

Chapter 15

Budget Acquisition and Corporate Commitment to Security

- Obtain Management Support
- Perform a Risk Assessment
- Determine Return on Investment (ROI)

The two things that are most often overlooked by security professionals are gaining management support and the acquisition of budget resources. In most environments, money is in scarce supply, while the demands on that money are not. As a security professional, you have to demonstrate the value of good security practices and resources in order to acquire more money. To do this, you must communicate the need for your security programs and projects to management by showing returns on investment, and you must involve management in a successful security program. You need to do the following immediately to ensure a successful security program:

- Obtain management support
- Perform a risk assessment
- Determine return on investment

Obtain Management Support

In this era of ever-tightening budgets, security can be seen by the non-indoctrinated as a target for budget reduction or elimination. Most upper management does not see security as a business-critical expense that will return dividends; rather, it is seen as an expense with little direct return on investment. In order to gain more funding for security initiatives you have to show management that there is a return on their investment. Typically, security is not a profit-generating expenditure for companies not in the information security realm; it is considered more as a cost of doing business. How much is spent is determined by how well the need for an aggressive security program is articulated. The first step in involving management and gaining their support—and budget resources—is to show the business need for security.

Show the Need for the Security Program

Showing the need for a security program seems to be an easy endeavor at first, but when approaching management with security requirements, you will need some facts to back up your claims. You will also want to gear your arguments to your audience, because speaking in techno-jargon to those not in the IT field will be meaningless and dilute the point of your requests.

Using comparable companies and their recent exploits or security posture is a good place to start. Most managers understand that there is an expected level of risk they can safely assume and still fall under duly diligent industry best standards. If your business competitors understand security and have vigorous security programs, this can be the catalyst for other management to meet or beat their security posture. Granted, this is not the most impressive way to gain acceptance from management for a security program,

but it can be a quick way to get your program started until a more formal plan can be put in place. This takes from the low-hanging fruit theory of attacking a problem from the easiest point, such as a person would do when trying to garner a piece of fruit from a tree. The person wouldn't necessarily go to the most difficult or highest point of the tree; rather, they would get it from the lowest accessible point. Management support can also be gained by focusing on legal requirements, prestige, industry benchmarks, or risk assessments.

The first step in determining what security policies and programs need to be put in place is through a risk assessment.

Perform a Risk Assessment

Risk assessments are a long-standing tool used by risk professionals to identify what a company's risks are in a quantifiable manner. There are two types of risk assessments in popular use: qualitative and quantitative. A *quantitative risk assessment* uses or attempts to assign real costs to the implementation of risk aversion methods and the costs of the incident and then assigns a quantitative figure for the likelihood of an incident. This type of risk assessment is usually in-depth and takes a great deal of time to formulate and create. It's generally not for those without prior experience in the risk assessment field, as incorrect data or assumptions can skew the results in an unexpected way, reducing the effectiveness of the security program. The benefit of this type of risk assessment is that there are hard numbers associated with risks and countermeasures. It can provide a solid ground for justifying expenditures in a way that management will understand immediately.

A *qualitative risk assessment*, on the other hand, involves subject matter experts to a greater degree, is more intuitive for the beginner, and is the predominant form of risk analysis in use today. A qualitative risk assessment involves first gathering subject matter experts in the processes within scope and then walking through possible risk scenarios. The team would then determine the degree of impact of the scenario and the possible outcome based on the degree of sensitivity of the assets used in the scenario. For the purposes of this book, we will focus on the qualitative risk assessment, due to its ease of use and quick results. If you have a disaster recovery, business continuity, or risk aversion report already completed for your business unit, you can draw heavily from the facts and figures they would have already calculated. Most disaster recovery teams will research some of the issues you will need to cover such as business downtime costs, remediation expenses, and so on.

In this chapter, we will be going over a very condensed version of what a true risk assessment is. Full-scale risk assessments often take a great deal of time and paperwork and have been the subject of entire books. You should reference some of the many risk assessment books available for further information on risk assessments.

