Chapter 3

Deciding What You Really Need

In This Chapter

- Getting management to listen to you
- Making your case with facts and figures
- Looking at situations that could benefit from the use of cryptographic systems

You wouldn't buy a car without first researching all the makes and models you were considering. Likewise, you wouldn't buy a truck if what you really needed was an economical sub-compact. The same considerations should be made when deciding what cryptographic systems or programs you need to protect your data and communications. You'd think that it would be obvious to do a little homework before entrusting your security to a new system, but you'd be surprised at how often it's considered just a necessary evil and the cheapest solution is considered good enough to do the job.

In this chapter, I give you the basis for making decisions about what you really need and offer some solutions that you ought to consider. I want you to also remember that it's not just the solutions you pick that will make your system work for you; it's also the personnel you need to manage and maintain the system. You wouldn't hire an inexperienced (albeit talented) teenager as a long-distance truck driver, and neither should you hire someone to manage your systems who has no practical experience in the field. Many systems require a certain amount of training of both administrators and users, so be sure to include that in your decision-making matrix.

Justifying the Costs to Management

Without a doubt, the most problematic area in almost any business is getting the management to approve the purchase. It doesn't matter if you're talking about office cubicles, copying machines, phone systems, or upgrades to the network. Whatever choices you give them, they always want to know if you can get the project done cheaper. It's a fact of business life that you just have to deal with, and I'm here to give you some tips.

First of all, you have to look at the situation from management's point of view. They have to make sure that the business shows a profit each year, and they may have a number of entities sitting in judgment of their business decisions — boards of directors, shareholders, and so on. This tends to make management very cautious, especially when dealing with a situation in which they feel insecure. How many managers do you know who really understand technology? So, in putting yourself in their shoes, you can often come up with persuasive arguments to make your case and covertly "teach" the technology to management so they can explain it to their higher-ups.

In simple terms, management responds to decisions that make good money sense — something that will either save them money or make them more money. Start up your spreadsheets, and I'll tell you which figures to start collecting.

Long-term versus short-term

Projects that will last a long time tend to pay for themselves over time. Consider solar-generated electricity for a home — it's very expensive in the short term, but in the long term you can eventually kiss your power bills goodbye. Not only that, but a homeowner can and will have power if a bad storm knocks out the power grid, and in some cases might be able to sell his excess power back to the power company. This foresight and planning is good for everyone in the long run.

Short-term projects generally take only a short period of time to complete, and the investment results are more immediate than with long-term projects. There are no rules that state that one type of investment is better than the other, but there are pros and cons to each.

Unfortunately, in this age of cut-backs and low employment, many companies are concerned only with short-term solutions for their problems. What they forget to figure into their equations is that the short-term solution may not look so attractive in the long run. Take the company who decided to purchase cheap desktop PCs with limited expansion capabilities and low amounts of RAM. In the short-term, that purchase probably saved the company a lot of money. But in the long-term, it also cost them a lot of money to expand and upgrade their system as the company grew. What initially looked like a good return on their investment turned out to be a waste of good time and money.

The addition of cryptography to your network can be seen as either a long-term or a short-term investment, depending on the size and scope of the project. If you are setting up SSL certificates on your Web server to accept secure transactions, that may be seen as short-term because it can be quickly implemented and the costs are generally low. On the other hand, if you are setting up a full PKI system for authentication, single-sign-on, and to protect the integrity of documents, that will probably be considered long-term due to

the increased costs in labor and equipment. Neither of these situations — or others — need to be viewed with a negative eye, however. You just have to figure out what management's bottom line is.

Tangible versus intangible results

Sometimes the things that push management's hot-button are not necessarily dollar figures; sometimes they are intangible results. If you can come up with a scheme that will make your boss look like a hero in his superior's eye, you can often get what you want. Another intangible that often works well is to promote the positive effect your changes make in costumer confidence. Customer confidence is hard to put into dollars and cents, but the end result is loyalty — the customer is more likely to stay with you than to go to a competitor if the customer has confidence in your ability and your technical expertise.

Positive ROI

For those of you not familiar with the term ROI, it simply means *Return on Investment.* When you buy stock and the price goes up, you get a positive ROI because you've made money with your initial investment; a negative ROI is when the stock price goes lower than what you paid. Simple, isn't it? For a number of years, the term ROI has been the buzz phrase with management. They often don't even ask if the system will work — they just want to see a positive ROI (on paper in any case).

To be honest, there is no single, fool-proof method of determining a positive ROI. Although the concept of ROI is standard, the method of obtaining and tabulating the costs and figures is a bit like black magic. You can find hundreds of companies on the Internet who are more than willing to sell you special applications that are supposed to help you obtain ROI figures by messaging your numbers to fit your arguments. I don't recommend buying these programs, and I can't give you a definitive method of producing positive ROI figures for cryptography, but I can give you some helpful tips.

In order to argue that the use of cryptography in the workplace will give a positive ROI, you must collect data for the following:

- Cost of current security measures
- Effectiveness of current security mechanisms
- Cost of recent security breaches
- Current and future levels of threat
- Increased security

- New regulatory requirements for security
- Cost of cryptographic system(s)

When you have these facts and figures, you can start building a persuasive argument for the inclusion of cryptography into your systems. Remember that crypto is scary to a lot of people, so do your homework well.

Cost of current security measures

If your business is large and has IT departments scattered all over the country, it may be difficult to get an exact figure on the costs and effectiveness of current security measures. However, you can figure the cost of your own systems and use that as an average cost. If other offices are larger or smaller than your own, you can weight your figures accordingly and come up with a weighted average. Some of the figures you'll want to include are replacement parts for electronics that will inevitably die at some point. You'll also need to gather the salaries of the people responsible for network security. The reason that these costs are shown as a *negative* ROI is that they don't generate any income in themselves and they are recurring yearly costs.

