

# Creating Information Security Awareness

By Daniel I. Didier

June 21st, 2008

Original document available at [www.NetSecureIA.com](http://www.NetSecureIA.com)

**NetSecure★IA**  
*Secure Network Design and Information Assurance Consulting*

## Introduction

Perhaps your organization is one of the millions of covered entities required to comply with the FACT Act Identify Theft Red Flags Rule.<sup>1</sup> Under the newly drafted regulation, covered entities must implement a written “Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft,” and must be implemented no later than November 1<sup>st</sup>, 2008.<sup>2</sup>

Under the new federal regulation, any consumer or small business lender including banks, credit unions, mortgage lenders, auto dealers, credit card lenders, payday lenders, landlords, utilities, and communications companies must comply. Much like other federal regulations including HIPAA, SOX, FISMA, and GLBA that specify requirements for awareness training, failure to comply may lead to civil fines and regulatory enforcement action in addition to private lawsuits, negative publicity, and potential loss of business.<sup>3</sup>

Identity theft isn’t the only reason to implement an information security awareness program; the biggest threat to information security comes from the unpredictable, sometimes tired, annoyed, disgruntled, careless, negligent, or simply *unaware* employee. The challenges facing an organization that wishes to change their biggest information security risk, their employees, into their most proactive security tool are many. This essay explores key issues associated with implementing effective awareness training and the subsequent enablement of the Human firewall.

## The Human Firewall

Perhaps one of the most complex and powerful components of an information system, people, are also one of the most vulnerable. Similar to the way the difference between a good watch dog and a lousy one can be attributed to proper training so, too, can the difference between an aware employee and an unaware one.

When discussing information security awareness for end users, the primary concern is data confidentiality, with integrity and availability as secondary issues. To use an analogy: while driving a car, a person doesn’t need to know the intricate details of how the engine, braking system, and other components work, yet the power to cause or avoid an accident is in the hands of the driver. As such, a person must know how to brake and

---

<sup>1</sup> “Compliance Coach Identified 23 New Identity Theft Red Flags Based on Recent Cases and Schemes that Millions of Companies Need to Review Prior to Compliance Deadline.” Business Wire, May 5, 2008. [http://findarticles.com/p/articles/mi\\_m0EIN/is\\_2008\\_May\\_5/ai\\_n25379243](http://findarticles.com/p/articles/mi_m0EIN/is_2008_May_5/ai_n25379243) (accessed June 21, 2008)

<sup>2</sup> Horn, Russ. “Identity Theft Red Flags, the reader’s digest version.” Bankwide, May 26, 2008. <http://bankwide.com/index.php/Issue-5-May-2008/Articles/Compliance/Identity-Theft-Red-Flags-the-reader-s-digest-version.html> (accessed June 21, 2008)

<sup>3</sup> “Compliance Coach Identified 23 New Identity Theft Red Flags Based on Recent Cases and Schemes that Millions of Companies Need to Review Prior to Compliance Deadline.” Business Wire, May 5, 2008. [http://findarticles.com/p/articles/mi\\_m0EIN/is\\_2008\\_May\\_5/ai\\_n25379243](http://findarticles.com/p/articles/mi_m0EIN/is_2008_May_5/ai_n25379243) (accessed June 21, 2008)

avoid potential accidents. As a user of an information system, a person should know how to avoid potential security breaches and maintain a safe computing path.<sup>4</sup>

If employees are properly informed, trained, and educated on how to detect and respond to potential security incidents, they will become well-trained watchdogs continually looking out for the safety of the organization. The safety net created by information security awareness is described as a Human firewall.<sup>5</sup>

How can a Human firewall be enabled and what exactly does it mean to be a part of one? To put it simply, “the Human firewall is the state of an organization whereby people understand their role in ensuring the security of information and information technology, and are empowered to make prudent decisions about security.”<sup>6</sup>

