Cybersecurity Performance Management

Analysis By: Claude Mandy

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Cybersecurity performance management can be split across two, nonsequential, but connected sets of activities. These activities are designed to continually assess the current performance of the overall cybersecurity function or individual programs and dynamically plan a strategic and business-aligned approach to driving improved cybersecurity performance based on defined goals and business outcomes.

Why This Is Important

Security and risk management (SRM) leaders are under pressure to reduce cyber risk and demonstrate the value, efficiency and maturity of their cybersecurity program(s) to a range of stakeholders with differing and evolving expectations. SRM leaders need to establish a defensible, predictable and traceable process for measuring the outcome of their security program and determining dynamically a strategic and business-aligned approach based on trends, early warnings, and investment indicators.

Business Impact

Cybersecurity performance management and supporting toolsets can help organizations demonstrate a business outcome driven approach to their cybersecurity program(s) and enhance the defensibility of the cybersecurity program(s). The focus on performance fosters continuous improvement over time against agreed business outcomes. This will also result in greater business resilience — adapting rapidly to changes in the business, technology and threat environments.

Drivers

- Pressure from boards and regulators for improved, consistent, and ongoing reporting on the defensibility of the cybersecurity program.
- Demands from internal stakeholders and executives to demonstrate a return of investment and improved financial management from the cybersecurity program, including a greater focus on the cost optimization of cybersecurity programs.
- The failure of rigorous, inflexible security programs to cope with the external pressures caused by moves to remote working and possible economic downturns.
- Overreliance on negative themes (scare statistics, inflated risk exposures and impending disasters) as the basis for cybersecurity investment has weakened the impact of factual risk analysis on investment decisions.

Obstacles

- Most industry standards and frameworks for cybersecurity reflect the need for implementation of controls or capabilities with little guidance on how to address their performance and delivery.
- Cybersecurity metrics are mostly trailing indicators of operational results, which are not useful in measuring the performance of the cybersecurity function through levels of protection or reduction of cyber risk.
- The supporting toolsets are still emerging and attempting to differentiate themselves from broader integrated risk management (IRM) and IT risk management (ITRM) solutions, which focus more on risk analysis or compliance assessment.

User Recommendations

SRM leaders looking to adopt a cybersecurity performance management approach and relevant tools should evaluate both stand-alone supporting tools and capabilities within IRM solutions based on their ability to help:

- Establish an achievable, realistic vision and strategy for the security program(s) that describes the business, technology, and environmental drivers.
- Utilize a combination of assessment approaches to assess the cybersecurity program(s) and identity gaps.
- Prioritize investments by facilitating informed conversations with executives and integrating risk, value and cost optimization into business cases, funding requests, and board reporting.
- Link strategy, identified gaps, specific projects and actions to help further prioritize improvements.
- Define clear targets and desired outcomes for each prioritized area of improvement and track security and business outcomes through outcome-driven metrics with a direct line of sight to the level of protection required.

Sample Vendors

Blue Lava; SeeMetrics; TrustMAPP; RealCISO; V3 Cybersecurity

Gartner Recommended Reading

Security Strategy Planning Best Practices

Cybersecurity Maturity Assessments

Analysis By: Claude Mandy, Sam Olyaei

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

A cybersecurity maturity assessment is the evaluation of an organization's cybersecurity program, and its underlying people, processes and technologies against a defined model, with distinct levels of maturity. The maturity levels are typically determined based on guidance from industry standards and frameworks. Maturity assessments are used to guide priorities and highlight areas for improvement that may be required.

Why This Is Important

Cybersecurity leaders find it challenging to articulate the benefits of cybersecurity and maintain support for further investment. Cybersecurity maturity assessments are a common method used by CISOs to measure the capability of their cybersecurity program against a set of predefined outcomes and desired capabilities. As a result, adoption is widespread across all industries.

Business Impact

Cybersecurity maturity assessments are critical during initial cybersecurity strategy planning, helping CISOs form an understanding of how well the security organization is performing in its current state, and guiding priorities and investments to achieve the desired target state. Increased maturity is an indirect measure of the reduction of risk from immature capabilities. It can help transform the overall security function and optimize investments based on dependencies between capabilities.

Drivers

Cybersecurity maturity assessments have become an essential tool to:

- Inform the strategic planning activities in pursuit of the desired level of cybersecurity capability.

- Demonstrate the perceived effectiveness of the cybersecurity function against an industry model by providing the ability to benchmark against similar organizations and industries, and ensure that a minimum standard of care is met when compared to peers.
- Demand investment in cybersecurity and subsequently demonstrating improvements over time, as a result of the investment.
- Help reach internal consensus on actual and desired maturity levels over time as expectations on the cybersecurity program increase.

Obstacles

- Most assessments measure only the implementation of controls, with "maturity" reflecting implementation tiers, such as the Australian Cyber Security Centre's (ACSC's) Essential Eight Maturity Model or the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework (CSF). The NIST's CSF explicitly states that the implementation tiers do not necessarily represent maturity. A small subset assesses people, processes and technology capabilities to determine overall maturity.
- Most maturity assessments claim to be based on the Capability Maturity Model Integration (CMMI) method, however, there is no industry standardization on the capabilities assessed, nor are there standard algorithms for assessing the maturity levels. Hence, no meaningful comparisons can be drawn between results from different assessments.
- Maturity assessments are typically self-assessments or facilitated self-assessments performed in conjunction with recognizable consulting firms. Neither is an in-depth assessment of capabilities' effectiveness.

User Recommendations

- Assess maturity regularly to guide priorities and inform strategic plans aimed at desired levels of cybersecurity capability. Remember that the value of a maturity assessment will diminish as maturity increases.
- Select a maturity assessment that evaluates the broader security function and not only the implementation of controls.
- Avoid using a maturity assessment in isolation. Maturity neither translates directly into reduction of specific risks or increased value nor does it replace an audit.
- Validate the outputs with an outcome-driven assurance program, and supplement with an assessment of external threats, value of the information assets being protected, business objectives, vulnerabilities, risk appetite and risk profile to translate maturity into an understanding of risk.
- Interpret the source of the assessment correctly to avoid creating a false sense of security based on a self-assessed maturity score.

Sample Vendors

Accenture; Blue Lava; Deloitte; EY; KPMG; PwC; TrustMAPP; V3 Cybersecurity; RealCISO

Gartner Recommended Reading

IT Score for Security and Risk Management

Frequently Asked Questions on the IT Score for Security and Risk Management