Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Moving from Consciousness to Culture: Creating an Environment of Security Awareness

Although the aftermath of September 11th has brought to the forefront the realization that security threats are real, most companies are still far from creating a culture of security awareness within their organizations. This is particularly true with information security even though recent surveys have shown that corporations are worried about the financial impact of threats and attacks against their computer systems. Unfortunately, many of these same organizations are still focusing primarily on technical solutions s...

Copyright SANS Institute
Author Retains Full Rights

AD

Moving from Consciousness to Culture: Creating an Environment of Security Awareness

Mary Munley
GSEC Practical Assignment
Version 1.4b, Option 1
April 10, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

Although the aftermath of September 11th has brought to the forefront the realization that security threats are real, most companies are still far from creating a culture of security awareness within their organizations. This is particularly true with information security even though recent surveys have shown that corporations are worried about the financial impact of threats and attacks against their computer systems. Unfortunately, many of these same organizations are still focusing primarily on technical solutions such as firewalls, anti-virus software, patches, biometric devices and the like, to protect themselves against these threats. They have failed to take an overall holistic approach to security by combining technology with awareness. Most have recognized the importance of having clear and enforceable policies, but have stopped short of developing a comprehensive, ongoing awareness program. Security professionals and administrators are often left with the undefined task of making sure that procedures and processes are in place to ensure these policies are carried out. There are many considerations to weigh and steps that can be taken to improve security awareness in your own organization. The ultimate goal is to inspire change to create a culture of security awareness . . . or simply, what to do after the policies have been written.

The Human Factor

Now more than ever, information and technology have become critical to the success of business operations. Organizations are increasingly more dependant on the Internet and other e-business functions for sales, marketing, purchasing, and other manufacturing functions. Companies rely on the availability and accuracy of data to stay competitive in tight markets. Government regulations and controls are increasing and organizations are being held responsible for data privacy and other employee obligations. All of these issues are prevalent in the midst of a rise in viruses, worms and other assaults on computer systems.

Companies are primarily answering these challenges by increasing the technologies in place . . . firewalls, anti-virus software, server patches, network monitoring, and the like. However, often overlooked is the human factor. The timeless saying, “To err is human …” summarizes the fundamental weak link in all security programs. Regardless of the quantity or sophistication of the security technologies that have been put into place in an organization, the biggest vulnerability still comes from the people within the company who have access or knowledge about the business and its data. Kevin Mitnick, one of the world’s most famous hacker and fugitive turned security expert, considers the human factor the weakest link in security. In his book, The Art of Deception, he expands on this to say that as security technologies improve and systems become more

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

difficult to exploit "attackers will turn more and more to exploiting the human element."[1]

This exploitation of people has become so prevalent that the term social engineering has been coined and adopted to describe the attempt to attack computer systems by attacking the vulnerabilities of the people who have access to those systems. Our human tendencies are to be helpful and open, particularly in the corporate world where customer service is admired and rewarded. In large companies, someone on the telephone claiming to be a member of the technology team or computer help desk can fool employees into providing important company information. Individuals, and even security guards, can be duped by attackers wearing an appropriate uniform or having a seemingly proper badge or identification. Computer users can naively open email attachments that may be disguised as legitimate correspondence, or they may be convinced to provide their system account information by official looking requests. Only knowledgeable and vigilant people can reduce the risks against these social engineering attacks.