To obtain some *positive* ROI figures, keep in mind, also, the cost of the cryptographic solutions you will be proposing. In some cases, the business can take accelerated depreciation and can write off the total cost of the system the first year. Because the costs of the cryptographic solutions can be viewed as an upgrade and their costs may be written off, the net result for the business is that the costs are balanced by the write-off. In some cases, it may also reduce the costs of your company's various insurance policies. That, certainly, is a positive result.

Effectiveness of current security mechanisms

This is somewhat of an intangible. If you haven't had any security breaches with your current security mechanisms, you can't really be sure if it was the security mechanisms that prevented breaches or if you have just been lucky not to have been targeted by hackers or other attacks. However, some real data can be computed by questioning the IT staff. Ask them how much time is spent reviewing firewall logs and responding to alarms sent by the firewall and intrusion detection systems. If the systems are sending out so many false-positive alarms that the IT staff no longer pays attention, then those security mechanisms aren't really effective. They've become the equivalent of the Boy Who Cried Wolf. Calculate the number of man hours spent responding to alerts and use that as a negative ROI figure.

If your new cryptographic system increases the effectiveness of your network security, that is a positive ROI. For example, if all of your important data is encrypted, the theft of that data may not be as serious as if it had not been encrypted. Your effectiveness is increased because you can spend more time trying to find out who was responsible for the theft and less time on damage control on the data that has been stolen. The hours saved responding to security breaches are positive ROI.

Cost of recent security breaches

The Gartner Group specializes in gathering data on network security, security policies, and the costs of security breaches. In a recent report, they found that a security breach costs medium- and large-size businesses $1 million for each security event. That figure is reached by calculating the amount of lost revenue (lost customers, drops in stock prices, labor costs to recover from the problem, and missed business opportunities). They also found that a significant number of businesses never recover from a serious breach. A serious breach is one that lasts three days or longer, and it must be noted that the average recovery time for most breaches is three days. Could your business survive three days with no network? Even viruses that don't do any harm cost businesses a lot of money because cleaning up the servers of virus infections is quite labor-intensive.

Use the cost of security breaches as a negative ROI. On the other hand, if you can show that the installation and use of cryptographic systems can reduce or eliminate costs of certain types of security breaches, put that cost savings down as positive ROI.

Current and future levels of threat

With the threat figures, you can extrapolate how much money the company would lose if it suffered a serious hack that was made public. You'd lose the confidence (and probably the business) of some customers, and negative press could adversely affect the stock price or the value of the company. Additionally, you have to include the cost of labor to stop the hack, reverse any damage done, and plug all the holes that let the hackers enter in the first place. If trade secrets or future product data were stolen, that could well mean the end of the company.

The new regulations on financial companies and the health care industries require that you be able to prove you have done all you reasonably can to ensure the security of your corporate network. There are other situations in which you might have to prove your network is secure, like an audit by the FTC stemming from consumer complaints. Regardless of the reason, you want to have the best security possible to avoid lawsuits and governmental fines. If you see that your company could be included in any of those situations, you must pull together figures for legal advice, trial lawyers, PR firm consultations, and more. These can be very convincing numbers to management, and the likelihood of being found guilty of disregarding possible security mechanisms is a lot less if your system includes encryption.

Conversely, if you were to introduce some type of cryptographic solution into your network, you could avoid certain types of risk and show a positive ROI. For example, if all the personal data of your customers is encrypted, you save yourself the cost of lawsuits that can occur when personal data is either inadvertently released or when someone steals those files in order to sell the information. It's pretty rare in the world of network security that you can say that a solution eliminates risk completely, but some crypto solutions can certainly help mitigate the risks.

Increased security

Many companies have spent tens of thousands — or even hundreds of thousands — of dollars on firewalls, intrusion detection systems, VPNs, and more. However, all of that protection works only on the data in transit. After the data lands on the servers, its only protection is access control. And we all know how easily access controls are subverted — old accounts, guest accounts, bad passwords, and sloppy administration allow unauthorized persons to access the data on the servers. This is the equivalent of connecting two wicker baskets with a steel pipe (see Figure 3-1). The steel pipe protects the data in transit, but almost anyone can get access to the wicker baskets (the data at rest).

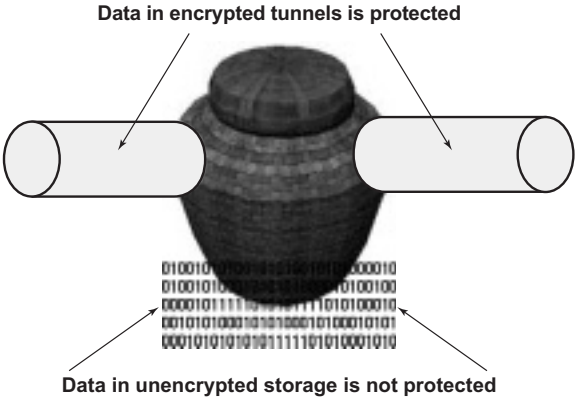

Figure 3-1: Protecting the data in transit and not the data at rest.

Intruders can and will get past firewalls, they can fool intrusion detection systems, and they can hijack network connections. In fact, if you read the stories and statistics, you'll soon see that most hacks have focused on the data at rest and have not attempted to pick up the data while it was in transit. Credit card numbers, personal financial data, trade secrets, and software are usually stolen right off the server.

Imagine a scenario where the data in transit is adequately protected with a VPN or SSL connection. Likewise, the data at rest (on the servers) is protected by encrypting it. It would be hard enough for a hacker to get access to the VPN, and he would be doubly thwarted by finding that all the data he got looked like gobbledygook. This is an example of increased security at its best. It's a bit like changing the wicker basket into a steel vault.

Increased security is always listed as a savings. Just look at the banking industry. By using encrypted SSL connections for online banking, the financial institutions have saved millions in the reduced number of staff needed to man phones for customer support. These companies have been able to let

the customer take care of his business without having to interact with someone at customer service. Certainly customer service calls are still important, but Web transactions with SSL allow the customer service personnel to focus on more important tasks, and the customer can take care of the smaller chores such as transferring money between accounts and requesting more checks.

