



Just What is Information Security Anyway?

When asking your IT leadership just what information security is, he or she may answer that it involves securing and protecting the electronic information within the IT infrastructure. Your IT leadership is only partially correct.

Information Security as defined by ISO17799 is *“an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.”* ISO17799 goes on to state that *“information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation.”*

Based upon this definition and the standards body from which it comes, it is clear to see that information security is much more than technology. Technology in fact is but a by-product of the overall security management practice that the organization need realize and employ. Information security must also ensure the information systems, organizational characteristics and operational standards are aligned to result in an information risk posture that is acceptable. Information systems pump life-giving information throughout the organization and therefore must perform well and be available when needed. The people of the company are trained to interact with that information and do so in a consistent way that yields the targeted quality of output. You must ask yourself: Can we afford to not safe-guard our money, image, reputation and potential - perhaps its very existence? What can I do to minimize the risks?

The consequences of security incidents can be disastrous - but they are avoidable. The old physical approach to security remains important but as businesses acquire a new virtual identity, it is not enough. A holistic, business oriented, cross functional approach is needed. Apart from commercial reasons for protecting information, businesses also have legal obligations to take care of personal information entrusted to them. Good information security implies actions which relate to the prevention of unauthorized or unlawful processing and of accidental loss or damage to the information. Information security also implies the availability information systems to meet the needs of the business. This means the implementation of an information security risk management practice that focus's on the business impacts of information security threats. This means planning for scenarios that could affect information security or the ability to provide information services.

Many organizations automatically delegate their security concerns to their IT departments whether it is due to HIPAA regulations, SAS-70 requirements or Graham-Leach-Bliley requirements. IT, that panacea for all your organizations information security needs (and focal point for blame when failures of various flavors occur) will get the job done. The

inherent nature of IT staff and the innate optimism that any problem can be fixed through technology provides you a sense of calm and well being that is in fact, false. Not to diminish the importance and capabilities of IT, but too much emphasis is placed upon technical solutions in solving information security needs. Is it enough to know that the firewalls are in place, DMZ fully functional and the intrusion detection system with multiple sensors are working and the incidence response team is charged and ready to go?

Information security starts with administrative controls that come from the top, most effectively in the form of written policy and standards, demonstrating due care and diligence, and serve as the blueprint for the overall organizational security model. Administrative controls guide and control the way work is performed and information is processed & protected. It permeates the entire organization and becomes a living, breathing entity governing people's behavior in ensuring the confidentiality, integrity, and availability of your information assets. It is a framework that must include all functional areas within your organization, technical controls and physical components that make up the symbiotic ecosystem called information security are derived from these administrative constructs. Administrative controls such as policies, procedures, guidelines, business continuity requirements, management constraints, methods for accountability and standards need come after executive commitment for an overall security management practice is clearly communicated and actively supported. Periodic security reviews and audits, new hire background investigations, separation of duties and duty rotation programs as well as periodic performance evaluations and an enforced vacation policy help determine how well your administrative controls are working and serves to detect fraud and abuse of your information assets that might otherwise go unnoticed. Such practices ensure the long-term viability of the information security program and promote alignment of IT & physical security with the organizations business needs.

Equally important but following in a sequential manner are the technical and physical controls. Technical controls consist of security hardware, smart cards, identification, encryption, authentication, anti-virus software, PKI, content filtering software, passwords, logging and audit trails, monitoring, event correlation software, and access controls that apply for the most part to IT. Physical controls are just that. Security guards providing facility protection, surveillance, perimeter and intrusion monitoring, locks, badges, alarms, backup power, motion/smoke/fire detectors, CCTV, fences, fire suppression systems, biometric devices, media handling and proper disposal, and other physical security mechanisms help protect your information assets from espionage, acts of terrorism, theft, and destruction or damage by accident, fire, or natural disaster (e.g., floods, hurricanes, tornados, and earthquakes).

In unison, administrative, technical and physical controls create a powerful security management practice. Your first thought may be that this is much more than we have considered as an organization. This may be beyond the convention view of security in your organization. You may wonder "How are we to tackle such a huge undertaking? How can we implement something that is in fact a culture shift? Where do we start?"

There is no way that you can expect to implement all these changes overnight. It takes time and careful strategic planning that can extend over several months and even years to get to the point of a tightly woven and fully integrated security management practice. As an example, HIPAA, which regulates information security practices for the healthcare industry, grants an organization from 24 to 36 months, depending upon certain criteria, to become compliant with the defined information security practices. Given the scope, it is clear that financial burdens need to be understood, planned for and spread out overtime. Daily activities need to run smoothly as your organization takes tactical incremental steps to towards compliance and the ultimate goal of true information security.

So where do we start? Typically, training and awareness programs that define information security are a good starting point. Tailored to the different levels within an organization, this program builds the foundation for understanding information security. In order to understand the policies, standards, training, and technology that your organization needs to protect your information assets, you need to understand information security fundamental principles and the rationale behind the processes. Security awareness and education programs help establish, maintain, and raise your employees' awareness of risks and threats. Knowledgeable employees will increase your overall security. Once you have performed the initial wave of training and the executive level has communicated and demonstrated their full support for your security management practice, an overall organizational gap analysis and risk assessment needs to be performed. It is from this effort that plans for the near-term and future information security needs will emerge.

There is a great deal more that can fill volumes on information security. Much more than this column will allow. Suffice to say that information technology is only a piece of the puzzle. Information security is a pervasive business concept that touches individuals across your organization and even beyond it. Before turning over your organizations information security effort to IT, ensure your IT leadership has the business acumen and organizational knowledge to handle the task. IT leadership must be fully in tune with your business needs, requirements, and organizational culture in order to successfully embark upon such a challenge.

The results of an effective information security program reach beyond the technical domain of firewalls and virus protection and affect the core viability of the business. Information security protects the building and the email but also protect product and service availability and quality. In general information security assures the continuance of normal business operations free from physical damage, operational disruption damage to the company's image. Not having an information security program leaves you susceptible to the same. Can you afford to take that risk?

Jeffrey S. Bardin
Chairman & CTO
Treadstone 71
jbardin@treadstone71.com

