Global Information Assurance Certification Paper

Sandra Meyers
GSLC Practical Assignment, Version 1.0
November 26, 2003

Breaking Down Barriers – How to Elevate Security to a Strategic Level in the Organization

Abstract
Despite headline news articles which describe costly downtime and significant financial losses, impending regulations that threaten to dictate corporate responsibilities with regard to security, and the recognizable day-to-day nuisances that challenge productivity, most management teams still remain dispassionate and unresponsive to IT security issues. What is the primary cause for management's lack of ownership of IT security? Is this disconnect a result of management's failure to recognize the business need or impact? Have IT organizations failed to effectively communicate the magnitude of risk or liabilities? Is it an inability of IT security teams to demonstrate a positive return on investment? Are the issues difficult to understand or relate to? Is there a fallacious sense of security? Maybe the business cannot justify the investment due to its size or lack of incidents. The answer to this baffling question most likely is a combination of all of these reasons.

As security professionals, with the education and technical skills in this complex and ever-changing industry, it is our responsibility to educate, communicate, and promote the benefits of information security programs. We also must obtain executive collaboration in order to implement the necessary policies, procedures, and tools to adequately protect the organization from security-related risks. Although this task sounds simple enough, several barriers still remain in the path of our journey to gain executive level ownership for IT security decisions.

This paper will identify the inherent obstacles that stand in the way of IT security receiving the scrutiny it requires and obtaining the executive level endorsement it needs to succeed. In order for security to become a strategically aligned initiative for any organization, management must first understand the risks, recognize its relationship to the business, and embrace its role in the overall corporate responsibilities. Additionally, this paper will outline some methods for overcoming the barriers that stand in the way of obtaining management's support and ownership for IT Security initiatives.

Introduction
In 2002, The Human Firewall Council introduced an online security survey as a benchmarking tool for key security issues facing every organization. Since that date, over 1000 security managers have participated in this survey with alarming results. "The vast majority of organizations taking the survey failed to meet what may be considered minimally acceptable standards for managing security across

the enterprise. All but one category (physical security) scored an "F" or failing grade across 10 key areas of security management." [1]

It is difficult to understand how this level of ignorance can still exist in today's global business environment, where daily cyber security incidents are the norm, spam infiltrates every person's electronic inbox, and destructive viruses reek havoc on corporate networks. Why hasn't corporate management sat up and taken notice, or more specifically, taken more aggressive action to prevent these issues from occurring? The first reason is that security professionals have not done a good job of educating management about the risks and also have failed to effectively market the benefits of implementing a corporate security program. Secondly, there still are too many barriers present that perpetuate indifference about the issues and fail to demonstrate the real business issues that need to be addressed. Some of the key reasons why management fails to give priority and support to information security initiatives are listed below:

- Lack of understanding of technical concepts and terminology
- Failure to recognize the associated risks and business impacts
- Failure to identify a return on investment or expected value
- Perceived lack of power in the decision-making process
- False sense of safety
- Failure to recognize security as a strategic business issue

With these types of barriers present, it is no wonder that IT security is still a low priority on the corporate portfolio. Inadequate communication is the underlying cause of all of these barriers. Failure to clearly communicate the relationship between security and business objectives and inability to effectively "sell" the need for security to management will continue to perpetuate the situation. In order to successfully turn the situation around, security professionals need to overcome the barriers described above and change management's perception about security.

IT Security is Too Technical

Even the most business-savvy executive can get lost in the fluent stream of acronyms and technical lingo used by the traditional IT professional. Failure to simplify security issues and translate them into business terminology may not only result in a misunderstanding of the facts but can risk the potential alienation of the entire audience. This is a common mistake of not only security professionals but of IT staff in general. Caution must be used to convey complex technical issues in a format that can be easily interpreted and comprehended by the audience. Talking over the heads of the audience only serves to alienate, not impress. MetaGroup recently highlighted complex technology as a primary barrier to dealing with management.

> From the business perspective, a major barrier to dealing with security threats is in comprehending the complexity of the issue. Design

[1] The Human Firewall Council. Security Management Index.

discussions often require use of technical terminology and jargon in order to convey purpose and intent. Although this may be necessary from a technology point of view, it can lead to credibility issues when used with a business audience. [2]

Keep it Simple

Here are a few suggested techniques that can be used to simplify technology-based discussions and prevent confusion for the audience.

