Global Information Assurance Certification Paper

Selling Security to Management in a Low-Risk Environment

Carolyn Rowland
GSEC Practical Assignment Version 1.2b
April 12, 2001

Security is difficult to sell to management in many environments, but in a low-risk environment it can be a formidable task. A low-risk environment can be any in which one of the following is true:

- The organization's product is in the public domain (i.e. freeware, government policies/standards)
- There is no perceived critical service provided to the public (i.e. no e-commerce or low-visibility e-commerce such as a small company providing on-line ordering for its customers).
- Management believes that no one would have a reason to break into the organization's network (i.e. the organization is low-visibility, small, or otherwise unknown).

Realize that low-risk does not mean that the organization has no risk, it means that management perceives a low-risk. If it is your job to sell security to management, then you will have to outline the risks associated with your organization.

If you read the bulleted statements describing low-risk environments again, you will see examples of confidentiality, availability, and integrity. These are the three elements to consider when looking at security for your organization. Confidentiality ensures that unauthorized persons do not view your data. Availability ensures that IT resources are operational. Integrity ensures that data your organization utilizes is accurate and uncorrupted. Examining how these elements affect your organization is critical when selling security principles to your management.

In order to sell security to your management, you will have to analyze your organization. Determining the level of security required for your organization will require a thorough risk analysis [2]. For your initial sell, you will want to perform an informal risk analysis in order to sell the importance of security in your organization. Start by asking, what is most important to your organization? One organization may focus on confidentiality while another is more concerned with availability. It depends on the organization's mission and nature of the business transacted [1]. An organization whose product is in the public domain may not be concerned about confidentiality. Availability may also be a hard sell if there are no critical services supported by your organization. If availability is not critical, then management may be relying on your network backups to protect the integrity of the data.

Understand that management is often mis-informed despite the risk to your organization. Often management believes that a firewall, virus protection software, and backups cover all the security bases for their organization [3]. This is where your informal risk assessment will help you to speak directly to management by focusing on areas that are directly in their field of view.

Confidentiality

In a low-risk environment in which confidentiality is not a major requirement, organizations will still have confidentiality issues. Personnel data such as social security numbers are considered sensitive information. If your organization does not make an effort to protect this data, those who are responsible (upper management most likely) could end up in a legal battle over privacy issues.

Here are some questions you can ask yourself to help determine confidentiality issues for your organization:

- Does your organization do a background check on every employee?
- Are salary records considered confidential?
- Where is this information stored?
- How is the confidentiality of this data protected?
- What about personnel actions (firing, layoffs, employee evaluations)? This data could also be considered sensitive and measures should be in place to protect it.
- Would it hurt your organization to have employee statistics such as salary, performance reviews, and social security numbers seen by unauthorized persons?

Availability

Even if your organization's mission doesn't include IT services to the public or high uptime requirements, availability can still be a major factor towards the organization's bottom line.

Here are some questions you can ask yourself to help determine availability issues for your organization:

- How productive are the employees if the network is down for an entire day?
- Does that hurt project due dates?
- How much salary money is being spent for the employees to sit idle during an outage?
- Does your organization have contingency plans to help recover availability?
- How much embarrassment is it to your organization when mail is bounced back to the originator because the mail server doesn't accept messages?
- Is your organization's credibility hurt when your e-commerce web site is down for several hours?
- Is there a big event or time of the month/year when availability would be more critical (i.e. during a company-wide audit or meetings with stock-holders)?

Integrity

Integrity seems like the most difficult to diagnose of the three elements. Without integrity it seems your organization would not survive. Integrity has the most difficult recovery requirements. To recover from a confidentiality breach, you have to deal with the unauthorized viewing of organization data. To recover from an availability breach, you have to bring services back to an operational state. To recover from an integrity breach, you have to determine the level to which the integrity of your data has been damaged.

Here are some questions you can ask yourself to help determine integrity issues for your organization:

- If your organization produces a product, whether it is a standard, a policy, a piece of software (free or not), how does it affect the organization's credibility and bottom line if the product has been altered (then released to customers)?
- Every organization exists to pursue a mission; what is your organization's mission?
- What does your organization produce?
- Would your organization lose profits if the product was released with a bug or inaccuracy due to someone altering a piece of it?
- How do you recover from an integrity breach?
- When did the breach occur? Are backups tainted as well?
- How much of your data might be corrupted?
- If your data is incorrect, how does that affect your organization's bottom line? How does this affect the organization's image (which can also affect the bottom line)?

Now that you have asked some important questions, how do you take this to management?

