



Interhack
5 E Long St Ste 1101
Columbus, OH 43215

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB <http://web.interhack.com/>

Information Security: Friend or Foe?

Matt Curtin, CISSP, IAM

Date: 2002/12/20 22:22:31

Abstract

Information security (INFOSEC) is a critical, if highly misunderstood, aspect of the processing of information. As information is at the heart of many businesses today, INFOSEC must be successfully addressed if we are to realize the full benefits of information technology.

Successfully managing INFOSEC is not significantly different from managing other challenges in a business environment. Organizations simply need to acknowledge the risks that are present and to address those risks. Quite a bit of help is available, both in the form of helping employees to understand the domain and in the form of products and services from vendors.

In this article, we consider what information security is from a management perspective. What is information security? What are the objectives of INFOSEC? How can INFOSEC contribute to, rather than draw from, successful business operation? Finally, we consider INFOSEC from the perspective of the health care industry.

Contents

1	What is Information Security?	2
1.1	CIA Security?	2
1.2	The Role of Policy	3
1.3	The Role of Technology	3
2	How Does Information Security Contribute to Success?	4
3	How Does INFOSEC Relate to HIPAA?	6

Copyright ©2002 Interhack Corporation

1 What is Information Security?

Information security (INFOSEC) has managed to get a tremendous amount of attention in the past few years, even grabbing headlines in the mainstream media. Despite this attention, asking ten people what INFOSEC is will likely result in ten different answers. To some people, security is about keeping the bad guys out of their systems. To others, security is about elimination of all threats. To still others, security is about management of risk. Despite the presence of security in the mainstream consciousness, outside of the INFOSEC community, there still isn't much agreement about what exactly security means.

By 2004, annual expenditures on security products and services is expected by IDC to climb to over \$17 billion. Yet with all of this spending, we see more security incidents taking place, and those incidents are becoming more expensive. Reality Research estimated that aggregate annual losses due to the single problem of viruses in 2000 climbed to over \$1.5 *trillion*. The insurance industry has been looking seriously at this problem, with computer attack insurance packages up to \$100 million being offered. Clearly, security—whatever it is—is important.

1.1 CIA Security?

Security practitioners can usually enumerate lists of properties that factor into security. When we're dealing with information security specifically, though, there are three issues that stand out for their clear agreement: *confidentiality*, *integrity*, and *availability* (CIA). Information can reasonably be called secure when these three properties are present.

Confidentiality simply means that the information is known no more widely than necessary. If you tell some medical secret to your physician, there has been no breach of confidentiality, because the fact was needed by the physician to render the requested service. If, on the other hand, your physician then tells your secret to someone else not involved in your treatment, confidentiality would be breached.

Integrity is the assurance that the information is untainted. Note that this does not deal with the *accuracy* of the information—it strictly means that the information put into the computer is the same as the information that comes back later.

Availability means that when the information is needed, it is ready for use. To many, this might seem counter-intuitive. But consider, if an attacker wants to put your company out of business, wouldn't the ability to deny you access to your own information for a long enough time do the trick?

Understanding properties necessary for information security is important, but not enough. To achieve the desired security, implementation becomes necessary. Successful implementation in computer systems will require both policy and technology.

1.2 The Role of Policy

Policy is really nothing more than a statement of organizational expectations.

Policy can be expressed at many different layers of the organization. At the broadest level, policy is a definition of the organization's objectives and guidelines for how to achieve those objectives. Down into the tactical and operational parts of the organization, policy will get into specific practices and guidelines that will help people and the systems that they use to stay within the framework expressed at higher levels.

The concept of layers of policy should be familiar to us in the U.S. Our highest-level policy is the Constitution. Following that definition of objectives and guidelines is necessary for any subsequent layer. Those layers typically consist of Federal law (the U.S. Code), state law, and down to city ordinances.

Similarly, an organization will have definitions of its objectives and guidelines at its highest levels. Following that will come various layers that deal with how particular business units, departments, and teams will operate.

At the highest levels of the organization will come definition of problems that it is trying to solve in the large. Obligations of the organization will be laid out, providing the organization guidelines on how to balance the interests of shareholders, employees, customers, and the communities in which they work. Following the highest-level policies will come the kinds of policy that identify how to identify and to manage market conditions, operational issues, and risk.

With the organization's definition of its risk management strategies and operational requirements for information will come a framework for defining INFOSEC-specific policy. That is, which kinds of information are critical to the business, and how must each of those types of information be evaluated for confidentiality, integrity, and availability.

