DITY™ Weekly Newsletter
itSM Solutions® IT Experience. Practical Solutions
The workable, practical guide to Do IT Yourself Vol. 6.21 • May 29, 2010

Making Security a Business Decision

By Thomas Witwicki CISSP, CISM, CIPP
Thomas Witwicki is the President of Assurance Point LLC, an organization created to help businesses manage information risk, and can be found at www.assurancepointllc.com.

Security is a business decision. Decisions about security cannot - and should not - be delegated to IT or even Information Security.

Why? Because a decision about security is a decision about risk. Information risk defines how much is at stake for a business (read $$$) if the confidentiality, integrity or availability of an information asset is compromised.

Security is a Business Decision

How much risk a business can accept is determined by its culture, its sensitivity to reputational damage, the laws and regulations it is subject to, and its tolerance for loss.

In my role as an information security and privacy consultant, I help organizations of all types and sizes manage the risks and liabilities of information. Coordinating IT security with business security comes as no surprise to IT Service Managers because, as ITIL V3 so succinctly states, "The goal of Information Security Management is to align IT security with business security and ensure that information security is effectively managed in all service and Service Management activities."

However, the purpose of aligning IT and business security measures runs far deeper than making sure everyone is singing from the same page of the song book. I believe that having an effective risk acceptance policy is the key to aligning IT with the objectives of the business, one of the primary goals of IT Service Management (ITSM).

Risk Acceptance Defined

When an organization makes a decision about risk it can make only one of three choices:

1. *Accept the risk as assessed* - the organization is willing to tolerate the potential impact of a compromise of security.
2. *Mitigate the risk* - reduce the level of risk through improved controls to an acceptable level.
3. *Terminate the activity* - this implies that the risk cannot be cost-effectively reduced to an acceptable level for the business activity that is creating the risk.

The way these decisions are made and by whom are defined in the organization's Information Security Policy. High-level risk decisions may need to be made by an Executive Committee while low levels of risk may be decided by a business owner.

In all cases, the decision should be based on a formal assessment of the actual risk. Not surprisingly, this is called a Risk Assessment and it is the job of Information Security to ensure that risk is assessed on a regular basis.

The Task of Assessing Risk

Risk = Impact x Threat x Vulnerability. This is not an actual mathematical formula, but is an equation that states that risk is a combination of the impact of a loss and the ability of a threat to exploit a vulnerability.

A Risk Assessment analyzes all of these factors to determine a level of risk. An organization's controls are also analyzed to determine if they are up to the task of managing the vulnerabilities. There are quantitative (i.e. $$$) and qualitative (e.g. high, medium, low) methods of risk assessment; both are designed to communicate risk for decision-making.

The SLA Connection

How much security is enough? The business has already made this decision in its formal acceptance of risk. On a practical level, the Service Level Agreement (SLA) can either refer to the organizational Risk Acceptance Policy, or define it in more detail for the particular service in question.

Often the SLA documents the frequency of risk assessments to be performed and defines the business owner who is able to make decisions about risk and at what level. It also might define levels of risk for which decisions must be delegated to other individuals. An SLA should produce cost-justifiable IT investments, and the risk acceptance process automatically produces cost-justifiable investments in security controls.

To Wrap it Up

As I stated earlier, I am a security and privacy consultant, but I did not travel that path directly. For the majority of my career, as an ITIL V2 Service Manager, I managed IT infrastructure and embraced the principles of ITSM. Now, as in my earlier career, it is embedded in my DNA to have a firm business foundation for the services I am responsible for delivering.

Information security has assumed much more importance to organizations in recent years due to regulation, reliance on systems and customer and employee privacy concerns. This criticality should be reflected in risk decisions made by the business owners directly experiencing potential loss.