CMMI® Institute
AN ISACA ENTERPRISE

## Uniting the Enterprise Behind a Single View of Cybersecurity

A unified view of cybersecurity shared by an enterprise's key stakeholders is paramount to the success of cybersecurity strategy. Ironically, though, even as the need for that united view grows with the size of the enterprise, the challenge of achieving it becomes harder and harder as departments and business units multiply.

Still, the critical task of building cyber-resilience requires just such a shared view among many different constituencies spanning the entire organization, from the board and C-suite to the CISO, IT security specialists, risk managers and non-technical employees.

For a cyber-resilience strategy to be successful, it is vital that those people all share the same, accurate understanding of the company's risks, cybersecurity capabilities, and priorities. Each constituency will use that information in different ways, depending on its role. But a single view of cybersecurity unites the enterprise behind a common goal: Everyone can focus their resources on mitigating the biggest enterprise risks.

In practice, many organizations find it extraordinarily difficult to achieve a single, objective view of their cybersecurity risks and capabilities. As mentioned, sheer complexity is a factor: It is hard to get an overall picture of cybersecurity across dispersed business units with differing needs and IT approaches. But an even bigger and more widespread problem lies in the way that cybersecurity information is gathered and managed, which makes it extremely tough to support the diverse information needs of different constituencies.

### Drowning in a Sea of Spreadsheets

Typically, IT and risk management teams assess and track cybersecurity using some variant of a home-brewed approach that involves recording information in spreadsheets or other individual documents. Many spreadsheets are usually needed to track the numerous security programs and their alignment to different regulations and frameworks. As cybersecurity complexity grows over time, so does the number of tracking documents—until eventually, IT is drowning in a vast sea of spreadsheets. It becomes extremely arduous to update and maintain consistency across these spreadsheets, let alone to get a coherent view across all cybersecurity-related initiatives.

This presents problems not only for the IT groups who have to maintain the spreadsheets, but for everyone else who needs access to cybersecurity information. Board members, for example, need jargon-free answers to key questions: What are our biggest risks? Where are we exposed? Are we compliant with regulations? Are we closing our security gaps?

These questions generate a continuous stream of one-off information requests to IT and risk management professionals. Imagine a company is entering a new market, and its board wants to know how close the enterprise is to complying with that market's unique regulatory and security framework requirements. Answering that question can be a difficult and time-consuming job. To respond to each request, specialists must dive into the sea of spreadsheets to find relevant details and combine them to provide answers, which then must be translated into non-technical language for non-technical board members.

The sea of spreadsheets also creates problems for the CISO, who needs a rock-solid source of accurate, objective information so that he or she can understand the organization's true security capabilities and present it to the board with absolute confidence in its accuracy. CISOs often have great difficulty gaining the visibility they need to understand whether IT groups are really doing what they should be doing. The team building the applications for the company's new target market may *believe* that its approach offers adequate security—but the CISO needs objective evidence that the team is using best security practices, and that it is focusing on the biggest risks to the organization as opposed to responding to the latest threats to make headlines.

In addition, home-brewed spreadsheets naturally tend to reflect their creators' views and biases. This can present issues for IT auditors and other risk management professionals whose role requires them to maintain a level of skepticism, and to seek data that accurately reflects reality.

**An Enterprise-wide Platform Solves the Problem**

It is clear that there is an urgent need for a way to objectively assess an organization's security capabilities and understand how effectively they mitigate its biggest risks—and to make the information easily accessible to all levels of the organization, including the board.

The CMMI Cybermaturity Platform was designed to meet this need. It provides a single platform for assessing an organization's risks and building its cybersecurity capabilities, based on known best practices. It delivers practical methods for determining the organization's risk tolerances and objectively measuring the organization's capability to mitigate its most important risks. By identifying the organizations residual risk - the gaps between the organization's current capabilities and the level required to match the risks—the CMMI Cybermaturity Platform generates a roadmap for driving investment to the most critical risk areas.

Most importantly, it creates that unified view at a level that doesn't inhibit individual business units' and departments' ability to execute based on their individual needs and the technology available to them.

Further, the platform benefits each of the constituencies involved in building and assessing cyber-resilience. The board gains better, faster insights into the state of the organization's security; the platform can quickly create board-ready visual reports featuring business-focused language to help explain the status, goals and evidence-based investment decisions of cyber programs. The platform also automatically shows how the organization's capabilities align with common security frameworks. CISOs get objective evidence showing the true state of security capabilities and practices throughout the organization. Auditors have a source of objective, consistent information that they can use to really understand and assess risk. And IT teams can finally escape from the morass of spreadsheets; instead of spending countless hours hunting through documents to respond to information requests, they can spend more time on productive work that actually improves the organization's security.

To successfully build cyber-resilience, organizations need a unified, consistent and accurate view of cybersecurity risks and capabilities. The CMMI Cybermaturity platform uniquely provides that view. It supports the needs of everyone involved in cybersecurity—from the board to the CISO, IT teams and risk managers. This single view of cybersecurity unites the enterprise behind a common goal: focusing cybersecurity resources on the biggest enterprise risks.