An NSI Special Report

Improving Security from the Inside Out

A Business Case for Corporate Security Awareness

Presented by

National Security Institute
116 Main Street, Suite 200, Medway, MA 02053
Tel: 508-533-9099 • Fax: 508-533-3761
E-Mail: InfoCtr@nsi.org • Internet: http://nsi.org

CONTENTS

I. INTRODUCTION

Many employees in today's workforce are not aware that they play an important role in their organization's security.

They engage in risky behavior on the Internet, open unsolicited e-mail attachments, carelessly divulge proprietary information, introduce wireless risks to corporate networks, and neglect to consider security in their daily routines — all activities that could put sensitive company information at risk.

Statistics prove that the internal threat is one of the greatest risks to corporations, organizations and governments today. The Gartner Group reports that compromises from the inside account for more than 70 percent of network espionage, yet less than 30 percent of corporate security expenditures are spent on the problem.

Theft of proprietary information and intellectual property cost U.S. companies as much as $59 billion in a single year.

Industry studies reveal that despite the best technological advances, security breaches are occurring at an alarming rate. About 85 percent of large companies and federal government agencies have detected security breaches.

Experts say that nearly 75 percent of security breaches are "inside jobs" — like the untrained employee who writes his password on a Post-it-note … or the worker who forwards sensitive information to his home computer …or the polite employee who neglects to challenge unescorted visitors wandering through her work area.

While much of the popular media concentrates on the high profile hacking and virus cases, it is company insiders, employees, contractors and others, who constitute the greatest risk.

The majority of incidents that have happened are not because the technology has failed to deliver but because of human failure.

In the information age, one thing is clear: everyone's job depends more and more on how ordinary employees comprehend and comply with security procedures. However, corporate security managers are in the unenviable position of having to answer for employee breaches that happen on their watch.

The best security organizations are those that have figured out how to change the culture of the company so that everybody's job is part of security.

While protecting the "human element" of information security may seem obvious, it clearly is not. In fact, most businesses do little more than pay lip-service to it — spending more time and money on free coffee for employees than on educating those employees on information security practices that help mitigate the insider threat.

Researchers say that businesses seeking to save money by scrimping on security awareness train-

ing are taking a foolish risk. An uneducated worker who opens an e-mail-borne virus can bring down corporate systems for days, costing millions. And as companies' information systems grow in complexity, with the addition of remote workers, wireless access, and other developments, the threats to those networks grow exponentially.

For all the precautions taken to keep their information systems safe, many companies often forget one thing. None are foolproof, because there's always a human element involved.

While the "human element" of information security may be easy to ignore; ignoring it is also dangerous and costly. Of this there is ample evidence.

This report presents an organizational security approach that corporate security managers can use as a roadmap to initiate an effective employee security awareness program.

> *"The human factor is typically the most critical variable in information security systems. Even the best policies and technologies can be rendered completely ineffective if users do not take responsibility for safeguarding the information they control."*
>
> — Amit Yoran, Director of the National Cyber Security Division of the Department of Homeland Security

II. AWARENESS TRAINING: IT VS CORPORATE SECURITY

Information security, for the most part, is still often regarded as a technology issue to be left to the IT department. To be effective, security must become part of every employee's job. Unfortunately, organizations are leaving themselves open to security breaches because their information security awareness training is woefully inadequate.

Teaching employees about security isn't an easy task. So, which department is best equipped to take on the challenge? IT or corporate security?

Experts say the real key to keeping information secure is managing the behavior of end users and changing the corporate culture. That's just the sort of thing that most IT departments aren't very good at. Their valuable time and energy is focused elsewhere — primarily in keeping critical systems properly configured and patched.

According to META Group security analyst Chris Byrnes " most organizations will fail to successfully secure their technology environment simply because the [IT] security staff lacks the communications skills to create this shift in corporate culture."

The nature of a corporate security organization is to protect the company from malicious or negligent behavior. A major part of the job is evangelical — sensitizing employees to the evils of the dark side.

One of the chief strengths of corporate security managers is that they're interpersonally involved with the employees. They're responsible for managing "Personnel Security," and ensuring that

people know their responsibilities regarding protecting company assets.