A recent survey sponsored by Ernst & Young and conducted by the National Computing Centre (NCC) highlights the need for companies to develop an information security culture and states that failing to take information security seriously will likely result in security breaches causing loss, interruptions, and failure. [2] Some additional problems revealed from this survey include:

- Perception that security is a technical issue
- Resource limitations for implementing security measures
- Failure of companies to take information security seriously

Another survey conducted by the Computer Security Institute in conjunction with the FBI in 2003, showed that virus incidents and insider abuse of access were the most frequently cited forms of computer attacks or abuse. This was true even though virtually all (99%) of the organizations surveyed employed anti-virus software and 92% used some type of access control measures.[3]

A look at the cyber crime sheets of the U.S. Department of Justice reveal many incidents involving employees who have used internal knowledge to exploit the data, information and systems of their companies. This exploitation is not confined to just the average employee, but also those in trusted positions. In November 2003 a federal grand jury issued a ten-count indictment against FBI analyst, Jeffrey D. Fudge, who was immediately arrested and fired. The charges facing Mr. Fudge revolve around his misuse of the information available to him through his position and access of the FBI computer systems. Steven P. Beauchamp, Special Agent in Charge of the Department of Justice stated:

---

[1] Mitnick and Simon, p. 4.
[2] Channel Minds, 2003
[3] Computer Security Institute, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> This indictment serves as a reminder that the Department will not tolerate the misuse and unauthorized disclosure of sensitive law enforcement information. In today's world, and with advancing technology, there is too much at stake. All of law enforcement must be vigilant and protect against those who would compromise our most important asset – our information.[4]

This vigilance must carry over to all sectors, government and non-government alike. Raising the security awareness of the people in these organizations can help mitigate the vulnerabilities that exist from the human factor.

The Elephant

Culture can be simply defined as the common attitudes and behaviors of a group of individuals. The task of creating a culture change and moving the employees of a company towards security awareness can seem monumental. Security professionals tasked with this endeavor should keep in mind the humorous question, "How do you eat an elephant?" So goes the process of creating a security awareness culture . . . "one bite at a time."

Numerous books and articles have been written about effective change management techniques and strategies. Although various steps and strategies have been endorsed, there are at least three main stages that are key to achieving change:

- Understand the current culture of your organization
- Define the vision
- Create a roadmap for implementing the change

In her article *Change, Change, Change: Lessons from the Field*, Susan Heathfield writes that organizations will need to be capable of change to succeed in the future. She goes on to state, "Effective communication, full and active executive support, employee involvement, organizational planning and analysis, and widespread perceived need for change, are the big five when successful change is achieved."[5]

Creating a cultural change in business does not happen over night, but requires time and patience. It is more than just a program. True change comes only when the vision is deeply engrained into the psyche and actions of every employee. When Lou Gerstner, former CEO of IBM, was asked what advice he would give on implementing cultural changes, he replied: "Be patient ... It takes time. And the progress, in my experience, is always going to come slower than you want."[6]

---

[4] U.S. Department of Justice, 2003
[5] Heathfield, par. 2
[6] Krames, p. 117.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Raising the awareness of employees knowledge of security and getting them to understand their own role in security cannot happen with a one-time event, but rather requires the development of a continuous process. This includes everyone from senior management down to janitorial staff . . . all have some degree of access to the computers, systems, and information of the organization. And all must participate at some level in the security awareness efforts.

As with any new initiative, you can expect hurdles and roadblocks. But by understanding the challenges and audience, you can effectively implement steps that will improve security in your company and help develop a cultural awareness for good security practices.

The Challenges

Understanding the challenges is the first step toward creating a proactive security climate in your company. Some of the key considerations that must be acknowledged and addressed are management buy-in, budgetary constraints, user resistance, legal requirements, monitoring, and auditing.

Data and information security historically have been seen as an IT issue; however, to have a truly effective security awareness program requires the alignment of business objectives to information security practices. Senior management should be actively involved in security-related decisions and should support awareness and training initiatives.

Achieving management buy-in is a challenge faced by many organizations. A global survey of financial institutions conducted by Deloitte Touche Tohmatsu in 2003 revealed that executives are worried about the increased sophistication of attacks and threats to their computer systems. Additionally, 39% of those responding acknowledged that their systems had been compromised in some fashion within the past year.[7] Unfortunately although this survey, and others, point to senior management concern with the rise in threats and attacks, these same surveys show they are slow to respond with resources or financial support.

