Addressing Information Security Risk

A journey, not a destination, security work is never done—the challenges just keep coming

By **Mohammad H. Qayoumi** and **Carol Woody**

Good information security does not just happen—and often does not happen at all. Resources are always in short supply, and there are always other needs that seem more pressing. Why? Because information security is hard to define, the required tasks are unclear, and the work never seems to be finished. However, the loss to the organization can be devastating if confidential information is compromised or networks become unavailable when communication channels become overloaded with virus and worm traffic. Some of the challenges are chronic; for example, universities face the regular influx of students whose personal equipment has poorly maintained security protection. Other problems are opportunistic, such as when a researcher loads patient data on a poorly protected machine, the information is compromised, and someone uses it inappropriately.

One of the key fiduciary roles of management is protecting the assets of the organization. By "organizational asset" we refer to the means by which the organization creates value for its stakeholders, and those assets include information assets. With the continual proliferation of information technologies today, an ever-increasing portion of the organization's data is in digital form. In fact, for many major enterprises, information constitutes a significant portion of the overall portfolio. In quite a few cases, that value may exceed the value of the organization's physical assets. With an estimated 90 percent of intellectual capital digitized,

and a major portion of that in the form of e-mail, managers must accept that their responsibility for asset protection includes information storage, transmission, and use that extends beyond the physical realm to include cyberspace.

Protecting information assets implies that we need to identify what is really at stake. Securing the growing proliferation of data communications in practically every aspect of an enterprise is one of the major challenges that every manager and administrator faces today. The underlying reason for concern is the continued, and highly publicized, success of hackers and crackers in breaking into enterprise data systems, compromising confidential information, and creating havoc in the operations of the organization.

As a response to these events, a plethora of federal legislation has been enacted within the past decade, such as the Gramm-Leach-Bliley (GLB) Act, the Family Education Rights and Privacy Act (FERPA), and the Health Insurance Portability and Accountability Act (HIPAA). Similarly, many states have passed legislation specifically targeting organizational responsibility for information security.

Today, no organization can afford to ignore the current state of affairs. Inaction by senior management will prove costly and will indicate a serious abdication of responsibility. This can lead to lawsuits and a negative impact on the institution's image.

Information is constantly updated and expanded, infrastructures are continually modified and replaced, and technology continues to change at an increasing rate, providing new tools and capabilities that give rise to new uses. Supporting the security of all these pieces cannot be viewed as a once-and-done activity. Information security must be a continual journey rather than a specific destination.

Challenges of Information Security in Higher Education

In many domains, the concepts of guarding trade secrets, protecting corporate data from competitors, and fighting patent infringements are well understood. These types of information security have a strong history in industries such as manufacturing and music, where patent and copyright infringements could destroy the viability of the organization. In domains where information security has a strong history, every member of the organization is sensitized to critical security issues and views information security as a pivotal element for the organization's survival. The practice of safeguarding corporate information is reinforced by practically all activities of the enterprise.

Not all industries are adept at protecting information. Even in domains where

regulations mandate information security, such as health care, applying sufficient resources to meet the mandates is difficult. Studies report that hospitals and medical facilities, for example, often fail to meet security requirements within the mandated time.[1]

Information security is even more problematic in higher education. The underlying values and vision of higher education call for sharing knowledge and providing access to information and technology. In other words, the concept of information security runs counter to the open culture of information sharing—a deeply held value in academe.

This phenomenon is not unique to information security. The tension of "the acropolis versus the agora" is recognized in the management of higher education. To ameliorate this challenge, we must look for creative ways to segregate university information systems into two major categories:

- the academic systems for which the faculty want to maintain open accessibility, and
- the enterprise systems where legal compliance, data confidentiality, and data security are paramount, rather than information sharing.

Beyond the cultural tension are other challenges inherent to information security. First, information security can be categorized as a hygiene factor rather than a satisfier. When a robust system functions properly, safeguarding critical and confidential data, it is not obvious to many people in an organization, with the exception of the few individuals who work with the system on a daily basis. In fact, the average user may never know that a system is secure. The absence of a secure system could be experienced by many users, however, usually after damage has been inflicted on the system and it is too late to avoid the impact.

