A CISO Executive Guide

TOP 10 CYBERSECURITY POSTURE METRICS EVERY CISO SHOULD USE

You can't improve what you can't measure

Balbix®

Cybersecurity Posture Metrics Matter More Than Ever

Metrics and modern cybersecurity are intrinsically linked. CISOs use metrics to determine priorities, inform decisions, support investments, track progress and maintain accountability. At this point, if you are a CISO, you are likely a data-driven CISO. Are you comfortable with your choice of metrics?

The challenge is that cybersecurity covers a broad range of areas, and each area has specific type of data, and different metrics. The purpose of this paper is to focus on the specific area of cybersecurity posture management and key metrics relevant to this area.

Cybersecurity posture management is the continuous process of managing an organization's cyber risk by quantifying and reducing the likelihood and impact of a successful breach. Cybersecurity posture management is essentially managing cyber risk. Cybersecurity posture management typically includes three practices:

- **Asset Inventory:** Managing the organization's digital assets
- **Vulnerability Management:** Discovering and managing risk items such as software vulnerabilities (Common Vulnerabilities and Exposures, or CVEs), misconfigurations and weak/reused passwords
- **Cyber Risk Quantification:** Quantifying and reporting on the identified cyber risks in dollars

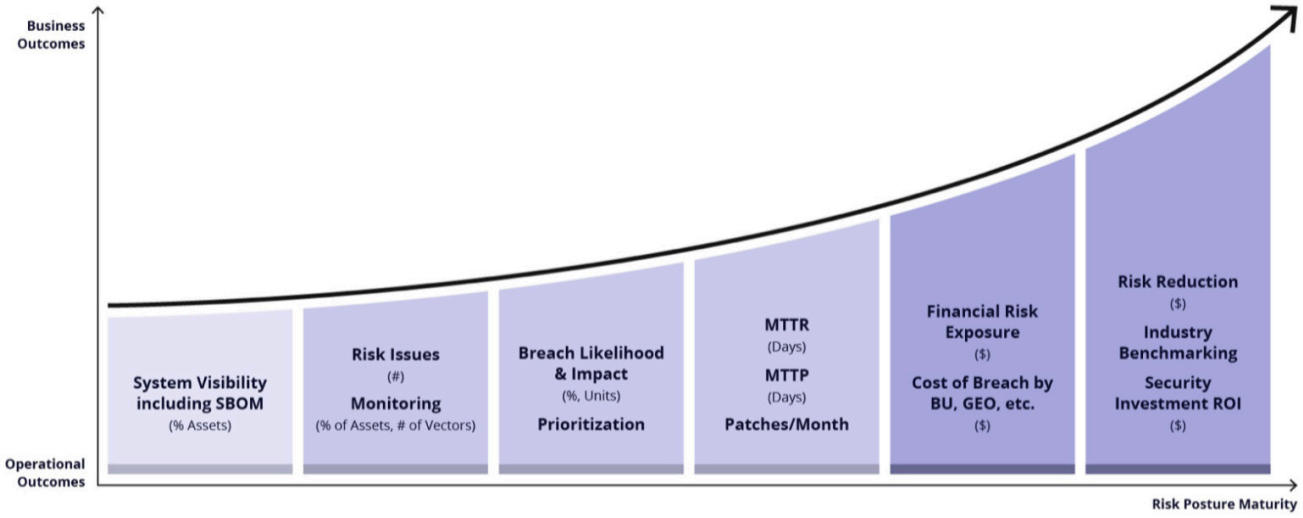
Three Practices of Cybersecurity Posture Management

Reporting on cybersecurity posture metrics to their executive leadership team in an easy-to-understand way is increasingly important for CISOs. This comes in large part because focus in the C-suite on cybersecurity as a risk area has rapidly risen over the past few years. Recent surveys of CEOs, CFOs and CIOs have consistently shown that cybersecurity is one of their top concerns. In fact, it's often ranked #1 or #2, right alongside digital transformation.

Similarly, cybersecurity reporting is increasingly a board issue. Regulatory requirements like the proposed SEC rule changes in the United States, and the recently passed SLACIP Act in Australia, make board involvement in overseeing cybersecurity posture mandatory. As a result, a growing number of CISOs are compiling security metrics appropriate for reporting to the board.