To take advantage of this incredibly powerful security tool, a cultural change must occur within an organization, starting with the CEO and continue down the line to each and every employee. The concept of the Human firewall “has its foundations in the realization that information security is not just a technology concern confined to the IT department, but can also be affected by human management and worker behavior issues.”<sup>7</sup>

The Human firewall is often related to the end user, but the primary line of defense is the organizational decision makers or stakeholders. Stakeholders enable, provide, and support critical business services, yet often lack the skills, time, and foresight to apply proper security. As such, these direction setting individuals are a primary audience for information security awareness.<sup>8</sup>

## Enabling the Human Firewall

Once an organization’s stakeholders understand the risks associated with the workforce and the benefits of creating awareness they must then take the next step to enable it by implementing an organizational awareness program. As this process commences, it is important to separate the learning process and realize that it starts with awareness, continues with training, and finally evolves into education.<sup>9</sup> Awareness is different than training or education and can be characterized as follows:

- It is designed to draw attention to security and change attitudes. By becoming aware, employees are prepared for training by changing individual perceptions and organizational culture so that the criticality of security is recognized.

---

<sup>4</sup> Wohnlich, Thierry. “Building a Human Firewall: Raising Awareness to Protect Against Social Engineering.” CiscoPress, Oct 27, 2006. <http://www.ciscopress.com/articles/article.asp?p=663084&rll=1> (accessed June 21, 2008)

<sup>5</sup> Khan, Basheera. “Building the Human Firewall.” ITWales, May 13<sup>th</sup>, 2002. <http://www.itwales.com/999562.htm> (accessed June 21, 2008)

<sup>6</sup> Ibid

<sup>7</sup> Ibid

<sup>8</sup> Wohnlich, Thierry. “Building a Human Firewall: Raising Awareness to Protect Against Social Engineering.” CiscoPress, Oct 27, 2006. <http://www.ciscopress.com/articles/article.asp?p=663084&rll=1> (accessed June 21, 2008)

<sup>9</sup> Rudolph, K. “Implementing a Security Awareness Program,” *Handbook of Information Security*, Vol 3 (2006): 767

Security incidents and failure to recognize them can threaten organizational survival. By creating awareness, individuals can recognize and respond accordingly to organizational security concerns.

- Learning is usually very specific, brief, and immediate.
- It is a broadcast of information that uses attention grabbing techniques in a one-to-many format.
- Learners only receive information.

In contrast, training is characterized as follows:

- It builds upon awareness with formal knowledge building and skill development that facilitate job performance.
- It is more in depth and develops skills and competency for individuals outside the IT security group.
- It is selective and focused based on specific roles and job functions.
- Learners actively participate.<sup>10</sup>

### **Motivating the Workforce and Raising Awareness**

People are often resistant to change simply because they do not like to change. To be effective, an awareness program must carefully address this common workforce resistance. To accomplish this, an awareness campaign may appeal to complementary attitudes and preferences. As an example, the practice of sharing passwords with new employees to “get them on the system sooner” may be a long-term behavior. By showing respect and recognition for people that protect system access, as opposed to placing the system at risk, an awareness program may gradually change this behavior.<sup>11</sup>

The ability to successfully market an awareness campaign directly influences its effectiveness. To change the behavior of the workforce communication and dissemination of information is a key building block. To ensure a successful campaign, proper research and planning must be performed so that a clear strategy can be developed. While the techniques in doing so are outside the scope of this essay, the following objectives must be accomplished:

- Define the program objectives
- Identify primary and secondary audiences
- Define the message to be communicated
- Identify approaches that meld with organizational culture and structure
- Describe the benefits to the audience

Furthermore, an effective awareness program must cultivate a professional, positive, and visible image. In doing so, the importance of the program will be communicated, morale will be raised, and the support of the workforce will be gained. The program should communicate a concern for the employees’ well being at home, on the road, and at work.

---

<sup>10</sup> Rudolph, K. “Implementing a Security Awareness Program,” *Handbook of Information Security*, Vol 3 (2006): 767

<sup>11</sup> Ibid: 772

In doing so, individuals will see how they can personally benefit from improved awareness and will have a vested interest in the program.

