Chapter I

Analyzing Risks to Determine a New Return on Security Investment: Optimizing Security in an Escalating Threat Environment

Warren Axelrod, United States Trust Company, N.A.

Abstract

This chapter expands upon standard methods of calculating the return on security investment (ROSI) in several ways. First, it accounts for the dynamic nature of threats, vulnerabilities, and defenses as they apply to the finance sector. Second, it takes a more holistic view of security investments using a portfolio method. The protection of information assets can be viewed in two ways. One is the hierarchical view of security measures, such as avoidance, deterrence, and prevention. The other is defense in depth, wherein various security tools and processes, such as firewalls, identity and access management, and intrusion detection and prevention products, are combined for greater overall protection. The reader will gain a deeper understanding of the factors that affect the risks and returns of investments in security measures, tools, and processes and will find that using the portfolio approach leads to more cost-effective security.

Background

The year 2005 became known as the year of the privacy breach, although the first half of 2006 is shaping up to be its equal or worse based upon the breaches reported. Security breaches involving personal information are announced in the press almost daily, and there are Web sites that track these incidents. Some of the more noteworthy recent incidents involving lost or stolen personal data are described in Appendix A.

The direct costs to individuals and companies from such breaches have increased by orders of magnitude during the past couple of years. This has in large part been due to recent laws and regulations that impose financial burdens and damage to reputation as a result of mandated or strongly suggested actions, such as customer notification, provision of credit monitoring, and the like.

In addition, regulators have begun to levy substantial fines and are requiring costly remediation and long-term auditing of those found not to protect customer data adequately. A number of U.S. examples, including Petco, ChoicePoint, CardSystems, and DSW Shoes, can be found on the Web site of the Federal Trade Commission (FTC) at www.ftc.gov. Resulting costs to companies are frequently orders of magnitude greater than what it would have cost to avoid or prevent these incidents in the first place.

The chapter covers the following topics:

- A brief history
- Nature and scope of breaches
- Security and privacy options
- In-depth defense strategy
- ROSI by category and in aggregate

A Brief History

In the late 20th century, the determination of how much to spend on security was mainly based on highly subjective analyses. First, statistics relating to the number of threats and successful attacks, cost of remediation, and costs of successful attacks (by viruses, worms, hacks, etc.) were collected and tallied up. The out-of-pocket costs thus estimated were further subjected to a risk analysis, where some "guestimates" of the chances of particular events occurring and the related level were used to determine expected loss. The *2005 Tenth Annual CSI/FBI Computer Crime and Security Survey* stated that the 639 respondents to the survey, who were able to provide estimates of incurred losses, suffered losses of $130 million in total, with the loss per respondent dropping 61% from 2004 (Computer Security Institute/Federal Bureau of Investigation, 2005). Analysts used that estimated loss as a basis for deciding how much should be spent on security measures. A positive return was achieved if the cost of security implementations was assessed to be less than the expected losses, which the security measures were to prevent.

While it was recognized that there were other risks and losses that might be affected by not having adequate security measures, it was mostly possible to justify some reasonable level of security expenditures from avoidance of viruses and hack attacks alone. Intangible costs, such as those relating to loss of reputation from the publicity surrounding a breach were seldom, if ever, identified and quantified, explicitly. However, it is no longer possible to ignore the indirect and intangible costs, since they dominate so many situations these days.

Highly Regulated Environment

Over the past several years, there has been a proliferation of laws and regulations advocating, and often mandating, tighter and more costly security processes for financial institutions. Recent laws in the United States, such as the Gramm-Leach-Bliley Act (GLBA), which is officially known as The Financial Services Modernization Act of 1999, and California Senate Bill 1386, focus on restricting access to and consequent misuse of customers' personal information. These laws have been followed by regulations, such as the Federal Reserve Bank's Regulation P for banking institutions and Securities and Exchange Commission (SEC) Regulation S-P for securities firms, and guidance papers created by groups of regulatory bodies. The recent rash of reported incidents of theft and loss of customer information (excerpted in Appendix A) has generated a further flurry of legislative initiatives at the federal and state levels, with attempts by Congress to supersede the proliferation of inconsistent, and sometimes contradictory, state laws. It is not clear how this will all shake out.

While the Sarbanes-Oxley Act of 2002 (SOX) did not appear to specifically address security, it has been generally recognized that there are implicit security-related requirements in the act. Examples of these include the controlling of access to certain information and restricting the ability of those with authorized access to modify the financial records of the company. SOX also addresses maintenance of the integrity of such data and its availability to authorized users when needed. The focus of such controls is on financial data rather than personal information. Nevertheless, the ability to control access to and use and modification of data is common to both GLBA and SOX so that, indirectly, compliance with SOX implies a measure of compliance with GLBA. While the argument might seem to be somewhat convoluted, I have seen a number of cases where such transference has in fact occurred.

Regulators, such as the SEC, also have focused their attention on how sensitive information should be erased and media containing such data destroyed. More recently, there have been a number of reports from government agencies, such as the Federal Financial Institutions Examination Council (2005), on identity theft and how it might be attenuated.

For affected organizations, this veritable flood of legislative and regulatory interest in the protection of personal information has raised the stakes considerably. It also provides organizations with the necessary justification for adding security controls and resources, whether or not a comprehensive cost-benefit analysis would favor such implementation. Particular measures, which might be favored by lawmakers and regulators, might result in the suboptimization of spending on security from the general data protection perspective. In fact, many of the proposed measures are aimed at solving what are arguably relatively small components of the overall problem. Be that as it may, such laws and regulations are intended to resolve certain high-profile issues, such as identity theft and fraud, and place responsibility squarely on the shoulders of senior executives of affected companies. This

latter aspect is probably the most important of all because without the enforced commitment of senior management, many critical security investments would not be approved.

Nature and Scope of Breaches

The population of compromised organizations includes such major firms as Bank of America, CitiFinancial, Ameritrade, LexisNexis, ChoicePoint, Time Warner, CardSystems Solutions, Marriott, and the Veterans Administration (VA). The CitiFinancial loss of tapes opened up 3.9 million personal records to possible abuse, and the CardSystems Solutions hack exposed personal information of 40 million members of MasterCard, Visa, American Express, and Discover to potential fraud. A laptop stolen from the home of a VA employee reportedly contained the personal information of some 28.6 million veterans and others. ChoicePoint has been fined $15 million by the Federal Trade Commission, in addition to other costs incurred. CardSystems lost significant customer business and was quickly bought out in its weakened state.

