

Sterling-Hoffman

EXECUTIVE SEARCH

Specialists in Software, Sales, People.

INTERNATIONAL HEADQUARTERS: 425 UNIVERSITY AVE., SUITE 800, TORONTO, ON M5G 1T6 TEL: (416) 979-6701 FAX: (416) 979-3030

Toronto, ON

Mountainview, CA

Burlington, MA

www.SterlingHoffman.com

Corporate IT Security Resources are Wasted!

By Al Payne and Jim Litchko, Internet Security Experts

Published in The Sterling Report, April 2006

Thirty percent of IT Security resources are wasted, because of the inappropriate approaches that are used to review a corporation's IT security needs and the misunderstanding of the roles and responsibilities for each of the key players: executives, IT managers and IT security professionals. Effective IT security programs are achieved when the IT manager is open, honest, motivated and realistic about the IT security status. This begins with conducting a practical system security assessment and ends with providing adequate safeguard options to reduce risk to an acceptable level for the business.

Thirty percent of IT Security resources are wasted, because of the inappropriate approaches that are used to review a corporation's IT security needs and the misunderstanding of the roles and responsibilities for each of the key players: executives, IT managers and IT security professionals.

Effective IT security programs are achieved when the IT manager is open, honest, motivated and realistic about the IT security status. This begins with conducting a practical system security assessment and ends with providing adequate safeguard options to reduce risk to an acceptable level for the business.

All too often, IT program managers are fearful of what security problems they will uncover, because they believe finding vulnerabilities reflects negatively on their work or it creates one more thing that they will have to correct on a long list of actions items. The supporting IT security professionals, either on staff or consultants, are typically very enthusiastic about finding vulnerabilities and recommending the ultimate (most secure, complex, technical and expensive) security solutions. The IT program manager finds no practical support from them resulting in a non-cooperative relationship between them. This further exasperates the problem.

This is where management and leadership must step in to set expectations by defining responsibilities and establishing a new approach for reviewing IT security.

Sterling-Hoffman

EXECUTIVE SEARCH

Specialists in Software, Sales, People.

Toronto, ON

Mountainview, CA

Burlington, MA

www.SterlingHoffman.com

Defining Responsibilities

First, executive management must ensure that all the players understand what their IT security roles and responsibilities are in providing security:

- The on staff security professionals, who are sometimes responsible for implementing, testing and monitoring the security of the systems, identifying any outstanding vulnerabilities in the system, and providing multiple safeguard recommendations for reducing the security risks to the system to an acceptable level.
- IT managers are responsible for understanding the security vulnerabilities impact on the business operations, provide a concise non-technical presentation with multiple solutions to management, and making a business/system based recommendation to management.
- Executive management are the only persons who can be responsible for determining "what is the business or mission based risk level that will be acceptable", not the IT manager or the security professionals, and make the final decision on the security solution to be deployed.
- The IT manager and security professionals will implement the final decision.

Knowing that the final decision on what risk level is successful is key to motivating the manager to demand a risk assessment. This one action will remove the IT manager's and security professional's frustration related to their feeling responsible for ensuring that their system must be 100% secure and that any security breach "outside of the acceptable risk perimeter" is their fault.

Second, executive management must also establish the procedure that the IT manager will offer multiple options, technical and non-technical, when presenting an IT security concern. The IT manager must also provide supporting business impact analysis so that the executives can make clear, realistic and cost-effective decisions. Requiring these two actions will help to eliminate the executives sitting through long, frustrating, complex, non-comprehensible, technical discussions that end with one expensive, "do it or die" solution.

Establish the Right Approach

Having established these responsibilities and procedures, the IT managers and security professionals must be re-oriented to approaching security from a business perspective. Why is this important?

There are three approaches that managers and security professionals use to approach IT security.

These approaches are:

- The Secure It approach
- The Technology approach and
- The Business approach

Sterling-Hoffman

EXECUTIVE SEARCH

Specialists in Software, Sales, People.

Toronto, ON

Mountainview, CA

Burlington, MA

www.SterlingHoffman.com

The first two approaches lead to inefficiencies and frustration. Our experience shows that the business approach is the most effective method to implementing acceptable business-based risk levels.

Why are the Other Two Approaches Less Effective?

The Secure It approach is where the goal is to build a 100% secure system. This approach is often accepted by "risk adverse", "risk avoidance" managers, who are easily persuaded by FUD (Fear, Uncertainty and Doubt) justifications or scare tactics from vendors or consultants. This is also an unaffordable and unachievable goal. The FUD approach is often very expensive and the 100% goal is unrealistic and businesses can never afford a system that is never 100% secure.