How Cybersecurity Posture is Measured Today

The challenge for CISOs to report on cybersecurity posture is that they can only report on the data they have. For example, if the general manager of a line of business wanted the CISO to share cybersecurity posture metrics for her business, she would likely receive one report for cloud assets related to the business, and a second report for laptops or servers residing on-premises. The language and metrics in each report would be different, and operational in nature. In the end, she would remain clueless about the cyber risk in dollars for her business.



Metrics should drive both operational and business outcomes

To be clear, it is good to have operational metrics. But, operational metrics don't translate directly to revenue and expense, and don't support business decision making about future cybersecurity investments or priorities. Reporting on a narrow set of metrics can also result in a CISO appearing to lack an understanding of the information that the rest of the C-suite and the board need to have in hand to make decisions that drive positive business outcomes.

Focusing on Business Outcomes

With a focus on business outcomes, CISOs can use metrics to change their role and the scope of their responsibilities. They can move from the old paradigm where the CISO was the person accountable for managing cyber risks, to a new paradigm where they are the person responsible for ensuring their organization's leadership and risk owners have the knowledge and tools required to make informed business decisions about cyber risk.

To align with this new direction, CISOs need to start talking more about costs and risks in dollars (or their local currency) as it relates to cybersecurity. They can do so by tying their metrics to business outcomes. By focusing on outcomes, CISOs can also communicate more clearly about how investments in their security program lead to measurable reductions in risk. This can happen in parallel with the use of metrics to manage the day-to-day operations of the security team.

Operational or Business Metrics?

Choosing between operational and business metrics is therefore a false choice. It is not one or the other. Rather, what is important is to identify metrics that tie operational security outcomes to the business mission. Primary consideration for CISOs should be the identification of metrics that connect the goals of their security team to the business mission of their organization.

Top 10 Cybersecurity Posture Metrics Every CISO Should Use

The following 10 metrics are grouped according to the three main practices of cybersecurity posture management, as outlined above: asset inventory, vulnerability management and cyber risk quantification.

Asset Inventory	Vulnerability Management	Cyber Risk Quantification
1 Asset Inventory Coverage	4 Vulnerability Assessment Coverage	8 Breach Likelihood
2 Software Inventory Coverage	5 Mean Age of Open Vulnerabilities	9 Breach Impact
3 Security Controls Coverage	6 MTTP–Critical Vulnerabilities	10 Breach Risk
	7 Mean Time to Remediate	

Top 10 Cybersecurity Posture Metrics Every CISO Should Use

Each metric has been chosen for its utility to link security operations to the business. As such, both security outcomes and business outcomes have been provided for each metric. Additional considerations have also been noted for many of the metrics to help CISOs think about what specifically they should measure given that each organization is unique.

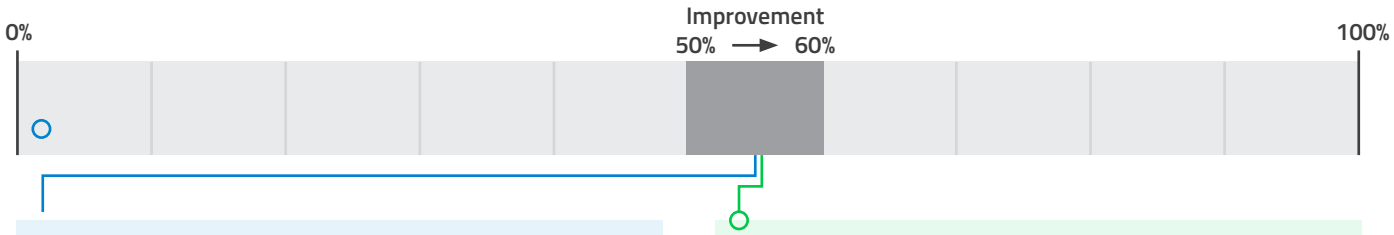
For each metric, CISOs should determine service level agreements (SLAs) aligned to their organizational needs based on the maturity of their security posture as well as the requirements placed on their organization by the business, by regulators and by other stakeholders. For example, a CISO may have a good software inventory for only 10 percent of their assets today but look to make a focused push to double that to 20 percent in six months time.