Given these realities, it makes sense for corporate security to initiate and administer an information security awareness program that consistently fosters awareness of security risks, communicates the business implications of security and reinforces security policies. Corporate security managers are increasingly taking the lead role in explaining in "non-technical" language, the "why" behind the myriad information security policies and procedures.

Their motives aren't completely altruistic, though. After a "preventable" security breach occurs, corporate security mangers are the ones who increasingly find themselves on the hot-seat having to explain why the incident happened and why the offending employee wasn't made aware of the threats ahead of time.

III. BEYOND SECURITY POLICIES AND PROCEDURES

Corporate America spends untold amounts of time and money every year to ensure that its information systems are secure from cyberattacks. But while Internet security technology is commonly deployed by companies of all sizes, there's one relatively low-tech flank that is often lightly guarded — employees.

When it comes to breaching company security, it's the people with daily, unlimited access to company trade secrets, customer lists, and proprietary information that warrant extra attention. And when company secrets can be sent around the world with the click of a mouse, it's increasingly critical to secure corporate data from the inside out.

Data theft is on the rise because of the portability of information. Trade secrets, personal identification or other proprietary information can be smuggled out of the workplace through discs, e-mail, laptops, PDAs, wireless systems and universal serial bus ports that can download information to a storage device the size of a key fob.

The trickiest part of achieving effective security may be in the least technological aspect of all — employee awareness and training. Just because there's a policy against a certain behavior doesn't mean employees will obey if they don't understand what the implications are.

There aren't enough firewalls, anti-virus software, and corporate security polices in the world to prevent computer users from doing things they shouldn't do when they're at the helm of their PC.

Information security isn't just the domain of a company's IT or corporate security director. It belongs to everyone because everyone is a player on the security stage, from the newest employee in the mailroom to the CEO and the board of directors.

Only through continuous exposure to appropriate awareness training can employees transition from the greatest risk to the greatest asset.

Experts say that without implementing an effective awareness program an information security policy is more or less useless. The best policy in the world will fail if the people who are affected by it most don't know the rationale behind it.

IV. HOW TO OBTAIN MANGEMENT BUY-IN/BUDGET

Get management on board first.

Experts warn that the first and most crucial step in developing an effective security awareness program is getting top management buy-in**.** However, getting management to understand the importance of something as nebulous and abstract as information security isn't an easy task.

Many managers may view information security awareness as one more puzzling piece to the computer infrastructure — another financial black hole with little chance for return on investment. As a result, security awareness and training projects are often neglected or among the first to feel the budget axe.

> *"Individuals that have not been properly trained on how to effectively identify and deal with [security] threats pose a significant risk to any organization."*
>
> — Allan Carey, program manager, Information Security Services, IDC

Companies spend tons of money on IT security every year because they are protecting something tangible that can be easily understood. It's your job to make management understand the intangible importance of information security.

Here are a few things to keep in mind.

— Remind them about the thousands of dollars they shell out each year in technical security: firewalls, anti-virus software, wireless LANs, encryption devices, laptops, PDAs and intrusion detection systems.

— Remind them how much of your valuable information is entrusted to employees and deserving of priority over technical fixes.

— Let them know you don't need a cyber-Fort Knox, you only need the resources necessary to secure your information system's greatest vulnerabilities — your employees.

Also, management understands the financial bottom line. Briefly talk about:

Reputation loss — Discuss the impact of a negative impression in the marketplace and competitive losses as a result of an information security breach. Mention the costs of having to send out 100,000 letters to customers explaining why their credit card numbers have been stolen.

Downtime — Talk about the hard dollars it would take to recover from an information attack. The time and expense it would take to get a database server up after a social engineer was able to persuade an unwitting employee to let him in.

Competitive disadvantage — Mention the lost revenues inevitable from compromise of sensitive data such as business and marketing plans or other proprietary information. And how internal breaches (which represent 75% of security incidents) cause widespread and lasting damage to profits.

Legal liability — Discuss how corporate leaders are increasingly being held accountable for failure

to secure their company's information. It's also impossible to successfully prosecute someone for computer crime if your company cannot prove in court that it took the necessary steps to secure its information.

The bottom line is that if you paint a realistic and honest picture of what can happen when any of these security holes becomes compromised, they will listen. Remember that in the end they want to protect their corporate jewels as much as you do.

