

Nearly 80 Percent of Information Security Breaches and Resulting Losses Originate from Inside an Organization

Here's How to Protect Your Company from the Inside Out!

***SECURITY*sense**

Information Security Awareness Service

Dear Information Security Manager:

Quietly, relentlessly, your company's information systems and business secrets are being attacked.

At stake is billions of dollars' worth of U.S. intellectual property, from computer codes and secret drug formulas to the plans for new products and technologies.

Among some of the secrets that corporations have reported stolen by corporate spies are General Electric's formula for manufacturing industrial diamonds, Kodak's filmmaking technology, the design for a new Gillette Co. shaving system and Schering-Plough Corp.'s recipe for manufacturing the anti-cancer drug Interferon.

Losses from computer crime and information attacks can reach into the millions of dollars. Omega Engineering Corp. was nearly forced out of business when one of its employees detonated a computer "time bomb" that wiped out all of the company's software. Result: [The company lost \\$10 million due to that one incident alone!](#)

Security experts agree that the [real threat to information is often from within](#) — ranging from disgruntled employees to outside contractors with insider privileges. In fact, "nearly 80 percent of security violations are caused by authorized users with legitimate access," according to the FBI.

Despite spending \$6 billion annually on computer security hardware and software to ward off hackers, companies are discovering that even the best firewalls and security monitoring tools can't prevent internal breaches caused by lax end-user security practices.

So, how do you make sure that your company's information assets are protected? [The first line of defense is employee awareness](#) — the critical "humanware" component of your data security armor.

Power-Up Your Information Security Program

Now there is an [innovative solution](#) to assist you in fortifying your information assets: **SECURITYsense** — a continuous information security awareness service for your employees.

Delivered to your desktop each month via e-mail, — for posting on your company intranet site or other media — this high quality, continuing education service promotes better security at a [fraction of the cost](#) of traditional awareness programs.

SECURITYsense offers the most bang for the buck! For just pennies a day you can now provide your entire workforce with timely security messages that will help them adopt a more security-conscious attitude and minimize the risk to your company's critical information.

[Here are just a few ways SECURITYsense can help raise awareness and protect your critical information assets:](#)

- Brings end-users up to speed on critical information security risks.
- Arms employees with common sense protection techniques.
- Bolsters the “humanware” component of your data security armor.
- Reminds employees of their ongoing responsibility to protect company data.

Your Security Awareness Task Just Got Easier

SECURITYsense will take the burden of educating your end-users off your shoulders, saving you both time and money.

[Here's how it works:](#) At the beginning of every month, you'll receive via e-mail, 20-professionally presented security awareness articles in [two](#) convenient formats: Plain text **and** HTML.

You and your employees may view items on your company's intranet site as HTML documents complete with color illustrations, charts and graphs or, if you prefer, you can periodically e-mail selected articles to your employees, or incorporate the messages into computer pop-up screens.

Even if you don't have an intranet site, you can print and distribute copies of **SECURITYsense**, post the articles on company bulletin boards or use them in internal publications.

Either way, the information in each issue of **SECURITYsense** is [easily accessible to all](#) of your employees, no matter the size.

Why is **SECURITYsense** so effective? Because each month it brings your employees practical information about security related issues on and off the job. And it's presented in a series of 20 easy-to-read-and understand messages.

For example, **SECURITYsense** tells your employees —
... how to protect the company's critical information
... how they fit in to the company's information security program
... how their job security depends on information security

If **SECURITYsense** helps you avoid just one information security breach during the course of the year, it'll pay for itself many times over.

SECURITYsense offers a cornucopia of awareness material including. . .

- Step-by step advice on protecting proprietary information.
- Prevention tips to help reduce computer crime.
- "Horror" stories of real life security breaches to catch reader's attention.
- Personal security items such as travel safety, home security and safety tips to maintain reader's interest.
- Password protection, E-mail security and Internet security.
- Threats from social engineering and competitive intelligence.
- Legal responsibilities for protecting information.
- Incidents of industrial espionage and trade secrets theft.
- Tips and techniques to protect information systems.

Currently being deployed at proactive companies like Bell Atlantic, Bank of America, Citicorp, MetLife, Kaiser Permanente, Pfizer, Microsoft, Coca-Cola Enterprises, Lockheed-Martin and Polaroid Corporation, **SECURITYsense** is already proving effective in raising employee awareness and safeguarding corporate information assets.

Protect Your IT Investment. Lessen Your Exposure.

If you're serious about protecting your information systems and creating an effective security culture that encourages compliance at all levels, you'll want to make sure that you have **SECURITYsense** in your corner.

Your company has spent a fortune building an information fortress comprised of the latest security hardware and software. The best way to protect that considerable investment is to beef up your "humanware," — the most vulnerable link in the information security chain.

Data Protection Must Start With Employees

Information security solutions involve three major controls: social, physical and technical. Of these, the most important is social controls.

After all, locks on the door won't work if people don't use them and computer passwords are useless if people share them with others. Ultimately, your [information security program is only as good as your employees](#).

For a growing number of enlightened companies — from large corporations to smaller companies — it makes better sense to try to prevent information security breaches than to pay for their cost down the road.

Now for as little as \$1,295 per year, you can [bullet-proof your information security program](#) and start your employees on the road to better security right away. Just one lesson learned — one single data security tip or technique that your employees can adopt as their own — could pay for this subscription many times over.

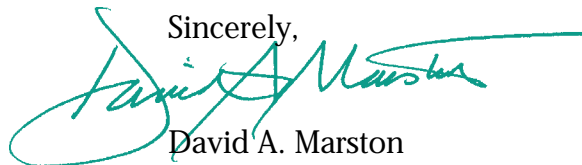
Find out for yourself how much this [proactive continuing security awareness service](#) can help train your employees to protect valuable information and ensure your company's competitive edge. Something this good — and inexpensive — deserves your utmost consideration.

Be Safe. Not Sorry.

I'm so confident that you'll find **SECURITYsense** to be of immeasurable value to you that I'll give you this [iron-clad guarantee](#). Subscribe today. And if, at any time during the course of your subscription, you decide to cancel — for whatever reason — just notify me and I'll give you a full refund for all unmailed issues. No questions asked!

As a security educator, I ask your company to try **SECURITYsense**. Not because the cost of promoting information security awareness is so low. But because the cost of not promoting it is so high.

Sincerely,



David A. Marston
Publisher