High-level INFOSEC policy will help the engineers and administrators designing, implementing, and operating information technology understand what they must do at a very detailed level. It is here that questions like whether direct Internet access is acceptable for particular systems or sets of users, whether packet-filtering routers are sufficient for separating networks, or whether application-layer proxies must be employed. Down at this layer will specific decisions be made about the kinds of authentication mechanisms in place—whether passwords are sufficient, how strong they must be against various attacks, whether token-based devices are necessary, or whether biometric authentication mechanisms must also be employed. In the trenches, the technical staff will understand how to configure the systems put into production.

1.3 The Role of Technology

What should be clear by now is that technology's role in INFOSEC is really one of *policy enforcement*.

Only with the clear articulation of INFOSEC policy can intelligent decisions regarding specific technology be made. Without such policy definition, questions like whether something is "secure enough" cannot be successfully answered, since each

individual's notion of what constitutes appropriate risk vs. benefit will differ. This is a common problem in organizations today, with the end result being large amounts of money being spent in the name of security, with remarkably little to show for the expenditure. At the same time, the best intentions of technical staff are frequently overrun by a manager's arbitrary decision about how much risk the organization is willing to accept. So while the technologists and management spend their time frustrating each other, the information critical to the organization's operation continues to be at risk.

Technology, through its design and configuration, will express policy. Though inappropriate for non-technical managers to decide whether particular protocols may be allowed between their sensitive networks and untrusted networks, such non-technical managers must provide the higher-level framework defining operational and risk management requirements. Technical people, understanding this framework, will be able to implement the organization's policy successfully.

No amount of spending will secure an organization whose policy is fundamentally flawed. No amount of policy will secure an organization where the policy is not effectively implemented. Cookies and milk are better separated than policy and technology.

Thus, INFOSEC can be described as "saying what you do, and doing what you say." Following this simple maxim is really the goal of information security. INFOSEC, however, is not an end to itself. Rather, it is part of a larger framework of how information is to be collected and managed—the processes that define a business operation.

2 How Does Information Security Contribute to Success?

Several issues come to the fore when considering how INFOSEC contributes to an organization's success. In a nutshell, a properly executed information security program will increase the likelihood that the organization will be able to achieve its objectives.

Consideration of Abraham Maslow's famous hierarchy of needs could be helpful here. As you'll likely recall, Maslow defined five levels of needs, physiological, safety, love, esteem, and self-actualization. The first of these needs, physiological, includes such things as air, water, and food. These must be satisfied to sustain life. Once these needs have been met, the next level of needs arises, safety. When addressing our need for safety, we establish a sense of stability and consistency in the world around us, and we have the ability to manage and to overcome adversity. Maslow's higher-level needs then move on to love and acceptance, a sense of belonging to something larger than ourselves. The fourth level of need is esteem, where we feel good about what we are doing, and are recognized for our efforts. Finally, the highest-level need is self-actualization, where we realize our potential, and become all that we possibly can be, the best that we have to offer.

While Maslow's hierarchy of needs was constructed to explain how people progress

toward unselfishness, the hierarchy also makes sense when being applied to organizations. First, organizations are simply made up of groups of people, aligned toward a goal. Second, organizations do function largely the same way. Without the “physiological” needs—those necessary to sustain “life”—being satisfied, the organization cannot continue. Instead of food and water, organizations need such things as capital and people. Safety needs include the ability to establish an operating environment that will allow the organization to deal with adversity. INFOSEC fits into this second level—achieving information security will allow an organization to deal with the kinds of dangers that could kill an organization whose basic day-to-day work is the management of information.

Moving then into acceptance, organizations have made a mark for themselves, where people understand what the organization is, and how it fits in with the landscape. Esteem of a company is really the esteem that the employees. Things like recognition for good work done fulfill this need. Finally, at the highest level, the organization becomes all that it can be, where its mission statement is achieved in some real sense, where it is offering all that it possibly can to the world around it.

To be able to achieve their missions—to reach self-actualization—organizations must satisfy the lower-level needs. Notice that issues such as safety and security fall into the second of Maslow’s five levels. To an information-based organization, INFOSEC must be satisfied not after it has become all that it can be, not after it has been recognized for its work, and not even after establishing itself as a player in the marketplace. The need for information security must be satisfied at the second level, immediately after basic issues of survival.

INFOSEC thus provides the ability for the organization to establish a sense of order in the world around it. Only after this has been achieved will the organization be able to navigate successfully through the world toward some higher-level objective. This is, incidentally, the same level as an organization’s physical security. You cannot stay in business if you do not take precautions to prevent thieves from breaking into your office and stealing your company’s equipment.

Once INFOSEC has been achieved, the organization will be free to move on to establishing a place for itself in the marketplace, to be recognized for its good works, and to become all that it can.