Ironically, in many cases, the data might not have actually been misused or otherwise compromised, particularly if devices or media items, such as laptops, magnetic or optical disks, or magnetic tapes, were lost or mislaid rather than stolen or purposely attacked and successfully invaded. For example, the above-mentioned VA laptop was subsequently recovered and a forensics analysis of the machine indicated that the data had not in fact been compromised. However the VA had already incurred significant costs and been subjected to severe embarrassment and criticism prior to the retrieval of the laptop and accompanying storage device. Also, if equipment is stolen for its intrinsic value rather than the data contained in its internal media (such as hard disks in laptops or flash memory in handheld devices), it is less likely that the data will be compromised. Nevertheless, costs of customer and public notification and remedial actions can be huge regardless of whether the misappropriated information was misused or not.

As of June 2006, some 32 states in the United States had passed breach notification and response laws. Some states require action on the basis of loss alone, regardless of what may have actually happened to the data. More lenient federal laws have not yet been enacted. As a result, many financial firms are taking a conservative approach by notifying customers and providing mitigation services to customers whenever devices or media are unaccounted for. In an excellent article by Smedinghoff (2005), he advises how companies should respond in regard to their disclosing security breaches to those who might be affected.

In its widely-quoted report *Lost Customer Information: What Does a Breach Cost Companies?* the Ponemon Insititute (2006) analyzed the results of a survey of 14 companies that had experienced data breaches. The Ponemon Institute found that the estimated total cost, which included direct and indirect costs as well as estimates of lost revenue, ranged from about $500,000 to $52.2 million, with an average cost per user in the $140 range. In one example, the cost per lost record was estimated at about $2,800, with by far the largest cost components being those relating to existing customers moving to other firms and potential customers deciding against doing business with any firm reporting a security breach.

Mimoso (2006) presents an excellent discourse on the aftermath of such incidents as they have affected security professionals. Five security managers, from such well-known organizations as LexisNexis, University of California at Berkeley, Georgia Technology Authority, ChoicePoint, and CardSystems, were asked about what they did differently after experiencing publicly announced incidents. Interestingly, even though the title of the article suggests survival, 40% of the original security professionals at these organizations had already been replaced. It is also of some concern that the remedies proposed in most cases only avoid the organization falling victim to the same threat as previously, rather than anticipating new threats and guarding against them also, as required for U.S. financial firms under GLBA.

While the above discussion references U.S. laws, there are many privacy laws on the books of a number of other countries. Here are a number of examples:

- Privacy Act of 1993 (New Zealand)
- Hong Kong Personal Data Ordinance of 1995
- Personal Data Protection Directive of 1998 (European Union)
- UK Data Protection Act of 1998
- Personal Information Protection and Electronic Documents Act of 2000 (PIPEDA) – (Canada)
- Privacy Amendment Act of 2000 (Australia)

Each has its own definitions, provisions, disclosure, and reporting requirements, and the like, so that multinational companies must allow for these laws and consequent regulations as they transact business across the globe.

It may be many years before there is a noticeable easing in the rate of increase of reporting such security breaches. After all, it is generally held that many incidents are not even reported to law enforcement and others. It is likely that the ratio of reported incidents to actual incidents will increase over time. This phenomenon will likely result in a continuing increase in reporting, as we are seeing in 2006, even if the absolute number of events were to go down.

As a consequence of this increased exposure, proposals to spend on security, which were previously rejected by management as not having a sufficiently high return on security investment (ROSI), may now show an excellent ROSI—or, perhaps more accurately, return on privacy investment (ROPI).

However, before going much further, we should define "security" and "privacy," especially as there is so much confusion and misuse of these terms.

Security is a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. The most widely used definition of computer security is confidentiality + integrity + availability (CIA).

Though the above CIA model has been generally accepted by security professionals, there are some, including this writer, who believe that the definition is inadequate because of its emphasis on protection. As a result of this focus, there are several important measures not being sufficiently addressed explicitly, such as deterrence, avoidance, awareness, and enforcement. I will write more on this later.

Privacy is, in a general sense, the interest that individuals have in sustaining a "personal space," free from interference by other persons and organizations. This definition and several other related ones can be found at Richard Clarke's (2005) Web site at www.anu.edu.au/Roger.Clarke/DV/intro.html. More specific to our discussion is "information privacy," which is defined as the interest that individuals have in controlling, or at least significantly influencing, the handling of data about themselves.

While privacy can be affected and enforced predominantly through security measures, it also should be noted that there are many aspects of security that are not aimed specifically at privacy.

Security and Privacy as Insurance

Spending on information technology (IT) security and privacy is similar to buying insurance. You can spend large amounts of money to buy security products and/or insurance premiums, but, if you are fortunate, you may never "collect" on either. You may choose to self-insure and possibly be hit by a catastrophic loss. You also may skimp on security and suffer major successful breaches and consequent losses. What it comes down to is the subjective estimates of the probability of a loss and what the corresponding magnitude might be; and what you are willing to pay to prevent and to recoup were such an event to take place.

Security measures today are heavily biased towards the prevention of incidents and limiting damage that might be caused by them. Insurance, on the other hand, is about survivability and compensation for losses. In fact, there is a trade off among prevention, protection, and survivability, since companies generally can elect to spend varying amounts on each aspect in order to maintain a desired level of physical, electronic, and financial protection.

In this chapter, we will take some well-established assessment models to demonstrate the impact of increasing risk and higher potential costs in the light of recent events, even though such models are often questioned in security and privacy circles. Recent events have pointed to areas of vulnerability not previously considered important. Current legislation and regulations have resulted in a much more painful and costly revelation process. Consequently both the *risks*, in terms of expectation of events happening, and the *losses*, in terms of the costs resulting from notification, remediation, and loss of reputation have all increased significantly.

Costs of Security Breaches

When a security breach is experienced, there are a number of costs incurred almost immediately and others that extend over time. Some, such as the cost of mailing notification letters, are tangible and easy to measure, while others, such as the loss of potential business, are intangible and can only be roughly estimated.

If a breach is internal and does not involve business partners or customers either directly or indirectly, it is likely that the costs, which can be tied to the breach, will be limited to those related to:

- Researching the root cause of the breach and its extent
- Ending further damage
- Repairing any damage done
- Restoring activities back to normal
- Coming up with means of avoiding recurrence in the future

Costs are likely to be limited to the time and effort needed to perform the above tasks. They can usually be readily calculated for both internal and external staff. The opportunity costs of diverting these workers to addressing the breach, resolving related issues, and not having services available need to be included also, even though they are much more difficult to determine.