The second challenge is the perception of many people that data security is a technical issue and, therefore, the sole responsibility of chief information officers (CIOs) and their staffs. This implies that as long as the CIO procures and installs the latest firewalls and other technical gadgetry, the system is protected. Such forms of myopic self-exoneration can exacerbate today's cycle of ever-increasing information security crises. Many authors have shown that technology alone is not the solution, that information security must be addressed by a combination of technical and administrative practices such as promulgating sound policies and implementing systematic processes to safeguard institutional data.

The third major challenge is the nonintuitive nature of information security and its adverse impact on productivity. The ease and low cost of collecting, storing, and sharing large volumes of information motivate us to assemble data at a continually faster rate and provide greater access to that data. Consequently, many view the steps that enhance security as a nuisance at best or a major impediment to improving productivity at worst.

Finally, another major misconception is that a single perfect solution exists to information security—that once this solution is implemented, the task of protection is complete. In reality, no single solution can address the information security requirements of an organization. Continual vigilance and ongoing effort are required because the job will never be done.

Defining Good Information Security

Good information security is analogous to good hygiene. No single activity ensures good health. Rather, many activities combined reduce the risk of exposure to disease and potential injury and provide early warning of potentially disastrous problems. *Prevention* activities include brushing your teeth, bathing regularly, eating a balanced diet, and exercising regularly. *Monitoring* activities confirm that the body is operating normally. Periodic *reviews*—annual physical, dental, and eye examinations—detect problems early. The specific activities (*standard practices*) you implement vary based on your personal risk factors, such as age, genetic heritage, and exposure to diseases, and these factors change over time. Choices made also vary based on financial arrangements in place for cost coverage and perceived impact should a problem materialize.

Key words (italicized in the preceding paragraph) apply to information security as well. Standard practices for information security target prevention, monitoring, and periodic reviews to *recognize*, *resist*, and *recover* from the impact of an information security problem. The practices your organization should perform will vary based on the potential impact of a problem, the perceived likelihood of occurrence, and the resources available to conduct the activities. Periodic systematic reviews identify changes in the risks to organizational information security, and you can select appropriate practices to address them.

To further our hygiene analogy, consider that each periodic review collects a range of information about health activities and medical history before care begins. Lab tests, an EKG, and x-rays might be ordered to check specific areas of concern, with additional procedures prescribed if new risks appear. For information security, this same process of data gathering and analysis should occur periodically through an assessment process, which will identify risks to the security of critical information assets and enable the organization to adjust its practices to eliminate or mitigate the potential impact.

Information security has too frequently been viewed as yet another overhead task primarily addressed by a small cadre of individuals with technical security training. This belief stems from a paradigm in which organizations consist of distinct building blocks and loosely connected operational silos. Creating an information security office and hiring an information security officer (ISO) address the issue.

Today, most managers realize that an organization is better described as a set of tightly intertwined, interrelated processes. Information security must thread through all aspects of the organization. The ISO role is primarily a coordination function ensuring that all pieces of the organization address their portion of security by approaching every major dimension of the organization systemically. Security practices relevant to the risks identified in both the technological and organizational aspects of each orga-

nizational segment must be considered. This implies that the culture of information security must permeate all aspects of the organization.

In most circumstances it is not economical to fully protect an organizational asset against all possible threats. The same concept applies for information security. The optimal solution will blend technological capability with business risk management approaches. Systems can never be fully immune from compromise, and development of a risk-based model is a critical aid to management in evaluating options.

Determining Where Your Organization Stands

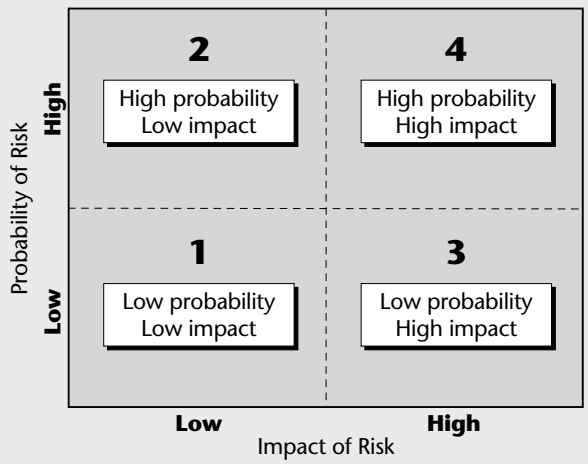
In considering information security risk, first identify the enterprise's mission-critical activities. Next, examine potential threats to and vulnerabilities of the information systems as they relate to the critical organizational activities. Develop a risk-based model by examining the frequency of various adverse events that could be triggered if the threatened event occurs or if the vulnerabilities are exploited, and link the resulting impact to the organization. This involves examining the current organizational practices, infrastructure, and methods for utilizing technology in the enterprise's daily activities.