Determine Scope

The first step is to determine the scope of your risk assessment. Scope refers to what your risk assessment will cover—in other words, what it encompasses. It is not feasible in most corporate situations to make the scope of a risk assessment encompass the entire organization and all processes. This approach would require the cooperation of people and groups that you may not have authority over. For your first risk assessment, you should cover the most critical aspects of the business for which you have authority. As an example, Robert works for a large telecommunications company as a system administrator for the support center's Linux servers and desktops. He is trying to gain management support and money to implement a firewall solution between the support computers and the Internet. In this case, Robert might have a scope statement of

The scope of this risk assessment is the support group's Linux server and all network connections for the server.

This simplistic scope statement explains the scope of what Robert wants to cover, allowing him to expand his scope as he progresses in his security upgrades. A scope statement of

The scope of this risk assessment is all of the support group's information processing systems.

has significantly broadened his scope, as these systems include desktops, servers, personal digital assistants (PDAs), and such.

Make your scope realistic and flexible to allow for increase if needed. Many first-time risk assessment teams try to be overly aggressive in terms of how big of a scope they should cover, only to realize halfway through the process that there is a need to scale it down.

Select the Team

The next step is to organize a team to determine the asset/information values (costs of equipment information to be protected) and the possible scenarios that may affect the in-scope processes, computers, and so on. If possible, try to convince management that you should select the team or at a minimum have some say in who is allowed on the team. The team should consist of subject matter experts or process owners for the in-scope processes or areas, as these people will be able to offer the most likely scenarios. The subject matter experts or process owners will also be able to provide the best resolutions to the vulnerabilities and risks covered in your risk assessment. In our previous example of Robert, the system administrator for the support desk, we would probably want to form a team consisting of the support manager, Robert (representing the system administrator), a networking staff member, a corporate security staff member, and possibly a member of the support staff. This team needs to brainstorm on the possible scenarios that could affect business processes from an information security standpoint.

Gather Issues and Determine Impact and Probability

This team should gather the possible issues and determine the following:

- The impact of the threat (on a scale of 1–5, with 5 being highest impact)
- The probability of the threat (on a scale of 1–5, with 5 being the most likely)
- Existing safeguards
- Countermeasures

The impact of the threat means what would happen if the threat occurred. This could be cost, loss of prestige, civil and criminal penalties, and so on. The probability of the threat is what the chances are that this would happen (use prior year information if available). The numbers for the impact and vulnerability should come from a group consensus, based on the best-guess perception of the group using the severity scale. The last step is to determine what countermeasures could effectively mitigate the risk and costs of those countermeasures. A sample page of our condensed risk assessment, using Robert's situation as an example, would be as follows:

Threat

An attack from the Internet through unblocked/unpatched service.

Description The support Linux server is directly connected to the Internet to allow customers to view open support tickets. This computer also allows SFTP from the support desk for customer patches. The only protection from outside FTP attempts is the username/password authentication provided in Linux.

Impact An attacker could attempt a brute force attack or other attack on the system directly from the Internet. An attacker could then deface the web server application, remove customer files or tickets, or use the machine to attack other computers in the network. This could cost the company up to \$15,000 per day in lost revenue, and \$2,200 in lost staff hours in repairs for each day the machine is not functioning.

Existing Safeguards The machine requires username and password for access.

Probability Known attacks have occurred in the past year from a disgruntled former employee. On February 15, 2004, the web server was attacked and all customer files removed, costing one day of downtime.

Countermeasure A firewall allowing only web traffic (port 80) at a cost of \$3,000 between the support server and the Internet connection.

Use the blank template in Figure 15-1 to create your cursory risk assessment threats.