When considered in this light, INFOSEC should seem less esoteric. At the same time, the requirements of an INFOSEC program in your organization should become more clear. Understanding the role of INFOSEC in an organization’s quest to self-actualization and our understanding of how technology and policy work together to achieve information security, we can see several requirements for any successful information security program:

- It must be in harmony with the organization’s highest-level objectives;
- It must be given clear direction so that conflicts that will arise (such as functionality vs. risk) can be resolved properly;
- It must correctly identify the information that is critical to the organization (what is it that we’re trying to protect?);

- It must understand the operating environment of the organization, including not only objectives and policies, but culture and technology;
- It must result in the kind of stability that allows people in the organization to stop worrying about the information itself, and to focus on higher-order needs.

A good information security program should simply allow the organization to manage the risks that it will most likely face, thus providing the kind of stability needed for it to go about the business of achieving its ambitions. In this way, INFOSEC is just as critical a piece of the overall formula for success as a viable offering, a good marketing plan, and the ability to accept customer payments.

3 How Does INFOSEC Relate to HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a law that charges the Department of Health and Human Services to establish regulations for the handling of certain types of health information (HI), collectively known as “protected health information.”

HIPAA itself does not establish the regulations, but provides the framework for regulations (generally known as “rules”) in four areas: *transactions and code sets*, *identifiers*, *privacy*, and *security*.

Transactions and code sets deals with the correct and complete transfer of information between health care entities. The idea is that electronic data interchange (EDI) will be made easier by having industry-wide standards for interchange codesets. Rather than needing to negotiate data interchange code sets each time that two entities establish a relationship, the entities can simply refer to a particular HIPAA transaction code set.

Identifiers is the specification for uniquely identifying entities in the health care system. Health care providers, clearing houses, and insurers are all given unique identifiers within the U.S. health care system to ease the identification of those entities.

Privacy is the rule that provides guidelines intended to protect the confidentiality of health information. Standards for identification and authentication of people and organizations requesting HI are enumerated in this rule.

Security is the rule that deals largely with the technical measures used to enforce the organization’s information-handling policy. Certain provisions of the Privacy Rule will require implementation of the Security Rule for enforcement.

For our present discussion, the Privacy Rule and Security Rule are most important.

Privacy is best defined as “informational self-determination.” HIPAA’s Privacy Rule helps to support large-scale privacy by providing policy guidelines, basically

spelling out who may share what with whom. The Privacy Rule goes a step further, actually providing additional requirements that deal with the *risk* of accidental exposure. Thus, operational procedures are also impacted. FAX machines, for example, used in connection with protected HI may not be left unattended in open areas.

Security, when defined broadly as the “enforcement of policy,” is achieved through both operational requirements and technical requirements of systems that deal with protected HI. To this end, HIPAA helps covered organizations to achieve security by providing a clear standard as to what minimum protection must be offered. The benefit that this provides is uniform protection of HI, and helps covered organizations to understand just where they are expected to draw the lines between functionality and security.

Information security is one of the goals of HIPAA. Through its Rules, clear and consistent standards have been established that will help covered entities to understand:

- Which kinds of information are critical (through the definition of protected health information);
- How to support confidentiality of information (through the policy framework articulated in the Privacy Rule);
- How to support integrity (through the interchange standards in the Transactions and Code Sets Rule, uniquely-identified entities in the Identifiers Rule, and the technical data integrity standards established in the Security Rule);
- How to support availability (through provisions in the Security and Privacy Rules).

Building an information assurance program that not only adheres to the letter of each of the rules, but supports the spirit and higher-order goals of HIPAA will not only help you to avoid regulatory compliance problems. Supporting the security of health information will also help the U.S. health care system to be worthy of its patients' trust.□

Matt Curtin is the founder of Interhack Corporation (+1 614 545 HACK, <http://web.interhack.com/>), a Columbus-based information security, privacy, and forensic computing firm, providing assessment, evaluation, and testing services to support policy definition and enforcement, as well as regulatory compliance to clients all over North America. He is also a lecturer at The Ohio State University, in the Department of Computer and Information Science. Matt is a certified information systems security professional (CISSP), holder of the U.S. National Security Agency's (NSA) INFOSEC Assessment Methodology (IAM) certification, and maintains active memberships in InfraGard (FBI's cooperative effort to protect the U.S. infrastructure), the Association for Computing Machinery (ACM), the Institute for Electrical and Electronics Engineers (IEEE) Computer Society, and USENIX (the advanced computing association). Matt is the author of *Developing Trust: Online Privacy and Security* (Apress, 2001).