

# A BALANCED APPROACH TO INFORMATION SECURITY

Richard Sheiman, President  
InfoScreen, Inc.  
Ithaca, New York  
sheiman@infoscreen.com

## ABSTRACT

*The importance of Information Security is widely acknowledged. Corporations invest significantly in firewalls, intrusion detection systems, and the network administration resources to support these technologies. Denial of Service attacks, network hackings, viruses, and other Internet based vulnerabilities have led to a myopic focus on technology oriented information security risks. Effective risk management for trade secrets, Intellectual Property (IP) and the systems that support business requires a holistic view of the Information Security challenge. Companies must look beyond network security to more actively consider how people handle their information assets. The best technologies are of limited value if employees don't recognize the importance of the company's information assets and participate in the security process. This paper provides senior managers with a framework for managing these risks in a manner that better reflects true vulnerabilities and actual adversaries.*

## WHY IMPROVE INFORMATION SECURITY

There are a variety of motives for a company to adopt Information Security best practices:

- **Competitive Advantage:** Many companies rely on the security of their Intellectual Property as a foundation for future competitiveness.
- **Operational Considerations:** Companies increasingly rely on the sustained availability of their information systems. Poor security practices can result in IT system downtime.
- **Commercial Imperative:** Many business partners are disinclined to do business with companies that have poor security, which breeds a reluctance to share sensitive information.
- **Regulatory Pressures:** HIPAA, GLB, Sarbanes-Oxley, and other regulations apply pressure on companies to adopt sound security practices.
- **Legal:** Poor security can create legal problems, such as allegations of negligence, breach of fiduciary duty, or privacy violations.

- **Goodwill:** Companies risk injury to their goodwill should they develop a reputation for cavalier security practices.
- **Financial:** A joint study between the Computer Security Institute and the FBI reports that companies willing to quantify financial losses due to security breaches report an average loss in excess of 2.04 million dollars. The most serious losses reported the theft of proprietary information, with losses averaging over 6.5 million dollars<sup>1</sup>.

## NARROW FOCUS ON TECHNICAL SECURITY

Companies that recognize the need to improve information security tend to focus narrowly on technical information protection. Executives often believe that the latest high-tech defenses will adequately safeguard their information assets. This focus is reflected in the statistic that more than 40% of companies report that they plan to implement three or more security technologies between now and 2005<sup>2</sup>.

While technical threats to proprietary information remain substantial, in reality roughly 70% of security breaches that involve losses above \$100,000 are perpetuated internally, often by disgruntled employees<sup>3</sup>.

True corporate espionage is often dismissed as a Hollywood fiction. In reality, virtually all companies engage in some sort of competitive intelligence work and many companies cross the line into unethical or illegal non-technical activities to gain a competitive edge. In a widely publicized recent case, P&G volunteered to the press that its traditional competitive intelligence project to gather intelligence on Unilever and others had gone awry<sup>4</sup>. Alleged non-technical methods included social engineering, dumpster diving, and other tactics.

The best defense against corporate espionage is to create a Human Firewall in which employees are trained to identify suspicious inquiries and other events, along with the tools to proactively respond to such incidents. An ad-hoc approach which contains the process of information protection within the realm of IT departments without viewing the overall security environment of a company will inevitably deliver poor results.

## A BALANCED APPROACH

Once a company determines that Information Security is essential to maintain competitive advantage, a structured risk management framework is required. In order to maximize a company's overall security performance with a finite commitment of resources, the security process must be balanced across the organization.

This framework segments the information security challenge into three focus areas:

- 1) Network security - the hardware, software, and policies in place to restrict access to digital and recorded information. Network security includes firewalls, system security settings, password controls, network architecture, and the policies and procedures put in place to protect sensitive electronic data.
- 2) Physical security - the systems and hardware in place to restrict and control the movement of people and documents into and out of facilities. Physical security includes name badges, keys, cameras, and other hardware to control and track access as well as the policies of identification and control used to restrict movement between physical areas.
- 3) Organizational security - the security awareness and actions taken by the employees and management of an organization on a daily basis. Organizational security includes the collective understanding of security policies, the actions management takes to enforce compliance, and the actions that employees take to protect sensitive information and maintain a secure Human Firewall.

The greatest risks to sensitive information and information systems will reflect a company's weakest links. Effective risk management requires a balanced approach across these three focus areas. Relatively poor security in one area will undermine security in the other areas and compound the organization's overall risk. For example, a strong network perimeter and other IT controls will not provide good security if employees can be easily duped by passcode requests from social engineers or if network users do not follow acceptable use policies for IT resources.

