

Ways to Determine or Prioritize Security Initiatives

By Matt Ege – ISSA member, South Texas, USA chapter

How do you as an information-security professional determine what security initiatives to work on each day? Prioritization efforts should include leveraging existing projects or activities that are already performed within the environment.

How do you as an information security professional determine what security initiatives to work on each day? Are mandates given by your company, department, boss, coworkers, regulators, monitoring systems, or industry groups? How does your company determine which initiatives to work on? Is there a process to prioritize initiatives? If so, is this process based on value, risk, or necessity?

In consulting with approximately 300 companies, large and small, I have seen a common theme: most companies struggle with trying to secure too many things. Often many security activities and responsibilities originate from an initiative undertaken several years prior. Are these activities still relevant today? Are they the best use of an individual's time or company resources? Similarly, many security projects are funded, initiated, and commenced with limited consideration of how they fit into the enterprise's goals, ultimately at the expense of other initiatives.

In addition to the sometimes inopportune process of initiating security projects, in general there are too many initiatives to undertake. It is impossible to get everyone within an organization always to agree on which projects to fund. How are information-security initiatives to be prioritized? Prioritization efforts should include leveraging existing projects or activities that are already performed within the environment, providing some insight into the priorities of the business as well as the effectiveness and relevance of existing processes. The following may be leveraged to prioritize information-security initiatives:

- Business initiatives
- Risk assessments
- Business impact analysis
- Penetration/vulnerability testing

- Incident response

Projects related to the aforementioned topics are a normal part of an organization's business and occur on a regular basis. Following is a short description of each, thoughts on how each could be used to prioritize information security initiatives, and items to consider when leveraging each for prioritization purposes. These descriptions are not meant to be all-encompassing; rather, they are meant to illustrate ways in which each item might be used to prioritize information security initiatives.

Alignment with business initiatives

We begin with an often preached, but rarely executed activity when developing security strategy: aligning security with business initiatives. Most organizations have business goals. Often these goals are set yearly by company leadership. A simple approach to prioritizing security initiatives is to align security to the business goals. This alignment often takes place directly at the business-initiative level, but may also occur at the IT-initiative level. In doing the latter, it is paramount that the IT initiatives map to the business initiatives. This exercise results in leveraging initiatives that the leaders of the organization have formally blessed as being important, and thus, supporting funding requests is often a much less arduous process.

Considerations

If no business or IT initiatives are defined, this becomes a tougher task. Additionally, often the security function is not privy to specific business and/or IT initiatives. Finally, if security initiatives are tacked onto business or IT initiatives after budgets have been set, many times there is no room for the inclusion of security. If business or IT initiatives are un-

known, a security professional should reach out to business-unit coworkers and ask them on what they have been asked to focus. This proactive questioning creates a wonderful opportunity to prove one's business acumen.

Risk assessments

Risk assessments come in many forms, but in general they measure risk and determine corresponding actions. Risk assessments may fall into three categories:

- Enterprise risk assessments
 - Conducted enterprise-wide
 - Include executive management and critical business units
 - Consider entity-level perspective on risks
 - Executed on a regularly scheduled basis (e.g., once or twice a year) or on an enterprise-event trigger (e.g., merger/acquisition, executive turnover, etc.)
- Focused risk assessments
 - Focused on a particular area of the business (e.g., IT, finance, sales, etc.)
 - Consider business-level perspective on risks
 - Executed on a regularly scheduled basis (e.g., once or twice a year) or on a business-event trigger (e.g., new regulation, outsourcing decision, etc.)
- Embedded risk assessments
 - Embedded within core processes such as
 - Software development life cycle
 - Change control
 - Strategic planning
 - Project management
 - Address risks which fester between executions of enterprise and focused risk assessments
 - Triggered by events within specific processes (e.g., delay in project, emergency change, etc.)
 - Often part of control framework (e.g., COBIT, ISO, etc.)