Consider what reduction in man hours can be had by incorporating encryption into your systems. If nothing else, you may be gaining disk space as some systems compress the data as they encrypt it. If the data is compressed to even 25 percent of its original size, that may save you having to buy new servers this year.

New regulatory requirements for security

California recently passed legislation that requires businesses to tell their customers when unencrypted data has been released — whether that release was accidental, intentional, or the result of a malicious act. If the business does not tell its customers of a security breach and is found out, huge fines could be the result. Notice that the law says *unencrypted* data. If your data is encrypted, you may have nothing to worry about!

Both the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA) have certain requirements for companies to protect personal data. If the data is not protected adequately and personal information is released, the end result could not only be huge fines, but jail time for top management, too. However, if all of that data has been encrypted, it's very likely that you can show due diligence in trying to protect your data. If you can show that you have done everything possible to protect your data, you may be able to save yourself from lawsuits and cumbersome fines.

If you think the California law and the two acts mentioned above are the only regulations you have to be concerned about, think again. The FTC has recently taken on the mantle of the protector of privacy rights, and they are not shy about prosecuting businesses. Even Microsoft has run afoul of the FTC and now has to comply with imposed security regulations and audits for the next 20 years. Think of the savings that would have been made if Microsoft had implemented their own encryption technologies — it would have saved them 20 years of submitting to audits and preparing reports. That would have been a huge positive ROI.

Cost of cryptographic system(s)

This is the main figure to start from, and it's the one that management is probably going to complain loudest about. Some solutions can be fairly simple and not altogether expensive. For example, if you plan to implement e-mail encryption only, you may consider S/MIME, which has many freeware components. On the other hand, a full PKI system that handles secure e-mail, encrypted files, and standard document exchange protocols is a very pricey investment. However, you must consider any cryptographic system as an

investment in ensuring your network security. If something reduces your risk of catastrophic events, then that isn't such a bad thing.

In addition to the encryption software programs or suites that you plan to buy, you will probably need key servers and certificate servers, too. You may be able to utilize some existing hardware if it is currently in excess of your needs. Remember to add the cost of training and administration for the system, too.

To add a positive figure to the cost of the system, see if the increased security enables your business to enter new markets that were previously closed to you. For example, does encryption give you an edge over your competition that would allow you to take some of their business? Or does the use of encryption allow you to partner with or at least work with European companies that have a much higher standard for data security? Check out the Department of Commerce "Safe Harbor" program. You could get your network certified by the Department of Commerce so you could work with European companies.

Think of other benefits that are likely to come about through the company's use of encryption. There may be lots of opportunities you may not have considered. Brainstorm with others in the company, and search the Web for ideas. Then present your case to management with all the positive aspects highlighted.

Government due diligence

As I mentioned before, there is new legislation that requires increased security, especially for personal data. If there is a complaint against your company, the government is duty-bound to investigate, and you better bet that they will. The government is very paranoid about network breaches allowing terrorists to gain entry to personal information and other sensitive data.

If the government decides to take a look at your network, they will do a complete security audit of your system. In addition, they will want to see documentation of all the security measures and mechanisms that you have considered, whether they were implemented or not. The government considers encryption a very good thing for network security. If your company can prove that you at least considered cryptographic systems to enhance your network security, you will be well on your way to showing that you exercised due diligence in considering every possible security solution. Many of the companies who have been recently dinged by the government with fines and 20-year oversight would never have had a problem if their data had been encrypted.

Insurers like it!

And last but not least is the fact that insurance companies are beginning to offer discounts for proof of increased network security. Insurance rates for businesses take a big bite out of the money bag, and the bean counters like to get every break they can. Like the government, insurance companies will insist on a full security audit, and the use of encryption adds a lot of positive check marks in the "good practices" column.

Presenting your case

Management is in love with PowerPoint presentations that are clear and well-designed. Get the best person on your team to put together the slides and don't try to cram too much information into each slide. Try to stick to just the highlights and good points for your bulleted items. Remember, you are going to be the salesperson to get them to buy into an encryption scheme.

Prepare a spreadsheet with all the figures you've assembled. Here's an example of what you might do:

Risks, Opportunities, and Solutions	***Cost***
Cryptosystem for encrypted e-mail and encrypted data storage	–$50,000.00
Labor (yearly)	–$75,000.00
Labor savings in reduced staff requirements (yearly)	+$100,000.00
Savings in reduced requirements for new storage capacity (servers)	+$90,000.00
Labor costs for disaster recovery for this system (yearly)	–$5,000.00
Labor costs for key recovery and help desk assistance (yearly)	–$3,500.00
Increased sales due to increased security (average 15 clients annually)	+$600,000.00
Total cost of system	+$656,500.00

Those types of figures should bring you a round of applause and possibly a promotion as well. In the table above, the negative amounts (–) are outgoing costs, and the positive figures (+) are savings or income for the company. In case you don't have a calculator, the figure I used for increased sales was an average of $40,000 per customer. You can probably get those figures from your marketing department. Just ask them how much, on average, each customer is worth to the company.

In the following sections, I look at some of the situations that would benefit from the addition of cryptographic solutions to your current list of security mechanisms.

Do You Need Secure Communications?

There are many ways that we communicate with others on computers, and 95 percent of those communications are not secured against secret listeners. You won't even be aware of the fact that your communications have been intercepted until or unless you suffer a security breach that can be related directly back to the messages.

Secure e-mail

If you aren't aware of it by now, let me tell you in no uncertain terms that e-mail sent in the clear can be read by someone other than the intended recipient. E-mail goes astray. E-mail servers get hacked. E-mail traveling across the wires gets snagged like fish in a pond. If your e-mail isn't encrypted, woe is you.

Imagine that you are working with an independent programmer who is building a new software program for you. Maybe that person sends you new code files every few days. Because your company is relying on this new program to make money for them, do you think it's a wise idea to be sending these messages in the clear? What if your competition got hold of the code?