It is useful to map a company's security preparedness against the threats it faces in each of the three focus areas listed above. Threat refers to the forces which jeopardize information and systems and include hackers, disgruntled employees and other likely adversaries. By visually mapping threats, this exercise serves as a gap analysis to highlight where the security improvement efforts should be concentrated.

To illustrate the application of this framework the security protecting information and the threats facing a representative company are presented in the following figures:



Figure #1 – Network Security

Figure #1 shows that the company faces substantial network security threats, perhaps reflecting a highly mobile workforce or heavy use of web applications that provide partners with access to sensitive information. The company's network security is prepared to meet this threat with strong technical controls in place. The network Security Bar is flat, indicating a carefully designed and managed network environment.

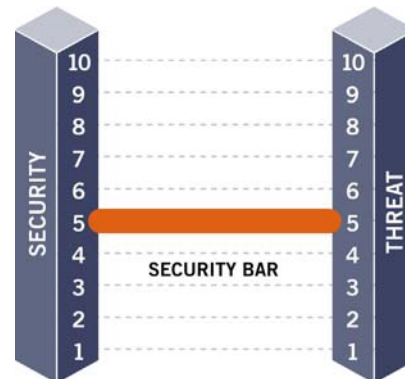
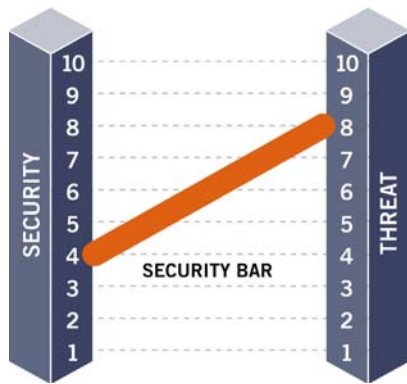


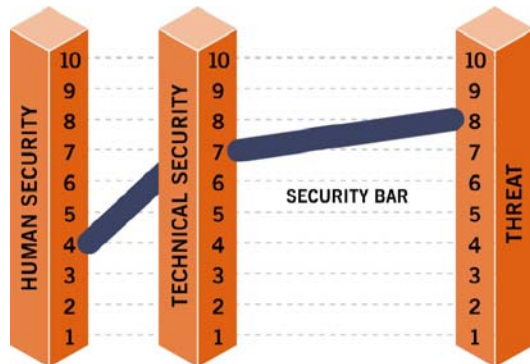
Figure #2 – Physical Security

Figure #2 indicates physical security threats that are collectively less pronounced than the company's network threats and physical security that is prepared but not over prepared to meet this threat. This is a common scenario, reflecting the maturity of trespass laws and the unlikely chance that adversaries will actually compromise a physical perimeter to jeopardize information or systems. Typical factors that may escalate physical security threats include satellite facilities, home offices, DOD facility clearances, and the presence of valuable goods.



**Figure #3 – Organizational Security**

Figure #3 indicates that the company faces pronounced threats to its organizational security, perhaps reflecting poor morale or the presence of direct competitors in the same community. The organizational Security Bar is seriously imbalanced due to a range of poor business practices undermining organizational security such as incomplete policies, employees that are not aware of security risks, and weak or non-existent compliance testing. While security breaches can occur elsewhere, there is a great likelihood that any serious injury will be traceable to an organizational security flaw.



**Figure #4 – Overall Security**

Figure #4 maps the company’s overall security, segmenting the vulnerabilities into technical and human indices. The imbalance across these two indices undermines overall security and heightens the risk of damage to competitiveness, productivity, and financial performance.

**INTERNAL EXPERTISE**

One of the most common pitfalls in establishing a sound information security program is to rest the responsibility squarely on the shoulders of an IT Director or purely with outside consultants. A sound security program is built from within and is based on leadership from across the organization.

Internal expertise can be formed through the creation of an internal Security Task Force with representatives from all key business functions that play a role in the Information Security process. Typical functions include HR, Legal, IT, Facilities, R&D, Finance, and Sales. This task force can tap external resources for the initial capacity and expertise required to assess and implement a robust security

environment. After the creation of sound policies and practices the security task force can lead the organization through the cultural shift to a secure environment.

A growing number of companies are creating the Corporate Information Security Officer (CISO) job function, or equivalent. The CISO is a senior manager who has broad responsibility for the company’s Information Security efforts across multiple corporate functions. This approach allows the company to address both the technical and human elements of a comprehensive information security program, in a manner that reflects the relative risks of many information loss scenarios.

**ORGANIZATIONAL SECURITY**

Once a structured and enterprise wide approach to the information security challenge is adopted, many companies discover that organizational security is the most difficult piece to devise and sustain. According to a recent Hurwitz Group survey of 500 corporations<sup>5</sup>, the greatest challenge to effective information security is not technology deployment. It is the far more difficult to overcome the human obstacles, including awareness training, policy enforcement, careless disclosure, error & omissions, and trade secret theft by insiders.

