Global Information Assurance Certification Paper

Manage your Security Initiative as a Project

An Internet research paper for the
GIAC GSEC course (v1.2e) — SANS Security Essentials

By Rex Robitschek

August 19th, 2001

The problem

In large corporations, information security of some sort is a foregone conclusion. There is probably an organization already in place whose job is to secure data. They may do so with varying degrees of skill and varying results, but at least the intention is there at the corporate level. Establishing sound security in such an environment is a matter of assessment, deployment and monitoring.

But what about small- to mid-size companies? Often, they've grown up out of a shoebox. At some point in their fledgling existence they realized that they needed a "computer guy," so they hired one. Soon they needed another one, then a couple more. So they hired more staff, or promoted from within. Eventually, they had an I.T. department, and that I.T. department was (and continues to be) scrambling to keep up with a company whose growth was always one step ahead of the I.T. department's capabilities. Along the way, information assurance always took a back seat to the more easily understood immediate business needs of the company.

At some point, somebody in the I.T. organization of such a company becomes aware of the need to systematically secure the company data — aware of the need to know that the data is reasonably secure, not just to hope that it's secure or suspect that it might be.

In companies like this, the biggest hurdle to overcome is also the first one: getting buy-in from management. The above-mentioned "somebody in the I.T. organization" probably has an incomplete understanding of the fundamentals of information security, but he's probably also the most knowledgeable InfoSec person in the company; his boss probably understands even less. Imagine how confused senior management is going to be when this "somebody" tries to explain the nuts and bolts of data security in an effort to get funding.

We Have a Project

In a situation like this, the goal is to establish reasonable security for the company's information assets. A vital preliminary goal is to get approval from upper management to proceed. These are clear, short-term goals. True, *maintaining* a secure data environment is a long-term endeavor, but *establishing* that environment is indeed a short-term goal.

A definable short-term endeavor is, by definition, a project. It differs from normal, operational work, and requires special attention and methodology, especially in a company that is geared toward operations rather than project work, as most companies are. Apply established project methodology, and your chances of success will improve dramatically.

What we have, then, is a security initiative *project*. It's two projects, actually: the nuts-and-bolts, *how-we're-gonna-do-it* project, and a predecessor project, *how-we're-gonna-get-them-to-let-us-do-it*. This paper focuses on that all-important predecessor project; namely: getting the necessary buy-in from management to get the go-ahead to do all these wonderful and necessary things.

Choosing the Project Manager

The person you choose to spearhead your security initiative project should be an experienced project manager. A good PM knows how to get things done at many different levels. He communicates with senior management, front-line workers and everyone in between with equal ease. These skills are important when selling ideas not only to upper management, but also to the people who will be implementing, and ultimately following, the security policy that will follow.

A good project manger knows how to ride herd on contractors. This is important because many companies lacking in-house security expertise will have to rely on consultants and vendors to assemble a sound information security system.

A good PM is also congenial and accommodating by choice, but firm when he has to be. These qualities are forged in the project management trenches, where the PM is ultimately responsible for the success of a project. Project failure can be a career killer, so the PM develops an arsenal of techniques, both soft and hard, to get the job done. This is especially important in information security, because the initiative may meet with resistance at many levels, from front-line workers who may be inconvenienced by new security measures to the exec who's watching the bottom line. Each pocket of resistance must be dealt with. The soft approach is usually the preferred approach. But when necessity dictates and authority allows, a firm stance may be the only way to get the job done.

Finally, and most importantly for our management buy-in project, a good project manager is a diplomat. This is another quality that experienced PMs develop under fire. In most companies, the project manager, even though he has ultimate responsibility for a project, has little actual authority. This is because the people he taps to execute his project do not report to him; instead, they report to their own departmental management. In the absence of authority, successful project managers must rely on their influence to achieve their goals, and they take pains to establish that influence. In many mid-size organizations, the I.T. department is thought of as an

accessory — a necessary, resource-draining wart on the body of the company. I.T. is outside of the strategic loop, and lacks the influence of revenue-generating departments. A seasoned PM who knows how to establish influence is a tremendous asset to any project that requires executive buy-in.

But What About Technical Skills?

It is an axiom of project management that a project manager need not be an expert on any facet of a project, but he must possess the technical chops to maintain credibility with the experts he works with. This imposes some constraints on our choice of a project manager. Clearly, just any old seasoned PM won't do.

First, the PM must have a solid grounding in information assurance fundamentals. He needn't be a security expert. In fact, he'll be so busy managing the security initiative that he will have little time to perform the actual implementation itself. But he must understand the technical basics of data security. He must understand the vulnerabilities of data confidentiality, integrity and availability. He must understand the potential threats, both internal and external, to data assets. He must understand the need for sound policy, safe operating procedure and effective incident handling, and he should know how to tell good policies, procedures and tools from not-so-good ones.

Second, the PM should have networking experience. Many security threats and countermeasures are sufficiently technical that it takes a working knowledge of how data flows to understand them. Most project managers in the I.T. world are applications oriented, and have little if any networking experience. Project managers with networking experience are harder to come by.