If the breach extends beyond the boundaries of the organization, then a whole series of other costs and losses are incurred. This particularly applies when sensitive customer information is disclosed, stolen, or lost. In a June 2005 report, *Governing for Enterprise Security,* Allen (2005) of the Software Engineering Institute at Carnegie Mellon University, lists the following enterprise security objectives:

- Achieving and preserving trust
- Maintaining stakeholder value
- Demonstrating ethical and socially conscious behavior
- Maintaining compliance with new and expanding laws and regulations
- Ensuring that use and handling of data complies with the enterprise's information security and privacy practices
- Offering and fulfilling business transactions

Incidents, which might be detrimental to one or more of the above objectives, will undoubtedly lead to considerable measurable and intangible costs and losses. Those who were responsible for evaluating and instituting (or *not* instituting) the security measures in the first place will likely not have accounted for these factors.

Validity of Risk-Return Assessments

Assessing risks and returns on investment are well-established techniques for project prioritization and capital budgeting. However, some (including me) have raised questions as to whether such methods are fully applicable to security investments. The argument is that since security risk depends on many uncontrollable and unknown circumstances, in addition to which the vast majority of security incidents may never be reported, then estimates as the probabilities of events and losses relating to them are so inaccurate as to invalidate the process. In place of such risk assessments, Parker (2005) recommends that one substitute such methods as safeguard and application benchmarking.

Parker (2005) describes a series of losses, which may be incurred when incidents are publicly revealed, including:

- Efforts and resources applied to assisting in the investigation for law enforcers and legal counsel (these will likely include time of internal staff, costs of consultants and outside counsel, and computer-related and administrative expenses)
- Civil and, possibly, criminal litigation costs as a result of infringing laws and/or regulations, including the loss of time and attention of key staff who must testify
- The replacement of staff who may have left voluntarily or involuntarily, and the costs related to the termination of such staff and the hiring of new staff
- Damage to the victim organization's public image and reputation, including the costs of public relations and other communications, the loss of current and prospective customer business, and the efforts to explain the incident to management, customers, business partners, and shareholders
- Possible increases in insurance premiums, increases in deductibles, and reductions of coverage
- Loss of customer trust, market initiative, and competitive position and strength
- Losses from copy-cat attacks as previously unknown vulnerabilities might be exposed to a broad audience, including potential evil doers
- Costs related to shoring up the vulnerabilities by increasing security posture through acquisition of products and services and possibly outsourcing (or insourcing—depending on the nature of the incident) of security or operational functions and services

Axelrod (2004, p. 64) notes that with risk assessments, "… some costs might be hidden or excluded altogether, either unintentionally or through the analysts' ignorance or inexperience." However, the author points out a potentially more sinister aspect, whereby an analyst might purposely distort the information to favor a particular outcome. This is easily done, as estimates of the less tangible items can be highly subjective.

The Risk-Return Relationship

Let us now examine the relationship between security and privacy risks and the returns that might be expected from investment in security measures.

Risk analysis provides management with estimates of the expected losses from anticipated events. Expected loss, which is the magnitude of a loss multiplied by the probability that the loss will be incurred, is a potential cost to the organization. Conversely, the avoidance of a loss is considered a benefit or saving. In evaluating the benefit of a particular investment in security tools or services, we are looking at loss reduction and risk mitigation resulting from security measures as a benefit, in addition to any direct cost savings, such as from staff reduction, which might apply.

It should be recognized that the reduction in losses achieved by particular security measures will likely change over time as new threats appear, new vulnerabilities are discovered,

and experience is gained through handling actual incidents. In addition costs of acquiring and implementing security measures will change over time because of competition in the marketplace, obsolescence of existing products and services, and the creation of new tools and capabilities.

Assuming that one is able to derive risk-based estimates of the benefits of security measures, and the costs of such measures are available, then one of a number of evaluation methods can be derived (Axelrod, 2006), as described below. Also, Harris (2006) provides an excellent summary of risk management and methodologies and frameworks.

Cost-benefit analysis (CBA). The measure used here is the benefits-to-cost ratio and is simply the benefits divided by the cost. If the result is greater than one, then it is a favorable investment, as opposed to an unfavorable ratio of less than one. For example, if the benefit derived from a security measure costing $100,000 is $125,000, then the benefit-to-cost ratio is 1.25. The extent to which the ratio must be above unity for an investment to be seen as worthwhile is a somewhat subjective management decision. It is interesting to note that some researchers have considered (incorrectly in my view) the cost-benefit ratio to be the same as return on investment (ROI).

ROI. This is really the "rate" of return on investment and is the ratio of the net benefits (total benefits minus total cost) to total cost. Using the same example as above, the net benefits are $25,000, so that the ROI is 25% or 0.25, being the $25,000 divided by the total cost of $100,000. It should be noted that the ROI is always the benefit-to-cost ratio less one.

Neither the CBA or ROI methods account for the time value of money, whereby a dollar obtained some time hence is worth less than today's dollar, because today's dollar can be invested and earn interest to yield an amount greater than a dollar at some future time. These methods also do not take into account the relative size of the investments, which is often required because of limitations in capital available for investing. Therefore, it is not too helpful to know that a particular costly investment yields a higher return, if the budget does not allow for the expenditure.

There are two methods that do take into account the time value of money, those being net present value (NPV) and internal rate of return (IRR). NPV is essentially the value of the net benefits of an investment expressed in today's dollars. As before, a positive NPV is usually required for an investment to be accepted, but how high it needs to be is again a subjective management view. The IRR is the interest rate that will make the NPV zero. This rate is then compared to a "hurdle rate." If it exceeds the hurdle rate, the investment is acceptable, though it might be rejected on other grounds, such as the size or the relative priority of the investment.

NPV and IRR also have their deficiencies. For one, they assume a constant interest rate over time, which clearly is not the case. A more detailed explanation of the limitations of the various approaches appears in an article by Gordon and Loeb (2002).

It is interesting to note that the CSI/FBI survey report (2005, p. 2), mentioned earlier, states that "[a] significant number of organizations perform some form of economic evaluation of their security expenditures." They report that of those performing such evaluations, 38% use ROI, 19% use IRR, and 18% use NPV.

For the purposes of this chapter, we shall use the CBA method, even though it is limited, because it simplifies the discussion. However, I suggest that you look into the NPV and IRR

methods, if you have not done so already, as they are more accurate and representative than CBA or ROI, despite the limitations of the former.

Security and Privacy Options

We now look at two major approaches available for implementing privacy and security. One approach is the so-called defense-in-depth structure, where a number of layers of protective tools are applied. This will be examined subsequently.

A more holistic approach views security as a hierarchy of measures such as deterrence, avoidance, prevention, protection, detection, response, restoration, or cure, and reconstruction, or any combination of these.