Organizational security is most difficult in a company that has an open culture. Employees and management appreciate this culture of openness, in terms of productivity and as the basis of a quality work environment. The most effective way to elevate Organizational Security is to build awareness around the concept of a Human Firewall. Employees understand that information is an asset and that they have roles and responsibilities to help protect it. By empowering employees to participate in the security process and form a Human Firewall, companies can dramatically improve their overall security performance.

Awareness training may yield the greatest returns among all of the information security risk management methods available to an IP driven corporation. Awareness training can dramatically reduce the risk of careless disclosure and social engineering exploits. Humans are social creatures. We like to talk and we seek the praise of others. A seasoned social engineer can develop great insight into a company’s operations and strategies simply by talking to people. A good awareness training program introduces ‘Need to Know’ principles and provides every employee with tools to participate in the information security process. A social engineer would need to shatter the ethical competitive intelligence line and possibly enter the criminal realm to extract sensitive information from a company that maintains a solid on-going awareness program that includes clear guidelines for handling suspicious inquiries.

## COMPREHENSIVE POLICIES

To legally protect trade secrets in the event of loss it is necessary for a company to adopt and enforce a comprehensive set of information security policies.

The following case demonstrates the pitfalls of poor information security policies and protections. In August 1999, Tyson Foods sued ConAgra, alleging trade secret theft, including a confidential feed formula. In its November 2000 ruling<sup>6</sup>, the Arkansas Supreme Court ruled that Tyson failed to adequately protect its trade secrets. The court noted "Obviously, the failure of a business to protect against the disclosure of information it considers to be a trade secret following employment is critical to our analysis and ultimate decision regarding whether the information is in fact a trade secret."

A common scenario for this type of information loss involves an employee who passes trade secret information to a competitor over the course of time in exchange for cash. In April 1999, the CEO of Four Pillars was convicted of paying an engineer at Avery Dennison \$160,000 over 8 years to obtain adhesive formulas and other trade secrets. Another common scenario involves a former employee who takes trade secrets to a subsequent employer. An often under-explored scenario is for business partners to violate their trusted relationship with trade secret owners. In March 1999, it was discovered that a patent attorney working for both Alcara BioSciences and Caliper Technologies passed trade secrets from one rival to the other.

All IP driven companies must have information security policies and associated legal instruments, such as invention assignment signatures and NDAs in place. The details of these policies, business practices, and legal instruments should reflect business culture and morale considerations. There is irony in the introduction of new security risks by creating disgruntled employees as a direct result of misguided information security initiatives.

Trade secret losses involving business partners are particularly difficult to prevent because they are generally unintentional and reflect the partner's lesser sense of ownership and responsibility for the trade secret information they possess. The IP owner's limited control over how the business partner handles this information presents real problems for risk mitigation. The best defense is to limit the business partner's exposure to trade secrets according to strict 'Need to Know' principles. Where trade secrets and other sensitive information must be disclosed in order for the business partner to perform its duties, well designed non-disclosure agreements should be in place along with a candid expression of the owner's expectations regarding the handling of its sensitive information.

Generally speaking, without comprehensive policies in place a company forfeits trade secret ownership rights in a court of law in the event of unintended loss through any means.

## CONCLUSION

Effective risk management to protect trade secrets, intellectual property, and information systems requires a balanced approach that takes into account the physical, network, and organizational security of a company. Sustained improvement of a company's security posture requires internal expertise and leadership, comprehensive policies that recognize the human side of security management, and ongoing awareness training to support a cultural shift to a secure enterprise.

## ABOUT INFOSCREEN

InfoScreen is a professional services firm that works with organizations to devise and sustain an optimal information security risk management program to protect intellectual property and stores of sensitive information. InfoScreen offers a comprehensive program of security risk and vulnerability assessment followed by policy implementation and compliance testing.

Contact Information:  
InfoScreen, Inc.  
118 Prospect Street  
Ithaca, NY 14850  
(607) 275-0292  
[www.infoscreen.com](http://www.infoscreen.com)

---

## REFERENCES

- <sup>1</sup> Computer Security Institute, April 7, 2002
- <sup>2</sup> Information Security, May, 2003
- <sup>3</sup> The Economist, November 1, 2002
- <sup>4</sup> Fortune.com. September 17, 2001
- <sup>5</sup> Schenk, Fanziska, "e-Business Security" [Hurwitz Group, Inc. proprietary research](#), July, 2001
- <sup>6</sup> Supreme Court of Arkansas, 00-446, S.W.3d, November 16, 2000