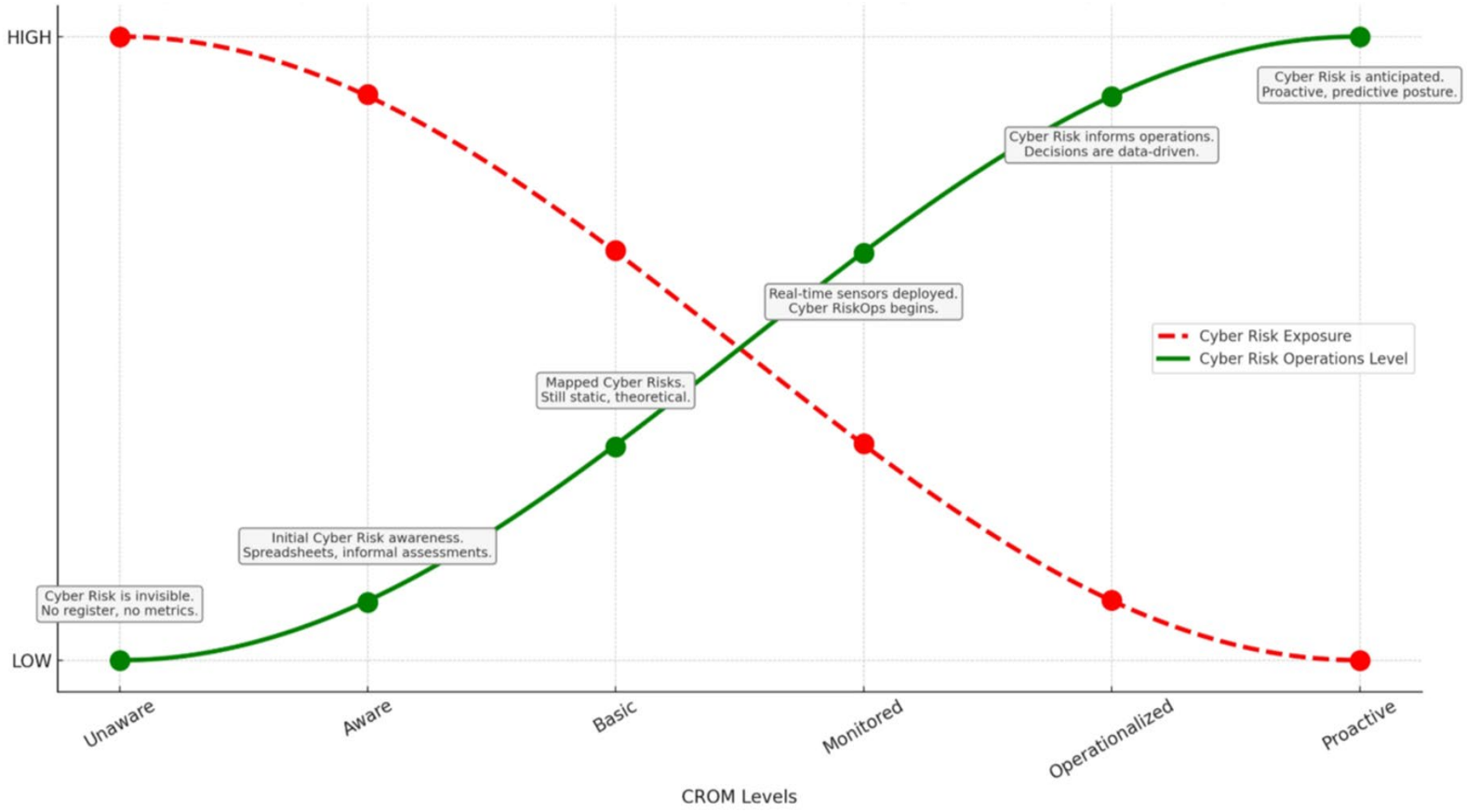
Explore options to determine approved methods of mainframe vulnerability assessment.

Align the vulnerability management process to the organization's requirements and critical success factors and risk metrics.

Let’s Talk Risks and Metrics

Cyber Risk Operational Model (CROM)