V. BUILDING A BEHAVIOR-BASED AWARENESS MODEL

A corporate security awareness program aims to make all the employees understand and appreciate not only the value of the company's information assets but also the consequences if these assets are compromised.

Employees are going to continue to defeat — intentionally and unintentionally — the barriers we erect to protect proprietary information. Ultimately, all information development, management, and dissemination remains under the control of human beings — not computers. The solution must be proper management of people and their security responsibilities.

Fear, uncertainty and doubt are strong behavioral stimuli. If every employee understood the irrefutable relationship between information security and job security, the business would be far more resistant to victimization resulting from subterfuge and passivity. If security were correctly perceived as synonymous with market capitalization, full employment, revenue growth, increased profits, and market expansion, attitudinal shifts would reshape workforce values.

> *"A tiny device like a USB storage key can suck an enormous amount of proprietary information out of your company in the blink of an eye."*
>
> — Vladimir Chernavsky
> CEO/President, Smartline, Inc.

Employees must accept responsibility as owners of the enterprise. They need to know that what threatens the company threatens the futures of everyone. Behavior-based awareness capitalizes on these elemental human dynamics, bridging the chasm of risk by instilling in every employee the empowerment to affect change and create value through awareness and action.

If companies can change employee behavior, they can tighten security quickly and cheaply. Only repetitive training can raise employee awareness and provide them with the critical knowledge and skills needed to counter ever-growing threats.

Employee Behavior Doesn't Have to be Malicious to be Dangerous

Some of the most common gateways to hacker attacks, information theft, viruses and other damaging incidents:

- Carelessness with passwords
- Willingness to open unexpected e-mail attachments
- Ignorance about the risks posed by wireless, mobile devices.
- Naiveté towards social engineers asking seemingly innocent questions
- Laptop loss due to theft or carelessness
- Reduced emphasis on physical security of personal workspace and materials
- Cavalier attitude towards security policy and procedures

What do they all have in common? ***They all involve people.***

VI. HOW TO ACHIEVE EMPLOYEE SECURITY AWARENESS

How do you start off on the right foot when implementing a security awareness program? How do you determine what tools will be effective in your organization? And the big question is: how do you make everyone aware? Our security experts offer a number of simple yet often overlooked strategies.

Whether the product is soda, sedans, or security, advertising works. Don't overlook its power and potential when developing an information security awareness program.

After you've set a strong policy and held awareness training to get the message out, the next step is making sure that people remember it. A successful message must be real, rewarding, easy to understand, and engaging.

Three essential ingredients go into creating a security awareness program that works:

1. It must convincingly demonstrate that security breaches don't just adversely affect the organization, but also harm individual employees.

2. It must focus on and consistently reinforce the fundamentals of strong security practice, over and over again in different and creative ways.

3. It must draw people in by appealing to issues important to your employees.

The Principle of Repetition

It's a known fact that repetition assists in the learning (awareness) process. Experts say that a message read or heard several times a day in a given week is virtually memorized and, over a period of a month, 90% of the content is retained.

The advertising world knows very well the benefits of repeating a message. Just think for a minute how many times you've seen the same ad on TV or in print. Madison Avenue uses the principle of repetition to get its messages burned into the mind of the consumer in order to influence their buying behavior.

Bringing Your Security Message "Home"

Experts agree that the key to getting your message heard is to make it relevant to your audience. That's why so often generic security admonitions fall on deaf ears. Employees passively think of information security as someone else's job, and therefore not something they need to be concerned about. It is a significant challenge to get employees to take an interest in a topic that seems to have nothing to do with them.

As employees better understand the information security threats to their own personal and family life, they begin to take seriously the impact of breaches in their workplace. Interspersing these types of personal and family-oriented security awareness makes your employees understand that when good security practices are not followed there can be dire consequences, and this newfound perspective motivates them to take seriously the damage that can be done to your company.

Communications experts teach that the most effective way to ensure your message reaches everyone in your intended audience is to deliver it through multiple channels. The more opportunities for exposure, the greater the likelihood employees will hear your security awareness message and change their behavior.