The Mission

Look at your organization's mission. Compare the issues pertaining to confidentiality, availability, and integrity to your mission. What is important to your organization? What will most affect the bottom line? The mission will state what the organization does and how well it does it. Each organization has different requirements for confidentiality, availability, and integrity. By looking at your mission and investigating the product produced by your organization you are building your informal risk analysis. This risk analysis will help you to guide your presentation to management towards the things they care about most: the bottom line, the organization's image, and the product created.

Let's build some examples for two generic organizations (fictitious).

Example 1: The Government Agency

This example government agency produces policies and procedures for private industry and other government agencies. Salary and much personnel data is public information due to the Freedom of Information Act (FOIA) under which anyone can request to see this information. On the other hand, social security numbers and some sensitive personnel data are not always available under FOIA. This agency might also utilize commercial company data in the development of it's policies and procedures. This company data is confidential and proprietary and the agency has a responsibility to the commercial companies to keep this information secured. Even though the final product (the policies and procedures) is public information, the handling of the data used to create the product is considered sensitive. Therefore, confidentiality is required for this data.

The mission of this agency might include the development of policies and procedures to improve some aspect of commercial and government run business. Now this agency must consider how critical the policies and procedures are to it's customers (the commercial and government organizations that receive them). If these customers depend on the information provided in the policies and procedures, then the accuracy (integrity) of the conclusions and recommendations must also be critical. Therefore, integrity is a requirement for this agency.

Availability may not be critical for this particular organization. There may be funds wasted due to much idle salary money if IT resources are unavailable, but delays in product due-dates are not as critical as they would be for most commercial organizations.

Federal agencies are also mandated by law to have security plans and a security infrastructure. Federal auditing agencies are starting to ensure that agencies are following these laws, so this may be another avenue to pursue in selling security to management in a Federal Government organization. Specifically, OMB A-130, Appendix III is widely known in Federal Government circles because it states the security requirements of IT systems in the Federal government. OMB A-130 requires a level of security appropriate for the level of risk for each organization:

Establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems. [4]

OMB A-130 and the more recent Government Information Security Reform Act (GISRA) include detailed information regarding Federal Government information security programs [5]

Example 2: The Small Company

A small company has just unveiled it's corporate web site. This company creates lesser-known widgets for an industrial or commercial process. The company's personnel data is not kept on-line (perhaps non-networked computers contain this information) because the office is small. The manufacturing process used is publicly known and competition is small. The only edge this company maintains are its marketing strategies which are ahead of the competition.

The company's mission is to be the best at creating these widgets and providing them to the industry it supports. Since the manufacturing process is known by all competitors and personnel data is not kept on-line, it appears that confidentiality is not required for this company. Wrong. The company still has a competitive advantage with its marketing strategies. If other companies are able to create the same product the same way for the same cost, and the only advantage this company maintains is its ability to market its product and be more visible to its customer, then these marketing strategies should be considered sensitive company information. The cost to the company could be immense if the competition were to capture these marketing strategies. In this company, the bottom line dictates the risk. If there is significant risk to the company's credibility (image), or the product it creates, the bottom line can be adversely affected.

Availability and integrity should not be forgotten here. This company could also be one of those whose management claims "no one would hack into our web site, we have no DOD secrets or the high visibility of Ebay or AOL." Management is misguided. Malicious hackers do not break into company networks only for glory or to acquire secret information, they do it for all kinds of reasons. Some may do it because they can, or to use a less-secure site as a hopping point to hack into other sites that have more security (using the horsepower of a victim's computer to run scripts to break into another site's computers) [6]. Believing that your company is not a target because you are not highly visible is asking for trouble.

If this company allows customers to order on-line, care must be taken that the web site is available when a customer tries to use it. Loss of availability of this service can hurt the credibility of this company. The same can be said for the integrity of the information presented on the web site or the information used to build the widget. If someone were to re calibrate the machines used to manufacture the widget, causing a minor flaw, the company could lose credibility in the market that no marketing strategy could erase.

What should you do?

First, you should understand your organization's mission. Be prepared to cite examples of security that can be implemented to address confidentiality, availability, and integrity issues that relate to your organization. You alone cannot create security in your organization, so you must sell the ideas of security to your management. To do this, speak at their level. You may have to do an informal risk analysis in order to provide the necessary information that will allow your management to connect their business with security. This risk analysis comes from the analysis of confidentiality, availability, and integrity discussed previously. Management is concerned with money, the image of the organization, and the products they produce. Be prepared to address these topics and make them part of your sell. Make sure your management understands how insecure transactions may be and how that will affect the organization's credibility or earnings.

If the cost of security is less than the cost of a security incident, this will go a long way towards selling management on the benefits of security at your organization. How do you put a value on the organization's credibility? This is the big question you must answer. The answer will be different for each organization. In order to get the attention of management, provide specific examples with best, medium, and worst case scenarios.