It is important to include a wide range of individuals within the team performing risk assessments. For example, the most successful teams executing risk assessments often include representatives from internal audit, risk management, and internal control, as well as business and technical subject matter experts. Additionally, it is critical to measure both inherent risk and residual risk, as this provides insight into which control or controls are most important (i.e., which controls mitigate the most risk). Accordingly, the results of risk assessments will provide insight into areas that are most risky and controls that are of highest importance.

Considerations

Risk assessments fall on a continuum with quantitative on one end and qualitative on the other end. This is a delicate

A balanced approach that includes a solid quantitative core along with a qualitative review provides most relevant results.

balance, as being too qualitative can result in human judgment weighting risks based upon preconceived conditions or preference. Being too quantitative can produce results that are not in line with the ever changing risk environment. It is difficult to anticipate all scenarios that would need to be considered for a purely quantitative risk assessment. If we could quantify all risk attributes correctly, then business decisions would be made solely by machines. Often, there is limited information to determine impact and likelihood for specific risks. To overcome these issues, a balanced approach that includes a solid quantitative core along with a qualitative review provides most relevant results.

Business impact analysis

A properly performed business impact analysis identifies and prioritizes business processes and the supporting sub-processes, people, technologies, facilities, and third parties. The execution of a business impact analysis provides an opportunity to align security initiatives with the most important elements that fundamentally drive business. A business impact analysis often reveals dependencies that were unknown, which is why it should be a precursor to a comprehensive business continuity and disaster recovery plan.

Considerations

Inherently a business impact analysis is a current-state exercise. In other words, it may not consider projects that are currently underway or are soon to start. These projects ought to be considered in prioritizing information security resources. Therefore, when leveraging a business impact analysis to prioritize information security initiatives, a security professional should reach out to the project management group in order to determine what current projects are underway. Then, additional research may be warranted to determine the impact of those relevant projects.

Penetration/vulnerability testing

Penetration and vulnerability testing comes in many different forms. In the purest sense, a vulnerability test identifies vulnerabilities within a target or set of targets. However, it does not involve the active exploitation of these vulnerabilities. A penetration test takes the vulnerability test the next step by performing exploitation. A penetration test may simulate a specific attack scenario. It is key for any vulnerability or penetration tester to vet results such that false positives are removed and to map technical vulnerabilities to root causes. A vulnerability or penetration test can provide a detailed, technical view into areas in need of improvement and can easily provide support for information security initiatives.

Considerations

Results of vulnerability and penetration tests often note technical vulnerabilities but do not speak to underlying process vulnerabilities. Therefore, it is important to discuss results with management and to ask questions to uncover root causes (often within the process level).

Additionally, testers may focus on low-hanging fruit and not identify more complicated or undocumented vulnerabilities. Therefore, it is key to understand the scope and approach of the test prior to commencing the effort.

Incident response

Any incident that occurs in the environment can and should be utilized as a lesson in how to improve the security posture. Hopefully prior to any incident occurring, a regularly tested comprehensive response plan would already be in place. With any occurrence of an incident, decisions would need to be made quickly on the appropriate course of action, and evidence most likely will need to be preserved. Once the response is complete, a “lessons learned” exercise should be conducted, ultimately leading to actions to prevent a similar incident from occurring again or to a decision to accept the risk of a subsequent occurrence. If the former is chosen, the required actions/initiatives become more of a priority.

Considerations

The main challenge in using an incident as basis for prioritizing information security initiatives is the tendency to over prioritize the initiatives, often resulting from the level of exposure of the incident across the organization. It is imperative that the cost to the organization that resulted from the incident, the risk of a subsequent event, and the cost of the solution be compared against similar factors for other risks within the environment.

Enterprise view

Up to this point, I have listed efforts that are common to many organizations. Each of these efforts can and should be leveraged to set the security docket. However, there is a need to consider each of these efforts from an enterprise view. In other words, focusing on one or all of these areas may result in inappropriately placing a priority on a specific initiative if not considering it within the context of the enterprise. An enterprise view may include business initiatives, business desires, compliance requirements, security threats, sustainability of current solutions (processes and technologies), company culture, company values, and other items.