Let's take the following scenario and fill out a sample worksheet. Tracy is leading a risk assessment team, which includes Karen from the systems administration team and Sally from the network operations group. The team has created the following scope statement for their risk assessment: "This risk assessment will cover the asset tracking web server (linux1) and network connections for the web server." The linux1 server is the only asset-tracking repository for the business unit and is used by offsite technicians to determine the location and configuration of equipment that is the core of the business. Due to frequent field hardware configuration changes, the documents are updated often and contain crucial information for the business to run normally. The team makes a list of threats and determines the top three are unpatched software, power outages, and weak passwords. They determine they will document unpatched software as the first risk worksheet because an incident based on unpatched software occurred in the last month and indirectly cost them many hours of downtime. Using this scenario, we will fill out the sample basic risk assessment worksheet shown in Figure 15-2.

After filling out a few of the risk assessment worksheets, go through them one more time with your risk assessment workgroup. This allows your group to ensure they didn't forget anything and to get a total view of the threats identified when compared to other ones noted in the risk assessments. One common result of this exercise is that the perceived highest threats may not be the ones requiring instant resolution because you may discover that other threats are far more important to mitigate.

Date: _____	
Preparer: _____	
Threat	
Description	
Existing Safeguards	
Impact (1-5)	
Probability (1-5)	
Countermeasure	
Rating	Probability + Impact = Risk Rating (___ + ___ = ___)

Figure 15-1. Basic risk assessment worksheet

Date: February 17, 2004	
Preparer: Tracy J	
Threat	Unpatched software
Description	The linux1 server is the primary asset-tracking repository for all field equipment. Due to the need for this machine to be running at all times, patches are scheduled to be implemented once a year.
Existing Safeguards	Patching occurs once a year on the server.
Impact (1–5)	4 (The system can be successfully attacked based on a known vulnerability.)
Probability (1–5)	3 (The lack of up-to-date patches has allowed an attacker to gain access to the system, based on a problem known for six months. The patch for the problem was available six months prior.)
Countermeasure	Scheduled downtime every quarter for routine issues, and a policy in place that will address high or medium patch alerts within two days of patch release.
Rating	Probability + Impact = Risk Rating (3 + 4 = 7)

Figure 15-2. Sample completed basic risk assessment worksheet

Prioritize Risks

As you populate your risk assessment with more threats, you should begin to prioritize the risks by adding the probability rating and the impact rating to get a total risk rating. This will allow you to focus on the most significant risks for presentation to management first. This has the side effect of enabling you to determine where your weaknesses are. The previous example listed the top three threats in the minds of the focus group as unpatched software, power outages, and weak passwords. The group created a sample risk assessment worksheet for each item and determined the rating for unpatched software as 7, power outages as 8, and weak passwords as 9. All the other threats except for denial of service fell below a rating of 5. With these ratings you can create a worksheet to show management what the experts think are the most significant risks to the organization. An example of this type of risk chart is shown in Table 15-1.

These worksheets will help you determine what the real threats are and which should be resolved first. The group had initially thought that resolving unpatched software would be the first priority, but as they progressed, they determined that weak passwords should be addressed based on the risk rating. As you work with your group to determine the threats to your organization, you might see that some of the threats can be addressed by a single countermeasure. This helps put more credence behind your findings for some

Threat	Probability	Impact	Overall Risk Rating
Weak passwords	5	4	9
Power outages	4	4	8
Unpatched software	3	4	7
Denial of service	3	3	6

Table 15-1. Sample Prioritization Chart

countermeasures and allows you to get management support for the issues that are most important. By prioritizing your risks based on the cumulative input from the risk assessment group, you can get surprising results. As noted previously, the risks you may have considered the most significant may have a lower risk rating than risks that were considered routine. The risk rating allows you to determine which are the most important and work on resolution of those risks first.

Quantitative Risk Assessment Overview

Throughout the majority of the chapter, the qualitative risk assessment has been the primary focus. To show real costs and return on investment using specific numbers (as opposed to educated estimates), we'll discuss a quantitative risk assessment example. As its name implies, the quantitative risk assessment is based on hard numbers, but it still relies on some qualitative methods. Like the qualitative assessment, you need to assign a value (Asset Value or AV) to the asset or information (or impact to the organization). You must consider for example the costs to recover from the incident or loss, maintenance costs, developmental costs, and revenue loss.