- Remove language barriers Any acronyms or technical terms that are used should be clearly defined for the audience. It is better to assume they do not know what the terms mean rather than running the risk of confusing the audience or creating questions later. When possible, provide a quick reference sheet or glossary of terms at the beginning of your presentation or discussion.
- Use an analogy An analogy provides a recognizable comparison of the situation to another business or personal scenario that has similar characteristics. This helps provide a visual relationship for the audience. If they can more easily relate to the other example, then they might be able to make the connection to the technical example. For example, explaining that a firewall is a security device that serves in a similar capacity as a guest list at an exclusive party, which only allows invited and documented guests to attend the party. Although simplistic, it makes the concept easier to relate to their experiences. Technical details should only be used as necessitated by the decision-making process.
- Provide diagrams and pictures – Whenever possible, use diagrams, flowcharts, and graphs to help clarify the situation. Visual representation is more powerful than spoken words or written text alone. Again, caution should be used so as not to provide a complex, hard-to-follow diagram that makes the concept more difficult to understand. For example, network diagrams may be too complex for the average audience to understand, but if a simplified diagram can be used to demonstrate network traffic patterns, it might be helpful to understand where the vulnerabilities lie.
- Seek functional assistance – It always is wise to seek feedback from a functional, more globally focused individual before presenting any communication or presentation to a less technical audience. The feedback could prevent you from making costly communication errors.

Difficulty in recognizing the business impact

Let's face it —security investments are difficult to sell. They are costly; they do not generate cash flow for the business, and are usually difficult to understand. So, it is no wonder that security professionals continually struggle to successfully pitch new security expenditures. Although this barrier appears difficult to

[2] Warrilow, p. 1.

overcome, all that is required is a new approach to marketing security initiatives. "You have to think like they think, prove it, explain the risks, benefits and payback, and explain how it benefits their business bottom-line," explains Mark Burnette of the Willis Group.[3] Since most security professionals come from technical backgrounds and usually are not trained to complete the detailed financial analysis required to build a successful business case, the prospect of selling their proposal is improbable. However, with a change in focus and a new approach to presenting these proposals, the odds of gaining funding approval are much more likely.

Get in touch with the business

Historically, IT professionals have been charged with the responsibility of understanding, implementing, and maintaining technology. Keeping up with the ever-changing face of the industry requires an intense focus on the tools, techniques, and technological advances of computer systems and their infrastructure. Understanding the business, and technology's relationship with the business has typically been a lower priority. "The security guys are often out of touch," notes Whit Diffie, CSO of Sun Microsystems.[4] This narrowly focused approach is no longer acceptable. The new security professional is responsible for understanding technical concepts and determining their impact on the business. Management does not have the necessary information or technical training to perform this analysis. They are relying on their highly trained, highly-paid security staff to provide this input. "Security professionals, especially those in top-level positions, will not only have to master technology to protect a company's IT systems, but they will also need to understand a company's entire business and be able to pinpoint which security breaches most threaten its bottom line." [5]

Build relationships

Another important aspect of getting in touch with the business is building relationships with peers and customers. Understanding what initiatives are important to the business units and determining how security can compliment or assist them in obtaining their objectives provides some value. When discussing the importance of building relationships:

> Most CSO's will advice you to get to know the business and to show your business peers that you think business first, security second. CSO's need to put a face on the security department, their face. And if they can build trust and credibility with their peers, other executives will feel that much more comfortable signing their names on the dotted line.[6]

Lesson learned; security professionals need to get out from behind their

---

[3] Duffy, p. 35.
[4] Duffy, p. 34.
[5] Tobias, p. 1.
[6] Wailgum, p. 55.

computer screens and begin to interact more with the business to gain more credibility and trust.

Develop a formal proposal

Security does not come without a hefty price tag. The cost of hiring a staff of highly-trained security professionals can be very steep, not including the on-going training costs to keep the team adequately trained and certified in a rapidly changing industry. The cost of implementing a basic security infrastructure also is very expensive. Purchases of firewalls, routers, IDS systems, identity management solutions, virus protection, and anti-spam tools all can add up quickly. Security investments may be considered a necessity in the security professional's eyes; however, management doesn't automatically share the same conviction. Management may not immediately recognize the benefits of the proposed investment, may require more information about the expenditure, and most likely will require a detailed analysis to be provided and alternatives to be outlined before they are able to make a decision. No investment should be allowed to stand on its own merit. In order to "sell" any business initiative, it must demonstrate a positive impact on the business or bottom-line. The best way to gain support for your proposal is to utilize common business analysis techniques that demonstrate this tangible impact on the bottom-line.