Awareness programs should be composed of attention grabbing techniques that peak interest and promote retention of the information. The use of clever slogans, eye-catching logos, and even mascots can be used to attract attention. Images and catch phrases have a greater impact than words. Organizational themes can unite several concepts into a single message.<sup>12</sup> For example, the theme of “an ounce of prevention is worth a pound of cure” would be fitting for healthcare organizations.

The use of stories about tangible people in the news or a fellow employee can be leveraged during presentations and course material. The stories should relate to situations individuals might face in their daily activities and can communicate a specific, relatable message. For example, stories about fellow employees that have been victims of or prevented identity theft would be valid in almost every organization and especially in financial institutions.<sup>13</sup>

## Awareness Resources

As you can surmise, raising awareness is a difficult job that requires a great deal of effort and coordination. As more and more organizations embark on an awareness campaign, many of them share past experiences, ideas, and materials to help others. Recently, Robert Danford, a SANS ISC handler, published a culmination of cyber security awareness tips submitted by readers. The following are selected resources of interest:

- Department of Homeland Security Prevention & Protection Resources  
[http://www.dhs.gov/xprevprot/programs/gc\\_1158611596104.shtm](http://www.dhs.gov/xprevprot/programs/gc_1158611596104.shtm)
- Computer and Network Security Task Force Cyber Security Resource Kit  
<http://www.educause.edu/7479>
- National Cyber Security Alliance, Stay Safe Online  
<http://www.staysafeonline.info/>
- CNET's Personal Security Dashboard  
<http://news.cnet.com/2009-1009-6038680.html>
- National Security Institute's Security Resource Net  
<http://www.nsi.org/>
- Anti-Phishing game hosted by Carnegie Mellon University  
[http://cups.cs.cmu.edu/antiphishing\\_phil/](http://cups.cs.cmu.edu/antiphishing_phil/)
- Computer Security Day  
<http://www.computersecurityday.org/>
- National Security Agency - Awareness Education and Training  
<http://www.nsa.gov/ia/academia/acade00001.cfm>
- OnGuardOnline – Security tips from the federal government  
<http://onguardonline.gov/>

---

<sup>12</sup> Rudolph, K. “Implementing a Security Awareness Program,” *Handbook of Information Security*, Vol 3 (2006): 776

<sup>13</sup> Ibid: 779

- Security Analogies – A Wikipedia like resource for security analogies  
<http://www.securityanalogies.com>

This is only a brief listing of resources available to help raise and create awareness. Additional cyber security awareness tips can be found by accessing the site directly at the following URL: <http://isc.sans.org/diary.html?storyid=3444>

In addition, the course material provided in the MSIA program at Norwich University provides links to valuable awareness resources:

- Computer Security Day Home Page  
<http://computeersecuritday.org>
- Computers at Risk  
<http://www.nap.edu/books/0309043883/html/index.html>
- DoD IA Training Products  
<http://iase.disa.mil/eta/>
- Held, R. (2001). Security Awareness – Are Your Users “clued in” or “clueless”?  
[http://www.giac.org/practical/gsec/Robert\\_Held\\_GSEC.pdf](http://www.giac.org/practical/gsec/Robert_Held_GSEC.pdf)
- Kabay, M.E. (2000-present). Network World Fusion Security Newsletter archives.  
<http://www.nwfusion.com/newsletters/sec/>
- Security Awareness Incorporated  
<http://www.securityawareness.com/>

## Conclusion

Through implementation of a properly designed information security awareness and training program an organization can greatly increase protection of its critical information. Although people are reluctant to change, especially if they feel it will add an unjustified burden, a well designed awareness program can gain the support of the workforce. This can be accomplished through the use of an attention grabbing and informative training program that addresses all individuals within an organization through focused training based on job-role and function. Many resources exist that provide information and support for starting, fortifying, or expanding information security awareness efforts and enabling the Human firewall. Who says old dogs can't learn new tricks? You've simply have to throw them a bone, be persistent, and keep them interested.