To evaluate the information gathered, plot the event data of frequency and impact in a simple graph as shown in Figure 1 by grouping the information into four basic categories. Evaluate impacts for both immediate and long-term effects, and include a full range of organizational stakeholders. Examples of such possibilities include:

- Student loss of connectivity and the expense of technical resources to isolate and repair a compromised machine.
- Loss of student study time, class time, or staff or faculty time depending on the timing and nature of a compromise.
- Time diverted from research along with the technical resources required to replicate and repair data resulting from the loss or corruption of critical files for students and faculty involved in lengthy research projects.

Figure 1

Risk Evaluation and Analysis



- Impact on completion of a sponsored grant activity and the subsequent effect on the organization's reputation, which could result in loss of future awards should critical data and intellectual property be leaked or compromised.
- Impact of litigation, financial losses, and serious organizational embarrassment should confidential institutional or personal data be compromised.

Adverse events that generate entries in the fourth quadrant of the graph in Figure 1, namely those that have a high probability of occurrence and high impact, require immediate mitigation. Those in quadrant three, namely low probability of occurrence but high impact, come second in consideration for mitigation. Subsequently, events in the second quadrant, namely high probability and low impact, may require attention if resources become available. In many circumstances, events in the first quadrant, namely low probability and low impact, can be ignored, as it might not be economical to apply resources to mitigation. This approach provides a simple method for grouping potentially negative events and prioritizing risk-mitigation efforts.

Integrating Security into the Institutional Culture

Promotion of a security-centric culture begins with sponsorship by senior leadership, to provide the recognition of information security as one of the essential elements of organizational survival. It requires the integration of information security into the institutional strategic plan through implementation of policies that hold all stakeholders accountable for the failure of information security. To align the activities of the entire organization with policies of accountability, managers at each organizational level must incorporate security activities into their areas of responsibility by developing metrics and measures to continually assess information security; defining and instituting monitoring mechanisms to recognize security problems; acting on metric deviations; and assigning adequate resources to ensure a specified level of compliance.

Managers also must continually communicate information security concerns to all stakeholders and incorporate information security as a key element in the performance evaluation process. A periodic assessment of the organization's information security should identify gaps in applied practices as well as new and changing organizational risks. The assessment serves to adjust organizational priorities and note opportunities for improvement. Continuous improvement is critical to an effective approach.

Required Actions

In principle, addressing information security is similar to any other management challenge. Merely reacting to regulatory and legislative mandates will not suffice. Organizations that have adopted a risk-based approach to information security quickly recognize that such a narrow focus falls far short of adequately addressing their needs. An effective approach to information security must be planned, monitored, controlled, and managed based on sound business decision-making principles. This requires coordinating multiple players across the organization.

Information security involves technology, but it also involves people interacting with the technology. Therefore, a technology-centric solution with minimal or no regard to organizational and human factors will fall short. In the words of Gonzalez and Sawicka, "Any security system, no matter how well-designed and implemented, will have to rely on people. A framework of information security must address the interplay of technology, work environment, and human behavior."[2]

In addressing information security, first develop a shared understanding of the goals and reach an agreement on a solution framework. Such an understanding must include, but not be limited to, concerns about confidentiality, privacy, integrity, reliability, and availability of data. The organization should consider what is required to:

- *Comply with federal and state regulations.*

In the past few years a number of federal regulations relating to data security have been passed. Moreover, many states have issued additional rules that are more stringent than federal regulations, such as California's Public Records Act, Information Practices Act, and Information Technology Act. It behooves every organization to compile a list of all the rules with which they must comply and develop action plans to achieve compliance. In addition, the organization should anticipate future legislation that might impose new requirements.

- *Define what constitutes confidential information.*

This can include segregating information into separate categories based on security needs and developing a layered approach to data security and confidentiality. The organization can then develop policies for the creation, retention, transmission, and destruction of confidential information, whether physical or digital. This should include all requests and approval processes for issuing access, as well as timely and efficient mechanisms for terminating access privileges.

- *Develop policies based on the business needs and priorities of the organization.*

These policies should ensure compliance, state the consequence of noncompliance, and hold everyone in the organization accountable for a strong degree of due care.