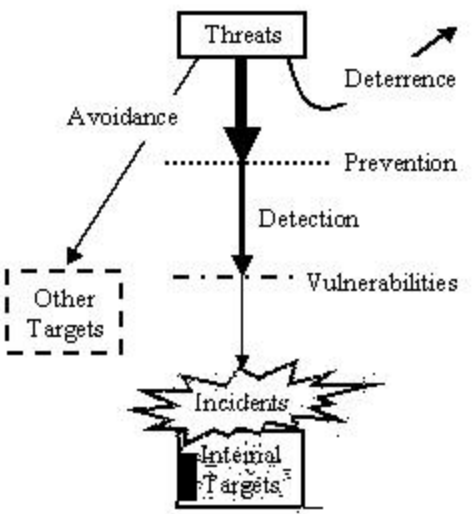
In Figure 1, we show how this hierarchy works. But again, we need to first define our terms.

A "threat" is an intentional or unintentional act which, if successful, might result in damage to, misuse of, or destruction of assets (in our case, information assets).

A "vulnerability" is a weakness or exposure, which if exploited by a threat, could result in a damaging incident.

Therefore a security or privacy "incident" or "breach" occurs when threat meets vulnerability and is successful in taking advantage of the "chink in the armor" to compromise the system, network, application and/or data.

Figure 1. Defending against threats



Consequently, as we see in Figure 1, going from top to bottom, threats might be diverted initially through avoidance and/or deterrence measures. With avoidance, the existence of a network, system, application, and/or data is not presented to a potential hacker or someone who might have otherwise inadvertently done damage. Deterrence should discourage a person contemplating doing something bad from acting adversely or encourage those with no evil intentions to be more careful.

Remaining threats are subjected to screening or prevention measures. To the extent that these measures are effective, there may still be some threats that get through the defenses. While not preventing an incident, monitoring or detection tools can help determine which threats are getting through for forensics purposes and to update the screening products so as to trap subsequent threats of the same kind.

Given that the threat is still active, vulnerabilities still have to be present for an incident to happen. Patching, upgrading and deactivation of offending features can go a long way to protect against threats.

We will now consider each of these categories in turn.

Avoidance

Avoidance is the first line of defense. The basic principle of avoidance is the "need to know." If it is not required that someone have access to certain functions and data, particularly personal information describing customers and employees, then such access should not be given to them. If particular server services are not required or specific ports are not needed, then those services and ports should be shut down.

It is specifically in the need-to-know area that GLBA and related laws and regulations kick in. Implementation of methods to affect this, such as restricting access or the blocking, disguising, or encrypting of data, is often complex, expensive, and time consuming, particularly for older systems, which were built for ease of use and access and not with the expectation of having to comply with such legal and regulatory restrictions. Also, recent publicity has highlighted the risks from the use and transportation of physical media, such as magnetic tapes, optical disks, and paper. Mitigation of this latter risk is generally thought to be achievable by converting to secure electronic transmissions of encrypted data, rather than encrypting and password protecting the data on the electrical, magnetic, optical, or other media, to avoid the risks of physical transportation. An indication of the importance of this area to financial institutions is the recent report by BITS (2006), the technical arm of the Financial Services Roundtable, entitled *BITS Key Considerations for Securing Data in Storage and Transport: Securing Physical Media in Storage, Transport, and for Data Erasure and Destruction*.

Deterrence

Deterrence—or what you do if avoidance and protection measures are inadequate, infeasible, or not cost-effective—usually involves specifying a detailed policy to interested parties, such as employees, consultants, and business partners, and delineating the consequences

of not following it. As perhaps the most underrated of all security and privacy measures, it is generally accomplished through awareness programs and enforcement procedures. It is often the least expensive of measures to implement, but its benefits are also among the most difficult to quantify. How do you know, for example, how many individuals might have been dissuaded from performing nefarious acts because persons were caught and publicly punished? Spending on deterrence includes creating security and privacy policy and standards, making anyone who might have the potential of doing harm (either intentionally or accidentally) aware of these, and otherwise enforcing them. The deterrent aspect of a security awareness program is to inform potential perpetrators of the painful actions that will likely be taken against them, were they to fail to comply with or actively evade the policy. Similarly those without evil intentions will likely take additional steps to ensure that they will comply with policy.

Another critical aspect of deterrence is for management to be seen to take the promised actions when someone contravenes policy. Such highly visible actions will give pause to those contemplating infringement. It is noteworthy that the U.S. Internal Revenue Service almost always publicizes high-profile tax evasion cases as a deterrent just prior to when most are about to prepare and submit their tax returns.

The downside of deterrence is loss of credibility and potential legal consequences, if the suggested remedial actions are not taken.

Prevention

The basic security rule of prevention is "defense in depth." Standard processes for preventing the unauthorized access to and misuse of information carried within computer systems and over networks include defensive technologies, such as routers, firewalls, intrusion detection and prevention systems, antivirus software, Spam filtering, Web site blocking, vulnerability patching, and the like.

Some of the benefits of these preventative measures can be estimated, although one cannot know with any precision what the cost impact of an intrusion might have been had it not been deflected. The direct cost of a virus or worm can be expressed in terms of staff resources required to determine the cause, to evaluate the extent of the damage caused by the infection, and to clean (or rebuild) the systems. Other costs, such as lost productivity, are much harder to measure, although the annual CSI/FBI survey (2005) attempts to do so.

Data Protection

Trends in legislation and regulation appear to be moving towards a universal requirement for encrypting electronically held personal data when created, at rest, and in motion, as a means of protecting the data against unauthorized access and use.

Encryption is not a panacea in that tools are readily available to criminals for decrypting data. It is well known that there are effective "cracking" programs used for decrypting password files. The same concept is readily extended to personal data. Encryption is also costly in resources, time lags, and administration. Nevertheless, the commonly held view

of lawmakers and regulators, often under the advisement of vendors, is that you are "off the hook" in terms of having to publicize a breach and/or notify customers if the compromised information is encrypted.

Detection

The most obvious tool in this category is the so-called intrusion detection system (IDS), which is currently morphing up the "food chain" to the intrusion prevention system (IPS). The concept here is that it is better to respond immediately and block an intrusion than to report it after the fact. IPS should more accurately be called an intrusion response system (IRS). An IPS does not actually "prevent" an attempted intrusion, rather it detects an attack and respond by blocking or diverting it, thereby avoiding damage. The danger with an IPS is that "good traffic" will often be blocked along with the bad. This is the opposite of IDS where the greatest is concern is a flood of "false positives," which increase the risk of missing real intrusions.