In another situation, imagine that you are an investigative journalist and you correspond daily with a number of sources who send you very sensitive material. Maybe it's documentation of war crimes or human rights abuses. Maybe the head of a Fortune 500 company is engaging in illegal activities. Maybe you're trying to track down the source of drugs coming into your community. All of these communications should be protected via encryption to ensure the confidentiality and safety of the informants. I could come up with a million situations, but you get the general idea.

Given all cryptosystems available, e-mail encryption is probably the easiest and cheapest system to implement. By "easiest" system, I don't mean to

imply that the setup is without problems, but it is an awful lot easier than setting up a full PKI system.

The two most common solutions for encrypted e-mail are S/MIME *(Secure/Multipurpose Internet Mail Extension)* and PGP *(Pretty Good Privacy).* MIME was created as a standard for transferring or transporting different types of files attached to e-mails, such as GIFs, JPEGs, DOC files, and so on. The *S* in S/MIME indicates a standard for incorporating secure encryption standards into the protocol. In a perfect world this would work perfectly; however, as is usually the case, the various vendors have taken to interpreting the standards to meet their own needs. S/MIME works, but different e-mail clients use it differently, and the results are not always fabulous. On the plus side, S/MIME is cheap and is included in most e-mail systems and e-mail clients (such as Outlook and Eudora).

Because there are interoperability problems with S/MIME, it might be better to go with a vendor who has developed special implementations of S/MIME that have been altered to ensure better interoperability. Baltimore and ArcticSoft are two companies that come to mind with good products. These purpose-built systems tend to be pricey, but you get some good technical support in setting up and troubleshooting your system.

In Chapter 8, I show you how to set up S/MIME in Outlook and how to obtain the digital certificates needed to sign and encrypt your e-mail messages. You'll need a friend or co-worker to do it, too, so you have someone else to exchange messages with. (As I mention earlier, encrypted e-mail is like video phones — you need two people to participate!)

PGP has a very long and interesting history. To make a very long story short, it was created by a very non-techie person by the name of Phil Zimmermann at a time when the government was intent on keeping encryption technologies out of the hands of common people (1991). At that time, the only legal use of cryptography was by the military or government systems. The government filed charges against Zimmermann for violating export violations and six long years later, the government dropped the charges. Today PGP is a corporate entity, and its use has become a type of standard and is probably the most widely used e-mail encryption software in the world.

PGP is available as freeware (GnuPGP) or as commercial software (PGP Corp). It's an encryption and key-sharing protocol with a user interface to use with popular e-mail programs such as Outlook or Eudora. Its first interfaces were horrible and did a lot to scare people away from it, but the new versions are much nicer, and the program inserts buttons in the e-mail command bar of your e-mail program. However, for individual use it still takes some rooting around the manual to figure out all the intricacies of the product. The enterprise versions for company-wide installations are a good deal because of the ability they give the administrators to fix things such as lost keys. I give it a big thumbs-up because of its wide use and the relative ease of installation. It also interoperates well with older versions of PGP, so you don't have

to worry that your correspondence can't be decrypted by the recipient. Another plus to PGP is that it has the ability to encrypt files and storage, where S/MIME does not have that capability. In Chapter 8, I give you some basics on setting up PGP.

Instant Messaging (IM)

Only a few years ago the world of IM belonged to teenagers. If Mom told her daughter she couldn't use the telephone to call her friends until her homework was done, she got on the computer and immediately initiated online conversation with all of her friends. Poor Mom didn't know her daughter wasn't doing her homework, and chances are that her friends' moms were just as clueless. Well, it doesn't take us old farts very long to catch on, and soon we took IM to work. Now your boss thinks you're preparing the big proposal that will land you millions, and you're actually berating your friend across the country over his poor choices in the football pool.

You'd better not be discussing this big proposal on IM, though, because IM in its default installation not only introduces all kinds of security holes into your network, but almost anyone can read your messages, too. Whoops. There went your million dollars to the competitor and, by the way, hackers used IM to get into your network and are using it to distribute illegal MP3s. There have also been cases of people in the IT department snooping in on IMs to get information about impending layoffs.

To the rescue are secure IM servers and clients. The market is currently flooded with competitors like JabCast, Jabber, Bantu, and Ikimbo, to name just a few. They are reasonably priced (sometimes even free), and some systems come with a secure IM server as well as secure clients. Some of the programs use symmetric key encryption (the same key encrypts and decrypts) while other programs allow you to use public/private key pairs (you encrypt with your private key; the recipient decrypts with your public key). If you use your own IM server, all text is encrypted as it travels across the wires and as it sits on the servers. If you are using a public IM server, be sure you trust that server and find out what its security policies are.

Secure e-commerce

Any Web server that collects private information from customers should be considered an e-commerce server, and all possible protections should be implemented. Traditionally, only Web sites that conduct sales or financial transactions have been considered e-commerce servers, but I want you to think outside the box. Because of new privacy regulations, it may be in your best interest (and your customers!) to make your Web site more secure by using encryption.

California declares encryption a necessity

The California Encryption Act, as it is sometimes referred to, is very interesting because it is the first in the nation to be passed. It went into effect July 1, 2003, and businesses and security experts are waiting to see if it will stand up in court. Basically the Act says that if you have names and other personal information such as addresses or Social Security Numbers, you must protect that data. Encryption is an acceptable form of protection, but encryption of the data in transit is not enough. In short, SSL and S-HTTP are not good enough. You must encrypt the database and/or servers containing the information. In addition, if the information is stolen or released, you must notify people of the security breach. The Act is strongly worded, and it remains to be seen if other states adopt this stance.

Most secure Web servers use SSL *(Secure Sockets Layer)* and/or S-HTTP *(Secure HyperText Transfer Protocol).* Both of these options will encrypt the data as it travels across the wires to prevent the hijacking of information in the clear. On the other hand, these options do not encrypt the data that stays on the Web server or that is transferred to the database server. To be totally safe, you should encrypt the data on both the Web server and the database server.

