

How to Mitigate IT Risks with Security Education and Training

By Paula W. Hamm, Vice President, Symantec Education Services

IT risk management is a practice for balancing the costs of developing robust and secure IT infrastructure against the likelihood and potential damage to the organization should an incident occur. IT risk management is generally divided into four categories:

- Security: Keep bad things out and important things in.
- Availability: Maintain the system and ensure rapid recovery.
- Performance: Optimize resources and ensure correct configuration.
- Compliance: Ensure adequate controls and automate evidence collection.

Corporate IT related incidents are attracting an ever increasing share of the public's attention. News headlines announcing the loss of unencrypted personal information on stolen laptops, credit card numbers stolen from corporate IT systems, business disruptions due to computer outages, and IT infrastructures failing corporate customers due to heavy load are all too frequent.

Putting People in the Process

Educating employees so they understand how IT risks can impact an organization is an indispensable step towards properly managing those risks. Organizations frequently focus on mitigating risk by investing in new technologies, while failing to leverage the most critical asset - people.

Common internal causes of corporate IT related incidents include poor password protection, failure to update protection software, failure to scan files, inappropriate on-the-job Web surfing and file downloading, and social engineering (techniques used to manipulate people into performing actions or divulging confidential information). The potential impact of these incidents leaves the infrastructure exposed and the organization vulnerable to exploitation, attack, and loss of proprietary information. These security gaps can also prompt a high rate of virus infection (and re-infection), along with a reduction in available network bandwidth. Ultimately, all of these translate into lost productivity due to downtime and increased costs to repair programs and replace lost or stolen equipment.

People are valuable resources and play a significant role in ensuring the security of an IT infrastructure. Through proper training and education employees can be key players in mitigating IT risks. According to a report issued by Gartner, implementing an effective security awareness program can eliminate time spent reacting to security incidents and lead to a 25 percent productivity savings.¹ This means that employees can focus on what they do best – their jobs.

Mitigating Risk through Education

Contrary to popular belief, IT departments should not shoulder the responsibility of managing risk alone. Security is everyone's job, and when it comes to information security, people are as important as technology, policies, procedures, and guidelines. However, it is unrealistic to expect employees to handle the complexities and nuances of today's security environment without any preparation. With proper education and training, employees can become an organization's strongest line of defense and its most valuable security asset.

When designing a training program, IT organizations should keep in mind the four risk management categories: security, availability, performance, and compliance. They should also follow several best practices which are outlined below.

¹ Gartner: [Information Security Awareness Training Is Essential to Protect IT Assets](#). Witty, Roberta J, et. al. 11 January 2005

Security risk

- Improve incident reporting and handling
- Properly classify and protect intellectual property
- Reduce unsafe communication channels such as Instant Messaging
- Design and implement more secure applications and infrastructures
- Educate all employees on the importance of security awareness

Availability risk

- Take a more proactive approach to IT availability issues
- Demonstrate the importance of proper backup procedures
- Increase awareness of common virus & trojan attack vectors, such as email attachments and file downloads
- Educate application developers on the importance of building robust and stable applications

Performance risk

- Demonstrate proper use of network assets (e.g., not watching online videos during office hours)
- Increase attention to system performance in IT systems design
- Educate application architects and developers on their ability to positively impact performance-related issues in IT systems

Compliance risk

- Support and follow internal IT safeguards and business policy requirements in an effort to help meet compliance standards such as FISMA, Gramm-Leach-Bliley, HIPAA, Sarbanes-Oxley, COBIT, and ISO 17799:2000

Successfully protecting information assets requires employees at every level—from the top down—to obtain a basic understanding of the security risks and policies, as well as their respective responsibilities in protecting the company's assets. Without this understanding, organizations cannot hold employees accountable for protecting the organization's resources.

The time has passed for the 'reactive' security model, where security incidents are always dealt with after the fact. Today's security environment has become so complex that the reactive companies will always be playing catch-up. Progressive companies must take a proactive approach that involves their people more in the company's IT risk management strategy. In the long-term, this is the only way to reduce the associated costs and maintain any level of security.

###