Asset Inventory

CISOs can measure and report on what they know about their assets. In doing so, the goal should be to reduce the number of unknowns about their cyber assets and their organization's attack surface. After all, you cannot protect what you don't know about.

1. Asset Inventory Coverage

METRIC: Percentage of enterprise assets for which there is accurate and detailed attribute information about the asset including asset category (server, container, laptop, IoT device, S3 bucket, EC2 instance, etc.), the asset location, users and so on.



Security Outcomes

- Identify unknown or unmanaged assets
- Determine appropriateness of asset location and access
- Build a foundation for vulnerability and risk assessment

Business Outcomes

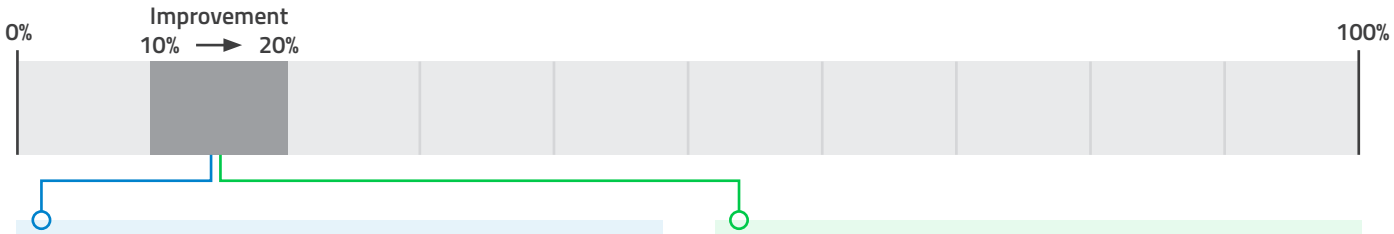
- Increase cost savings (in $) due to identifying unused, under-utilized or mis-used devices and assets.
- Reduce risk via more comprehensive vulnerability management.

Additional Considerations

- Unfortunately, CISOs can't know exactly how many assets aren't visible to the security team. However, CISOs can, and should, put practices in place to improve their visibility and can get to very good (95%+) coverage. Do you know when a new cloud asset is spun up? Are you monitoring your DNS environment in a continuous manner for new devices?
- Knowing the asset category, location and users is just the beginning. CISOs should look to inventory additional information about each asset. For example, inventorying software versions and security controls is important, and is covered below.

2. Software Inventory Coverage

METRIC: Percentage of assets for which software inventory is available, including the software versions.



Security Outcomes

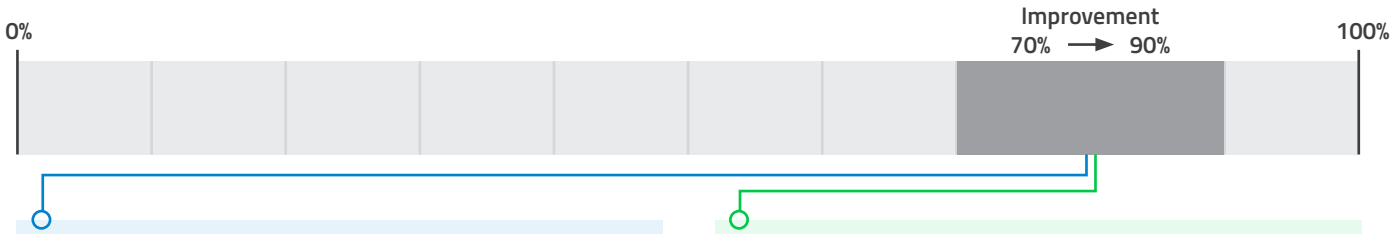
- Identify CVEs based on installed operating system and application versions.
- Identify supply chain vulnerabilities based on each application's software bill of materials (SBOM).