The perception of bureaucracy and production slowdown with increased security controls will be obstacles that must be overcome to achieve support from senior management. Focus on risk reduction, auditor requirements, and legal regulations will help gain the backing that is critical to a successful security awareness program.

The 2003 Global Information Security Survey performed by Ernst & Young revealed two major issues regarding budgetary constraints:

- Fifty-six percent of organizations cite insufficient budget as the number one obstacle to an effective information security posture.

[7] Ernst & Young, p. 10.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Nearly 60% of organizations say they rarely or never calculate ROI for information security spending.[8]

In terms of the percentage of information security spending, employee awareness and training ranked in the bottom two categories capturing only 29% of total spending. Security technologies such as hardware and software captured 83%. On this point the survey states:

> There is ample evidence, in our opinion, that the money spent on technology tools may in fact be at the expense of organizational and people issues. We regard the human capital part of the equation as very important in addressing information security and deserving of far more consideration that it is apparently receiving.[9]

The recommendations offered from the Ernst & Young survey include the fact that companies cannot just talk the talk, but need to walk the walk by backing up the importance of security awareness with their proactive investment into security initiatives. Many times it takes a security breach or government mandate before organizations take action; and often it is only to minimally fix the immediate problem. The survey states, "Measured, proactive spending is less costly in the long run than reactive spending, which is often overspending in response to an incident."[10]

Another challenge being faced by organizations is the growing number of regulations and restrictions that have been adopted by the United States and other countries. Mandates have been enacted to provide various levels of security aimed at protecting the privacy and information of consumers and/or employees. These regulations can impact the responsibilities of your organization and should be examined for their relevance and inclusion as part of the awareness program. Although not a complete list, nor specifically applicable to every industry, some of these regulations include the following:

- Gramm-Leach Bliley Act (GLBA). This law requires increased security, integrity and confidentiality of consumer information for financial institutions.
- Health Insurance Portability and Accountability Act of 1996 (HIPPA): Focused for the healthcare industry, this act protects sensitive information including such as patient identity, medical records, financial data, and behavioral information.
- Europe Union Data Protection Directive: Geared for companies who conduct business in Europe, this law addresses the delivery of personally identifiable information across country borders.

---

[8] Ernst & Young, Issues at a glance
[9] Ernst & Young, p. 8.
[10] Ernst & Young, p. 2.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Sarbanes-Oxley Act: Requires that publicly traded companies must certify their controls over financial reporting, including information security.
- Fair Credit Reporting Act (FCRA): Recently amended on December 4, 2003, this law is designed to promote both the accuracy and privacy of information in consumer reports; businesses that supply information to Consumer Reporting Agencies have added responsibilities under the revisions of this law.
- Federal Information Security Management Act (FISMA) of 2002: Ensures proper information security controls are provided for federal information and systems.
- USA PATRIOT Act: Controversial since its enactment in October 2001, this law gives government enforcement agencies a broad scope of surveillance and investigative powers, including information transmitted over the internet and via other technologies.
- Personal Information Protection and Electronic Documents Act (PIPEDA): Legislation enacted in Canada in April 2000, addresses the protection of personal information and electronic documents.

In addition to the challenges already stated, one of the more difficult one to deal with is auditing and monitoring compliance to policies. Without enforcement, policies are just words on a piece of paper. Additionally, in the event of a security breach an effective information protection program is measured by whether the organization exercised due diligence in trying to prevent criminal conduct on the part of its employees.[11] There are many examples of recent convictions of former employees that may have been prevented with better controls and enforcements in place. One such case involved a former employee of Viewsonic Corporation. Mr. Garcia was a network administrator where he was in charge of several computer servers and had access to system passwords. Two weeks after Mr. Garcia was terminated from the company, he gained access to the company systems and destroyed critical data. This action shut down a server that was critical to the company's foreign operations.[12] Strict enforcement of an efficient termination procedure with immediate system access lock out may have prevented this attack.