However, the area of detection, which comprises monitoring, analyzing, and reporting, is becoming increasingly sophisticated. It is beginning to offer the detection of anomalous behavior and suspicious traffic emanating from both authorized and unauthorized individuals and systems, often insiders and trusted systems, which are thought to comprise the vast majority of security breaches—most of which very likely go undetected.

It is interesting to note here that very many security breaches are not detected directly. Most often the consequent fraud is what alerts companies to the fact that a breach might have occurred. For example, the recently announced CardSystems Solutions breach was first noticed when fraudulent activity took place on accounts that had the common feature that they were processed by CardSystems. It was only after the fact, when CardSystems brought in a third party to perform a forensics analysis, that a malicious program, which had been inserted into the processing company's systems to harvest credit card data, was discovered. This common occurrence of not detecting the malware when it is first introduced, calls into question the efficacy of detection systems.

The current art of detection systems has greatest value in after-the-fact forensics analysis, where the systems record and report activities that can be readily searched through once the analysts know what they are looking for.

IDS is somewhat controversial, with the Gartner Group essentially stating in 2004 that IDS was dead and that IPS was taking over. However, given the difficulties in implementing IPS products, it is likely that the market for IDS with IPS features will continue in the marketplace for some time to come.

IDS is quite expensive to implement and use—especially in terms of trying to aggregate, correlate and analyze the huge quantities of data thrown off by these systems—and might be of questionable value relative to other approaches. However, IDS has become a security standard, much as firewalls were in the late 1990s.

Response and Recovery

Protective measures are designed to prevent bad things from happening to a company's computer and network environments. However, one can argue that funding for preventative measures should be balanced against funding for responding to actual events, since it is not possible to avoid all bad events. Such survivability spending includes costs of resiliency and recoverability.

While the scope of the incident response process generally extends throughout an organization, the security incident response component can be considered to be a real security expense. Security incident response is triggered whenever a significant security incident occurs. One can consider a security event to be the result of a failure of the deterrence, avoidance, prevention, and protection measures since if the latter had been fully effective, the event would not have occurred. Thus, in a very real sense, additional funds and effort expended on the incident prevention measures will likely result in a reduction in the frequency and extent of required response exercises.

As noted above, IPS products really can be considered to be in the response space, since they automatically react to a detected potential incident. The concept here is that an automated IPS can respond much more quickly and accurately than a human responder and, thereby, contain an incident before it becomes more extensive. The downside of such systems is that they might misinterpret an event and react to it in a way that diminishes the value of the environment that it is trying to protect. It should be noted that this is a long-standing problem of detection and prevention programs. Missile detection systems have been known to mistake a flock of flying geese for incoming missiles, for example. Such an error could result in unfounded retaliatory actions that would have a devastating impact in the case of nuclear missiles.

Restoration

Restorative or curative measures include on-site fall back, disaster recovery, and business continuity efforts aimed at bringing back an acceptable level of operation in the light of a compromise or destruction of the primary capabilities and facilities. This is not the re-establishment of the former primary facility, which we will call "reconstruction" and comment on in the next section.

The money and effort spent on redundant backup facilities is usually determined by the resilience and strength of the primary facility and the criticality of the functions operating in the facility. Moitre and Konda (2000) call this "survivability," and they indicate that survivability can be traded off against protective security and resiliency measures. That is to say, if the critical functions operate in a "military strength" primary facility, with hardened perimeter, back-up power, communications, and so on, the likelihood of having to roll over to a back-up facility is reduced. Therefore it can be argued that one might reduce expenditures on the back-up facility, possibly by using a shared service, since the likelihood of invoking the back-up is small.

However, in the United States, the financial services sector is subject to resiliency requirements mandated by its regulators. Consequently, the back-up and recovery requirements are strongly advised, if not compulsory in many cases.

Reconstruction

Often restored facilities are not permanent, as they may not have the infrastructure, location, facilities, and so on required of a permanent facility. Therefore there is frequently a final step, namely, bringing everything back to the way it was prior to the incident. This means rebuilding facilities, replacing equipment, and so forth. Information security is involved here as it would be in any set-up situation, and there are consequent costs of installing and testing the necessary security components.

Defense-in-Depth Strategy

It is well recognized that any single product does not provide the protection needed in today's complex environment. Consequently, security products and services are usually layered within and across the system and network infrastructure of an organization in order to protect against different threats and to catch attacks that have been able to penetrate other layers.

There are a variety of products, such as network and application firewalls, IDS, IPS, antivirus and antispam software and services, e-mail and message traffic content scanners, Web site blockers, encryption, and identity and access management products. Some of the newer products embody artificial intelligence or behavioral capabilities, which avoid the need for human intervention in many situations.

Firewalls

Firewalls can block traffic of certain descriptions and from specific sources and not permit access to certain ports and services. Application-based firewalls look at the specific nature of the traffic as it pertains to particular applications and block unsubstantiated traffic. Firewalls differ from routers in that they produce logs that can be analyzed after the fact to determine inappropriate activity.

Use of firewalls is practically universal. It is a minimum requirement, certainly in protecting what falls within the perimeter from nefarious activities. They also are used on internal networks to section off parts of the infrastructure. The management of firewalls has become commonplace and is usually controlled from within the network engineering group.

As they have reached commodity status, firewalls are seldom subjected to ROI analysis. They are a basic requirement and as such must be installed at critical nodes of the infrastructure. To the extent that some firewalls might be considered discretionary, particularly those on the internal network, they might be subjected to analysis.

IDSs

IDSs do not block traffic. Instead, they monitor the traffic as it flows across the network or on the host computer or endpoint (personal computer) and report against previously determined profiles or signatures. They are also after-the-fact devices in that they do not take any action but can be used for forensic analysis. From time to time, an IDS might pick up the early stages of an attack, where the attacker is reconnoitering prior to invasion. Usually some form of data aggregation and correlation "engine" is needed to identify and draw attention to such suspicious behavior. If the curious activities are detected, then action, such as blocking traffic emanating from a particular source, can be taken proactively.

There have been heated discussions in the industry, with the Gartner Group at the fore, about whether or not IDSs are passé. Gartner is looking to IPSs as the proactive technology to supercede IDSs. In fact rhere is room for both devices and manufacturers are coming up with hybrids, which encompass both technologies. IDSs only monitor, so there is a risk that they will either miss something or detect malevolent activities when it is too late to do much about them. On the other hand, IPSs can cause problems if they misinterpret good traffic for bad and block it, and it is the risk of screening out valuable transactions that has concerned a number of potential buyers.