On the other hand, there are a lot of network people who have spearheaded projects, and therein lies a pool of more-or-less qualified people to lead our executive buy-in project (remember that you may not have the luxury of finding a fully qualified PM to take on the job).

The chosen network project person may not have the security basics down, but that can be taught. SANS and other organizations offer courses in information security fundamentals that cover the fundamentals well, and are regarded as real eye-openers, even by seasoned network veterans. Such courses can give a reasonably experienced network person the knowledge he needs to manage the security initiative project.

Tips for the PM

Now you know your project. You know your goal (executive approval to launch a security initiative). You've selected a project manager to spearhead the project, and the follow-on implementation project that will ensue. Now what?

Here are some tips to guide the PM and the project to successful completion:

Know who your audience is — The person who brought you into the project will probably be your chief collaborator. He supports the project, because he envisioned it in the first place. He can inform you of the current state of data security in the company, who does what, and what some of the political currents are. He can also help you assess when the time is right to make the necessary presentations. Get to know him, and his chain of command.

Know who the players are at the top. After all, these are the people whose approval constitutes the success of this project.

Get to know the I.T. people as well. They are the ones who will implement the full security project, once your approval project is complete.

And don't forget the people who are handling security currently. They're probably working under considerable pressure, compounded by the fact that the nature of their job has probably made them less than completely popular. They probably have some in-depth knowledge of networking, and may consider themselves security experts. They may be offended or intimidated if your security initiative project hits them like a steamroller. But if you make them collaborators in your project, they can be of tremendous help. It's your choice; you and your project could be just the thing to validate them, develop them and help them shine, or you could simply make them look bad. Remember that they can be the cornerstone of the security system that you leave behind (you *will* move on to another project one day). Win their support early. Let them know how a solid, manageable security infrastructure will benefit them.

Have a plan — Before you start making presentations and writing proposals, you need to know what you're going to ask for. Make an inventory of the company's information assets. Assess the risks those assets face, at least on a gross level. Define the requirements for an effective, practical infrastructure to secure those assets. It may be helpful to engage a qualified security consultant for a few hours to help you through this process, but remember that you're not developing a detailed deployment plan at this stage. What you want is the 10,000-foot view of what appropriate security will look like at your organization, and a rough idea of the cost.

Keep it simple — Remember that your executive audience, while intelligent, motivated individuals, probably possess very little technical knowledge. Don't dive too deeply into technical issues. Keep your presentations and written work as non-technical as possible. You want to see nods of understanding and agreement, not the glazed eyes of group of execs who are stuck listening to the technical details of the latest Internet exploit.

Stick to the basics. Speak in terms of risks and costs — risk analysis is something executives are familiar with, and is a mainstay of information security. Then proceed to a list of requirements that minimizes both the risks and the costs.

Remember that you and senior management share a common concern: Asset Protection — Executives understand assets and the need to protect them. Make it clear that their company's data is an asset, and explain its value, both monetary and intangible (e.g., the potential loss to the company's reputation, and its customers' good will). You are, after all, simply trying to protect a valuable company asset. Make that message clear, and your job will be easier.

Execs speak in dollars — Business exists, after all, to make money. Executive management rates everything the company does according to how well it supports that moneymaking function. Revenue is good, costs are bad. And you are about to ask them to swallow a significant cost.

You must convince them that the benefits to the company outweigh that cost. Speak in terms of cost avoidance, and the prevention of lost revenue. Explain the potential losses if company financial data, plans or trade secrets fall into the wrong hands. Explain the potential loss of revenue and productivity that would result if a DoS attack or system failure left their systems down for an hour, or a day, or longer. Explain the public relations costs in the event of a publicized incident.

Wherever possible, quantify actual and potential costs in dollar amounts. This will lend concreteness to your message that will be easily understood by management.

And don't forget to mention the less costly procedural measures that are an important part of data security. Explain that promoting employee awareness of data security and fortifying procedure is a low-cost, effective way to improve security.

Be realistic — Make sure your executive audience understands that information security is a trade-off. Whenever you gain something on the security side, you usually lose something in terms of time, convenience or availability. After all, the only way to truly secure a computer is to disconnect it from the network, wipe its drives clean, melt it down, pulverize it and scatter the resulting dust to the four winds. The computer will be as secure as can be, but as you can imagine, data accessibility suffers somewhat.

The point you want to make is that no matter how much money, time and sweat you throw at data security, you cannot guarantee an incident-free network. You don't want to be in a position where the execs think you can deliver total security. If you do, the next incident will leave a lot of egg on your face, and may threaten the subsequent implementation project. If you keep management's expectations reasonable, your position will be much more tenable. Also, management will value your honesty and candor, and that will work to the project's benefit.

Write your policy early — The cornerstone of any coordinated security effort is a sound, comprehensive security policy. The first milestone in the implementation project that follows will be establishing that policy. Your current project, of course, is obtaining executive approval for your implementation project. Ideally, you want to get executive sign-off on policy as part of your executive approval package. This leaves you ready to roll when the implementation project kicks off.

