RBCS
Ray Bernard
Consulting Services

Advancing the Mission of Security:

Reduce security risks to acceptable levels,
at an acceptable cost.

Rate Your Security Program

Security Program Manageability

Businesses objectives change. Personnel change. Economics change. Threats change. *Thus security risks change.* This is why an organization's risk profile either improves by plan and action or backslides by neglect or lack of initiative. Even a static security program drifts away from business relevance, either slowly or quickly, depending upon the rate of business and changes to the threats facing the business.

This is why the managing of a security program must include periodic assessments of the effectiveness and relevance of the security program elements.

But there are other reasons why the effectiveness of security programs decreases over time. Results don't remain consistent and sometimes are not acceptable. As it turns out, there are specific factors that determine how easy or hard it is to maintain intended results and performance.

Maturity Models: The Key to Improving Manageability

Just over 20 years ago the U.S. Department of Defense approached Carnegie Mellon University to help solve the key problem of its massive industrial software development programs: the lack of consistent and acceptable results across the spectrum of companies who—at one time or another—were high performers. **A key insight was that in addition to having capable people** and **technologies**, ***organizational capabilities were needed that had not been defined or given adequate attention***. A *capability maturity model*[1] for software development organizations was created that would enable any organization to be brought forward from its current situation to one of stable and improving success.

Since that time the basic principles of the *capability maturity model* developed by Carnegie Mellon have been applied by many organizations to create many dozens of successful maturity models[2], which enable business functional areas to sustainably deliver excellent results while incrementally improving.

The simple chart below can be applied to all aspects of security, from high level security strategy and planning to daily security operations and incident response. No full security program is entirely at one place on the chart. For example, some aspect of your security program may be "repeatable - intuitive but not documented" while other aspects are "documented".

[1] Capability Maturity Model® and CMM® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

[2] For a list of 34 maturity models, along with an entertaining overview, see: http://tinyurl.com/sticky-minds-maturity-models; for over 200 charts on a wide variety of maturity models, see: http://bit.ly/maturity-model-images.

Rate Your Security Program

The chart below summarizes the basic maturity levels as they apply to a security department or functional area. Without drilling down any deeper into the other aspects of a maturity model, the concepts in chart provide useful perspectives from which to rate a security program overall as well as the individual elements in it, and to identify ways in which valuable improvements can be made.

More about the Chart

The chart does not address the risk-orientation or business alignment of your security program. It looks only at the status of processes and organizational effectiveness.

Without a good handle on security processes, security technology by itself is unlikely to be as effectively as it could be for you.

The experience and training of your work force is not always enough. Working harder is not the answer. A well-defined process can provide the means to work smarter. It also shifts the blame for “problems” from people to the process. As processes improve, problems become fewer and effectiveness becomes greater.

Clearly defined and documented processes also make it much easier to evolve your security program to be more aligned with the business, to take advantage of new technology capabilities, and to adjust for changes in the risk picture.

This chart is not in any way the ultimate security program maturity tool—it is simply a high-level way of looking at the manageability and improvability of security management and operations functions.

Table 1. A High-Level Security Maturity Model Characterization[3]

Level	Characterization	Description	Results and Objectives
Level 0	**No security program**	• Security is given little to no attention. • Security measures implemented reactively after incidents occur	The occurrence of incidents **invariably leads to the maximum business impact** that could be expected.
Level 1	**Ad Hoc**	• Processes are ad hoc and disorganized, and the organization or department does not provide a stable environment. • Success depends on the competence and efforts of the people in the organization, and not on the use of proven processes. • Technology is not always used effectively or correctly. • In spite of this ad hoc, chaotic environment, organizations at this level often produce products and services that work; however, aspects of operations and projects frequently exceed the resource budgets and schedules planned for them. • Success depends upon having high quality people. • The talents and capabilities of people are generally not	The occurrence of incidents **often results in the maximum business impact** that could be expected. *The results of the improvement efforts are unstable and hard to sustain.* Thus security ROI is low because the levels of effort and cost are higher than anticipated, and results are less than hoped for.

