Keys to Effective Risk Reduction

How an assessment is a good first step on the path to improving the way your organization manages cyber security risks

Declaring victory in the quest to secure your enterprise may sound satisfying today, but it could look premature tomorrow.

Maybe that's why 87 percent of board directors and C-level execs said in a recent EY Global Information Security Survey that they lack confidence in their organization's level of cybersecurity. They know that something can go wrong. A formal risk reduction program can help instill confidence. Unfortunately, determining at a detailed, practical level what's at risk and how to protect it is not a simple task.

Given the enormous variety of potential attacks and the distributed nature of data targets – ranging from mainframes to the cloud to smartphones — simply defining exactly what safety means is a huge challenge, and so is achieving it cost-effectively.

Today, many of the cybersecurity concerns of senior management can be summed up with two central questions: "Are we compliant?" for regulated industries, and "Are we secure?" for all the rest. Yet these questions overlook important issues that affect not only a company's security posture, but its bottom line as well.

Compliance-driven security measures only provide a minimum set of defenses, often ignoring specific risks that organizations might encounter due to their market segment, geographic location, risk tolerance, and other such factors. Furthermore, established industry standards don't take into account the newest challenges of today's rapidly evolving threat environment. Finally, these standards are highly compartmentalized, and likely don't serve all of an organization's needs.

The "Are we secure?" approach is broader, but it focuses too much on coverage, while leaving out the crucial factors of efficiency and cost-effectiveness. These two factors are extremely important in an era where threats are increasing while budgets aren't. Any risk reduction plan that doesn't take them into account will jeopardize a central mission of all organizations: cost control.

A Holistic Approach to Risk Reduction

The ultimate goal of every risk reduction initiative must be to reduce the most risk in the most efficient, cost-effective manner. This demands a comprehensive vision that enables leaders to view all the threats and targets in the context of a cohesive strategy.

The newly introduced CMMI Cybermaturity Platform gives organizations this vision. It allows them to meet the challenge of cost-effective risk reduction, and ensure that threat prevention, detection and mitigation serve business goals. The assessment also provides a common language for all cybersecurity stakeholders, so they can have a productive risk reduction dialog based on a clear understanding of the issues.

A CMMI assessment takes a holistic approach that measures the four key components of cyber security: risk, capability, maturity and resilience.

- **Risk areas** are evaluated by estimating the likelihood of an attack and quantifying the possible damage should an attack be successful.

- **Capability areas** define the tasks that people, processes and technology must execute in order to support cybersecurity goals. Access control management, employee training and incident analysis are examples.

- **Maturity levels** define the levels of skill and sophistication that organizations can achieve in any given capability area.

- **Resilience** refers to an organization's ability to deliver security in the face of adversity, such as employee attrition, reductions in budget, or emergency situations.

The program systematically identifies and prioritizes risk areas, and then establishes maturity targets for each capability related to those various risk areas. There are five maturity levels, ranging from unpredictable and reactive, where work gets done but is often late and/or over budget (level 1) to stable and flexible, where organizations are proactive and guided by quantitative, enterprise-wide standards (level 5).

The CMMI Cybersecurity Program enables organizations to achieve risk reduction more cost-effectively, by matching the allocation of resources to the level of risk so that scarce budget dollars and technician hours aren't wasted. It details actual measured maturity vs. target maturity in every risk area. It allows companies to compare their maturity levels to those of other companies in their sector. Finally, its comprehensive architecture supports all the major industry-specific standards, including ISO, NIST, (ISC)2, the U.S. Department of Homeland Security, COBIT5 and CIS Critical Security Controls.

Ultimately, cybersecurity must serve the business needs of an organization. This is difficult to achieve when senior management and those charged with security don't have a clear, comprehensive view of the problem and a framework that promotes mutual understanding and trust. The CMMI Cybersecurity Program

provides that framework, and enables companies to plan an informed risk reduction strategy that will lead to a secure, resilient future.

Cybermaturity.cmmiinstitute.com