Other Areas

All that can really be stated with certainty is that technologies are evolving and that what may have been valid just a short time earlier may no longer pertain. This is particularly true when a new type of threat or incident is observed. For example, prior to the highly publicized losses of computer tapes, there was little to justify more secure and expensive handling methods. Once financial firms learned of several incidents and the ensuing adverse publicity and costly responses, they quickly upgraded their own handling and transportation procedures.

ROSI by Category and in Aggregate

Each category of security tools or procedures should have a demonstrable value if used in isolation. Categories of security tools and procedures include firewalls, IDSs, IPSs, correlation engines, antivirus, identity and access management (IAM), awareness/training, and incident response. The value of any of these tools is difficult to measure, if indeed it can be measured, because no organization implements just a single method or tool. Therefore any analysis will be contaminated with the effects of the interaction of the tools.

For the sake of example, let us assume that the specific value of an individual method can be measured, as can the variance or variability of that value around some mean value. As an example, we might identify a threat for examination as "the proliferation of computer worms and viruses." The means of mitigating this risk might include the deployment of antivirus software and an aggressive awareness program.

In general, an awareness program is among the least costly of avoidance methods. It is simply a matter of advising e-mail system users not to open "suspicious" e-mails, particularly any attachments thereto, and not to click on any links incorporated into the e-mail. This can certainly assist in avoiding the most blatant of viruses. However many viruses and worms will infect systems without anyone having to do anything. It is here that the antivirus software comes into play. It scans for known viruses and blocks threatening attachments. It does not block viruses of hitherto unknown form (or "signature"), which is where its weakness lies. However, it is possible that a well-defined awareness program can lead to behavior that from time to time will avoid a virus that the antivirus software has been unable to detect.

Awareness or notification (warnings) may be less effective than antivirus software for known viruses, since the former is more prone to human error. Also the range of effectiveness is likely to be much broader for awareness. Antivirus software, in this case, not only has a greater return, but it is less variable in its effectiveness. Since both methods work in a similar manner in that they work well if the threat is known from prior experience, then they can be considered positively correlated. That is to say, their combined impact is some aggregation of both approaches.

There might be cases where the combined impact of two or more tools is less than the sum of the components or even less than one or both of the components. That is to say, by adding one tool or process, the effectiveness or the benefit of the other tool or process may be reduced, possibly by more than the benefit of using the second tool. It is difficult to come up with good examples, but one example might be the use of firewalls and the addition of a correlation and notification engine, where the notification engine might have a negative effect, if it produces so many false positives that an actual event is camouflaged and ignored, but management has the sense that greater control has been invoked. This would not be a condemnation of the tool itself, but more of the way in which it has been set up.

Optimizing the Security Portfolio: Or, How Much Security is Enough?

Given that one might be able to evaluate individual security technologies and tools, one against the other, the question arises as to what is the ideal combination of tools, practices, and procedures that will provide the optimum level of security. Would that the answer were as simple as the question?

In the above section, we looked at comparing one tool against another. In the portfolio approach, we determine the optimal combination of tools and practices that lead to the highest level of security for a given expenditure.

As an example, let us assume that we have $1 million to spend on protective measures, such as firewalls, IDS, IPS, and encryption as well as awareness training. We also assume that, for a given expenditure on a particular technology, we know what the benefit is. This is shown in Table 1.

This means that, for example, if $100,000 is spent on firewalls, then the estimated benefit will be $200,000. However, once the expenditure reaches $300,000, there is no incremental benefit for additional investment in firewalls. And even at $300,000, it is a break-even proposition, suggesting that there may be better places to put the company's money. These

relationships are similar for other tools and technologies. However, for IPS in this example, there is very little benefit (i.e., $50,000) to spending $100,000, but an expenditure of $200,000 yields a $300,000 benefit. This is meant to illustrate a case where the benefits do not kick in until a critical mass is in place. In Table 2 we look at the benefit-to-cost ratios for each of the cases in Table 1.

If we were to just take the maximum benefit-cost ratio for each tool category (indicated with an asterisk), we could decide that the expenditures should be as in Table 3.

Thus an expenditure of $1 million, distributed across the various tools as shown, would yield $1.9 million in benefits, which is an ROSI rate of 90%. If we had an additional $100,000 to spend, the benefit-to-cost ratio would be increased slightly to 1.909, as shown in Table 4.

However, this might not be the overall best selection from a benefit-to cost perspective. For example, if the additional $100,000 were to be spent on IPS and $100,000 less were spent on IDS, the benefit-to-cost ratio would increase to 1.950 for the same $1 million cost, as in Table 5.

Please note that the absolute and relative numbers here are fictitious and meant only to illustrate the argument. Also note that there are computational methods, such as linear programming, that calculate the optimum combination of expenditures on security tools subject to constraints on costs. The particular method used depends on the nature of the cost and benefit equations, whether the equations are linear or not, how the variables might change over time, the measurability and predictability of costs and benefits, and so on. In this chapter we have adopted a simpler approach for the purposes of clear exposition.

Now we look at the impact of a change in laws or regulations that requires notification of customers if personal information is lost and was not encrypted. In the example in Table 6, the value of encryption has suddenly jumped because having personal data encrypted might avoid having to go public with a breach. An additional investment in encryption could yield so much more in benefits that it ups the average benefit-to-cost ratio considerably.

This demonstrates that, rather than optimizing for each individual tool, additional value might be squeezed out from an equivalent expenditure by adjusting expenditures on specific tools. As shown above, the incremental value per dollar spent on various tools will differ. It makes economic sense to apply the funds to those areas yielding the highest return but only to the extent that the incremental value remains highest and greater than the incremental cost.

Table 1. Benefits derived from various security measures and different expenditure levels

Expenditures >	$100,000	$200,000	$300,000	$400,000	$500,000
Firewalls	$200,000	$300,000	$300,000	$300,000	$300,000
IDS	$100,000	$250,000	$360,000	$360,000	$360,000
IPS	$50,000	$300,000	$600,000	$800,000	$800,000
Awareness	$400,000	$450,000	$450,000	$500,000	$500,000
Encryption	$50,000	$250,000	$450,000	$450,000	$450,000

Table 2. Benefit-to-cost ratios for various security measures and expenditure levels

Expenditures >	$100,000	$200,000	$300,000	$400,000	$500,000
Firewalls	2.0*	1.5	1.0	0.75	0.6
IDS	1.0	1.25*	1.2	1.2	1.2
IPS	0.5	1.5	2.0*	2.0	1.6
Awareness	4.0*	2.25	1.5	1.25	1.0
Encryption	0.5	1.25	1.5*	1.13	0.9