The factor to consider is the Single Loss Expectancy (SLE), which is the impact of a single incident. Before determining the SLE, you need to determine the Exposure Factor (EF) of the incident. The EF is what expected percentage of the asset would be lost in a given incident. For instance, if a fire were to occur in the primary server room, only 25 percent of the in scope system would be destroyed (as it is unlikely the entire system would be destroyed because of fire suppression systems). This would give you an exposure factor of .25. The asset value multiplied by the exposure factor results in the SLE:

$$AV \times EF = SLE$$

If we had a network operations center that had an asset value of \$960,000 (considering loss of revenue, replacement costs, personnel costs, etc.) with an exposure factor of .25 to a fire incident, we can now derive the SLE:

$$\$960,000 \times .25 = \$240,000$$

The next step is to consider the Annualized Rate of Occurrence (ARO) or, more simply put, the expected regularity of incident occurrence. This can be represented by 0.0 for something that will never occur to 365.0 for something that will occur every day. So, if we expected a fire every 25 years, we would have an ARO of 0.04. We can now determine our Annualized Loss Expectancy (ALE) using the following formula:

$$\text{SLE} \times \text{ARO} = \text{ALE}$$

Continuing with our previous example, we have an SLE of \$240,000 and an ARO of 0.04, so our ALE would be

$$\$240,000 \times 0.04 = \$9,600$$

You could now put that information in a chart for management showing them the costs of security programs and procedures. In order to show a positive Return on Investment (ROI), we would put this information in a chart comparing the costs of mitigation programs and compare that cost to the costs we calculated in our quantitative risk assessment. We wouldn't spend \$1,000,000 a year in fire suppression mechanisms when the ALE was \$9,600 a year. When considering these types of risks, you must also consider non-monetary issues such as personnel safety and regulatory requirements, so even though the ROI wouldn't necessarily directly compare with the mitigation mechanism costs, the other factors come into consideration as well.

Report to Management and Obtain Guidance

The sample risk assessment provides management with a clear-cut view of what risk they are facing in monetary terms, and how much it would cost to remove that risk. For the final report, create a short one-page summary of your findings in what is typically called an executive overview. This allows management to get a quick overview of your findings, without having to dredge through the entire report. Make sure to emphasize your most important points and the most critical security issues, as this is your attention-getting page. The rest of the report is available for management review, but most managers will review the executive summary and trust the judgment of their staff on the needs, especially if you based your recommendations on hard facts. When management sees that the countermeasure costs less than the actual risk mitigated, the business need becomes evident. This allows you to request budget and management support in your effort to mitigate your shown risks to business goals. Executive summaries are by definition a very condensed version of the original report. You should remember to keep an executive summary to one page, or in extreme cases, it should not exceed ten percent of the overall page count of the report being summarized. In your executive summary, you need to first identify the scope, what threats were identified, and the countermeasures that are recommended. You should not try to include every threat your team discovered. Limit yourself to the top five or the most urgent issues noted and how they can be mitigated. Using the previous example with Tracy's group, here is a representative executive summary with all the elements listed above.

Executive Summary

The asset-tracking web server, also known as linux1, is the only asset-tracking repository for the business unit and is used by the offsite technicians to determine the location and configuration of equipment. Due to frequent field hardware configuration changes, the documents are updated often and contain crucial information for the business to run normally.

The subject matter experts involved in the operation of the web server formed a risk assessment group and determined the top three threats to the normal operation of this machine:

- **Weak passwords** User passwords have been found to be deficient based on previous experience and the amount of compromised accounts based on poor password selection by users.
- **Power outages** Power outages occur frequently at the data center, causing the system to shut down forcefully, sometimes causing data corruption.
- **Unpatched software** Software is currently patched once per year, leaving the systems vulnerable to known software weaknesses for up to one year after release of a patch.