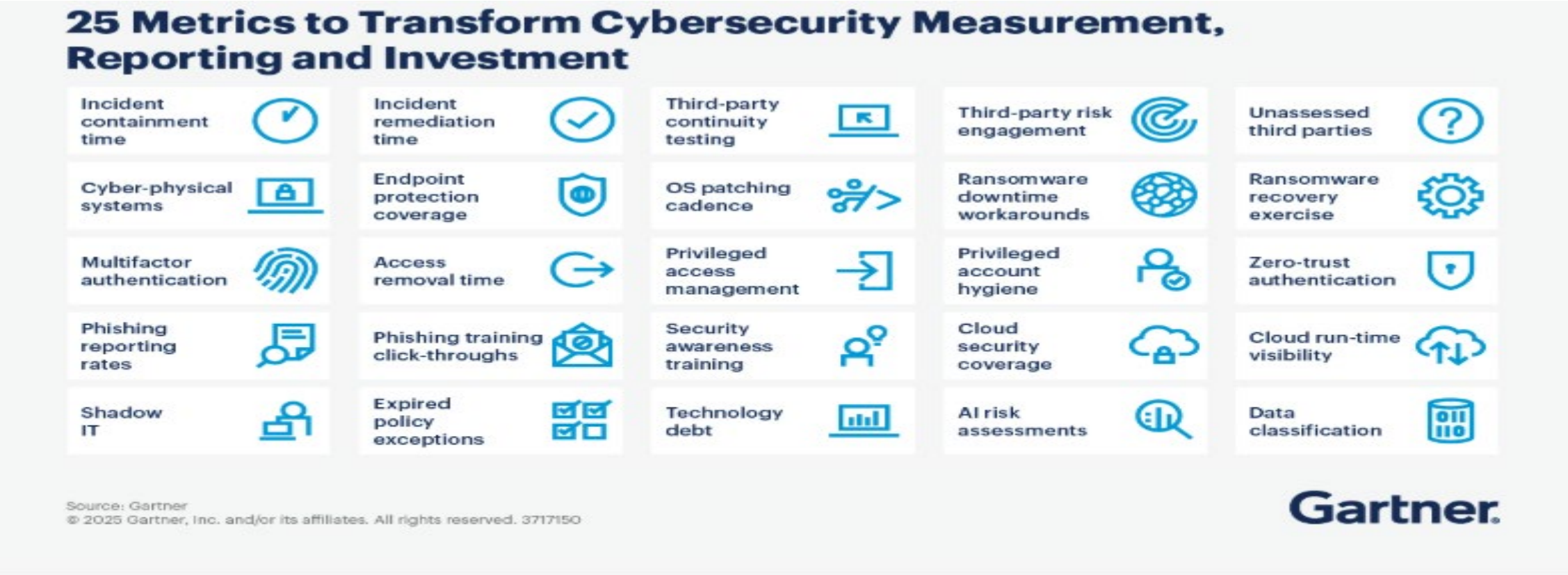
The CROM graph visualizes cyber risk management maturity along two critical dimensions:



1.Cyber Risk Exposure: How vulnerable the organization is to cyber threats (HIGH to LOW).

2. Cyber Risk Operations Level: How effectively the organization operates. (Unaware to Proactive)

Outcome Driven Metrics (ODM's)



https://emt.gartnerweb.com/ngw/globalassets/en/cybersecurity/images/infographics/cybersecurity-business-value-benchmark-25-metrics.png

Develop a Plan for Vulnerability Management

The second phase is to convert the strategy into a plan with rules and guidelines for all vulnerability management teams. Each team needs to understand what is expected of them and how they will use the resources they are provided.

Goal 1 – Stakeholders need to understand the need for mainframe vulnerability management and agree to the remediation process and procedures.

- ✓ Senior management endorses the establishment of a mainframe vulnerability management program, assigns budgets, and agrees to implement the processes and operation of the plan.

Goal 2 – Budget for vulnerability management

- ✓ The budget will drive identification of vulnerabilities. Tradeoffs for developing expertise inhouse or using a service should be considered along with long-term costs such as program and skills maintenance.
- ✓ Tools selection will impact the quality of information on vulnerabilities and ease of mitigation.

Implement the Vulnerability Analysis and Resolution Capability

- The third phase is when the organization actually *implements* the vulnerability management plan and conducts vulnerability analysis and resolution activities.

- The following are the foundational steps in the implementation of a mainframe vulnerability management plan:

✓ Provide training on the tools and processes.
✓ Determine and execute on vulnerability assessment activities.
✓ For program vulnerabilities submit to the appropriate vendor for mitigation.
✓ Record discovered vulnerabilities in RMS.
✓ Categorize and prioritize vulnerability mitigation.
✓ Manage disclosure of discovered vulnerabilities.
✓ Determine effectiveness of vulnerability dispositions.
✓ Analyze root causes of configuration vulnerabilities.

Reporting?

- If you’re not including a strategy to report out on all mainframe vulnerabilities in your risk/vulnerability management program, you are not reporting out accurate data, and your risk reporting is incomplete.

- Regulators are now looking at critical assets and where they reside; not just systems, not platforms, not cloud. Where do your critical assets reside?

Continuous Improvement

Assessing the overall vulnerability management program ensures that both analysis and discovery are meeting the organization's needs.

- **Discovery requires the expertise to assess the assets and associated processes of critical services.**
- **Analysis is the ability to determine the extent of the vulnerability and its anticipated effect on the organization and its critical services.**

Review the strategy with stakeholders.

- **Are all relevant stakeholders represented? Determine what each stakeholder needs.**
- **Is the process reaching the appropriate work products? What information directly impacts stakeholder processes?**
- **How are stakeholders using the information?**
- **Is the process providing the appropriate work products?**
- **What information is missing?**

What Do Companies Stand to Lose?

- Forfeiture of revenue
- Remediation expenditures
- Diminished market share
- Business disruption
- Collateral security risks
- Compromised intellectual property
- Legal and Regulatory fines (GDPR, PCI DSS, DORA)
- Degraded brand reputation

> It takes 20 years to build a reputation, and five minutes to ruin it.
>
> WARREN BUFFET

Thank you

coverby@rocketsoftware.com

Rocket® software