Keep your business assets safe

Part II: Organizing your organizational security

This is part two of a four-part series that identifies business information assets, helps business owners understand the value of their information and then explains how best to protect information as a valuable business asset.

Last month we began our journey though the vast world of information security. We talked about identifying the true value of a business's information – the cost of acquiring the proper software and hardware; the cost of implementation and training, and staff-hours needed to create and manage the data. We pondered the potential cost of a information security breaches – time and money invested into it, lost production and sales during the downtime, cost of recovery or recreation, and overall customer loss of goodwill.

Creating a secure, safe environment for your business information may seem like a daunting task but it can be done with a little planning and persistence. First, one needs to understand that security isn't just a technical issue. According to the Computer Security Institute (CSI) – in conjunction with the San Francisco Cyber Crime Taskforce office of the FBI – noted in 2004 that 34.5% of all intrusions occurred from outside the organization; another 34% occurred from internal intrusions; and the balance of the intrusions were from unknown sources. What this tells us is that we are as much at risk from within our own organization as we are from outsiders. Because of this, every business should evaluate security from three points of view – organizational, technical and physical. In this article, we will examine the issue of organizational security.

Organizational security begins with your overall attitudes about protecting assets within your organization. Do you know the true value of your information? Have you developed an information security plan with defined policies and procedures? Have these been communicated to your employees so that they understand their importance? Security implementation is no better than the attitudes establish by management. Based on this, the organizational component of security is as important – if not more so – then the technical or physical components. Management is responsible for establishing best practices, making sure employees understand and agree with the practices, and ensuring that staff adheres to those practices.

Organizational security practices are standard processes that ensure ethical, safe operations. They establish who, what, where and how the business will operate, and their importance is most valued in the prevention of a disaster or loss of business operations. Best practices begin with a policy.

The definition for policy is "a program of actions adopted by an individual, group or government, or the set of principles on which they are based." In an organization, this means a policy establishes the rules and processes employees must follow to ensure proper operational integrity. All good policies include:

- Purpose – A general statement of the policy, such as the rule or guideline to be applied.
- Scope – The who and what the policy applies to, i.e. all employees, all Internet users, etc.
- Acceptable and Unacceptable Use – Outline, if applicable, of what are acceptable and unacceptable practices.
- Audit – A plan for how the policy will be monitored for acceptable usage.

- Enforcement – A plan for how the policy will be enforced, what will happen if the policy is not followed or violations of the policy occur, and including disciplinary actions if needed.

Once the policy is written, procedural actions should be outlined. Procedures generally explain which steps employees should follow on a regular basis. They should also include acceptable versus unacceptable alternative actions, as well as actions that will be taken should the policy be violated.

Policies and procedures, for example, are fundamental to hiring and termination practices within your organization. To maintain information security, policy and procedures are necessary for employee Internet usage, working late, and even closing and locking up after business hours. These examples of policies and procedures help limit unwanted intrusions on your informational and physical assets. All policies and procedures require an implementation plan that includes auditing and enforcing.

The audit process provides checks and balances for the whole policy and procedural system. An audit plan should include tactics for monitoring and reviewing the policy. The audit should define – through documentation and reporting – what constitutes a violation of the policy and which tools will be used to discover the violation, such as Internet usage tracking or routine assessments of physical security measures. Finally, managerial enforcement of the policy is essential to effective security. Upon identification of a policy violation, disciplinary or corrective actions need to be taken. It is important to have an enforcement plan in place.

Once this process is complete, you are ready to prioritize areas of need, identify specific assets at risk, determine the value of those assets and the potential return on security investment and finally the development of a comprehensive security plan that:

1. Fits your organizational needs,
2. Can be communicated, agreed to and supported by your employees and
3. Gives your physical and informational assets the best protection within your budget.

How to do this:

4. Have a security audit or risk assessment performed by a qualified outside consultant or consulting firms (how to determine if qualified)
5. Based on findings and recommendation prepare a security plan to address and implement best practices for your business.
6. Create a communication plan to communicate and educate your employees on good security practices as outlined in your security plan.

In closing, security isn’t a technical issue or a financial issues or even just a physical control issue. It is a combination of organizational attitude and direction, good integrated and appropriate technical controls and finally good physical controls.