To mitigate the possibility of these threats affecting the normal business operations of the organization, the following countermeasures were determined to be the most cost effective while adequately reducing the exposure to the threat:

- **User education** Security newsletters should be sent every month and immediately after significant events. If possible, users should also attend security awareness training quarterly at which time password selection and strength will be emphasized.
- **Installation of uninterruptible power supplies (UPS)** The installation of a UPS for the linux1 server will allow the system to shut down in a graceful manner, preventing data corruption.
- **Scheduled maintenance periods every quarter** Scheduled downtime should be made available every quarter at a minimum to allow the system staff to patch vulnerable software. If business requirements allow, critical patches should be allowed more frequently.

The implementation of these countermeasures will alleviate the majority of problems currently encountered by the linux1 server, providing better availability to the end user.

Determine Return on Investment (ROI)

Return on investment is simply showing management, in terms they understand, what the results of their security investments will be. This doesn't necessarily have to be profits from the investment; it can be the culmination of savings and risk aversion from the investment. You will need to conduct a risk assessment to realize the full value of your security efforts, as they show the threats and countermeasure in a formalized, rated way. Part of the risk assessment should include costs for each type of incident. The previous one-page risk assessment showed in precise terms that the cost of mitigating the risk was far less than the impact of doing nothing. Sometimes showing the return on investment is not quite so straightforward. In those instances where you can't determine the costs of an issue and the return on investment, use the best figures you can gather (realistic and within reason). You can use the estimated costs of a previous incident that was similar in scope and convert the numbers to cover the issue you are working on. You must also keep in mind any regulatory considerations as well as insurance adjustments related to your security program.

Perform Fact Finding

To effectively convey the importance of the security program, you will need to do some fact finding and coordinate with other groups. This step can be time intensive, but the results of your effort can be tremendous. A methodical fact-finding effort will allow you to present management with factual evidence for the need for a good security program, without opinions based on preconceived notions or guesses that can degrade your overall security message.

Determining what information you need is often the most difficult aspect of the information gathering phase. Some sample facts to gather are

- What is the average income per day of your business unit?
- What is the cost of hardware in your business unit?
- What is the average salary of the staff?
- What laws or regulations apply to your business unit?
- What penalties are associated with process failure of your business unit?

There are other facts to gather, but these are largely determined by what problem you are addressing. It is good to take some time to figure out what you are trying to accomplish and how you are going to go about meeting that goal.

After determining the facts you need to gather, you then need to get the information from those who can provide the best answers. This may include financial, legal, and human resource staff, as well as subject matter experts. Your management should have an understanding of the business relationships and who would be the most helpful in

your fact-finding phase. Another good resource to consider is the office manager, who usually knows the major players in the organization and can help lead you in the right direction for information.

Determine Revenue and Revenue Loss

The first step is to determine the typical revenue produced in one normal business day. This allows you to show what a worst case scenario of complete loss of business functions would be, upon which you can begin determining more long-term effects of business failure. Another important area to consider is if there are fines associated with failure of business activities. If your company has a contract to provide services to another company or individual, do you have an associated fine or deduction when your service doesn't meet predetermined metrics? Are there governmental fines associated with failure to deliver goods or services that could be levied for failure of business delivery? Has a similar company in your industry faced an information security incident? If so, what were the costs of the incident? The costs associated with business interruption or failure could be of tremendous impact, even causing severe degradation of business revenue. If you are a business in the government sector, you must consider the ramifications of potential fines or investigations by government oversight committees and the costs associated with those activities. Government and business entities must consider the impact of incidents on operating budgets and future budgets/revenues.

A good way to determine return on investment (or return on security investment) is to use some previous examples of security issues that caused downtime or business disruption and compare the cost of the downtime to that of the mitigation solution. For example, the fictional company ACME Sprockets has an application called Sprocket Tracker. If the Sprocket Tracker application went offline for 30 minutes, it could directly cost the company \$10,000. Using that figure, you can reasonably estimate that in an average business day, you could lose \$160,000. This was determined by figuring out the average work hours in a business day, dividing by 2 and then multiplying by \$10,000 (average loss per 30 minutes). These are the types of calculations you will need so that you can provide management with reasonable information on potential losses associated with a security event. Figure 15-3 shows an example of determining an incident's cost for a very small company suffering a minor virus outbreak.