- *Devise operational procedures for controlling various key types of information.*

This includes password management (including password length, expiration cycle, maximum log-on attempts, and so forth), downloads to shadow systems, non-encrypted data transmission on non-secure lines, disposal of physical files and hard drives, network management, monitoring and auditing, and system authentication and authorization.

- *Develop an incidence notification and response system.*

This capability, led by a computer security incident response team, would be used to identify and respond to compromises or breaches. Additional information on defining this capability is available at <http://www.cert.org/csirts>.

Data Stewardship Is an Organizational Duty

Senior leadership must recognize that institutional data are similar to any asset owned by the enterprise. Therefore, as with other resources, executives have a fiduciary responsibility to manage data, keeping in mind its utility and cost/value relationship. The benefit of data can be realized when they are shared

Additional Resources

Risk assessments and management programs:

- SEI Operationally Critical Threat, Asset, and Vulnerability Assessment (OCTAVE), <http://www.cert.org/octave>
- Security Targeting and Analysis of Risk (STAR), developed at Virginia Tech, <http://security.vt.edu/playitsafe/index.phtml>
- Five-Year Rotating Audit Focus Based on Risk Assessment at Georgia Tech, < http://www.educause.edu/ep/705?ITEM_ID=199>
- Information Security Governance Assessment Tool, <http://www.educause.edu/ir/library/pdf/SEC0421.pdf>
- Maricopa Integrated Risk Assessment, <http://www.dist.maricopa.edu/mira/>
- IT Security Risk Management Program at the University of Virginia, <http://www.itc.virginia.edu/security/riskmanagement/>

Higher education sources:

- EDUCAUSE Security Risk Assessment and Analysis, <http://www.educause.edu/645?PARENT_ID=665>
- *Computer and Network Security in Higher Education*, EDUCAUSE Leadership Strategies No. 8, M. Luker and R. Peterson, eds. (San Francisco: Jossey-Bass, 2003), <http://www.educause.edu/content.asp?page_id=5746>

with the right parties in a thoughtful manner. On the other hand, if data are misused—or worse, if they fall into the wrong hands and adequate precautions were not taken to ensure their protection—not only would the value of the asset diminish, but it could result in serious harm to the institution. The following are key aspects of data stewardship that every institution of higher learning must address:

■ *Availability*

The organization must have processes in place to support access and easy use of institutional data by all legitimate users. It should also provide guidelines and procedures that support and ensure access to data by authorized end users.

■ *Integrity*

Data integrity is of paramount importance for every organization. The expansion of data-driven decision making increases the reliance on organizational data. All legitimate institutional data users have a right to expect integrity of institutional data. The enterprise must establish processes to collect, maintain, and store data to guarantee their consistency, reliability, timeliness, and accuracy. This implies adequate security measures that protect institutional data from unauthorized access, modification, or destruction.

■ *Confidentiality*

Data should be available to users on a "need to know" basis—that is, based on what users require to carry out their assigned duties and legitimate tasks. Strong controls are needed to ensure partitioning of systems and data in a way that limits access to legitimate users. Moreover, robust systems and control mechanisms must be in place to prevent others from accessing sensitive or confidential data. Guidelines must be established for disposal of electronic or hard-copy downloads of sensitive and confidential data.

Information security is a growing challenge for every organization. Effective organizational data stewardship, initiated from senior management and permeating all levels of the organization, is needed to motivate everyone in the organization to provide a high degree of due diligence. Anything less risks disaster. *e*

Endnotes

1. AHIMA, "The State of HIPAA Privacy and Security Compliance," April 2005, <http://www.ahima.org/marketing/email_images/2005PrivacySecurity.pdf> (retrieved August 25, 2005).
2. J. J. Gonzalez, and A. Sawicka, "A Framework for Human Factors in Information Security," paper presented at WSEAS International Conference on Information Security, Rio de Janeiro, 2002, <http://ikt.hia.no/josejg/Papers/A%20Framework%20for%20Human%20Factors%20in%20Information%20Security.pdf> (retrieved August 25, 2005).

Mohammad H. Qayoumi (mo.qayoumi@csun.edu) is Vice President for Administration and Finance and Chief Financial Officer, California State University, Northridge. Carol Woody (cwoody@cert.org) is Senior Member of the Technical Staff, Software Engineering Institute, Carnegie Mellon University, Pittsburgh.