An example of this might include the loss of the marketing strategies for our example company. Worst case this loss might cause the company to collapse due to loss of competitive advantage. The cost to the company would be immeasurable. A best case scenario might include the loss of marketing strategies to someone who does not know what to do with the information. The company loses some money in the cleanup effort and trying to prevent another breach of confidentiality. A medium case scenario might include the exposure of marketing strategies to the competition which would require new strategies to be formed within the organization in order to regain the competitive advantage. Look at the possible costs and probability that these scenarios could happen. Compare the probability of the risk times the cost to recover from exposure to the cost to secure the resource. Is the pro-active security less or more than the recovery?

Some tools that may help you sell security to your management:

- www.sans.org, specifically: The 7 Top Management Errors that Lead to Computer Security Vulnerabilities. The SANS site can provide you with eye-opening accounts and documentation that will be useful as you try to impress upon your management that security affects every organization. [7]
- www.securityfocus.com, specifically: Internet Security and Your Business - Knowing the Risks. This site provides security news and technical information, but also has information for the beginner. [8]
- csrc.nist.gov, specifically: "Training and Education" and "Best Practices". The NIST Computer Security Resource Center [9]

Conclusion

This document should have provided you with some of the necessary information and tools to sell security to your management. Sometimes it seems that selling security to management in a low-risk environment is more difficult because management does not perceive a risk. The risks are there; your job may be to find the risks that affect your organization in order to make them known to management. Risk assessment and risk management are basic parts of any security program.

Also realize that once you have sold your management on appropriate security for your organization, your job will not be complete. Re-education is required in order to maintain the understanding of how important security is to your organization. The people in management can change over time and they focus on issues that affect them directly. Security is below their sight-lines most of the time so part of your sell may include showing them how security relates to their responsibilities. Stressing the affect that risk will have on the organization's bottom line, the organization's image, and products produced will help to impress upon management the need for an effective security program.

Once you have management's endorsement to begin a formal security program in your organization, you can use the tools and sites listed in this paper to research more information on performing a thorough risk analysis of your organization, creating security documentation such as policies and procedures, and implementing best practice. There are many more resources available on the Internet to help you build a successful security program.

My experiences with this topic include two sites whose management considered security an afterthought. Management at both sites thought that they were below the horizon for malicious attacks from the Internet and had little to fear (even if they were to suffer from an incident). In my current environment, I have used many of the principles and tools outlined in this paper to advertise and sell security principles to my management. I have an annual talk that I present to the upper management and another for the entire staff. In my talk, I outline the potential risks that our low-risk site takes by doing business with today's technology. I have found my job much easier when I have management support, and I even find that management is more in tune with security issues.

After I began my security awareness talks, I noticed that I received calls from management when they perceived a potential security problem (social engineering, viruses, denial of service). It takes more time to investigate each of these issues, but I believe that it is beneficial to my organization to have management thinking about security as part of their daily responsibilities instead of thinking that it is only my responsibility.

References

[1] Troffer, Lawrence. "Information System Security: How Much is Enough?". August 21, 2000. http://www.sans.org/infosecFAQ/policy/ISS.htm (April 14, 2001)

[2] Micksch, Allan. "Information Systems Risk Analysis, Assessment and Management". September 13, 2000. http://www.sans.org/infosecFAQ/policy/risk.htm (April 16, 2001)

[3] Marsh, Jerry. "Myths Managers Believe About Security". January 25, 2001 http://www.sans.org/infosecFAQ/start/myths.htm (April 13, 2001)

[4] "OMB Circular No. A-130 Appendix III - Security of Federal Automated Information Resources". December 12, 2000 http://www.cio.gov/docs/Recompiled_A-1301.htm (April 14, 2001)

[5] "Guidance On Implementing the Government Information Security Reform Act" Title X, subtitle G of the 2001 Defense Authorization Act (P.L.106-398) October 30, 2000. http://www.cio.gov/docs/Security_Act_Memo_and_Guidance.htm (April 16, 2001)

[6] Dion, Denis. `Script Kiddies and Packet Monkeys - The New Generation of "Hackers"` January 29, 2001. http://www.sans.org/infosecFAQ/hackers/monkeys.htm (April 16, 2001)

[7] The SANS Institute. "The 7 Top Management Errors that Lead to Computer Scissored Vulnerabilities." 1999.

http://www.sans.org/newlook/resources/errors.htm (April 15, 2001)

[8] Jenkins, Joe. "Internet Security and Your Business - Knowing the Risks" http://www.securityfocus.com/frames/?focus=basics&content=/focus/basics/articles/risks.html (April 13, 2001)

[9] Computer Security Resource Center, National Institute of Standards and Technology. http://csrc.nist.gov (April 15, 2001)