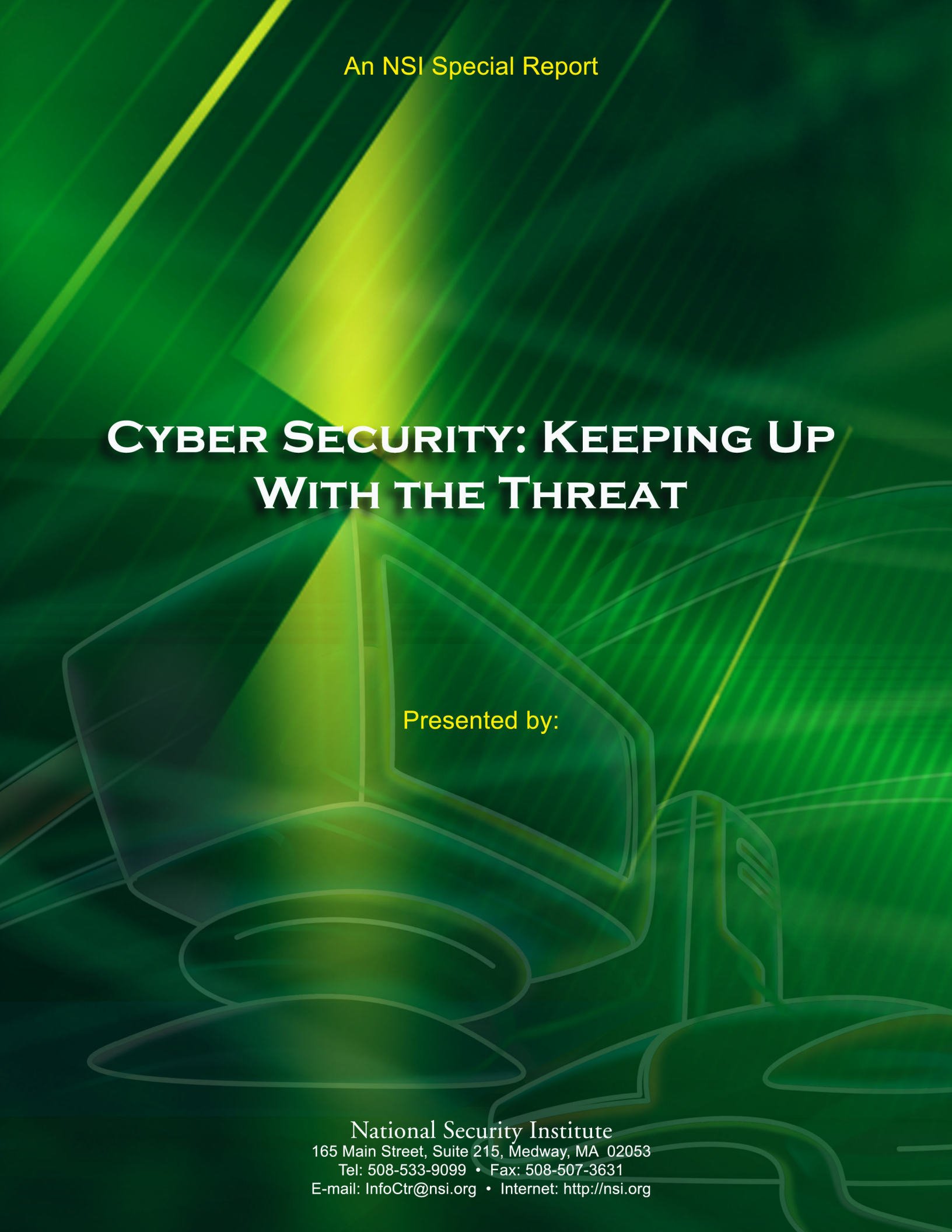
An NSI Special Report

Cyber Security: Keeping Up With the Threat



Presented by:

National Security Institute
165 Main Street, Suite 215, Medway, MA 02053
Tel: 508-533-9099 • Fax: 508-507-3631
E-mail: InfoCtr@nsi.org • Internet: http://nsi.org

Cyber Security: Keeping Up With the Threat

Aside from nuclear war and weapons of mass destruction, cyberattacks pose the single greatest threat to U.S. security – and they are growing more and more difficult to prevent.

That's the grim take presented recently by FBI cybersecurity analysts and other experts, who are warning of a possible "cybergeddon" – a scenario where the nation's economy, in which almost everything of importance is linked to or controlled by computers, is sabotaged by hackers.