Here are a few simple, cost-effective ways you can deliver security awareness in your organization. We

Helping Employees Transition from Greatest Risk to Greatest Asset

- Only through continuous exposure to appropriate awareness training can employees transition from the greatest risk to the greatest asset.
- One of the most effective security awareness methods for employees is consistent positive reinforcement through well-articulated security messages that are easily understood, digested and applied to their everyday lives at work and at home.
- Managers must ensure that people receive the training they need and that they are motivated to use it.
- Only when security becomes as second nature as buckling up your seatbelt, will it really be effective.

recommend you take an approach that incorporates as many of these methods as possible.

Post security stories on your Intranet site
Create an online resource for your company by archiving security related material. You can even organize articles by subject for future employee reference, e.g. virus alerts, corporate espionage, social engineering, travel safety, etc.

Create links to your security policies
You can also create links between an individual policy and a security story that help illustrate the need for that policy. When an employee is finished reading a story about stolen passwords costing a company millions of dollars, he or she can easily hit the link to see what your company says about password protection.

Publish articles in your company newsletter
Create a security article for your organization's internal publication. Be sure to select stories that have the widest range of interest. When you need to make a point or send out a policy reminder, use a security story to help employees understand the reality and importance of your warning.

Use an attractive poster(s)
Reach employees even "around the water cooler. " Print selected images/stories on a color printer for posting on bulletin boards, especially in areas where employees don't have ready access to the network.

Create a pop-up window that features an article or tip
Pop-up screens can be positioned to display each time a user logs on to the network, or as a lead to your organization's security Web page, Human Resources page, and other frequently visited locations.

Use videos, booklets and flyers
There are a variety of off-the-shelf, 10-to 15-min. videotapes that address information security. There are enough of them out there that you can find ones that reflect your theme. Booklets and flyers are also effective in emphasizing various aspects of security, such as how to defend against "social engineering" attacks.

1. Train employees to recognize security-robbing behaviors in themselves and others.

2. Bring management into the program. Make sure the company's top executives understand and support security awareness initiatives.

3. Involve employees in setting security goals, and make sure everyone understands what the lack of good security can mean.

4. Don't intimidate and use security as a big stick. Educate and inform.

5. Make sure employees and management know there is a clear chain of security responsibility: that everyone has a role and everyone owns a piece of the problem and the solution.

6. Make security fun. Have pizza Fridays or use games to raise levels of awareness. One company held a contest to see which employee could come up with the most creative security mascot.

7. Encourage security roundtable discussions, where employees and management discuss risks to the company based on news reports they may have seen. Recent hacker and virus attacks made good entry points to security discussions.

8. Bring in an out p e ace employees$ o ity ss es.

VII. BUILDING A BUSINESS CASE FOR A CORPORATE SECURITY AWARENESS PROGRAM

In today's resource-constrained environment, corporate security awareness programs must compete with other top projects to get management buy-in and support. By building a business case that addresses the most compelling issues surrounding employee security awareness, managers can secure approval from top executives to implement a successful corporate program that enhances the company's security posture.

Most companies aren't doing enough to create a culture of security, according to Bruce Murphy, CISSP and CEO of Vigilinx, Inc., a provider of managed security services. "They don't understand the value, since it is hard to quantify" the hard-dollar return on security spending. Many companies also underestimate the importance of people and processes in creating a culture of security.

Demonstrate Security's Positive Return

How to secure more spending on training and awareness:

• Get executives who understand the risk posed by employees to put money where their fear is. Although many companies don't direct information security spending toward employees — via training or awareness — many executives are, in fact, mindful of the risk. When leaders understand the risk posed by employees, it should be easy to convince them that technology tools are not the total solution.

Here's the point: Once you compare the potential costs of an act of sabotage or negligence by an insider to that of basic personnel security measures, the cost of the latter doesn't seem so high anymore. If corporate leaders don't understand the risk posed by employees, explain to them how the security team perceives the risk. Executives who think of information security as a computer problem may be surprised to learn that most information security professionals are more fearful of employee misconduct than they are of attacks on systems, hackers, cyberterrorism, cyberwarfare, competitor espionage, or natural disasters.

In fact, the 1,400 information security representatives who responded to the 2003 Global Information Security Survey ranked employee misconduct involving information systems as the second most critical threat, surpassed only by major viruses and worms. Without necessary resources, security directors can't protect the company's information systems. At the same time, security teams can't bemoan a lack of resources if they haven't adequately communicated the company's risk profile to its leaders.