Whether or not you use SSL and/or S-HTTP, you should know that the default installation of Web servers introduces train-sized security holes into your network. That's because traffic to and from a Web server is supposed to be anonymous and, if the Web server is behind a firewall, you have to allow this traffic through the firewall. The default installations also frequently include scripts and default directories that can be used against you. So, if you plan on going into e-commerce in the future, be very, very careful and implement the best security possible. If you already have e-commerce up and running, then you need to double-check your security policies and procedures — and you really need to consider encrypting the data at rest, too.

Why the concern? Well, there are departments within the Federal government and agencies within state governments that impose severe penalties on companies that even inadvertently spill personal data. If you accidentally send out a customer list with personal information to all of your customers, you will be caught and charged. If a hacker gains entry to your Web server, database, or other network server and can gain access to personal unencrypted data, you will be found out and prosecuted. In fact, a new California state law states that if you have the personal information of even one California resident on a server, it must be encrypted — even if your servers are not located in California.

Online banking

Online banking is just another form of e-commerce. You're collecting and disseminating personal information across the Internet. The Federal Gramm-Leach-Bliley Act of 1999 laid down regulations on safeguarding personal information collected, especially if the collecting is done online. And you don't necessarily have to be a bank to fall under the shadow of this Act, either. If you handle information for banks, or if you counsel people on debt reduction, you will have to provide the following to the government:

- Risk assessment results
- Risk management decisions
- Results of testing for security weaknesses in your systems
- Attempted or actual security breaches or violations
- Responsive actions taken to breaches or violations
- Recommendations for improvements to the information security program (on a regular basis)

That's a lot for some small companies or nonprofit organizations to bite off and chew. Again, encryption of your data in transit should be imperative, and you'll have to show that you gave strong consideration for encrypting the data at rest. If you suffer a serious breach and you can't show that you did all you possibly could (with the technology available at the time), then the FTC is going to take a big bite out of your bank account and certain company executives could end up wearing special jumpsuits for a long period of time.

In addition to protecting the data coming, going, and resting, you should also be making sure that the user logon IDs and passwords/passphrases are encrypted. It won't do you any good to install all kinds of fancy security mechanisms if people can get the UserIDs and passwords with little or no effort.

Virtual Private Networks (VPNs)

When businesses communicate over the Internet, there is no protection promised or implied. Everything is done out in the open and can be seen, captured, destroyed, or copied by anyone who cares to try. It's like cities, towns, and villages connected by roads. You transport whatever is on those roads at your own risk. Businesses began to see the need for a safer alternative as they did business with remote partners and employees in remote locations. Thus, the *Virtual Private Network* (VPN) was invented.

VPNs use encryption to protect the traffic between any two points. It's like building a tunnel with special access controls between those cities, towns,

and villages. The tunnels aren't available to everyone, and to the people up above, they are invisible. Before you can enter the tunnel, you must prove your identity, your packages must be of certain types, and the delivery address must be verifiable. If that isn't secure enough for you, a VPN also has the ability to disguise the packages through encryption, too. That way, if someone manages to gain unauthorized access by fooling the access guards or by digging another tunnel that intersects with your tunnel, the intruder won't know which packages to steal because he can't tell one from another.

VPNs have been around for enough years now to consider them a standard security mechanism. On the other hand, the way vendors create their VPN hardware and software is not necessarily interoperable. If you are communicating with someone who doesn't have the same sort of setup, it may take a few days or weeks of juggling cables and commands to get it working correctly. In general, VPNs are considered fairly reliable as far as security mechanisms go. Sure, there are hacks, but you really don't hear about too many of them. Either they are not happening often, or companies are just not telling.

VPNs are capable of encrypting two different ways: *transport* and *tunneling*. The transport encryption sets up a secure, encrypted link across the Internet wires, and it encrypts the data (payload) you are sending to the other end. This is the equivalent of the delivery truck carrying a package via the underground passageway. (I'm not using the word *tunnel* here because I don't want to confuse you!) The encryption is invisible to the user — other than passwords, passphrases, or a special card to plug into the computer, the user doesn't have to press a button that says "encrypt" or "decrypt." All the data in transit is protected from sight. The only drawback to transport encryption is the fact that the headers on the data are sent in the clear. In effect, that's like disguising the package and then putting a label on it that says what's inside. Maybe not the smartest thing to do considering that intruders may occasionally gain access.

The other form of VPN encryption, tunneling, not only sets up a secure, encrypted link between two points, but it also encrypts the headers of the data packets. That's better. Not only do you have a disguised package, but the address and the contents listed in the package's label are in code so it's not easily recognizable. As I mention earlier, the VPN standards aren't necessarily standard, so you'll have to see what protocols the vendor is using. The vendor will have tons of transfer protocols to choose from, but the tunneling protocols are fairly limited. Just to give you an introduction, here are the tunneling protocols:

- GRE = Generic Routing Encapsulation
- IPsec = Secure Internet Protocol
- L2F = Layer 2 Forwarding
- PPTP = Point To Point Tunneling Protocol
- L2TP = Layer 2 Tunneling Protocol (PPTP + L2F)

If you set up a VPN for your customers, business partners, and employees, they can gain some comfort in the fact that their data isn't traveling in the clear. One point to remember, though: Many road warriors have automated the process of logging in to their VPN and have a shortcut on the desktop. On top of that, a laptop is not properly protected with proper access controls — turn it on, and it's yours. In that instance, a stolen laptop can easily be used to log on to a VPN, and you'd never know it unless the employee alerts you. In addition to access controls for laptops, you may also want to consider disk encryption to protect the data stored on the laptop. Just something to keep in mind.

VPNs are relatively easy to set up now, and you can usually find experienced staff to install and manage them. As I mention earlier, sometimes it takes a little effort to get two different VPNs talking to one another, but that doesn't last forever. Many vendors are including VPN capabilities in their routers so the system is practically "plug and play." Just remember to change the default settings such as the administrator password. VPNs are great at protecting the data in transport, but they do not encrypt the data on your drives — that data is still in the clear.