User resistance is a predominant challenge and one that cannot be overlooked when implementing an awareness campaign. As Kevin Mitnick reiterates in his book, the ultimate goal of any awareness program is to "influence people to change their behavior and attitudes." This can be accomplished by:

> … motivating every employee to want to chip in and do his part to protect the organization's information assets. A great motivator in this instance is to explain how their participation will benefit not just the company, but the individual employees as well. Since the company retains certain private information about every worker, when employees do their part to protect

[11] Peltier, p.149.
[12] U.S. Department of Justice, 2004

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

information or information systems, they are actually protecting their own information, too.[13]

Consideration of these and other challenges within your own organization is actually half the battle. It is much easier to address a known challenge since you have the advantage of preparing your defense. The next step towards building a cultural change, however, lies in how these challenges impact the various people in your organization.

The Audience

Unlike the truths that Thomas Jefferson proclaimed in the Declaration of Independence that "all men are created equal," not all users are equal. Motivating and educating the different types of people in your organization will require tailoring your security message to meet their individual circumstances and concerns. Although some basic security measures, such as the use of difficult to guess passwords, apply to all systems users, safe laptop security practices should be reviewed specifically with those who are issued or use a laptop. Additionally, the type of job you hold in an organization will determine the type of security issues that may affect you. Someone in human resources will need to be more familiar with data privacy issues surrounding employee information and people in the financial areas will need to understand fraud and similar issues.

Ideally, your policies will address the responsibilities of each individual in the organization. It is from these that you will define the message for each group. An important thing to remember, however, is that the presentation of an awareness program is really a sales pitch. Thomas Peltier wrote in his guide, Information Security Policies and Procedures, A Practitioner's Reference, "Remember that the employees already know what is expected in the workplace. The goal is to remind them that information asset security is part of that process."[14]

Here are some general factors to consider in preparing the message and material for the primary types of individuals in any organization.

Executives and senior management are the essential element to any awareness program since ultimately it will require their support and funding. The primary concerns and information that must be provided to upper management include cost justification, best practices with industry comparisons, risk analysis, and legal or auditor requirements. A brief written report or executive summary stating the background, issues and goal or vision is a good place to start. This should be followed up by a presentation to restate the issues but expanding with current examples taken both from recent conviction cases and real life examples within your own organization. The presentation should provide data from similar

[13] Mitnick, pgs.249 and 250.
[14] Peltier, p. 231.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

businesses and recommendations from auditors and companies who specialize in security, such as SANS Institute, Computer Security Institute (CSI), Information Systems Security Association (ISSA), and the NIST Computer Security Division of the U.S. Department of Commerce. Additionally, the presentation should outline an implementation plan that focuses on continuous improvement rather than a specific project life cycle. Funding and support are the final elements of the presentation and are essential to the success of the awareness program.

It is always a good idea to seek management support and even find a business champion of the initiative prior to the formal presentation. These individuals can help review the material presented and guide you in presenting the information so that it aligns with the goals and objectives of the organization as a whole. Additionally they can assist in determining the appropriate budget. Although support and funding at this stage are necessary for ultimate success in changing the security climate, failure in receiving full commitment from senior management does not mean you are finished. Although not desirable, it is still feasible to achieve some level of awareness without any budget and/or little support by upper management by simply continuing the message in a grassroots fashion. Track your efforts and any successes and go back to senior management.

Information Technology and Help Desk employees are also critical for the overall success of an awareness program. These folks must buy into the fact that security is important and must be willing to stand behind that commitment with their actions. Mixed messages are sent out if you tell your users to keep their passwords secret and a member of the IT staff comes along and requests the password from a user to troubleshoot problems. It is imperative that these individuals know and understand the company policies and strictly adhere to them, as they will be interacting on a daily basis with the entire user community in your organization. These are the ambassadors of the message and they have the power to make or break that message.