Using the report shown in Figure 15-2, you can propose a possible resolution or ways to mitigate the risk and directly compare the two to show the business case for the resolution. For instance, in this case, you show how a patch management system for your Windows machines, which might cost \$1,000, could reduce the damage, potentially saving the organization \$5,600 per incident.

Determine Government and Industry Requirements

Other areas that can assist in the determination of return on investment and can greatly impact budget resources are governmental and industry requirements. There are many different legal requirements for security practices throughout the world, which if not

Incident Cost Report		
Incident description	Virus outbreak on Windows user's laptop, due to opening an attachment.	
Remediation staff hours used	Two support staff spent 15 hours over two days to remove the virus from end users.	2 staff members at \$30 hour for 15 hours = \$900
End user hours used	End users had to wait for staff. A total of 15 users had an average of three hours non-productive time each.	15 users at average \$60 hour for 3 hours each = \$2,700
Business hours down	Network problems caused three hours of downtime due to network resources being over-utilized. Typically \$8,000 a day is generated in revenue.	3 hours at \$3,000
Total Cost		\$6,600

Figure 15-3. Sample incident cost report

properly followed can result in severe monetary penalties, censure, or even criminal penalties. Most security legislation is still in its beginning stages and many businesses have not seen penalties yet, but the provisions are available for regulatory or investigative agencies. Examples of current legislation (pending and enacted) include

- The Health Insurance Portability and Accountability Act (HIPAA), which sets provisions for how personal health information is handled, disclosed, and used. This is applicable in the United States. More information is available at <http://www.hhs.gov/ocr/hipaa/>.
- California SB 1386, relating to reporting of security incidents to California residents and applicable to all businesses that hold personal information on California residents. This particular legislation is seen as far reaching due to the global nature of business, and the fact that a lot of private businesses will hold information on a California citizen due to the nature of interstate and global commerce. More information is available at the California State Senate home page: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.
- The Gramm-Leach-Bliley Act (GLBA) or the Financial Services Modernization Act defines some guidance on information security obligations for companies in the United States and sets out requirements for the protection of consumers' personal financial information. More information can be found at <http://www.ftc.gov/privacy/glbact/>.

- The Sarbanes-Oxley (SOX) Act of 2002 deals with accountability for public companies. Of special interest to information security professionals is section 404. Violation of the requirements set forth in this act can lead to civil and criminal penalties for executives and directly impact a security program. The basics of this legislation are that it requires certification of a company's internal controls on a yearly basis, requiring a need for the protection of your company's data. Go to <http://www.sec.gov/spotlight/sarbanes-oxley.htm>.
- European Union Directive 95/46 EC on the Protection of Individuals with Regards to the Processing of Personal Data, and on the free movement of such data within the European Union. This legislation concerns the protection of personal information and how that information is stored, used, and processed. Go to http://europa.eu.int/comm/internal_market/privacy/law_en.htm.
- The Personal Information Protection and Electronic Documents Act (PIPEDA) covers the collection, use, and disclosure of personal information on Canadian citizens. Further details on this legislation are available at <http://www.privcom.gc.ca/>.

Information security has become a major concern of governments and citizens, and legislation is being enacted throughout the world. The six pieces of legislation listed previously only cover a small portion of the wide-ranging information security laws and regulations that apply to business today. Contact your legal department for further clarification on what legislation applies to your company and industry based on your operating regions, what type of information and services you provide, and other factors. The legal department should also be able to define the potential penalties accrued when a company is not in compliance with these regulations. The security controls required by governmental and industrial regulations should be brought to management's attention immediately and enacted as soon as possible as these represent the most immediate security fulfillment requirements.