Business Outcomes

- Increase savings (in $) in subscription costs or maintenance fees due to the identification of obsolete or over-licensed software. For example, analysts could identify and cancel the user license for software instances that have been unused for a certain number of days.
- Reduce unscheduled outages due to vulnerabilities being exploited (measured on a quarterly or yearly cadence).
- Reduce risk via more comprehensive vulnerability management.

3. Security Controls Coverage

METRIC: Percentage of assets covered by company required security controls (EPP/EDR, IAM, VPN/ZTNA, DLP, backup, etc) for those assets.



Security Outcomes

- Improve the percentage of assets that include company-required security controls.
- Reduce assets (#) with security incidents.
- Improve results when doing gap and coverage analysis.

Business Outcomes

- Reduce unplanned downtime (in hours), or other business impacts, due to security incidents.
- Reduce partner and customer issues (#) related to security incidents.
- Improve regulatory compliance (# audit issues).
- [if MFA is a required security control] Reduce unauthorized access (#) to sensitive data.
- Reduce risk due to more complete protection.

Additional Considerations

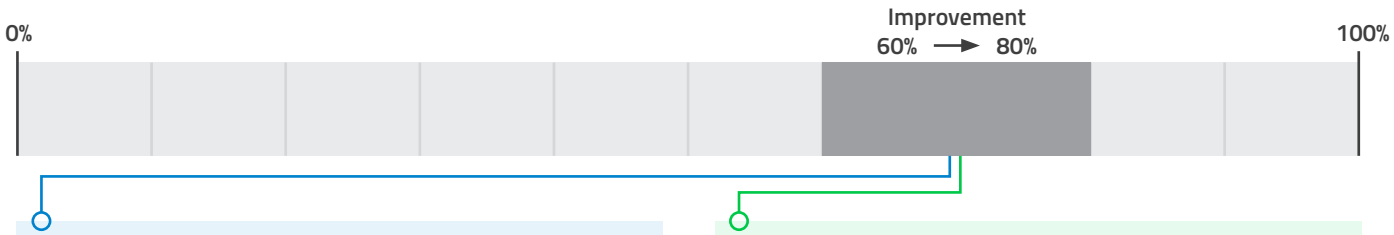
- This metric could be measured separately for specific controls, for example for endpoint protection or MFA, or as a single metric across a broader set of controls.
- This metric likely requires categorization by asset type. For example, the security controls for laptops may vary from the security controls required for cloud workloads. Similarly, IoT devices may not have a universal build or set of security controls. This ties back to the importance of having an asset category inventory.

Vulnerability Management

Vulnerability management has traditionally focused on software vulnerabilities (CVEs). In recent years, security teams have also started to expand their focus to also include access/trust issues and misconfigurations (weak encryption, insecure services, TLS/SSL certificate issues, cloud misconfigurations). Cloud misconfigurations are especially important since many organizations on their cloud migration journey overlook the reality that cloud systems do not have the usual protections of the corporate firewall.

4. Vulnerability Assessment Coverage

METRIC: Percentage of assets covered by vulnerability assessment tools.



Security Outcomes

- Improve visibility of vulnerabilities (CVEs, misconfigurations, reused passwords, weak encryption, access and trust issues, etc.).

Business Outcomes

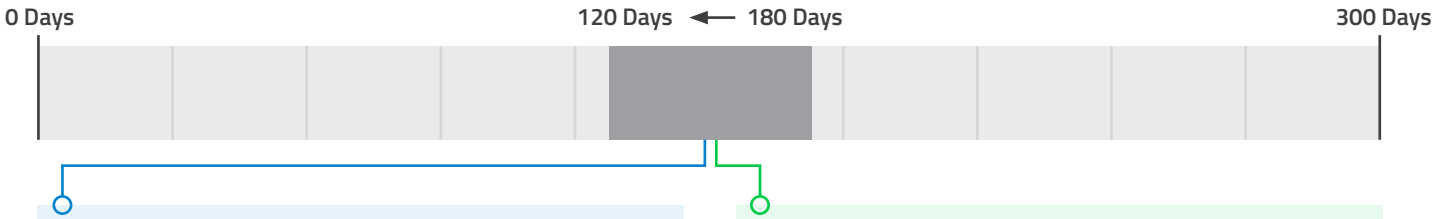
- Identify areas of business with vulnerabilities. Assets can be grouped to map risk by line of business, geography, asset type, data center, etc.