Security ROI is Real

• A reduction of exposure to successfully launched viruses and other types of computer hacks, which have short-term and long-term costs to companies. Reducing that hacker and virus damage figure of $1.6 trillion goes a long way to demonstrating ROI.

• Liability exposure will be reduced. In an age of e-commerce, partnering and other third-party relationships, companies face more exposure and more liability. Improved security reduces that liability.

• Validation of a strong awareness program is critical proof that the defendant company in a trade secret case, for example, took all reasonable measures to protect its data.

• Reduced liability insurance premiums for strong,

demonstrable security program is a developing marketplace trend.

• A strong security culture among the entire employee population may very well be the only defense against a disgruntled employee with intent to sabotage the company.

How to Justify the Cost of Security

Consider this. Three-quarters (75%) of information security incidents are "inside jobs" — resulting from employee negligence, carelessness, or just ignorance. Experts point out that security incidents are poised to take off and organizations that fail to invest in employee awareness are at greatest risk of being victimized by a costly breach.

If up to seventy-five percent of security breaches are caused by insiders, then the majority of these deficiencies can be addressed and remediated through proactive security awareness and education. In that case, employee awareness programs are the tool of record in advancing security ROI.

What's a reasonable investment for deploying an ongoing security awareness program? First, consider the costs of a breach — your sensitive information, your reputation, and the money involved. How much money? The FBI reports that the average security breach costs companies $115,000 per incident.

Average cost of a single security breach = $115,000

Estimated cost of creating and staffing a security awareness program divided by the cost per employee.

Total cost vs. investment = ROI

Think of it this way: If you relate employee awareness to a never-ending high-stakes chess match

Companies Without A Strong Security Awareness Program Should Ask These Questions

- When the incident will occur, and how bad will it be?
- Will the breach be confined to internal company operations, or will customers, partners, and global supply chain members be impacted by the security incident?
- Will such a breach create a significant liability?
- Will valued customers hear about the incident, and will that force them to reconsider doing business with you?
- Will your competitors take advantage of such an event in an attempt to lure customers away from you?
- What is the cost of an information security awareness program versus what a significant event might cost?
- What is the best way to launch a security awareness program?

between the good guys and the bad guys, the security awareness program influences one side in the chess match — the company's employees — which may help that team make smarter moves. Prudent investment in security awareness can reduce the probability of an incident.

The business benefits (resulting from increased compliance, improved control, reduced risks and reduced losses through security breaches) will substantially outweigh the costs of the program.

The Case for Outsourcing

The primary argument for outsourcing is financial: a company can get the security awareness expertise it needs much more cheaply by hiring someone else to provide it. While it is possible for companies to build security awareness programs on their own, it's rarely cost-effective.

When you factor in how many staff hours it would take to create a continuous employee awareness program on your own, your cost savings and ROI are even greater. This is an area where outsourcing really pays off.

By not having to pay salaries for your own security staff, you'd save about $40,000 to $60,000 annually per security training professional (based on average salary rates for current security professionals seeking employment to provide security support in-house). Also, consider the costs associated with outsourcing that you wouldn't have to deal with otherwise, such as management costs.

The benefits, then, are clear. You can focus your time, money, and worries on your core competency because information security awareness training is in the hands of experts.

Talking with others and asking industry experts will reveal the best security awareness providers. Go with an industry leader with a long and well established reputation. You don't want a little-known maverick.

VIII. RECOMMENDATIONS: A PRIORITY SECURITY MANAGEMENT AGENDA

Employees are going to continue to defeat — intentionally and unintentionally — the barriers we erect to protect proprietary information. Ultimately, all information development, management, and dissemination remains under the control of human beings — not computers. The solution must be proper management of people and their security responsibilities.

Demystifying security: that's the first step. Employees don't really understand security. They don't understand because they haven't been exposed to it. Too often, security is perceived as an "us versus them," adversarial relationship. Changing perceptions about security begins with recreating part of the corporate culture.