Before approaching management with your concerns, budgetary requests for new Intrusion Detection tools or additional headcount to search through the endless security logs, you first must diligently prepare a thorough financial analysis or business case for your recommendation. Executive management evaluates all expenditures and investments in terms of expected return on investment or cost benefit analysis. By using an analysis tool or format they are familiar with, it will make it easier for them to compare the proposal in relation to other business proposals being presented.

Unfortunately, most security professionals are not trained to complete the financial analysis required to build a business case. Just explaining the risk of the investment is not sufficient to warrant the allocation of budget funds in the minds of executives. Because security investments typically don't generate cash inflows, security managers assume they cannot demonstrate a positive impact on the bottom-line. This simply is not true because security investments can easily demonstrate value in the form of reduced thefts, improved productivity, preservation of reputation, and reduced exposure to litigation.

Regardless of how the analysis is presented, all security investment proposals must address some commonly asked questions. A sample business justification format is highlighted below and identifies the critical areas that need to be addressed in any business analysis layout.

1. Define the need – Describe in detail the technical issue/business problem that needs to be addressed.

a. Who is impacted? – Identify the business units or users that are be impacted by the issue identified.
b. Why is it needed? – Explain the potential consequences of the situation and what has caused the need to be elevated.
c. Driving force behind the request – Identify who or what has elevated the need.
d. When is it needed? – Determine the critical timeline in which action is required.

2. Possible alternatives – Outline several potential solutions that will address the need. Make sure to include "doing nothing" as an alternative.
3. Estimated costs – Outline the associated costs of each alternative, making sure to include direct cash outlays, internal labor estimates, and any potential indirect costs, such as lost productivity.
4. List known benefits and risks – Identify the associated benefits and risks of each alternative identified.
5. Proposed solution – Identify which alternative you are proposing to be selected. Make sure to highlight the reasoning for this selection and offer detailed analysis information upon request.
6. Alignment with corporate strategic plan – Explain how the proposed solution aligns with the organization's strategic objectives.
7. Known issues– List any other pertinent information or issues that management needs to consider.

Although all costs are not easily estimatable, every attempt must be made to make an educated guess. Be sure to include indirect costs, which may not be easily recognizable at first, such as lost reputation of the business, potential legal liabilities, or failure to comply with regulations. All of these considerations may incur costs for the business and should be evaluated. When you are unsure of some costs, don't hesitate to seek input for your analysis from the business units, outside vendors, or available statistics.

Present honest and realistic information

Security professionals need to use care when discussing and representing risk in their proposals. Evaluation should be realistic for the organization and should not be a knee-jerk reaction to the latest security trend. "Although risk is increasingly employed to justify and evaluate security investment, as well as build a dialog with the business – care must be taken to ensure that it does not lead to misunderstandings or miscommunications."[7] In order to build trust with management, we must present proposals that are realistic and in the business' best interest rather than taking advantage of their lack of technical knowledge to elevate the priority of our own pet projects.

Lack of Awareness

Despite the dramatic increase in security incidents worldwide, many

[7] Warrilow, p. 2.

organizations, especially smaller ones, have yet to be detrimentally impacted by cyber crimes. What this has done is instill a false sense of security in some corporations. According to Chad Dougherty, an Internet security analyst at Carnegie Mellons's CERT Coordination Center (CERT/CC),

> Despite the rising threat, CERT/CC finds that most CSO's don't even think about their response to an incident until after they've experienced an intrusion of some sort. That's because most companies feel relatively safe.[8]

This lack of awareness is just another barrier that makes security investments hard to justify.