Additional Considerations

- In addition to basic coverage, CISOs may want to also track the quality and fidelity of the data that is being gathered. For example, how many assets have authenticated vs unauthenticated scans?
- Another factor to consider is how frequently vulnerability information is updated. Are the assessments being done continuously?

5. Mean Age of Open Vulnerabilities

METRIC: Average age (in days) of all open vulnerabilities.



Security Outcomes

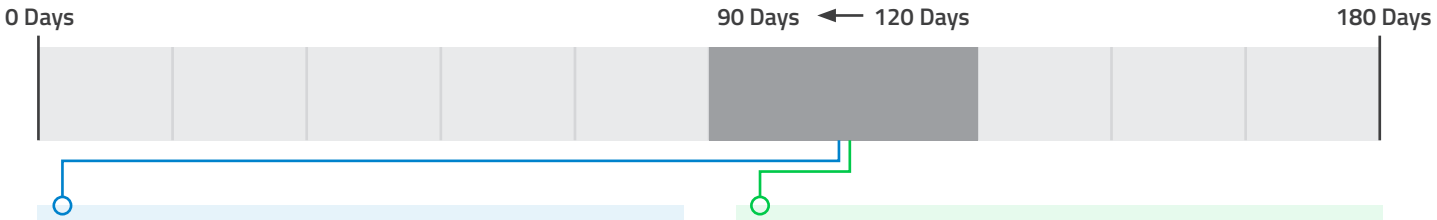
- Reduce the time available for critical vulnerability exploitation.

Business Outcomes

- Reduce unscheduled outage time due to critical vulnerabilities being exploited (time period: monthly, quarterly).
- Reduce (%) regulatory findings.

6. Mean Time to Patch (MTTP)—Critical Vulnerabilities

METRIC: MTTP for critical software vulnerabilities that are being actively exploited in the wild.



Security Outcomes

- Reduce the time available for critical vulnerability exploitation.

Business Outcomes

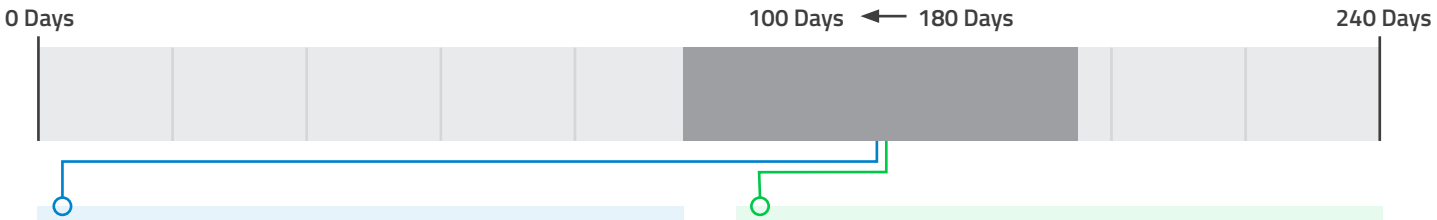
- Reduce unscheduled outage time due to critical vulnerabilities being exploited (time period: monthly, quarterly).
- Reduce (%) regulatory findings.

Additional Considerations

- A system of record (vulnerability assessment tool, RBVM tool, etc) should be identified to record the software vulnerabilities that are critical.

7. Mean Time To Remediate (MTTR)

METRIC: Mean time to remediate (MTTR, in days)



Security Outcomes

- Reduce (%) the time available for software vulnerability exploitation.

Business Outcomes

- Reduce (%) negative business outcomes (exposed data, unscheduled outages, etc.) due to vulnerabilities being exploited (cadence: quarterly, yearly).
- Reduce the time (in days) to meet audit requirements.
- Reduce (%) regulatory issues.