Table 3. Expenditures and benefits for highest benefit-to-cost ratios

Tool	Benefit-to-cost ratio	Corresponding expenditure	Corresponding benefit
Firewalls	2.0	$100,000	$200,000
IDS	1.25	$200,000	$250,000
IPS	2.0	$300,000	$600,000
Awareness	4.0	$100,000	$400,000
Encryption	1.5	$300,000	$450,000
Total	1.90 Average	$1,000,000	$1,900,000

Table 4. Expenditures and benefits for highest benefit-to-cost ratios with increased expenditures

Tool	Benefit-to-cost ratio	Corresponding expenditure	Corresponding benefit
Firewalls	2.0	$100,000	$200,000
IDS	1.25	$200,000	$250,000
IPS	2.0	$400,000	$800,000
Awareness	4.0	$100,000	$400,000
Encryption	1.5	$300,000	$450,000
Total	1.909 Average	$1,100,000	$2,100,000

Table 5. Expenditures and benefits for highest benefit-to-cost ratios with different mix

Tool	Benefit-to-cost ratio	Corresponding expenditure	Corresponding benefit
Firewalls	2.0	$100,000	$200,000
IDS	1.0	$100,000	$100,000
IPS	2.0	$400,000	$800,000
Awareness	4.0	$100,000	$400,000
Encryption	1.5	$300,000	$450,000
Total	1.95 Average	$1,000,000	$1,950,000

Table 6. Expenditures and benefits for highest benefit-to-cost ratios with different mix

Tool	Benefit-to-cost ratio	Corresponding expenditure	Corresponding benefit
Firewalls	2.0	$100,000	$200,000
IDS	1.25	$200,000	$250,000
IPS	2.0	$400,000	$600,000
Awareness	4.0	$100,000	$400,000
Encryption	3.0	$400,000	$1,200,000
Total	2.208	$1,200,000	$2,650,000

Trade Off Against Survivability

Another point to add is that, in many circumstances, it might be worthwhile to invest in recovery and restoration, or survivability, rather than put that same money into data protection. Table 7 shows an example of increasing total expenditures by $500,000 over and above the example in Table 6. Nevertheless the total benefit-to-cost ratio rises to more than three.

The results of restricting the budget to that which was originally suggested to be spent on information security by reducing spending on security by $500,000, which is the estimated cost of response improvements, are shown in Table 8.

Again we have a situation where, if the activities with the higher cost-to-benefit ratios are substituted for those with lower ratios, the overall ratio will increase substantially.

Table 7. Comparison of benefits and expenditures

Tool	Benefit-to-cost ratio	Corresponding expenditure	Corresponding benefit
Security	2.2	$1,200,000	$2,650,000
Response	5.0	$500,000	$2,500,000
Total	3.029	$1,700,000	$5,150,000

Table 8. Comparison of benefits and expenditures with different mix

Tool	Benefit-to-cost ratio	Corresponding expenditure	Corresponding benefit
Security	2.45	$700,000	$1,715,000
Response	5.0	$500,000	$2,500,000
Total	3.51	$1,200,000	$4,215,000

Enforcement Pays

Enforcement not only pays, but it is crucial to the success of any security program.

While security tools might avoid and prevent adverse security incidents, they are valueless if they are not properly implemented and managed. Also, if employees, consultants, vendors, and others are not aware of the preventative and protective measures or if they have not been adequately trained in their use, then all may be for naught. The ideal security measures are those that do not require any actions to be taken by unknowledgeable individuals, apart from those that are forced by the systems.

However, if certain security-related decisions cannot be completely avoided, then one might have to resort to deterrent measures. These may require awareness, training, and signoff by individuals, accompanied by a warning that, in the event of noncompliance, certain disciplinary measures will be taken. That is why awareness and training can have such a high return, since the success of the program depends on them.

The Dynamics of Deterrence

The risk equation is rapidly changing based on two major trends:

1. The increased privacy legislation and regulations making for higher penalties and costs were a breach of personal information to take place
2. The greater culpability within organizations whereby the board of directors and executive management are increasingly becoming personally exposed to civil and criminal charges

As a result, the deterrence factor is increasing rapidly, However, there are major problems in regard to compliance.

The rate of change of the rules makes it difficult, if not impossible in some cases, to introduce appropriate and acceptable measures to comply with the laws and regulations within a reasonable timeframe. This leaves organizations exposed during the implementation phases to the extent that the mitigation projects extend beyond deadlines for compliance.

The need to comply with laws and regulations will sometimes divert valuable resources to relatively low-risk endeavors at the expense of not dealing with much higher risk issues. At the same time, projects to protect personal information, highly demanding of the same resources, are put on the back burner, often with damaging repercussions.

Summary and Conclusion

This chapter reviewed the basis for decisions on how much to spend on new and/or enhanced security measures. Largely, even if organizations are quite successful in determining returns at the technical level, risk factors and returns, which include less tangible costs and not readily measured benefits, make for results that are often much more difficult to measure and interpret.

While the examples shown in this chapter are somewhat simplistic, they are provided for illustrative purposes. The reader should make the mental transition from these examples to more sophisticated techniques, which they can either apply themselves or engage the services of an expert.

Overall, the security professional must constantly keep abreast of the latest laws and regulations and what they mean to the organization. This chapter promotes the idea of examining the risks related to security and argues in favor of the rational selection of products and services that provide the most cost-effective mitigation.

References

Allen, J. (2005). *Governing for enterprise security* (Tech. note CMU/SEI-2005-TN-023). Pittsburgh, PA: Carnegie Mellon University/Software Engineering Institute. Retrieved June 28, 2006, from http://www.cert.org/archive/pdf/05tn023.pdf

Axelrod, C. W. (2004). *Outsourcing information security*. Boston: Artech House Publishers.

Axelrod, C. W. (2006). Cybersecurity and the critical infrastructure. *Information Systems Control Journal*, (3), 24-28.

BITS. (2006). *BITS Key considerations for securing data in storage and transport: Securing physical media in storage, transport, and for data erasure and destruction*. Washington, DC: Financial Services Roundtable/BITS. Retrieved June 28, 2006, from http://www.bitsinfo.org/downloads/Publications%20Page/bitsdatatrans.pdf

Clarke, R. (2005). *Introduction to dataveillance and information privacy, and definitions of terms*. Retrieved June 28, 2006, from http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Computer Security Institute/Federal Bureau of Investigation. (2005). *The tenth annual CSI/FBI computer crime and security survey.* Retrieved June 28, 2006, from www.gocsi.com

Federal Financial Institutions Examination Council. (2005). *Authentication in an Internet banking environment*. Retrieved June 28, 2006, from http://www.ffiec.gov/pdf/authentication_guidance.pdf

Gordon, L. A., & Loeb, M. L. (2002). Return on information security investments: Myths vs. realities. *Strategic Finance,* 26-31.