Determine Impact of Loss of Trust

Another area to consider when determining the return on security investment is the estimated losses from prestige or trust in the industry. If your company is a high profile or especially sensitive industry (financial, utility, and so on), the losses incurred by a publicized security incident could be far greater than the more obvious short-term losses on operations, recovery, and maintenance. You must also consider how it would affect future customers. This is particularly hard to determine because there are usually no definite future sales or revenue figures, so you must take average sales and consider what could potentially be lost due to lack of confidence in security. For instance, imagine if your company provides information systems services to a credit card processing facility and the company suffered a malicious event. How would future customers view your service offering and how much more difficult would it be for sales staff to close future deals? This is the most obscure portion to determine, but your best guess based on

previous sales will have to suffice to give management a realistic expectation of the cost of loss of prestige and trust.

Show Return on Investment

Now that you have gathered the appropriate information as outlined in the preceding sections, you need to show the return on investment. Most security practitioners consider information security in terms relative to insurance. Having a vigorous information security program affords an organization insurance against the outcome of poor security. Using all the information gathered, you can now determine the costs of an incident or potential incident and weigh that against the outcome of the possible scenarios.

One suggestion is to write a paper correlating all the information you gathered in conjunction with the risk assessment and provide management with an overview of the benefits of the security program. This should include the worst case scenarios along with the costs of those scenarios. Then provide a direct link to the planned and implemented security mechanisms and procedures to show how these things mitigate, reduce the likelihood, or reduce the impact of that threat. Note that the cost of the countermeasures should not exceed your costs of the risk, as this is not in the best interests of the company. For instance, the countermeasure for an intruder coming on the premises might be to hire roving security guards and erect a fence around the premises. This might be reasonable in some situations, but if the cost of the assets and information protected do not warrant this level of protection, the business requirements for this solution are diminished. Gather your information and show how the costs of implementing countermeasures will provide real benefit to the company. This will show management how important security is to the overall business objectives.

Seek Outside Help and References

In some instances, management may want the input or guidance of an outside, independent source to provide validation for your recommendations. This is a prudent step and having the information available to management allows them to make a more informed choice and provides legitimacy to your recommendations.

Gather Industry Statistics

Statistics are a great way to enhance your security expenditure and policy requests. There are many security statistics available online, as well as sites that provide industry research at a reasonable cost. Providing a hard-hitting statistic that shows management what others in the industry are saying or experiencing can sometimes be the determining factor between project approval and rejection. Use the experiences of others and the statistics they provide as an attention grabbing point in your research to prevent your company from becoming one of those statistics.

Statistics on security that will assist you in your security goals can be found in several places. You can also use statistics based on your own experiences, such as firewall logs,

security incidents per quarter, or other pertinent facts as these statistics can have more impact than general reference ones. A few of the more popular sites for security statistics are

- CERT/CC (http://www.cert.org/stats/cert_stats.html)
- CSO Magazine (<http://www.csoonline.com/>)
- ISSA Journal (<http://www.issa.org/>)
- SANS (<http://www.sans.org/>)
- SecurityFocus (<http://www.securityfocus.com/>)
- ZDNet (<http://itpapers.zdnet.com/>)
- LinuxSecurity (<http://www.linuxsecurity.com/>)
- InfoSecurityMag (<http://infosecuritymag.techtarget.com/>)
- Linux Weekly News (<http://lwn.net/security>)
- Linux Today (<http://linuxtoday.com/security/>)
- Vendor web sites
- General use search engines such as <http://www.google.com/> can provide the most up-to-date or relevant statistics.

Contract a Consultant

An uninvolved third party can provide insight from a viewpoint that you may not have previously had. They can also back up your recommendations if they are based on sound research and foresight. If you are not a security professional or if you don't have a security background, this is the favored course of action. A consultant is usually versed in management and business practices, and can articulate your recommendations in a way that conveys the urgency and need for a vigorous security program. This is not to say that a consultant is going to come to your business and rubber-stamp your proposal without providing feedback or new recommendations if yours need enhancing. A good consultant will take your research and recommendations and weigh them against industry best practices or prevalent levels of security. Most consultants will also conduct some form of audit to determine the current security posture and what level of security management desires. Having the research discussed earlier in this chapter available to the consultant will allow them to create recommendations in a timely manner, with the least disruption to staff.