Additional Considerations

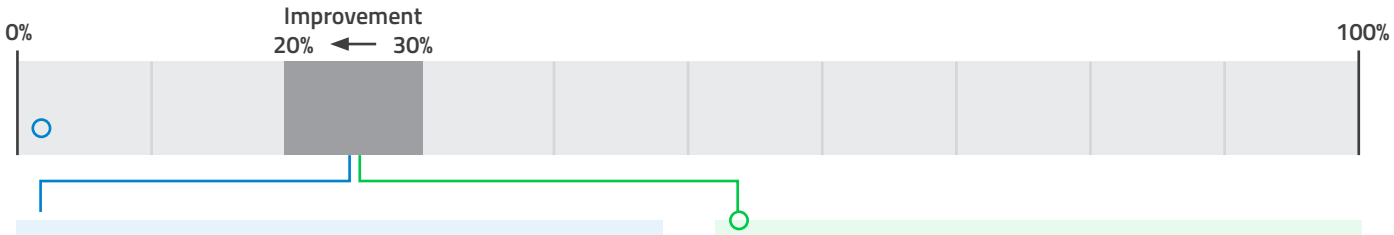
- This metric is typically tracked separately for high, medium and low severity vulnerabilities.
- This metric is similar to MTTP but should also include vulnerabilities that are resolved by means other than a patch such as access/trust issues and misconfigurations (weak encryption, insecure services, TLS/SSL certificate issues, cloud misconfigurations).
- For software vulnerabilities, recovery also includes system reboot and confirmation of a patch being properly applied. It may include testing.
- If possible, continuously calculate the value of this metric and track how it changes over time.
- Exclude vulnerabilities that are automatically remediated and closed (this is likely more common for cloud assets).

Cyber Risk Quantification

In many respects, the ability to confidently measure cyber risk in dollars, or other local currencies, is the ultimate achievement in cybersecurity posture metrics. Calculating risk in dollars allows CISOs to discuss risk with the C-suite, board, cyber insurance providers and other stakeholders in a common language: the language of money.

8. Breach Likelihood

METRIC: Likelihood (%) of a breach



Security Outcomes

- Reduce the frequency of breaches.

Business Outcomes

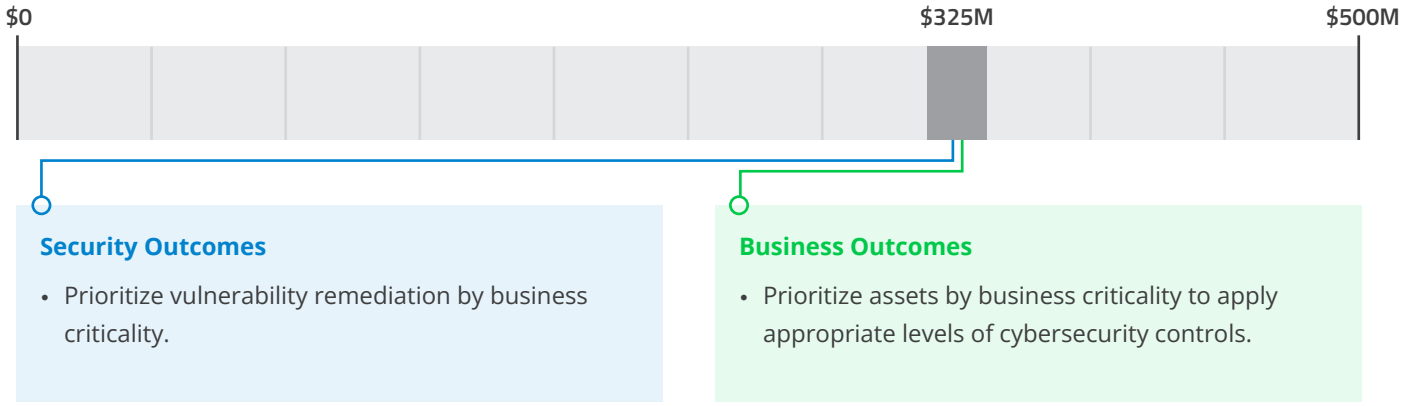
- Improve trust by customers, employees, suppliers, community, shareholders and other key stakeholders.

Additional Considerations

- Complex data requirements underpin this metric. It requires a detailed inventory of an organization's assets and those assets' vulnerabilities. Consideration should be given to the severity and threat level of each vulnerability as well as the exposure and security controls of the underlying asset.