Wireless (In)security

If you haven't heard about wireless networking yet, you need to get out a little more often. Nothing has created such excitement as the introduction of "portable computers" in the '80s. Now we not only have portable computers (our laptops, of course), but you can sit in a café, in a park, or in your back yard and connect to the Internet. No wires. No hassles. Just free and easy surfing the Web. Well, for every upside there has to be a downside, right? That's certainly true for wireless networking. By default, anyone within radio wave distance can use your Internet connection and probably can hop on to your network as well. Shortly after wireless networking made its appearance, hackers created very small software programs that search the airwaves for unprotected wireless networks. And believe me when I tell you that there are tens of thousands of unprotected wireless business networks in America alone.

The act of snooping for wireless networks is called *war driving,* so called because you can do it while you drive around town in your car (with a laptop inside). Teams of people have a war to see who can gain access to the most networks. (It also refers back to an old practice of "war dialing," in which a hacker used a special modem that continually dialed telephone numbers in sequence in order to find modem tones to find networks.) Lists of open wireless networks can be found on the Internet, and in some cities the war drivers mark the sidewalks with chalk to indicate where the network is located and what you need to do to log on *(war chalking).* That's why I called this section wireless "insecurity." Wireless access points and wireless network cards are so easy to install that I doubt it would confuse a three-year-old. Even your grandmother can do it!

Wireless networks do have some security capabilities, and one of them currently in use is *WEP* (Wired Equivalent Privacy). Don't stake your life on WEP, though, because it's only an equivalent of security; it isn't real security. WEP encrypts the packets going out over the air. It doesn't encrypt them particularly well, though, and much of the information about the network is sent in the clear. There are many hacker programs available that can crack the basic configurations of WEP, too. AirSnort and WEPCrack are two popular programs. Of course I should also mention that WEP is much better than using nothing!

Given the number of business networks that appear on the war-driving Web sites, not many people have gotten the hint to at least turn on WEP, and even fewer know anything about securing WEP properly. I discuss this in depth for you in Chapter 13.

Because WEP employs fairly weak encryption, you can add to the security by adding a VPN and an authentication process. This will greatly enhance your security, but you should never give a wireless network totally trusted status. In the near future there are supposed to be more secure versions of the wireless protocol appearing, but they haven't quite made it yet. You can buy totally secure, NSA-approved wireless access points from Harris at about $5,000 each, but I doubt that many organizations will want to lay down that sort of money. The NSA has tested the encryption on the Harris wireless networks and found them to be safe. Well, probably not safe from the NSA, but you probably won't have any problem with war drivers.

Do You Need to Authenticate Users?

If you aren't concerned with who is using your network and its resources, then you probably don't care to implement any form of authentication. If, on the other hand, you want to know who's on and control where they go, then you'll have to at least list your users, give them logon accounts, and assign them passwords.

Authenticating your network users is one of the big bugaboos of network security. Currently the majority of networks around the world only require a valid User Name (UserID, Logon Name) and password to give a person access to files, directories, databases, and all other forms of network goodies. That's all well and good, but it really does nothing to ensure that the person who is logging on is really the person he's supposed to be. It turns out it's quite difficult to verify users' identities from a remote location. When you have thousands of users on your network, you can't realistically spend time verifying users by phone call or video links.

There are a number of very good authentication systems that utilize encryption. The encryption is used for a number a reasons, but mainly it is used to create and pass digital certificates and to encrypt the transmission of data between people and/or computers. I've included much more about cryptographic authentication systems in Chapter 10.

Who are your users?

Do you really know if your customer, Bob Jones, is really who he says he is? Yeah, you probably got a request from your client to create an account in his name and add him to the access list, but unless you've actually spoken to and met Bob Jones, do you really know who he is? Another point, when Bob Jones logs on to your network, can you really be sure it's him? Maybe he gave his logon and password to a co-worker to use. Maybe a hacker guessed the password and is using that account. You have no way of knowing whether or not the users currently on your network are who you think they are unless you take pains to authenticate them accurately.

The problem with most network logons, e-mail, and Web transactions is that there is a certain amount of *plausible deniability* involved. That is, the person who supposedly logged on, sent the e-mail, or bought something on the Web can deny he or she ever did it. And this is completely legal. The reason for this is that you can't verify, without a shadow of a doubt, that the person on the other end of the action is really who he or she appears to be.

Say that Mary Jones sent a libelous e-mail about you to everyone in the company. Mary is called into the office by the CEO and asked to explain her actions. She can deny she sent the e-mail, and the company would have to prove otherwise (presumption of innocence, you see). Mary could say that she walked away from her desk to go to the restroom and she forgot to lock her computer before she left. It's possible that one of her co-workers sat down at her desk while she was away and used her e-mail program to send the message to everyone. Don't laugh — it's happened.

The only way you could prove that Mary sent the e-mail would be if you had a strong authentication system. Strong authentication basically means submitting at least two out of three forms of identification: something you have, something you know, and something you are. It's not unlike paying for your groceries by check. In addition to your signature on the check, the cashier will also request another form of ID, like a driver's license. You've submitted something you have (driver's license) and something you are (your unique signature).

Encrypted tokens, certificates, signing keys, and biometrics are just some of the additional forms of identification you can submit in addition to your UserID and password for network access. I discuss some of these and more, coming up next.

Authentication tokens

Authentication tokens come in many forms and are designed to hold information about the owner's identity that is verified via special servers. In addition, the tokens are handed out in person, so there is verifiable evidence that the token was given to the correct person. Tokens usually employ a high degree of security, like encryption of the data, and most will destroy the data if the token is tampered with.

Proximity cards

Prox cards, as they are sometimes called, have small radio transmitters in them that send coded signals to specially built receivers. The receivers are programmed to accept only certain persons or restricted access codes. Each prox card transmits a unique code for each person. A log is created of the time and place of access. A prox card itself can't be a strong authenticator because it can easily be given to someone else. However, when combined with a PIN, you achieve two out of three factors for strong authentication. These systems are usually the most inexpensive to implement, but that doesn't mean they are cheap!