Alarmist? Hardly. Shawn Henry, assistant director of the FBI's cyber division, says terrorist groups are working to create a virtual 9/11, "inflicting the same kind of damage on our country, on all our countries, on all our networks, as they did in 2001 by flying planes into buildings."

An online attack of that scale hasn't happened in the U.S., but computer hacking – once something of a sport for brilliant delinquents – is rapidly evolving around the world as a tool of war.

Incidents skyrocketing

One clear indicator of the growing threat is the sheer volume of breaches. Federal civilian agencies reported three times as many cyber-related incidents in 2008 as they did in 2006 to the Homeland Security Department's office that coordinates responses to cyberattacks.

The agencies reported to Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) a total of 18,050 incidents in 2008, compared with 12,986 in 2007 and 5,144 in 2006. The total number of incidents reported by commercial, foreign, private, and government sectors rose from 24,097 in 2006 to 72,065 in 2008.

The Federal Information Security Management Act requires agencies to report cyber incidents, which are defined as acts that violate computer security or acceptable-use policies. The types of incidents include unauthorized access; denial of service; malicious code; improper usage; and scans, probes and attempted access.

Myriad threats

There are, of course, several types of threats that businesses and government agencies alike must be on the lookout for including:

- **Cyber espionage —** occurs when a government or business uses technology to steal sensitive information. This may entail sophisticated hacking, but it may be much simpler – as when spies compile publicly available information from company websites, legal documents, etc.

● **Cyber terrorism —** the worst nightmare of U.S. security experts, entails seizing control over a networked computer system to inflict damage. Imagine, for example, terrorists hacking into the country's air-traffic control system, or the electrical grid of a major city.

● **Mobile computing—** while a powerful productivity tool when used securely, offers serious breach potential. Lost or stolen laptops, PDAs, and smart phones often carry sensitive data that could harm a business or even the government if it fell into the wrong hands.

● **USB drives —** they can be used by disgruntled employees to easily steal sensitive company data, and they can also be used to introduce crippling viruses to corporate networks.

● **Social engineering —** occurs when hackers or spies trick workers into divulging sensitive information, and remains perhaps the biggest threat. Why? The weak link is typically an employee who compromises security by inadvertently giving up a password or other vital bit of data.

In addition to these threats, experts are warning companies to expect an increase in insider security attacks by disgruntled or laid-off employees. A study last year conducted by the Identity Theft Resource Center found that insider breaches accounted for 18% of attacks. And workers needn't even have malicious intent to cause damage. Innocent but careless employee actions often set the table for attacks by more malicious parties.

A recent report from the Ponemon Institute found that 88% of data breaches were caused by simple negligence on the part of staff. This negligence can take many forms:

- Using weak passwords.
- Leaving sensitive information unattended on a desk.
- Having a laptop or PDA lost or stolen.
- Unknowingly allowing strangers access to work facilities.

Malicious insider attacks, while not as common as innocent mistakes, have the potential to be more devastating because the employee knows where the crown jewels are kept – the truly valuable company information coveted by competitors, hackers, or identity thieves.

Innocent but careless employee actions often set the table for attacks by more malicious parties.

A "subway survey" of London commuters conducted by InfoSecurity Europe Conference found that more than two-thirds of workers believe it's easy to take information out of their organization. And a whopping 88% believe the data they access at work, including business plans and customer databases, is valuable.

If you want to get worried, couple that with more survey results that found a third of employees would sell company secrets to a stranger for $1.5 million – or even, in many cases, far less.

Exploding risk

Having more sensitive information being seen by more people and accessed on more devices drives up risk significantly, analysts point out.

And the slumping economy doesn't help. Mass layoffs have increased internal threat levels dramatically. There are a lot of ex-workers with a grudge out there, and they need money. Not only that, but one traditionally weak area for company security is removing a user's network privileges as soon as he or she leaves the company – so plenty of ex-employees with an ax to grind have ready access to sensitive data.

Employees worried about job security face rising temptations to seek out and hoard proprietary data that could help boost their job performance, or at least make them more marketable should they get laid off.

Of the 400 information technology pros who participated in a recent survey conducted by security vendor Cyber-Ark, 74% said they knew how to circumvent security to access sensitive data, and 35% admitted to doing so without permission. Among the most commonly targeted items: customer databases, email controls, and CEO passwords.

Digital spy threat

As the world's engine room of research and development, the U.S. is vulnerable to espionage, especially in the technology-rich aerospace and military industries, telecommunications, cars, and pharmaceuticals.

Corporate espionage costs the world's 1,000 largest companies more than $45 billion each year according to PriceWaterhouseCoopers.

