



Look Before You Leap Into a Security Program

By Mark E. Egan
Partner StrataFusion Group

Introduction

A question commonly asked by security executives is how to get started with an Information Security Program. This interest may have been prompted by a recent security-related event inside an organization that needs to be addressed, or heightened awareness around security in general, and a desire to be more proactive in this area.

The first step is to establish a baseline assessment of where you are today. This includes taking a critical view of your existing information security program to assist you with developing a plan to move you towards an optimal program in the future. You must complete a thorough review of your current state before you begin to put an improvement plan in place.

This article is the first of a four part series that highlights the steps involved when developing an Information Security Program for your enterprise. In this article, we will focus on establishing your baseline, or "as is" environment. The subsequent articles go on to address the key components of implementing your future Information Security Program—People, Policies & Procedures, and Technology.

Establishing Information Security Baseline

Follow these steps when establishing the baseline of your existing computing environment:

1. **Inventory your assets** – Take an inventory of all the assets within your organization that you need to protect. This would include computers, servers, networks, etc., and where they are located. Then, classify these assets into categories such as mission critical, critical, and standard, based upon the impact to the business if these assets would not be available.
2. **Assess assets for vulnerabilities** - The next step would be to evaluate your assets for known vulnerabilities. Vulnerability management tools can be used to automate this process and produce reports that identify potential vulnerabilities for your assets.

3. **Assess risks and develop remediation plan** – Prioritize your vulnerabilities in terms of business impact, likelihood of exploitation and regulatory requirements. The objective here is to determine which areas are important to focus on. This could be based upon risks such as loss of revenue, damage to brand and image, etc. Finally, you need to categorize vulnerabilities into groups that require attention within set periods of time -- 30, 60, 90, and 180 days -- and then develop recommendations for mitigating or eliminating risk for each vulnerability. Based upon this information you can follow up with a project plan and appropriate staffing requirements to address these vulnerabilities.

Information Security Policies & Procedures

Security policies and procedures are a key component of your Information Security Program. As a part of establishing your baseline, you need assess the coverage of the policies you currently have in place. Ask yourself the following questions:

1. Do you have written security policies today?
2. Are employees required to sign information security policy?
3. How do you handle account administration for employees, contractors, and temporary workers?
4. What is the policy for remote access?
5. Do you have formal incident response procedures?
6. Do you have a security awareness program in place for employees?
7. Do you have an acceptable use policy for Internet, email, and laptop computers?

Your answers to the above questions will indicate if you have addressed some of the relevant information security policies that should be in place today.

Information Security Organization

Having a dedicated Information Security organization in place is a necessary component of your Information Security Program. The following questions are examples that can be used to determine if you are appropriately staffed:

1. Who is currently responsible for Information Security?
2. Is he/she part of a formal Information Security organization?
3. What are the background and credentials of the staff?
4. What are the roles and responsibilities of this organization?
5. What is the reporting relationship for this organization?

This is by no means an exhaustive list of questions, but it does provide examples of what should be asked in order to assess your existing Information Security organization.

Conducting the Baseline Evaluation

The guidelines provided in this article offer a top-level view of the process that should be followed when establishing your baseline. If you have not conducted a baseline assessment in the past, you might consider bringing in a third party to assist in this

process, as they will have methodologies to support the process and can also train your staff on how to conduct future baselines.

Next Steps

The next step is to summarize the results of your baseline evaluation and develop an Information Security Roadmap. The roadmap would summarize the current state of your Information Security environment, and call out the milestones to help you accomplish your desired state. The roadmap would also include staff and budget required to reach a secure environment for your enterprise.

Upcoming articles will focus on how to develop your Information Security Roadmap and will be divided into three separate topics; People, Process & Procedures, and Technology.

About the author

Mark Egan is a partner of the StrataFusion Group, Inc. and has over 25 years of experience in information technology. Prior to joining StrataFusion, Mark was a CIO at Symantec Corporation for 6 years during the company's rapid growth from a consumer software publisher with \$600 million revenue to the market leader of security with \$5 billion revenue. During his tenure with Symantec, he led the information technology integration through 28 acquisitions, including a \$13 billion acquisition of Veritas Software that helped Symantec become the world's 4th largest software company.

Mark's expertise includes information technology strategy & planning, information security, and mergers & acquisitions. He is the author of *Executive Guide to Information Security: Threats, Challenges, and Solutions* and was a contributing author of *CIO Wisdom* and *CIO Perspectives*. Mark is also a frequent speaker on best practices for information technology and security. He currently teaches a graduate class, "Building Business Value through IT Innovation", at the Haas School of Business at UC Berkeley.