Contact cards

These tokens are like credit cards with a magnetic strip on one side. The data on the magnetic strip is encrypted when it's created. You slide the card through a special reader and the data is transmitted to a special database or authentication server. Again, these are most secure when used in conjunction with a PIN or password.

Challenge/response generators

Remember the old war movies where the guard on duty challenged the stranger wanting to enter the restricted area? The conversations usually went something like this:

Guard: Halt! Who goes there?

Stranger: A friend.

Guard: What's the secret password?

Stranger: The Yankees are playing the White Sox.

Guard: Thanks, you can enter.

That little scenario is referred to as *challenge/response* because the guard challenges the stranger to come up with the correct response. Challenge/response generators are the same idea but updated for the cyber age. The user has a card that resembles a calculator or small PDA. When the user logs

on to the network, a special server recognizes the UserID and sends a challenge in the form of a number, word, or phrase to the user's computer screen. The user enters that challenge into the challenge/response generator, and it uses a special algorithm to come up with the correct response. Finally, the user types the response on his computer keyboard and the system gives him access.

This is a pretty good form of authentication because it uses both the UserID and password (something you know) and the challenge/response generator (something you have) that is interactive rather than passive. To increase the security and authentication, most challenge/response generators are also protected by a PIN. That gives the system two instances of something you know and one instance of something you have.

One-time password generators

We're just generating up a storm here! (You can groan now.) Very similar to the challenge/response system I've just described are the one-time password generators (also known as *OTP*). As with the previous system, you need to have special servers for this process and the servers must sync with the OTP generators to create the password. This type of system has proven quite successful.

The user enters a secret passphrase into the OTP generator, which transfers the data to the server. The server takes the passphrase, seeds it, and then goes through multiple iterations of secure hashes. The result is a code that is changed into human-readable form and sent back to the OTP generator. The user simply types the password, and he's in. This system also allows the user to log on to multiple stations, each time with a unique, one-time password.

Smartcards

Smartcards have often been touted as the hottest new technology, but the lack of standards has really put a damper into the product taking off like bottle rockets. Their use in the United States is slowly rising, but they've become very common in Europe for use as transit cards, health information for providers, and credit information. Americans seem afraid to have that much sensitive information stored on a little chip on a piece of plastic the size of a credit card.

For authentication, smartcards are great because they can carry any and all types of information: digital signatures, encryption keys, personal data, and even biometric information. The trouble is that there are six different standards for the type of chips used and the type of information each chip can store. Interoperability becomes a problem. But, if you're using a single vendor for your smart card needs and it's only used in-house, it could be the answer for you.

There is a lot that these various types of smart cards are capable of handling in regards to authentication. Some of the smart cards have cryptographic processors in them to be able to create new encryption keys on the fly. These cards can sometimes store digital certificates and digital signatures as well as biometric information, like a fingerprint. The next couple of paragraphs fill you in on some of the jargon used with these cards because it can all quickly become very confusing. After reading the sections below, you should be able to speak with a smart card vendor and know what he is talking about.

Memory cards

These types of smart cards can store only static information and cannot work as a computer processor. There are different data types and different degrees of security, depending on which type of memory chip is used. There are three main types of memory cards: *standard*, *protected*, and *stored value*.

- **Standard** cards are like unlocked floppy disks — they store data that can be overwritten and so should not be considered terribly secure.
- **Protected** smart cards can write-protect the data and can restrict access with a password.
- **Stored value** cards are the best of the memory cards. They have security mechanisms that are hard-coded into the chip. These usually don't store data files; rather, they store values such as encryption keys, hashes, or digital certificates. These cards also have "counters" in them that can limit them to a finite number of uses. When the counter reaches the end, you can either have the card recharged or simply throw it away. They're great for infrequent users because it doesn't matter if the user loses one, and you can set a limit to the number of times a guest can access the network.

Microprocessor multifunction cards

These cards are like their own little computers on one little bit of circuitry. They have their own operating system, file allocation, and access controls. It's amazing how computers went from the size of entire rooms in the 1970s to the size of a pinhead at present. These are the best cards to use when the security token is needed for a number of functions. Not only can this card store symmetric and asymmetric key pairs, but it can also house multiple digital certificates and the cryptographic software needed for special functions and interactions.

Java tokens

Java tokens come in smart card forms and buttons the size of a flat battery. Their coolness factor is very high, partially because they are programmed with the Java programming language and because they are almost exclusively

used to perform cryptographic functions. The cards are known as *JavaCards,* and the buttons are commonly referred to as *iButtons*. The iButtons can be inserted into rings, dog tags, watchbands, and any number of wearable holders.

The JavaCards are usually interoperable with other smart card systems that follow the PKCS #11/Cryptoki standards. Cryptoki (pronounced *crypto key*) is an API *(Application Program Interface)* for devices that hold cryptographic information and perform cryptographic functions. Because the iButtons require specially shaped readers, they can't be used with smart card reader systems.

The iButton contains a microprocessor similar to the one you might find on a smart card. It is capable of storing cryptographic functions as well as any form of cryptographic key you can imagine (digital signatures, symmetric keys, asymmetric keys, message digests, and so on). It has the ability to perform 1,024-bit public key operations, too. In addition to storing crypto functions and keys, it can store personal data such as driver's license information and medical information. The iButton has a tamper-proof case and if anyone tries to pry it open, all information will be destroyed.

Biometrics

How many movies have you seen where the good guys place their hands on a scanner to gain entry to the lab? You've probably also seen eye-scanners, voice authenticators, and fingerprint scanners on TV and in movies. But for some reason, most Americans see the use of these products as the downfall for liberty and freedom. All a biometric device does is measure a certain characteristic of the human body. The machine does not store the actual fingerprint, voiceprint, or iris scan. It stores a mathematical equivalent of the characteristic. When you submit your body part to a scan, it converts what it sees to math and then compares that mathematical figure to the one stored in the database. No one can actually steal your fingerprint because it doesn't look like a fingerprint.