"It will never happen to us"

The Internet is an empowering tool, which allows business to participate in a global market. But along with this power comes new risks. There no longer are physical boundaries to crimes. Although a company may be isolated by location, their connection to the Internet makes them globally exposed. Cyber crimes have different incentives than a traditional felony. Traditionally, crimes have a specific victim targeted, and the criminal's motives are usually clear-cut and traceable. It is hard to recognize a threat if we don't know it exists. Internet incidents are "faceless" crimes that seem surreal. In today's new global economy, our enemies are no longer easily identifiable. According to Chad Dougherty, an Internet security analyst at CERT/CC,

> They (companies) believe that the hackers won't target them, specifically, he says. But they'd be wrong, says Dougherty. The majority of computer incidents are no longer focused on a particular company. Most attacks now are automated," he says. They spread with the intent to damage everyone and everything they can. [9]

Despite the mistaken comfort that companies enjoy, statistically it is just a matter of time before all businesses become victims of a cyber incident. The only way to educate management of these risks is to continue to share the details of real incidents, identify the losses, and single out the victims, in order to demonstrate that it can happen to anyone at anytime, regardless of size or location.

Regular reporting

Although your company may not have been detrimentally impacted yet, there is a good chance that it regularly experiences unwarranted traffic on their network. How better to open their eyes than to provide regular incident reporting to executive management. Obviously, the logs will need to be carefully screened and analyzed to "weed out" false positives first; however, the final results should be very educational. If you have never shared these types of stats, management may be surprised by what they see.

---

[8] Kaplan, p. 51.
[9] Kaplan, p. 51.

Show Me!

How better to convince management of the vulnerabilities that exist than to demonstrate the company's exposure with a test. Sometimes you must "show them" how unprotected they are in order for them to believe it. Although hiring an external consultant to conduct a security audit can be costly, it is a great exercise to perform. Management will quickly learn just how exposed and vulnerable the organization is, both from an external and internal perspective. Ideally, if the external penetration test can be performed with zero-knowledge of the organization and its infrastructure, the more telltale it is. Another beneficial outcome of such an exercise is a prioritized list of vulnerabilities, which highlight the greatest risks to the organization. The final report is a great marketing tool for the critical security initiatives that need to be completed.

Failure to recognize security as a strategic issue

When discussing the challenges of Information Security, the Human Firewall Council noted,

> Management of organizations, in particular, has tended to view information security as a technical problem confined to the Information Technology department. But to be genuinely effective information security needs to become part of the way everyone conducts his or her daily business, from the CEO at the top on through the entire organization.[10]

As the number of cyber security threats continues to multiply and the level of corporate exposure grows, due to impending regulations and litigation, executives can no longer ignore security issues. Security needs to become a principle consideration when making business decisions. Management will have to accept more accountability and elevate the role of IT security in the corporate framework in order to avoid large financial losses. "As companies place an increased emphasis on security," says David Foote, a managing partner at a research and consulting firm, "the role of the security professional is changing from a strictly back-office IT support role to one that's strategically tied in with the entire company."[11] This is a huge transformation for IT Security to make, and there are many obstacles to overcome. In order to accomplish such a dramatic change in perception, IT security managers must work hard to educate their peers and to build credibility for their role.

Building awareness

One very important part of the Security professional's job is to create awareness for security issues in the minds of their peers. Management cannot support what they don't know exists. It is security's role to outline risks, recommend policies and procedures that need to be followed, and to explain the relationship of security issues to the business. If management is not aware of the risks, then they cannot make educated decisions. Just as important is establishment of

[10] The Human Firewall Manifesto, p. 1.
[11] Tobias, p. 1.

clear roles and responsibilities for the entire organization with regard to security. Everyone in the organization needs to be educated and trained to support corporate security objectives.

Although not universally accepted, more and more organizations are allowing Security teams to play more of an advisory role with regard to business decisions. Executives are starting to understand that security is an important factor that must be part of the decision-making process. "It wasn't that long ago when security didn't even have a place at the proverbial table—it was more like a seat at the kid's table. But for whatever reason—9/11, computer viruses, workplace shootings, terror alerts, war-security has finally been invited to dine with the rest of the adults."[12] Another important shift in the security arena is the realization that security is more of an emphasis on people rather than technology.

Outline a plan

The only way for this paradigm shift to occur is for management to recognize the relationship of IT security to the business and it's strategic objectives. Rather than demonstrating a set of reactive business decisions and investments, security professionals need to act with foresight and strategic planning for their security initiatives. The creation of a detailed security program will serve as the foundation for security directives and will highlight the critical program objectives and their relationship with the strategic plan of the organization. With a security program, management will have a more clear understanding of IT security's role in the organization; they will be able to establish realistic expectations, and they will gain a mechanism for timely feedback and accountability. A well-thought-out and planned security effort should help to gain credibility and accountability from the rest of the organization.