Most organizations have various individuals not connected to the information technology group, but who are perceived by the business as experts on the computer systems in the company. These super users should be identified and targeted to act as emissaries or messengers to promote and disseminate the materials for security awareness. Representation from this group of individuals on the security team initiative would be valuable in understanding how best to convey the message throughout the organization. These are the people who generally have their finger on the pulse of the user community and know the concerns and issues that need to be addressed to obtain approval and ultimately acceptance of the awareness program.

Managers, team leaders, or line supervisors are another group that require special attention and focus. These are the individuals who will be in the best position to control the actions of the large end user community. In order to obtain

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

their commitment to the initiative, it will be important to demonstrate how the tighter controls and processes will help improve their own job performance and delivery. They are focused on achieving goals, affecting profits, and delivering a high quality product. They will resist anything perceived as slowing down their own process or negatively impacting their goals or objectives. The message for this group will require focus on how the new process or controls will give employees better tools in terms of access or data integrity in a more efficient and/or timely manner. Additionally, they need to know where to go to raise or address any problems that might arise as a result of the program initiatives.

Office workers and support staff are usually pretty savvy with computer systems and business procedures in general. This group, however, will be very skeptical of any new process or initiative; as they have seen many programs come and go. They will be taking a “wait and see” approach and be reluctant to jump on the bandwagon until they recognize that awareness is important for their own needs or they see an overall benefit to the organization as a whole. Until then they will probably only do what is minimally expected of them. The message here must simply state what is expected for compliance with additional input on how improving company awareness will actually increase protection in their own areas from unauthorized access, abuse, disclosure or destruction. Many different media of publishing this message should be used for this group. Frequency and repetition of the topics conveyed in a variety of ways will provide the best impact. This will help show that management is serious about changing the culture, but at the same time will keep this group interested in the message.

Similar to the support staff are the manufacturing, plant, operations, or maintenance workers. These are the “nuts and bolts” of an organization whose time is focused on production, and who generally have less computer knowledge than their office counterparts. The message must be constant, repetitive, simply stated, and varied with focus on one point at a time. This group does not have easy access to personal presentations or on-line training expanding on the “how to” or “whys” of awareness. Quick and to the point messages targeted to areas closely affecting their own environments will be more successful than other methods. Brief stories or incidents that make the potential problems of unawareness a reality will have the biggest impact on reaching these individuals.

Finally, a group often overlooked in many awareness programs but potentially the one that holds the biggest risk, are the contractors and consultants who work side by side with the company employees. Corporate information should be available to non-employees only as it relates to their specific assignment or job responsibility; and there should be a general awareness among regular employees about this limitation of access. Sometimes contract employees are not easily recognizable as over time they tend to blend in with everyone else. Employees do not always know who is working on a contractual basis, as the focus in business tends to be the job at hand, not who is doing it. At a minimum, confidentiality and non-disclosure agreements should be signed by all

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

consultants and contractors at the time of hire and reviewed again upon termination. When contracts extend over a long period of time, six months to a year or more, there should be a review or recommitment of these agreements periodically. Messages focused at this user base should reinforce the fact that data and information in the company is completely proprietary and should not be discussed or divulged within their own companies.

To promote an effective security awareness message, it must be visible and understandable to all employees. Overall the message is the same, but the delivery needs to be tailored to each individual in the manner that will cause them to embrace and support the vision.

The Plan

All initiatives require planning and an information security awareness campaign is no different. The development of a comprehensive strategy will go a long way towards achieving the desired results of greater employee awareness. The National Institute of Standards and Technology (NIST) is compiling Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program* (currently in its second draft). In addition to this newest publication, the NIST previously developed Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. According to NIST, "The two publications are complementary – SP 800-50 works at a higher strategic level, discussing how to build an IT security awareness and training program, while SP 800-16 is at a lower tactical level, describing an approach to role-based IT security training."[15] Although written to address security for federal government agencies, both publications are great reference documents and can be adapted and used as a guide for developing your own awareness strategy.