9. Breach Impact

METRIC: Breach impact ($)

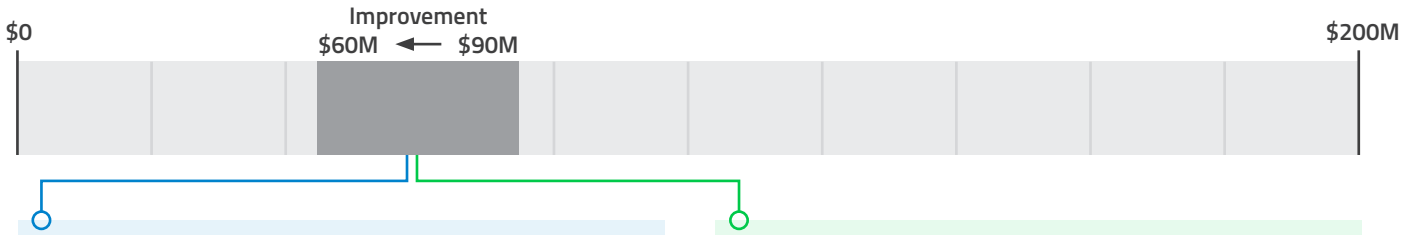


Additional Considerations

- The calculation of breach risk can be informed by the CISO's own knowledge of their organization as well as publicly documented data from past breaches.
- Both the primary and secondary costs of a breach need to be considered when estimating breach impact. Primary costs include the effort to detect, investigate and recover from a breach. Secondary costs include lost business costs, regulatory fines and breach notifications.

10. Breach Risk

METRIC: Breach risk ($)



Security Outcomes

- Upgrade to risk-based vulnerability management based on business context (not just vulnerability severity and threat level)
- Calculate breach risk by asset, asset type, site (cloud vendor/site, data center) and more.
- Calculate the ROI of security investments and gain the ability to justify current and future investments.