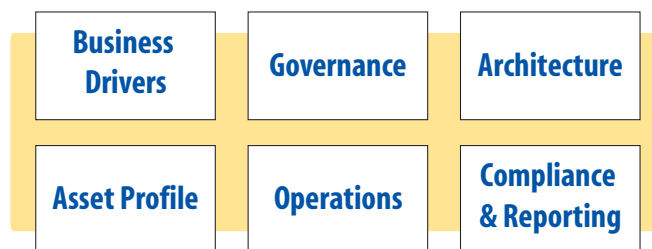
In formulating an information security plan, it would be wise to leverage a scorecard in which to process and report on initiatives, such that the resulting security agenda is sufficiently supported. The scorecard could follow a proprietary framework or a best-practice framework. Either way, the goal should be two-fold:

- Measure to make decisions

- Keep simplicity in mind

There is no reason to measure if the metrics cannot be leveraged to make decisions. The concept of meaningful metrics could be discussed and debated at length. Suffice it to say that selecting a few key metrics for each area of the scorecard helps to provide a view into what needs to be addressed and the priority of the needed efforts without inundating the scorecard with less relevant metrics. The key metrics selected will most likely change over time, as the measurement program evolves and improves.

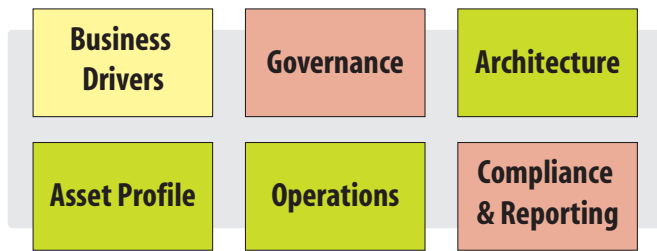
An example of a framework is illustrated below:



Each of the areas within this framework should have a few key metrics that would help shape the information security agenda. Examples of such metrics might include:

- **Business drivers**
 - Average SPAM in mailbox
 - Security bugs in production version of product
- **Governance**
 - Number of automated versus manual controls
 - Critical residual risk items identified within risk assessments
- **Architecture**
 - Downtime
- **Asset profile**
 - Number of critical vulnerabilities present
- **Operations**
 - Time without incident
 - Average time for access removal
- **Compliance and reporting**
 - Number of deficiencies (SOX)

Again, these metrics need to be carefully selected based upon the current environment, and they may change over time. The results of audits within the environment can then be funneled through this framework and put into perspective of the overall environment. In this way, the effectiveness of current processes and technologies (i.e., current initiatives/operations) can be measured in addition to risk, in order to provide further information for the prioritization of information security efforts. As a simple example, the above graphic could be color-coded based upon the current state of the union, similar to the following:



If a best-practice framework such as ISO 27002 were to be used, the scorecard summary may look like chart 1.



Chart 1 – ISO 27002 framework

These illustrations are simply summary heat maps. Obviously, the colors need to have meaning, and various levels of reporting would be required (e.g. executive summaries, aggregated findings, detailed analysis, etc.), as reporting will need to be specifically tailored to the organization’s needs.

Conclusion

Is there reason behind the information security initiatives within your company or is information security a reactive afterthought?

As information security professionals, we should all strive to demonstrate value to our organization. By measuring the effectiveness of information security initiatives, our current and future efforts can become more valuable to the organization and prioritized in a logical, risk-based manner. Additionally, for those organizations where information security is “out of the loop” with regards to management initiatives, we can demonstrate the risks and rewards to the business, allowing for information security to be included (and possibly required) in future business decisions. If we all began to do this, perhaps the world’s information would become more secure, and organizations would realize the value of information security.

About the Author

Matt Ege, CISSP, CISA, CPA (TX), a director of strategic services at Fishnet Security, advises clients and the industry on various disciplines of information security. Prior to his role at FishNet Security, Matt spent six years within two of the Big Four firms, delivering services related to IT security, business process and controls analysis, governance, IT audit, risk assessments, SAS 70, business continuity, and disaster recovery. He is a frequent speaker at conferences and universities and can be reached at matthew.ege@fishnet-security.com.