Harris, S. (2006). Alphabet soup. *Information Security, 9*(4), 48-54.

Mimoso, M. S. (2006). Security survivor all-stars. *Information Security, 9*(4), 25-36.

Moitra, S. D., & Konda, S. L. (2000). *The survivability of network systems: An empirical analysis.* (Tech. Report CMU/SEI-2000-TN-021). Pittsburgh, PA: Carnegie Mellon University/Software Engineering Institute. Retrieved June 28, 2006, from http://www.cert.org/archive/pdf/00tr021.pdf

Parker, D. (2005). Learning from our enemies. *The ISSA Journal,* 20-25.

Ponemon Institute. (2005). *Lost customer information: What does a breach cost companies?* Retrieved June 28, 2006, from http://www.pgp.com/library/ponemon_reg_direct.html

Smedinghoff, T. (2005). The new law of information security: What companies need to do now. *The Computer & Internet Lawyer, 22*(11), 9-25.

Appendix A: Recent Security Breaches Involving Sensitive Information

Prior to February 2005, there were occasional notices of security breaches involving the potential compromise of sensitive data, particularly personal customer information, hitting the press. In the past several months, there has been a veritable flood of announcements. It appears that the frequency of major events has increased from one or two every couple of months to weekly occurrences, such as:

- On Feb. 15, 2005, it was reported that persons falsified their identities to gain access to ChoicePoint's applications and obtain personal information on 145,000 individuals.
- On Feb. 25, 2005, Bank of America, 205, DSW Shoes revealed that 100,000 customer accounts had been hacked. That number was then increased by 1.3 million accounts as was revealed on April 18, 2005.
- On March 10, 2005, it was announced that hackers had broken into databases held by LexisNexis and obtained personal information of some 32,000 individuals. A month later, on March 12, 2005, they revealed that an additional 280,000 accounts had been compromised.
- On May 2, 2005, Time Warner made public that computer tapes lost in transit to an Iron Mountain facility, contained personal information from 600,000 current and former employees.
- On June 6, 2005, CitiFinancial announced that UPS had lost computer tapes in transit containing personal information of some 3.9 million loan customers.
- On June 16, 2005, MasterCard announced that data from as many as 40 million accounts, including its own customers and those of Visa, American Express, and Discover, had been jeopardized by a breach at CardSystems Solutions.

- Georgia Technology Authority announced on March 30, 2006 that 573,000 state pensioners had had their bank-account details compromised by a hacker exploiting a security flaw.
- On May 19, 2006, the American Institute of Certified Public Accountants (AICPA) reported that an unencrypted hard drive containing the personal information of some 330,000 members had been lost in transit.
- The Department of Veterans Affairs announced on May 22, 2006, that an employee's laptop and computer storage device, containing personal information about 28.6 million veterans, had been stolen.
- On May 30, 2006, Texas Guaranteed Student Loan Corp. let it be known that they had been notified by subcontractor Hummingbird that equipment, which contained personal information of 1.3 million Texas Guaranteed borrowers, had been lost by an employee.
- Ernst & Young disclosed on June 1, 2006, that a laptop, which contained personal information of 243,000 customers of Hotels.com, had been stolen from an employee.
- The Internal Revenue Service (IRS) disclosed on June 5, 2006, that a laptop has been lost in transit and it contained personal information of 291 employees and job applicants.
- On June 14, 2006, American Insurance Group (AIG) announced that a server, which had been stolen on March 31, 2006, contained personal information, including medical records, of 930,000 customers.
- The Federal Trade Commission (FTC) announced on June 22, 2006, that two laptops had been stolen, containing personal and financial data of 110 persons.

The Privacy Rights Clearinghouse maintains a list of data breaches reported since the ChoicePoint incident, which was reported on Feb. 15, 2005. The list is available at www.privacyrights.org/ar/ChronDataBreaches.htm. As of June 27, 2006, the list includes more than 200 incidents accounting for some 88.4 million persons in the United States exposed to potential identity theft. In a number of cases, the extent of the exposure was reported as "unknown," "thousands," "a significant number," and the like, so that the actual number of persons exposed could be much higher. For example, there were two reports from March 2, 2006, alone, that were not included in the total but together may have accounted for the compromise of 3.3 million identities.

Appendix B: Return on Cyber Security Investment (ROCSI) as it Relates to Return on Critical Infrastructure Protection Investment (ROCIPI)

Critical infrastructure protection is the stepchild of security. That is because no one appears to be willing to take on the responsibility and costs entailed. Every enterprise is dependent, to a lesser or greater extent, on the broad-based infrastructure, particularly the critical infrastructure sectors of the nation and the world. The critical infrastructure includes such sectors as energy, IT, telecommunications, financial services, and transportation.

Is it that there is just not an adequate ROCSI for the public and/or the private sectors to invest in protection for the common good? Or is it that everyone understands that there will be a huge return, but no one is willing to put in the effort and funds? If there is a real need (as I think many recognize, at least intellectually), then it will take legislation and regulations to make it happen. In that way, legislators and regulators tilt the balance of the ROI equation, making it so painful not to comply, in terms of cost and other deterrents, that the investment will be made (no matter what).

An early attempt at this was Presidential Decision Directive No. 63 (PDD-63), which dealt with the protection of the nation's critical infrastructure. Issued in May 1998, PDD-63 required that the government and private industry do what was considered necessary to protect the critical infrastructure from attack or other events by May 2003. Unfortunately PDD-63 was a casualty of the change in administration and has not to date been fully replaced. Consequently, little has been achieved beyond the initial flurry of effort in response to PDD-63, when information sharing and analysis centers (ISACs) were formed for sectors such as finance, IT, and energy.

Recently there has been some attention paid to establishing a cyber-security research and development program (R&D), although funding for such R&D remains an issue. Other initiatives proposed by PDD-63, such as assessing the vulnerabilities of the critical infrastructure and embarking upon an awareness program, have been given little attention. A more extensive treatment of this topic can be found in Axelrod (2006).

As with other endeavors that require huge amounts of funding, securing the nation's critical infrastructure will need major government and private sector commitments and strong, determined leadership. It also requires sufficient incentives and/or threats of punitive action to "persuade" the private sector to play its part in shoring up the 80% or so of the infrastructure that they are deemed to own. The perceived ROCSI has to be shifted to a level that will result in ameliorative action being taken.