[3] This chart is based upon the original Capability Maturity Model work by Carnegie Melon University, and the initial maturity model work of Vicente Aceituno, who is the principal author of the Information Security Management Maturity Model (ISM^3), version 2.7 of which (121 pages) was released in 2011 by the Open Group and is available for complimentary download here (registration required).

		well-utilized, while at the same time people tend to be stressed or burned out.	
Level 2	**Intuitive But Not Documented, *Also known as* Repeatable**	• Security is acknowledged as an important aspect of the business. The level of incident impacts is a combination of good fortune, individual efforts, and organized operations. • Expectations, incidents, and assets are sometimes evaluated. • Processes follow a regular pattern. • Reactive security measures are taken until the security budget is exhausted. • The environment is generally stable. The procedures and practices of the processes can drift somewhat what is intended, but are corrected once the results are noticeably less than needed. • Technology is not used as effectively as it could be. • The minimum process discipline is in place. Process discipline helps ensure that existing practices are retained during times of stress. • Basic processes are established to track cost, schedule, and some performance aspects of operations. • The talents, capabilities and insights of people are often shared and have a positive impact on operations. • However, the results of improvement efforts fade with time, due to personnel changes, business changes, and human nature.	The occurrence of incidents **usually doesn't lead to the maximum impact** that could be expected. The results of improvement efforts drift from the intended levels of performance and effectiveness over time. Thus security ROI is deceptive and in the long term turns out to be less than expected.
Level 3	**Documented**	• Security is acknowledged as an important aspect of the business. The absence of significant incident impacts is the result of organized operations. • Expectations, incidents, and assets are usually evaluated. • Security policies and procedures exist. • Some best practices are in use. • Processes are documented and communicated. • Security responsibilities are clearly defined. • The organization's or department's set of standard processes are established and improved at intervals over time. • Standard processes are used to establish consistency across the organization. • Technology is generally used effectively as part of well-defined processes. • The security's management establishes process objectives and ensures that these objectives are appropriately	The occurrence of incidents **normally doesn't lead to the maximum business impact** that could be expected. The results of improvement efforts are as intended and permanent. Security ROI is as expected.

		addressed. • An effective security management system is implemented as part of a well-documented security program. • A baseline security program is established based upon commonly accepted security practices. • Key security measures are audited.	
Level 4	**Controlled**	• Security is acknowledged as an important aspect of the business. The absence of incidents is the result of continuous organizational efforts. • Expectations, incidents and assets and risks are evaluated qualitatively on a systematic basis. • Security planning ensures that the best security measures are taken considering the budget. • Processes are not only documented and communicated, they are monitored and measured. • Security responsibilities are clearly defined and are up to date with security requirements. • A business continuity plan is in place that considers the organization's current status, and is properly implemented. • Security standards are developed for the various security domains, to establish a minimum level of effectiveness and quality for security operations and actions. • A risk-based security management system is established and operating. • Using precise measurements, management can effectively control the quality and effectiveness of operations. • In particular, management can identify ways to adjust and adapt the processes without measurable losses of quality or effectiveness. • Organizations at this level set quantitative quality goals for security operations and event response. • Sub-processes are selected that significantly contribute to overall process performance. • These selected sub-processes are controlled using statistical and other quantitative techniques. • Best practices are generally followed. • The results of the department or function's efforts are permanent.	The occurrence of incidents **virtually never leads to the maximum potential business impact;** many incident impacts are negligible due to effective security measures, but not all incident impacts are acceptable. Improvement efforts are ongoing, and their results are as intended and are permanent. The breadth of security ROI increases over time. Security is appropriate for the business sector of the organization.
Level 5	**Continuously Improving**	• Security is well known to be an important aspect of the business. The absence of incident impacts is the result of systematic efforts to continually improve process performance through incremental and innovative	The occurrence of all but catastrophic incidents results in negligible business impacts. Security improvements are

		improvements. • All of the Level 4 elements remain in place and are enhanced by Level 5 improvements. • Security standards are developed for the various security domains, to establish a minimum level of effectiveness and quality for security operations and actions. • Security measures are audited against objectives. • Quantitative process-improvement objectives for the organization or department are established, continually revised to reflect changing objectives, and used as criteria in managing process improvement. • The budget is developed consistent with security objective and strategies. • Best practices appropriate to the business sector and to the specific organization are applied in the physical, IT and corporate security domains. • A validated “Business Continuity and Disaster Recovery plan” exists. This plan considers the organization’s evolution, is properly implemented, and is kept current. • Third party agreements define mutual security commitments at the organization’s borders with others. • Quantitative information is collected about incidents or close calls. • Security measures are selected using objective criteria. • The effects of deployed process improvements are measured and evaluated against the process-improvement objectives. • Optimizing processes that are nimble, adaptable and innovative depends upon alignment with the business values and objectives of the organization. • The organization’s or department’s ability to rapidly respond to changes and opportunities is enhanced by finding ways to accelerate and share learning. • A business continuity plan is in place that considers the organization’s evolution, and is properly implemented. • The results of the organization efforts are permanent and are kept well-aligned with the business.	continuous and are easily sustained. Security operations become more efficient over time, providing an increasing return for the ongoing security investment. Security is well-aligned with the business.