Security must be an enabler

If the business unit managers don't believe Security managers are balancing their business objectives with security objectives, they may not embrace their recommendations. According to William Besse, a security manager at a large media company,

> CSO's have to be an enabler rather than an obstructionist. Although CSO's can mandate what to do, the business managers will leave the security function out of the process if you don't listen to their business problems. He also stresses that you have to be clear about the business specifics- to know exactly how the security issues relate to the businesspeople and their decisions.[13]

Business managers need to believe that you have their interests in mind. Security managers must also demonstrate how security can help them to meet

[12] Wailgum, p. 53.
[13] Wailgum, p. 55.

their business objectives. This involves developing trust with peers and encouraging a partnership in security decisions.

Give them the power of choice

Security needs to be a part of the business decision equation. Decisions, which involve security issues, should be a partnership between business units, management, and IT security. The security team brings technical skills and risk analysis information to the table. The business units offer the required functional expertise and operations experience, while management provides the strategic oversight. This situation, however, is not the norm. Often, business units consider Security a hindrance, a dictated practice over which management feels they have no control. For this reason, security usually is not a welcome participant in business decisions. One way to ensure security's involvement in the decision-making process is to give management more power to make the decisions with some guidance. "Interaction with security is much more appealing for businesspeople when they have some control over what kind of security controls are going to be put in."[14] According to MetaGroup:

> Enabling input from the information owner in terms of determining the appropriate level of security to be implemented is essential. Business management will be more motivated to make judgments with guidance and assistance from the security team if it is granted a level of discretion. In effect, the business becomes able to determine the necessary level of security from a predefined set of acceptable options.[15]

Conclusion

IT Security still is a very immature discipline that is not readily embraced by executive management. It remains an obscure practice that still is considered technical and the primary responsibility of the IT department. However, as security incidents continue to rise and regulators begin to assign corporate responsibilities, management can no longer afford to take a backseat on security issues.

Security professionals are charged with the responsibility of changing the existing perceptions of management and to earn their buy-in, support, and ultimately a shared ownership of the issues. In order to accomplish this feat, Security teams first must overcome some existing barriers and establish some credibility with their peers. Security initiatives must be easier to understand, demonstrate value to the organization, and must be strategically aligned with the organization's business objectives in order to gain Management's attention and support. This ownership can only be accomplished through open, honest communication channels, shared understanding of the issues, financial accountability, and the development of trusting relationships within the organization.

---

[14] Duffy, p. 34.
[15] Warrilow, p. 2.

References

Duffy, Daintry. “Money Well Spent”. CSO. November 2003 (2003): 31-36.

Wailgum, Thomas. “Fault Line”. CSO. November 2003 (2003): 50-55.

SANS Institute, Course Material from “Track 12 – Security Leadership for Managers”, 2003.

The Human Firewall Council. “The Human Firewall Manifesto – A Call to Action”. URL: http://www.humanfirewall.org/rhfwm.htm. (November 4, 2003)

Kaplan, Simone. “When Bad Things Happen to Good Companies”. CSO. May 2003 (2003): 50 – 54.

Warrilow, Michael. “ A Question of Trust: Justifying a New Security Paradigm”. Delta 2537. October 15, 2003.
URL: http://www.metagroup.com/cgi-bin/inetcgi/jsp/displayArticle.do?oid=43973&fmt=lpt (November 17, 2003)

The Human Firewall Council. “The Alarming State of Security Management Practices Among Organizations Worldwide”. Security Management Index.
URL: http://www.humanfirewall.org (November 4, 2004)

Tobias, Zachary. “The New Security Pro”. Computerworld. May 7, 2001.
URL: http://www.computerworld.com/printthis/2001/0,4814,60207,00.html (November 4, 2003)

Byrnes, Christian. “Chasms on Both Sides for Security, and a Tradition of Jumping In”. MetaGroup Research – Client Advisor. October 7, 2003.
URL: http://www.metagroup.com/cgi-bin/inetcgi/jsp/displayArticle.do?oid=43839 (November 17, 2003)