Business Outcomes

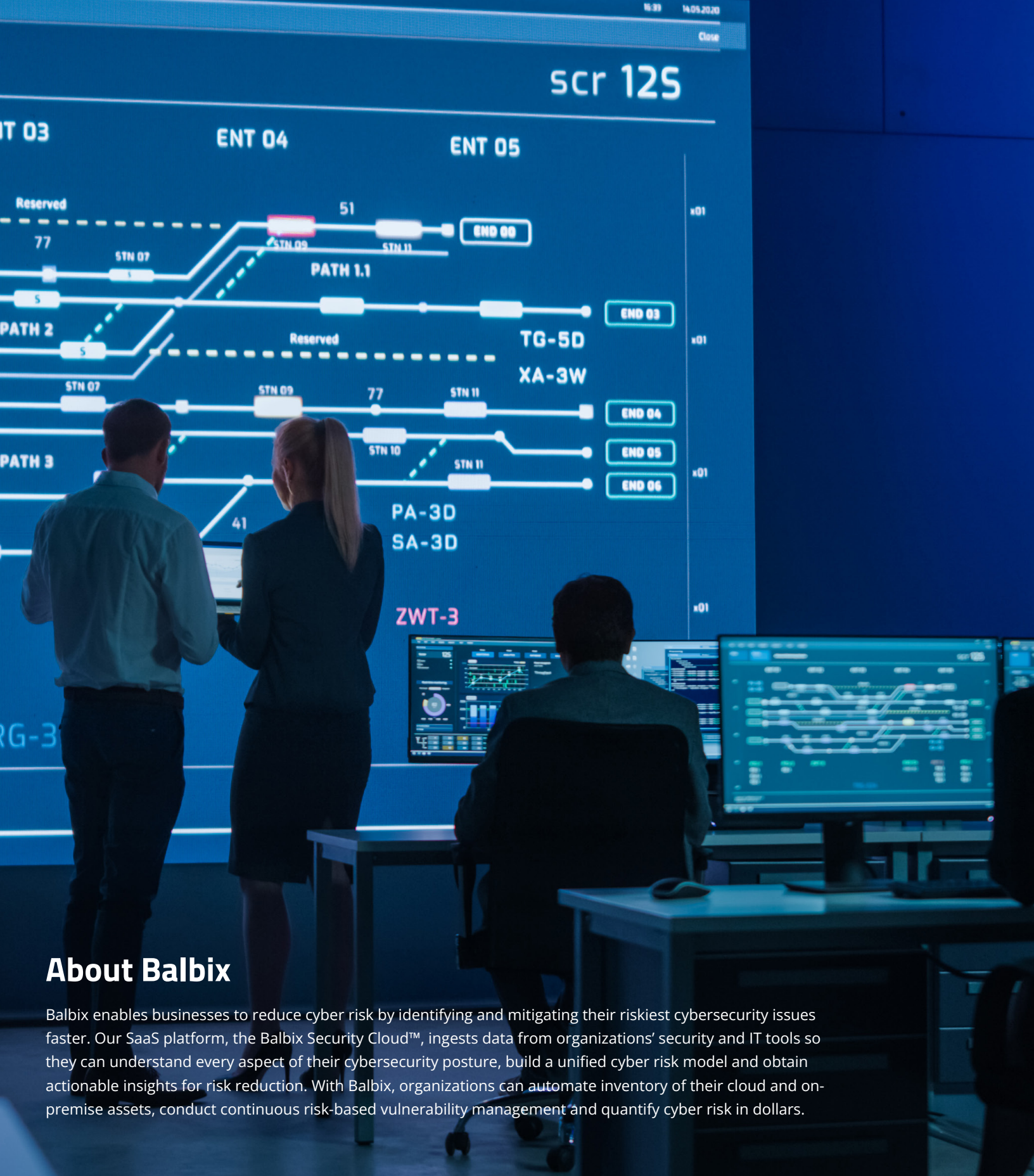
- Reduce breach risk.
- Gain the ability to communicate breach risk to the C-suite, board and other stakeholders.
- Calculate breach risk by business unit (line of business, geography, etc.).
- Reduce ($) cyber security insurance costs.
- Improve regulatory compliance. For example, gain the ability to comply with the proposed SEC rule requiring companies to report on the impact of an incident within 4 days.
- Compare residual risk to acceptable risk.

Additional Considerations

- Breach risk can be calculated by multiplying the likelihood of a breach (%) by the impact of a breach ($). For example an organization with a breach likelihood of 70% and potential breach impact of $100 million has a breach risk of $70 million.
- CISOs should consider developing the ability to report on all of the following in dollars to guide business decision-making: inherent risk, mitigated risk (due to investments in controls and security programs), accepted risk (due to risk acceptances and SLA policies agreed with the business stakeholders) and residual risk which would need to be addressed by cyber insurance or other means. These risk levels can then be compared with acceptable levels of risk from business and financial standpoints.
- CISOs may need to gather supplementary data to harness some of the business outcomes from being able to calculate breach risk in dollars. For example, to compare their residual risk to their acceptable risk, they may need to work with their CFO and CEO to determine what risk is acceptable.

Automate to Implement

As stated at the outset, metrics and modern cybersecurity are intrinsically linked. The 10 key metrics discussed in this paper will allow CISOs to determine priorities, inform decisions, support investments, track progress and maintain accountability related to their cybersecurity posture. To realize these outcomes, CISOs need to put these metrics into practice. This isn't trivial. These metrics often require gathering and analyzing large amounts of data on a continuous basis. Fortunately, advances in technology now allow CISOs to ingest and analyze the required data and automate the calculation of these metrics. CISOs can then easily integrate them into their practice as a data-driven CISO.



About Balbix

Balbix enables businesses to reduce cyber risk by identifying and mitigating their riskiest cybersecurity issues faster. Our SaaS platform, the Balbix Security Cloud™, ingests data from organizations' security and IT tools so they can understand every aspect of their cybersecurity posture, build a unified cyber risk model and obtain actionable insights for risk reduction. With Balbix, organizations can automate inventory of their cloud and on-premise assets, conduct continuous risk-based vulnerability management and quantify cyber risk in dollars.

Balbix®