In its latest publication, the NIST identifies these four critical steps that encompass the life cycle of an information security awareness and training program:

- Awareness and Training Program Design: This step includes the development of a needs assessment and training strategy.
- Awareness and Training Material Development: This step includes gathering available training sources, content, and development of training material.
- Program Implementation: This step addresses the communication and roll out of the program.
- Post-Implementation: This step provides guidelines on program continuation and monitoring.[16]

[15] NIST, p. vii.
[16] NIST, p. vi.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

There are many considerations and phases in the design stage, but basically this encompasses the assessment and strategy. It is always a good idea to perform a baseline assessment of the current security awareness level in your organization. This can be done in a number of ways and may include employee surveys, interviews with technology and help desk staff, review of current training initiatives, review and analysis of existing User IDs and application access information, review of existing security technologies, and review of security incidents or events at your company. Some of the questions that should be answered from this assessment include:

- Are all system users required to acknowledge or sign off on the security policies of the company? Upon hire? Annually? Upon termination?
- Do all employees know and understand their own responsibilities for computer security?
- Are the policies adhered to and/or enforced?
- Are there processes in place that support the enforcement of existing policies?
- Are there processes in place that monitor the enforcement of policies?
- Have the technology and help desk staff received previous training on security issues? What types? How recent? How frequently?
- What type of training and/or certification do your security professionals have?
- What types of security attacks or issues have occurred in your company? Frequency?

An additional indicator of where your organization stands in relation to securing information can be found from doing a physical check of the premises during lunch or after hours. Walk around the premises and take note of these five key elements that Thomas Peltier believes to be a good indicator of the level of concern over computer and information security:

- Offices are locked
- Desks and file cabinets are locked
- Work stations are secured
- Diskettes are secured
- Information is secured[17]

A review of the assessment in conjunction with the existing security policies for your organization will help layout a blueprint of the awareness strategy. Creating a template, such as the one shown below, can help to highlight the areas that should be the focus of the awareness program. The template should not be viewed as static, but should be continuous and updated as organizational changes or new threats and vulnerabilities occur. Additionally, your available budget will be a factor on what can be accomplished, but your design should be completed based on the ideal awareness and training program for your

[17] Peltier, p. 161.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

organization without regard to budgetary constraints. This will help provide a future checklist of items to cover or repeat when additional funding or other opportunities become available.

Objective or Focus Area	Audience	Priority	Method or Activity	Schedule or Frequency	Evaluation
Review/acceptance of Security Policies	Everyone	High	Email/web form confirmation	Annually and upon hire and termination	
Security Handbook	Everyone	Medium	Publication	New Hire	
Laptop safety	Laptop users IT support	High	Fact sheet	Annually and upon laptop issuance	
Password use	Everyone	High	Bulletin board; flyers; logon messages	Quarterly; individually with password reset	

The second phase of the plan is the development of material, both for raising awareness and providing training. Awareness and training are not the same and they each have different goals. The NIST provides a good contrast:

> Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. … In awareness activities, the learner is the recipient of information … Awareness relies on reaching broad audiences with attractive packaging techniques.
>
> Training is more formal, having a goal of building knowledge and skills to facilitate the job performance. … training seeks to teach skills which allow a person to perform a specific function … The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material.[18]

There is no shortage of security topics or issues that can be covered for your awareness program. Evaluate the major concerns or issues in your own organization and start with those. Password protection is still viewed as one of the most cost effective safeguards for reducing attacks on computer systems. The recent increase of virus attacks makes email security a great topic. Incident response: Who should be contacted in the event of a possible breach? The list goes on.

There is also a surplus of information available to help you construct or compose materials for various types of communications. Ideas can be found at numerous security web sites including those companies who specialize in providing security awareness services. Universities, government agencies, and other public organizations have information about their own security practices available on the Internet to anyone who is interested. The difficulty here will be in deciding what information to use and how to best communicate the message. Keep in

[18] NIST Publication 800-50, pgs. 8 and 9.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

mind the audience for each topic and tailor the message to best suit the needs for each group within your own organization.