The policy should state the risks to information assets, what will be done to alleviate those risks, and who is responsible for doing it. It should cover not only malicious attacks, but other threats to data as well, such as server failure, viruses and plain old ignorant negligence. In other words, don't forget to include the more mundane issues, such as backups, anti-virus deployment and updates, and what is expected of employees as they work with company data.

And make sure the policy you write doesn't conflict with other existing company policies. You don't want to hear the vice president of manufacturing, for example, mention in a presentation that the policy you're presenting flies in the face of an existing policy. That can stall your project, and may kill it in certain political climates. If your company has a policy-writing guideline, obtain it and use it. Get the company policy book and scour it for existing policies that may touch upon data security. And don't overlook existing tacit policies that may be undocumented, but are still a part of "the way it's done here."

Make sure the policy you write is clear and understandable, and that it's realistic. Impractical or unenforceable policy will devolve into a joke, not the useful tool it should be. Avoid legalese or other jargon as much as possible. You want your policy to be understandable to as many people as possible: the I.T. staff, management at all levels, and anyone who comes into contact with the company's data assets, even if they're essential computer-illiterate.

Be sure also that the policy supports the people who will implement and assess data security. Security people who will handle incidents, for example, need reasonable protection from liability, as do those who will legitimately probe the network for weaknesses.

Finally, make sure the policy you write is a living document, subject to regular review and updating (see *Plan for your departure* below).

We have a firewall, so we're safe — At some point in your project you are likely to hear an objection such as this, not only from senior management, but possibly from I.T. staff as well. Be prepared to explain the limitations of firewalls: how they can be circumvented by a single modem, how improper configuration can leave gaping holes, and how they offer no protection from internal attack. Make it clear that many threats have procedural solutions, not technical ones, and that no single security measure is a panacea. When your audience understands that no security measure is perfect, they will be more receptive to the layered defense that you're proposing.

Plan for your departure — Finally, remember that you are a project manager, and this is a project. One day you will move on to your next project. You want to leave behind a sound security infrastructure that will perpetuate and improve itself without your care and feeding.

Groom people for security implementation and leadership roles. Work with them as you get into the development and implementation phase of the security initiative project. Make sure they understand what you're doing and why, *while* you're doing it. If they're a part of the initiative, they'll be more ready and willing to maintain the security infrastructure you put in place.

And make sure that key people understand the fundamentals of information security. Some companies may need to rely on outside consultants for some aspects of security design or deployment, but there is no substitute for an in-house understanding of what information security is all about. Ideally, you would supply them with formal training on the fundamentals, but budgetary or other constraints may require that you pass on your own knowledge as best you can. At the very least, make sure that key I.T. people understand what you've done and why, understand the policy front to back, and know how to review and modify the policy as needed.

If you've done your homework on the policy side, you've already provided authority for the people whose job it is to enforce information security. Make sure those people are on the job and performing effectively before you leave.

Conclusion

Effective information security is vital for any business. The implementation of sound security depends upon executive buy-in. Obtaining that buy-in is a short-term, definable project, and is best handled by someone with a combination of project management skills and technical knowledge.

The chances for success of the executive buy-in project are greatly improved by the application of project management methodology. This paper has been geared toward project managers who already know the methodology, and is intended to give them tools that are pertinent to this specific project.

For this project, set aside your work breakdown structures and much of the other PM esoterica. Your chief tool will be your communications plan. Unlike most projects you've probably seen, your concern with work effort, detail planning and procurement will be minimal. Getting buy-in is all about communications.

If you take the things covered here to heart, and make sure you have a firm understanding of information assurance basics, you have every reason to expect a successful outcome, sign-off on your policy, and the go-ahead to make your plans a reality. Good luck!

References

General Accounting Office. *Information Security Management: Learning From Leading Organizations*. http://www.gao.gov/special.pubs/ai9868.pdf (August 2001)

Alberts, Christopher J.; Behrens, Sandra G.; Pethia, Richard D.; Wilson, William R. *Operationally Critical Threat, Asset, and Vulnerability Evaluation(SM) (OCTAVE[SM]) Framework, Version 1.0*. http://www.sei.cmu.edu/publications/documents/99.reports/99tr017/99tr017abstract.html (August 2001)

Sweltz, Ken. *Information Security Leadership*. http://www.sans.org/infosecFAQ/securitybasics/leadership.htm (August 2001)

Behrens, Sandra. *Between a Rock and a Hard Place.* InfoSec Outlook, Volume 1, Issue 4, July 2000. http://www.cert.org/infosec-outlook/infosec_1-4.html (August 2001)

McDowell, Mindi. *Who's Securing Networked Systems?* InfoSec Outlook, Volume 1, Issue 6, September 2000. http://www.cert.org/infosec-outlook/infosec_1-6.html (August 2001)

Project Management Institute. *A Guide to the Project Management Body of Knowledge*. http://www.pmi.org/publictn/pmboktoc.htm (August 2001)