The Technology approach's goal is to prevent attacks on a system using technical solutions (i.e., firewalls, encryption, intrusion detection, authentication tokens, etc.). Security justifications, using technical terms and complex explanations (i.e., SSL, Cracker, DDOS, VPN, IDS, PKI, etc.), rarely provide management with a clear understanding of the problem and their options, making it very difficult for them to make an effective security decision.

After supporting over 150 security assessments on systems that have used these approaches, we have identified the following truths:

- A 100% secure system is not affordable, nor will it meet operational requirements, or be user acceptable
- Using the best, complex and strongest security solutions can kill a business faster than any hacker, insider, virus, worm, or terrorist
- The most successful system security programs are 10-30% technology to augment the traditional security solutions (policy, procedures, physical, personnel, etc.)
- Securing any system without understanding the organization's business model, operations and the users' culture, capabilities and expectations will negatively impact the corporation's profitability. It will also result in dollars being spent on ineffective safeguards.

A Business Approach

The best approach is from a Business perspective where the goal of security is to meet an organization's business goals and objectives. This approach starts with knowing the organization's business goals, operations, information flow, and users.

Business is about meeting the goals and objectives of the organization. What is the business of the organization? Examples might be: providing services, distributing information, selling and shipping products, reserving transportation or properties, etc.

Operations are about how they accomplish the goals and objectives and with what structure. Some examples might be: interfacing with banks, shipping products, communicating with partners and employees, advertising products and services, etc.

Building Software Companies... One Leader at a Time.

Sterling-Hoffman

EXECUTIVE SEARCH

Specialists in Software, Sales, People.

Toronto, ON

Mountainview, CA

Burlington, MA

www.SterlingHoffman.com

Information Flow is important because: it explains how things are controlled; how people receive the information they need to take actions and/or make decisions; what is sensitive and what is public; how fast information has to move; etc.

Users' expectations, culture, environment and capabilities (knowledge and capabilities – computer and network connections) are critical to determining what security solutions will be most effective for a system. Would an accountant and researcher accept the same authentication solution? What personal information is considered sensitive to individuals filling out the forms? What would be the result if an online store required the buyers have a smart card to conduct a transaction? Do they understand why security is important to the business?

The **Business** approach allows anyone to gather the security information without asking a single intimidating security question. This makes the security assessment a more cooperative effort for corporate personnel. It also allows for everyone to understand why the system is there, how it operates, what elements are critical, and why security is required. Examples:

The computer providing the corporate homepage only needs integrity protection to protect it from unauthorized changes. Whereas, the system selling products must protect customer information, so it requires confidentiality, integrity, and authentication.

The system providing forms can be down for days, but the system coordinating harvested organs transfers must be available 24/7.

The **Business** approach will also give the system manager an understanding of the business, business terminology, motivations and justifications. The manager will then be able to explain the need for security in business operations' terms to senior management.

Finally, it will allow senior management to understand how the system's residual security risks and deviations from standards need to be corrected or are acceptable for business and operational reasons. This also allows management to make cost effective decisions related to corporate security.

Summary

Identifying each individual's responsibilities and basing IT security on business needs are the keys to effective IT security and to reducing frustrations at all levels of the organization.

Sterling-Hoffman

EXECUTIVE SEARCH

Specialists in Software, Sales, People.

Toronto, ON

Mountainview, CA

Burlington, MA

www.SterlingHoffman.com

Al Payne, CISSP, has 30 years of IT experience including nine years in security. He is a Certified Information Systems Security Professional (CISSP), has been a business owner, executive, operational manager, strategic advisor for business, and is an entrepreneur whose business plans have secured millions in business capital. He is also senior computer security consultant for Certification & Accreditation, Risk Assessments, Plan of Action and Milestones (POA&M), and co-author of "KNOW Cyber Risk". For article feedback, contact Al at alpayne1@earthlink.net.

Jim Litchko, CAS, is Founder and President of Litchko & Associates, Inc., which provides proactive, innovative approaches for industry and government managers and executives to secure their IT systems. He has 30 years of security experience, including five years at the National Security Agency (NSA), has conducted over 100 security assessments, and worked as an executive at three IT security companies. Since 1988, he has been an adjunct professor at Johns Hopkins University and taught courses at many professional security institutions. Jim is also a professional member of the National Speakers' Association and the author of "KNOW Your Life and KNOW IT Security". For article feedback, contact Jim at jim@litchko.com

Building Software Companies... One Leader at a Time.