Training materials will also need to be planned and used for the technology staff and other designated employees who will require a higher level of understanding and commitment to the security awareness program. These may be done in a series of sessions using presentations, interactive role-playing, discussions and review of recent media exploits or cyber crimes, playing a security video, and reviewing internal threats or recent issues.

After the design and preparation stage comes the implementation of the awareness program. Keep in mind that this will be a continuous process and you can actually go through all four stages for just one objective. Of course, ideally, you will want your awareness campaign to be far-reaching and frequent for better results, but even without much support or funding, implementation is still possible.

Plan on using a wide variety of media for your message. As with any marketing campaign, repetition, variety, humor, and eye appeal are some of the secrets for success. Here are just a few of the many suggestions that can be incorporated into your own program:

- Flyers or brochures
- Bulletin-board notices
- Electronic banners
- Email reminders
- Newsletters
- Security related screen savers
- Internal web bulletins
- Trinkets . . . pens, mouse pads, key rings, etc. with security messages

Again, the ideas are endless, but don't try to develop or create these on your own. Look for ways to get others involved. Not only will you be surprised with the creativity, but also the fact that involvement is widespread will help promote the awareness message and sway resistance. A contest for a company security slogan or rewards for the creation of posters about security facts are two ways to engage the people in your organization.

Often overlooked in promoting security awareness across an organization is the existence of many forums already in place where messages can easily be delivered. Piggyback on the things already available in your own company:

- Security articles or cartoons included in company newsletters
- Policy reminders or security tips at employee meetings
- Fortune cookies with security messages at company events such as blood drives, luncheons, project kickoffs, etc.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Security messages on your email signature information

The final stage of the life cycle model is post-implementation. This is really a combination of evaluating the results and effectiveness of the campaign initiatives, plus continuous improvement efforts. Encourage feedback on the various events or communications. The use of prizes and rewards are great motivators. Recognize the security contributions of individuals. Repeat the initial assessment steps after various security implementations to gauge improvement levels. Review existing security policies and procedures to determine if updates or additional monitoring are required. Provide status reports of initiatives and progress to management.

An essential element of post-implementation and key to ongoing awareness is the constant review of policies and processes against vulnerabilities. This cannot be over-emphasized. A breaking news story highlights this fact. Air Canada has just filed a lawsuit against WestJet Airlines and two of its employees in Ontario Superior Court. The suit alleges that WestJet used information from a private Air Canada website for strategic planning and pricing. One of the employees named in the suit, Jeffrey Lafond, left Canadian Airlines International Ltd. just as it was being taken over by Air Canada. As part of his separation package in 2000, he received space-available airline tickets over a five-year period, along with an access code to a special website where the tickets could be booked. WestJet Airlines subsequently hired Mr. Lafond as a financial analyst. The allegations in the suit state that "… Lafond's identification number was used 243,630 times between May 15, 2003, and March 19, 2004, to access the website." It goes on to cite "Its abuse of the plaintiffs' confidential information has enabled WestJet to expand its service, its revenue and its profitability at a more rapid pace than it would without the plaintiffs' confidential information."[19] Although the outcome of this suit is yet to be known, it does raise the question of what controls could have been in place to prevent this type of situation.

The four steps of the life cycle model are constant and continuous. As the old saying goes, "When you stop getting better, you stop being good." This is particularly true with security . . . you can never have too much knowledge or be too protected against attacks. Technologies continue to change and the threats against computer systems are like moving targets.

The Result

Creating a culture of security awareness is not an overnight feat. It will be slow and agonizing with many peaks and valleys of successes and failures. Financial commitments for security initiatives will be difficult to obtain in an economy that is geared on cutbacks in spending and resources. People by nature resist change and will easily revert to old habits. Keep in mind, however, that there is no such thing as perfect security. A quote originally from Dr. Eugene Spafford, professor

[19] Canadian Press, 2004

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

of Computer Sciences at Purdue University, offers these words of wisdom: “The only system which is truly secure, is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn’t stake my life on it.”[20]

Patience and persistence is the best advice available. An anonymous quote aptly sums it up, "Difficult things take a long time. The impossible takes a little longer." Rejoice in your successes and accomplishments, however, small they may seem. And remember, “Rome was not built in a day!”