Very simply, security is a guideline for modeling positive behaviors while discouraging negative behaviors. Security means every employee taking responsibility not only for themselves but for everyone else, too. Security means making sure that every employee knows the rules of the game, and holding themselves and others to this standard.

Lack of Awareness: Your Biggest Threat

Volumes of unread, un-enforced policies and

procedures line corporate bookshelves, created by security and read largely by security. Many of them are complicated, unreadable, dense tomes that bear little relevance to the practical realities of security across the enterprise.

Effective security policies and procedures are enabling, embracing, and inclusive. Most importantly, though, they are accessible. Every employee should be exposed on a "continuing basis" to security awareness and why security is important. Policies and procedures should be easily readable and understandable. Compliance and enforcement expectations should be clear and concise.

One of the most dangerous approaches to security is passivity, assuming employees know what correct security behaviors are. Employees need to be taught positive, defensive behaviors before they can serve as reliable sentries to the corporate fortress. While the obligation to work securely falls upon the employee, helping employees understand security is the obligation of the corporate security department.

Communications with employees, exposing them to the right awareness programs, is the key. Constantly reinforcing the benefits of security at work and at home and their role in it, and what is expected from them as the first and most significant line of defense, will over time help create a stronger security culture.

Basic Awareness Curriculum

Security awareness goes beyond annual refresher briefings or a few posters hung in the lobby. In a truly secure company, awareness of security practices permeates the organization's culture and consciousness.

Education is a critical element of security awareness. It's hard to be aware of security incidents if you don't even know what the issues are. Education can't be effective and concise if the material is too long. That's why well-crafted security awareness messages are so important.

Here's a sampling of some of the critical topics to include in your security awareness program:

- Social Engineering
- Proprietary Information Protection
- Wireless Security Risks
- Computer Viruses
- Password Protection
- Office/Physical Security
- Workplace Violence
- Industrial Espionage
- Identity Theft
- E-Mail Precautions
- Data Back-Up
- Internet Concerns
- Computer Crime
- Hacking Incidents
- Security Breaches
- How to Report/Respond to Threats
- Internet Attacks
- Legal Use of Software
- Laptop Theft
- Privacy
- Travel Security Concerns
- Cyberterrorism
- Personal Security

IX. THE SECURITYsense SOLUTION

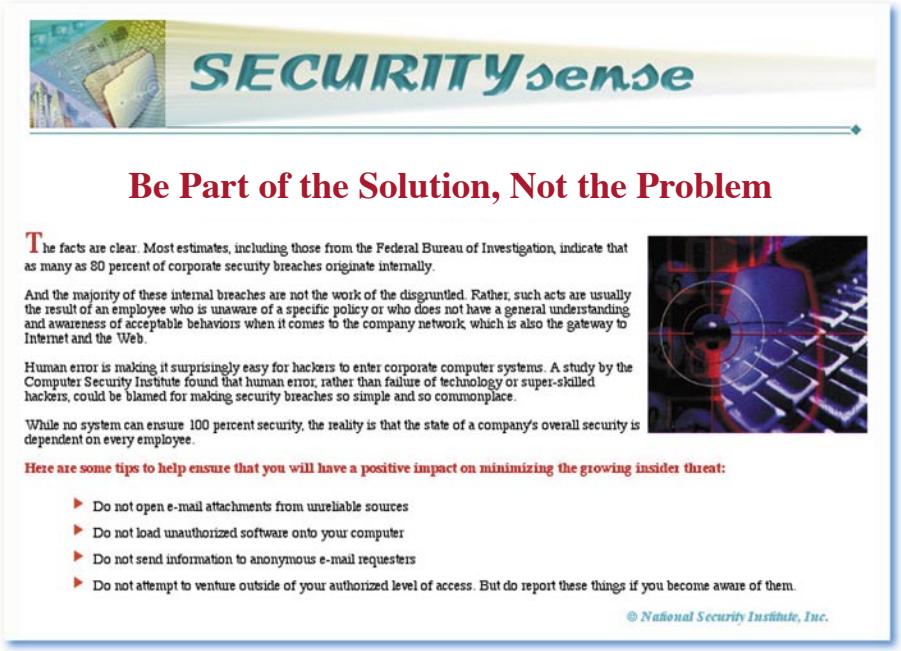
Successful, proven security awareness programs must both convince employees of the need to protect their organization's information assets, as well as teach the techniques they need to know.

