Considering Information Security

By Dr. Julio C. Rivera, Associate Professor, University of Alabama at Birmingham

In the past few years it has become commonplace to find stories in the news about identity theft, computer hackers, stolen information, Internet scams, and a host of other computer related maladies. These stories are the result of the confluence of people and technology, and illustrate the mixed blessings that stem from technology adoption. The result is that many of our information resources and essential systems are at risk. The level of risk our information and systems are exposed to has increased as information technology becomes more widely adopted. For people charged with delivering information services, this means that there is now the added burden of designing and adopting safeguards to maintain the integrity of their systems and information. This paper will briefly discuss what Information Security is, what types of threats information systems are exposed to, and how an organization may go about dealing with these threats.

What is Information Security?

As developed by the National Security Telecommunications and Information Systems Security Committee (NSTISSC), Information Security is the protection of information and the systems and hardware that use, store, and transmit it. While originally information security was concerned only with Confidentiality, Integrity, and Availability (CIA triangle) of information, the widespread use of information systems requires a more comprehensive view of information security. In the National Training Standard for Information Security Professionals NSTISSI No. 4011, we find a more thorough model for information security. This model (Figure 1) may be represented as a 3×3×3 cube, with 27 cells representing areas that an information security plan must address.

The model illustrates how an Information Security plan must address a wide range of issues. First, confidentiality means that information should only be available for those for whom it was intended, while integrity means that information must be accurate and free from tampering. Underlying these issues is the need to make information available to those who need in order to fulfill their responsibilities. These may at times be conflicting requirements, and require careful planning to deliver the required results.

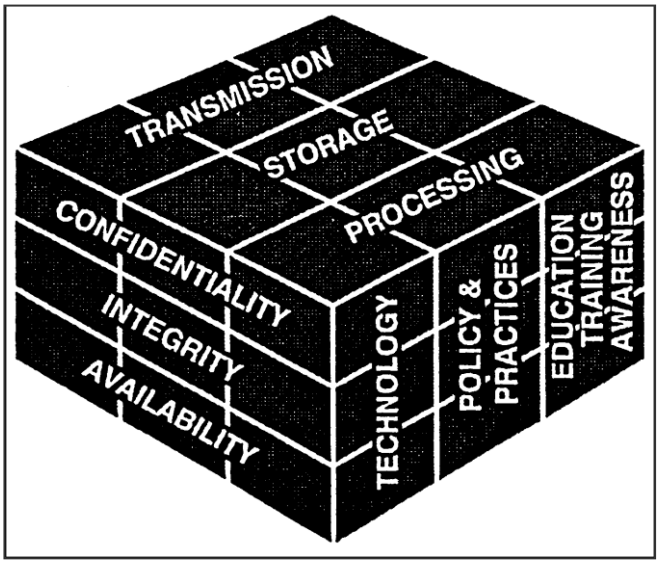

Figure 1: Information Security Model

Those first three issues, however, are only part of the puzzle. Information systems typically use a variety of technologies in order to deliver results, and all of these technologies may have a

negative effect on the confidentiality, integrity, and availability of information. Regardless of the technologies used, though, deficient organizational policies and practices may compromise the confidentiality and integrity of information as well as its availability. Finally the human element plays an important role in this mix. Whether intentional or not users can through their actions have an adverse effect on information security. This points to the importance of educating users and making them aware of their responsibilities in safe guarding information.

The third facet of this model indicates the impact that the transmission of information, its storage, and processing can have on information security. The transmission of information is rife with opportunities for compromising the confidentiality and integrity of information. After all, moving information from one place to another may expose that information to environments beyond the control of the organization. While information storage and processing do not at first glance appear to impact information security, modern distributed systems also make these areas of concern. How and where information is stored may be problematic if the information is in a position to be lost or tampered with. Finally, information processing may also be subject to problems, particularly when the means of processing the information can potentially introduce errors or compromise its confidentiality.