Nonetheless, biometrics are expected to provide a higher level of security than other forms of authentication because the biometric trait (your finger, eye, or voice) can't be easily lost, stolen, or duplicated. A biometric provides undeniable authentication. Of course there are arguments that a fingerprint can be copied and a voice recording can fool the device, but how often is this likely to happen? In reality, hackers go for the soft, easy targets like bad passwords and security holes in operating systems. Why would they focus their attention on getting *one* form of authorization when they can get literally hundreds with a password cracker? Unless you are a secret squirrel working for an unknown spy agency, I doubt that anyone would go to the trouble trying to crack your biometric trait.

To enable biometrics, you must first scan the part of the body that is going to be used for identification. When that is done, a template for that person's body part is created. The template contains the mathematical equivalent of the scan as well as some parameters for future acceptance. These parameters can be set from very loose to very strict. When the body part is offered for identification, it is compared to the template — there will never be an exact match, so the parameters in the template are consulted. If the template offers a loose interpretation of the scan, you might allow access to someone with attributes similar to the owner. If the parameters in the template are too strict, then even the real owner of the attributes might never pass again. The trick is to create a happy medium. In that way, you keep out possible imposters and you don't make the actual owner scan over and over again to get a positive match.

Do You Need to Ensure Confidentiality and Integrity?

When your company has spent tons of money in research and development (R&D) of a new product, you want to guarantee that the data stays on your system and that no changes have been made to the latest build. The same is true for sensitive proposals, financial data, and anything else considered a trade secret. Many companies understand the need to use firewalls, intrusion detection systems, access controls, and so on to protect the data from theft, but few are considering masking or hiding the data through the use of cryptography.

Additionally, personal data needs to be protected so its theft can't be used for identity theft or other nefarious purposes. The Department of Homeland Security is concerned about terrorists stealing personal data and assuming the identity of bona fide American citizens because these people are unlikely to be caught on visa violations.

There's one more thing you should consider: How valuable is your data if you can't ensure that it hasn't been changed and contains erroneous information or malicious code? It won't do your company's reputation much good if the data you sell is not dependable.

Protecting Personal Data

This goes beyond protecting the private, personal information of individuals just because the government has told you that you must. Protecting the privacy of your customers and clients is a good thing, but it shouldn't take an

act of Congress to make you incorporate that type of security into your total security solution. There are times when you may need to protect a person's identity to protect that person from real or imagined harm.

If you are required by law to protect personal data, saving it in encrypted form will pass the government's due diligence test if it's ever stolen. That is, if you use encryption, the government will likely rule that you did all you possibly could to protect the data. In addition to making the data look like scrambled eggs in digital form, it can also be used as a form of access control if you give only the keys and/or passphrases to open the data to certain people. If someone other than the authorized group opens the data, then you can be certain that there is a security problem inside the company.

Think of people in witness protection programs. All of their data has to be locked up tight so the bad guys don't figure out who they've become and where they've moved to. Data encrypted with a good algorithm and a very long key would be next to impossible for the bad guys to break. Again, unauthorized people would not be able to decrypt the data. The same holds true for people who give aid in countries torn by civil war, political uprisings, or other forms of unrest. Attorneys wouldn't want their defense strategies read by opponents, and political candidates for office wouldn't want their opposition to know their campaign strategies.

What about the software you spent so much research and development money on? You wouldn't want your source code to suddenly appear on the Internet. Likewise, you need to guarantee that your customers get what they paid for. There have been cases where software was shipped containing back doors to security, Trojan programs, and viruses. If the software had a message digest or checksum, then you can discover if the code had been changed from the original.

There are thousands more situations where companies need to protect the confidentiality and integrity of the data they store, transmit, and/or sell. Encryption is an easy way to accomplish both tasks. A file full of encrypted gobbledygook is indecipherable. Its confidentiality is protected because the contents of the file can't be read, and its integrity can be guaranteed because it would do no one any good to make changes to an indecipherable mess.

File encryption can save storage space because some systems compress and encrypt data. It remains accessible to those with the keys and/or passphrases, but it's almost worthless to steal. There is no time limit to storing encrypted data, so you can rely upon it for the long term. Even if you do a bad thing like put your database on the same server as your Web server, a hacker can't use the security holes in the Web server to come away with anything useful.

Encrypted e-mail is also included here because after you encrypt a message, it stays that way. Hacking the e-mail server won't decrypt encrypted messages. If you remember to encrypt e-mail attachments as well (and that should be standard practice), that data is protected, too.

There are literally thousands of companies that offer long and short term encrypted storage solutions. They vary in cost depending on the amount of storage you need and the type of encryption you want to include. This is not necessarily the time to go with the lowest bidder because you want to make sure that you have the ability to recover lost encryption keys. Not all companies or products offer that capability.

What's It Gonna Cost?

I'd love to be able to give you a chart, spreadsheet, or even a rough idea of what your solutions are going to cost you. Unfortunately, asking how much encryption is going to cost is a lot like asking how much a car is going to cost. The answer is, "It depends." It depends on what you need, what you decide to implement, how much support and training you need, and what systems you are currently using. It wouldn't do you any good for me to recommend a solution for UNIX systems if your network is totally Windows-based. Likewise for Macs or special network transports like ATM.

You'll need to do your homework on the Internet for the solutions that suit you best. Some you'll be able to install and run yourselves, and others will require a team of specialists to get it up and running. Again, it all depends.

One thing to keep in mind, however, is interoperability. You need to be able to continue to operate with other offices, your customers, and even employees on the road. Ask yourself if you plan to change systems anytime in the near future. Talk to your customers to see what they are running and what their needs are. As I mentioned before, cryptography is a two-way street and you can't do it alone. You need to have your partners in-step and in agreement with your decisions so your ultimate roll-out will be as smooth as possible.