© SANS Institute 2004, Author retains full rights.

[20] Texas A&M University, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

List of References

AT&T. "Achieving Network Security." URL: http://eb.eiu.com/upload/Network_Security_White_Paper_FINAL.pdf (September 2003)

Business Software Alliance. "BSA-ISSA Information Security Study Online Survey of ISSA Members." URL: http://www.issa.org/PDF/research-BSA-ISSA.pdf (December 3, 2003)

Canadian Press. "Air Canada suing WestJet." URL: http://www.globeandmail.com/servlet/ArticleNews/TPStory/LAC/20040409/RAIR09//?query=Air+Canada (April 6, 2004)

ChannelMinds. "Survey Shows: Organizations Need to Develop Information Security Culture." URL: http://www.channelminds.com/article.php3?id_article=1582 (January 28, 2004)

Computer Security Institute. "CSI/FBI Computer Crime and Security Survey." URL: http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf (2003)

Deloitte Touche Tohmatsu. "2003 Global Security Survey." URL: http://www.deloitte.com/dtt/cda/doc/content/Global%20Security%20Survey%202003.pdf (2003)

The Economist print edition. "The weakest link." URL: http://www.economist.com/printedition/displayStory.cfm?Story_ID=1389553 (October 24, 2002)

Ernst & Young LLP. "Global Information Security Survey 2003." URL: http://www.ey.com/global/download.nsf/International/TSRS_-_Global_Information_Security_Survey_2003/$file/TSRS_-_Global_Information_Security_Survey_2003.pdf (2003)

Heathfield, Susan M. "Change, Change, Change: Lessons From the Field." URL: http://humanresources.about.com/library/weekly/aa021201a.htm

Krames, Jeffrey A. What the Best CEOs Know. New York: McGraw-Hill Companies, Inc., 2003.

Mitnick, Kevin and William L. Simon. The Art of Deception. Indianapolis: Wiley Publishing, Inc., 2002.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

NIST. "Information Technology Security Training Requirements: A Role- and Performance-Based Model." URL: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (April 1998)

NIST. "Building an Information Technology Security Awareness and Training Program." URL: http://csrc.nist.gov/publications/drafts/SP800-50-version2Draft.pdf (2nd Draft: April 2003)

Noticebored. "Business Case for a cost-effective Information Security Awareness Program." URL: http://noticebored.com/NB_generic_business_case_for_infosec_awarenes s_program.pdf (February 25, 2004)

Noticebored. "Creating a Security Culture." URL: http://www.noticebored.com/html/creating_security_culture.html

Peltier, Thomas R. Information Security, Policies and Procedures, A Practitioner's Reference. Boca Raton: CRC Press LLC, 1999.

Rasmussen, Michael. "IT Trends 2003: Information Security Standards, Regulations and Legislation." URL: http://www.csoonline.com/analyst/report721.html (December 18, 2002)

Schneier, Bruce. "Are you sophisticated enough to recognize an Internet scam?" URL: http://www.mercurynews.com/mld/mercurynews/7529172.htm (December 19, 2003)

Schneier, Bruce. Beyond Fear: Thinking Sensibly About Security in an Uncertain World. New York: Copernicus Books, 2003.

Texas A&M University, "Security Awareness Training." URL: http://infosec.tamu.edu/sat/test/overview.html (2003)

U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS). "Computer Intrusion Cases" URL: http://www.cybercrime.gov/cccases.html (March 9, 2004)

U.S. Department of Justice, Press Release. "Former Employee of Viewsonic Sentenced to One Year for Hacking into Company's Computer, Destroying Data." URL: http://www.cybercrime.gov/garciaSent.htm (February 23, 2004)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**