Locating a good consultant can be difficult. A good place to start is by contacting your local Information Systems Security Association (<http://www.issa.org/>) or Information Systems Audit and Control Association (<http://www.isaca.org/>) and talking to chapter representatives. They will usually be able to provide some references and contact information for local security consultants. When interviewing security consultants, ask what types of certifications they hold, level of education, how long they have been doing

security consulting, references from the last few customers they had, as well as if they have experience in your organization's field of business. A good consultant will be happy to provide this information, and by doing your homework on your prospective consultant, you will ensure that your company gets sound, unbiased advice.

After contracting a consultant, you should start by telling them what your objectives are and provide them with access to the information required to effectively do their job. A consultant who doesn't have enough access to resources and information will prove to be useless to your company and can actually lead to results that are detrimental. Consultants are sometimes seen as the untrustworthy outsider or competitor to many in the information technology field, so you may need to assist the consultant in their fact-finding duties.

A consultant who understands your business and needs can prove invaluable to your company's security goals and often provides the final catalyst needed to implement security mechanisms and policies.

Reference Current Industry Standards

A great place to reference your current security posture against a worldwide reference is ISO 17799 (BS 7799-2), Code of Practice for Information Security Management. This standard provides a framework that is beginning to be accepted worldwide as an information security standard. There are other industry standards available online, but ISO 17799 is rapidly becoming the de facto guideline for creating a security program that will meet the needs of most organizations. Referencing the ISO standard and using it as a guideline for your program will show management that you are utilizing tools that are in use worldwide and widely accepted as best practice in the information security industry. The ISO standards do cost money to obtain (around \$250) and can be ordered at BSI Americas (<http://www.bsiamericas.com/InformationSecurity/>). There are other guidelines in use worldwide, even industry-specific guidelines, so you must do your research to determine what the best documentation for you will be. Some of the other guidelines for a security program or audit of a security program are

- Generally Accepted System Security Principles (GASSP), available at (<http://web.mit.edu/security/www/gassp1.html>).
- Generally Accepted Information Security Principles (GAISP). This is a project to rework the GASSP and move it forward. It is still a work in progress, but information about it can be found at <http://www.issa.org/gaisp/>.
- Commonly Accepted Security Practices and Recommendations (CASPR), available at <http://www.caspr.org/> (currently inactive).
- Control Objectives for Information and Technology (COBIT), available at <http://www.caspr.org/www.isaca.org/cobit.htm>.
- Common Criteria, available at <http://csrc.nist.gov/cc/>.

Involve Management in Creation of Security Policies and Spending

This is possibly the most crucial step to gaining management support for your security program. Management must perceive some ownership in the overall security plan. This sense of ownership will ensure that they fully support your process and influence their management and staff to support your security initiatives. The first step was to show the need for the security program through the use of costs versus return on investment. The next step is to involve management in the creation and formulation of the security plan through education. The more informed your management is, the better equipped they are to support your programs to their management. Provide timely, management audience targeted newsletters and news segments to management to show how important security is to the overall security architecture. There are many magazines (online and hard copy) and newsletters in print today, targeted at the management audience. Some of these magazines are

- Corporate Security (<http://www.straffordpub.com/products/csn/>)
- CSO Magazine (<http://www.csoonline.com/>)
- ISSA Journal (<http://www.issa.org/>)
- Network World Fusion (<http://www.nwfusion.com/>)
- InfoSecurityMag (<http://www.infosecuritymag.com/>)
- SC Magazine (<http://www.scmagazine.com/>)

When determining what your security program should entail, seek management's guidance on what solutions will be the least disruptive to the organization as a whole. Management can provide invaluable insight on the interdependencies and social relationships between business segments that you may not have been aware of. These relationships can prove beneficial when seeking to influence change across business units.

With the introduction of information security legislation on the rise worldwide, management in most companies is beginning to understand that security is not just a cost of doing business, but a requirement of doing business. Your job is to show that your security solutions can provide maximum benefit at a reasonable cost. By involving management in all aspects of your security program and showing why security is crucial to business operations, you will obtain the budget resources and management support you need to be successful.