How do you focus employee awareness on the security issues that really matter — on an ongoing basis? SECURITYsense answers that important question for you — and provides the solution.

SECURITYsense is a continuous awareness program that keeps your entire workforce abreast of security threats, hacking tricks, social engineering attacks, and security breaches — so employees can protect the company's priceless information assets.

Produced by the security experts at National Security Institute, SECURITYsense offers 20 eye-catching conversational, and topical security awareness articles per month delivered via e-mail in HTML format — that's an average of one message per workday. You can display these messages on the company intranet, publish them in employee publications, or e-mail them as-is to employees. You can even customize the content to your company's specific policies.

Many businesses do not have the necessary time, resources, or expertise available to conduct a comprehensive security awareness initiative. With SECURITYsense, you can implement a cost-effective, turnkey information security awareness program



SECURITYsense

Be Part of the Solution, Not the Problem

The facts are clear. Most estimates, including those from the Federal Bureau of Investigation, indicate that as many as 80 percent of corporate security breaches originate internally.

And the majority of these internal breaches are not the work of the disgruntled. Rather, such acts are usually the result of an employee who is unaware of a specific policy or who does not have a general understanding and awareness of acceptable behaviors when it comes to the company network, which is also the gateway to Internet and the Web.

Human error is making it surprisingly easy for hackers to enter corporate computer systems. A study by the Computer Security Institute found that human error, rather than failure of technology or super-skilled hackers, could be blamed for making security breaches so simple and so commonplace.

While no system can ensure 100 percent security, the reality is that the state of a company's overall security is dependent on every employee.

Here are some tips to help ensure that you will have a positive impact on minimizing the growing insider threat:

- Do not open e-mail attachments from unreliable sources
- Do not load unauthorized software onto your computer
- Do not send information to anonymous e-mail requesters
- Do not attempt to venture outside of your authorized level of access. But do report these things if you become aware of them.

© National Security Institute, Inc.

immediately. It requires no technical expertise to distribute — or to understand. All of the planning, development and coordination of implementing an awareness program has been done for you.

In the information age one thing is clear: your job depends more and more on how ordinary employees comprehend and comply with security procedures. And with SECURITYsense in place, your employees can never say they "didn't know" or weren't kept informed about their ongoing security responsibilities.

To inquire about NSI's SECURITYsense awareness solution for your organization send e-mail to dmarston@nsi.org or call our security experts at (508) 533-9099. You may also view past samples of SECURITYsense articles online by pointing your browser to http://nsi.org/SECURITYsense.html

How Other Organizations Are Spreading the Security Awareness Message

Major organizations from both the private and public sector have embraced SECURITYsense including:

- Wachovia Corporation
- Bell South
- Federal Deposit Insurance Corp.
- Federal Express Corp.
- IBM
- Aetna, Inc.
- Federal Reserve Banks
- Kaiser Permanente
- Pfizer, Inc.
- PPG Industries, Inc.
- St. Jude Children's Hospital
- City of Phoenix
- LG&E Energy Services, Inc.
- Comerica Bank
- Genzyme
- Ernst & Young, LLP
- The Boeing Company
- Aerospace Corporation
- Federal Aviation Administration
- McDonald's Corporation
- Memphis Light, Gas & Water
- Palmetto Richland Hospital
- America West Airlines
- Texas State Comptroller
- Federated Mutual Insurance Co.
- Webster Bank
- Los Alamos National Laboratory
- Lockheed Martin, Corp.
- Burlington Resources
- Commerce Bank

About NSI

Founded in 1985, the National Security Institute (NSI) is a publisher and educator serving the needs of security professionals in government, the corporate sector and defense contracting.

NSI has a long history of setting the standard for excellence in providing security newsletters, special reports, seminars and consulting services for security executives throughout the United States and Canada. With more than five-hundred clients, the National Security Institute has trained thousands of security professionals and created numerous security awareness programs and services.

For more information on any of our services, contact:

National Security Institute
116 Main Street, Suite 200
Medway, MA 02053
Tel: 508-533-9099 • Fax: 508-533-3761
E-Mail: InfoCtr@nsi.org • Internet: http://nsi.org