Taken altogether the Information Security model in Figure 1 is an indicator of the complex interaction between all elements of an information system. This complexity cannot be ignored in developing an information security plan. Thus, good information security plans address the interaction between all of the elements named in the information security model. In practice this means bringing together users, system designers, systems administrators, security experts, and other stakeholders to develop an information security plan. The nature and breadth of such a plan makes it essential that all stakeholders be involved.

Information Security Threats

The previous discussion would not be necessary if the confidentiality and integrity of information was not threatened by a variety of sources. A good information security plan will address these threats by analyzing them in relation to each of the elements of the model. Further, the nature of information security threats is constantly changing. Constant change therefore requires ongoing evaluation of any information security plan in order to adjust to new threats.

Broadly speaking information security threats stem from sources internal to the organization, as well as outside. Typically the most publicized threats originate from outside sources, but the majority of information security breaches occur from within the organization. Five categories of threats have been identified by information security researchers. These categories are identified in Figure 2.

- Inadvertent Acts
- Deliberate Acts
- Acts of God
- Technical failures
- Management failures

Figure 2: Information Security Threats

Inadvertent acts are often the result of user mistakes. These mistakes may come from inexperience or improper training, or in other circumstances are due to incorrect assumptions. Either way, these acts must be addressed by educating the user community, and raising awareness of the consequences of their actions. While user mistakes are an internal source of inadvertent acts, outside sources may come from vendors or suppliers of hardware, software, or services. Any of these groups can make mistakes or have problems that have damaging

consequences. This especially true with communications services, now an essential part most information systems.

Deliberate acts are probably the most often discussed source of threats to information security. Here again, there are internal and external sources. The largest number of deliberate acts comes from internal sources. Although seldom publicized, an organization's own employees typically posses the most knowledge about its information systems, and thus have the greatest ability to deliberately compromise their security. They may do so for any number of motives, and because of their knowledge and access they can perpetrate serious information security compromises.

Probably the most often heard of deliberate acts, are those originating outside organizations. There are a number of motives for the perpetrators of these acts, from the economic to the feeling of power some experience in perpetrating these acts. These acts are typically the work of hackers, ranging from experts who discover new system weaknesses to script kiddies who use freely available software to exploit known weaknesses. The existence of this threat means that organizations must put in place a variety of means to defeat this threat. Even with these means in place, though, organizations must remain constantly vigilant for new exploits of their systems.

An often overlooked category of security threats is that of "Acts of God". No matter where we are located there is always the possibility that something catastrophic may occur. Although it may be impossible to protect the organization's information from these acts; an organization should always make provisions for mitigating the consequences of these acts. This category is usually addressed by putting in place facilities and procedures that can replace the information and facilities subject to these acts.

Technical failures are a less common source of information security threats. These usually stem from flaws in hardware or software that can lead to the loss or compromise of information. While most of these threats may occur within the organization, they may be the result hardware or software sourced outside the organization. These threats may be difficult to identify and deal with, since they may only occur under certain circumstances. Dealing with this type of threat requires everything from contacting vendors and downloading fixes, to meticulously documenting and tracing problems to their source.

Finally, and most importantly, an organization's management must be proactive in developing and implementing plans to insure information security. Management has to recognize the risks inherent in ignoring information security. While it is seldom feasible to protect an organization against every potential threat, management must analyze the risks and decide what threats to protect itself against. It is also important to recognize that the nature of the threats to information security changes over time, and it is again a management responsibility to recognize and adjust to these changes.

Conclusions

This article presents a glimpse at the concerns an organization faces when dealing with information security. The nature of the threats to information security requires organizations to evaluate their exposure to these threats and put in place measures to mitigate them. The nature of these measures should be determined by an analysis of the risks an organization faces. In general though, a good information security plan will address the areas outlined in the information security model presented earlier, and be updated as information security threats change. It is important to note, however, that an organization's management is ultimately responsible for insuring its information security.

Dr. Julio C. Rivera is an Associate Professor of Information Systems at the University of Alabama at Birmingham. Dr. Rivera may be reached at jrivera@uab.edu.