Changing Face of Cybercrime

How are cyber criminals working today? According to the security experts, three major changes stand out:

1. Hackers are in it for profit. The web is now a vital tool for criminals looking to make money, not merely mischief. Malware-infected systems are used as a network of bots (that is, remote-control robots) for a wide variety of inappropriate activities. Bots can perform denial-of-service attacks, send out spam and phishing emails – they're the Swiss Army knife of malware distribution, analysts say.

2. Cyber criminals are quieter and sneakier. While early hackers wanted to make a big splash by attacking as many computers as possible in a show of genius and savvy, today's criminals don't want to be detected. So their takeovers are done in a slow, methodical fashion. These crooks know that if they can operate as stealthily as possible and take over systems in a selective manner, they stand a better chance of not getting caught.

3. End users are now the primary targets. Large organizations were the main target of attacks less than a decade ago; now end users are the primary targets, experts say. One bit of fallout from this shift is the massive growth of phishing websites, which lie in wait for consumers seeking fantastic bargains.

While all industries are vulnerable, firms in the defense and high-tech sectors need to be especially watchful. All told, U.S. businesses lose up to $250 billion in revenue as well as 750,000 jobs annually.

Researchers at the University of Toronto have uncovered a computer spying operation they called GhostNet that was based primarily in China and had stolen documents from governments and private businesses around the world.

In another worrisome sign, there have also been recent credible reports that cyber spies from China, Russia, and other countries have penetrated the U.S. electrical grid with the aim of disrupting the system.

Moreover, cyber perpetrators are known to have sought access to information about the Pentagon's next-generation fighter aircraft, the $300 billion Joint Strike Fighter.

In the case of the Joint Strike Fighter project, attackers were able to copy and siphon off multiple terabytes of data related to the design and electronics systems, which could make it easier for hostile nations to defend against the aircraft.

Analysts agree that evidence points to China as being the base for spies responsible for the GhostNet attacks, and that they've hacked U.S. servers too.

The U.S. has listed China as one of the key targets for cyber espionage in the next four years, and views that nation as well as Russia as aggressive players in cyberspace. While "aggressive players in cyberspace" may seem a relatively innocent term, keep in mind that analysts expect cyberspace to be the new battleground in espionage wars for the foreseeable future.

Savvy cyber criminals

Internet criminals are increasingly operating like successful businesses, borrowing the best strategies from legitimate companies and collaborating in partnerships with each other to profit from their illegal activities says networking giant Cisco.

According to security analysts, more companies are coming under attack from business-aware criminals who are creating spam around major news events, such as swine flu, to gain access to company systems or persuade victims to visit malware-laden websites.

Savvy cyber criminals are taking advantage of our increasing reliance on computers and the Internet.

Other threats wielded by the sophisticated new generation of crooks include botnets, which are being rented out on a software-as-a-service basis, according to the report.

Social nets targeted

Social networking sites are also coming under fire. The problem with sites such as Facebook and LinkedIn is that they create an environment of trust among users, who generally assume that links and downloadable content at the sites are always safe. Nothing could be further from the truth, of course.

The recession and the threat of job losses, meanwhile, has led to a rise in disaffected

workers who are much more likely to compromise corporate data.

Analysts point out that in addition to using their technical skills to cast a wide net and avoid detection, the new-generation of cyber criminals are also demonstrating some strong business acumen. For example, they are collaborating with each other, preying on individuals' greatest fears and interests, and increasingly making use of legitimate Internet tools like search engines and the software-as-a-service model.

For businesses, experts say the defense strategy is clear: organizations need to adopt ever more advanced ways to fight cyber crime and remain vigilant across all attack vectors.

Mobile insecurity

Up to 12,000 laptops are lost in U.S. airports each week, believe it or not. And even though more than half are simply left behind at security checkpoints, a whopping 65% to 70% are never returned.

The average value of a lost corporate laptop is about $50,000, according to a Dell sponsored study of lost or stolen portable computers.

The value of the laptop was arrived at by estimating the cost of the data, the loss of

Mobile Security: Rules of the Road

Laptops, PDAs, and smart phones are easily lost or stolen – and as most people realize, the information residing on them can cost a business millions. Here are some expert tips to help safeguard mobile tools:

- Label electronic devices with your name, address, and cell phone number. As noted above, most laptops lost in airports are left at security checkpoints, where they're found by the Transportation Security Administration (TSA) or airport staff. If there's no identifying information on the device, the authorities have no way to return your property.

- Always carry smaller electronics like cell phones and iPods in the same place in your handbag or carry-on. Knowing where to look for them will not only help you access and use them quickly, but will also help you realize quickly if an item is lost.

- Charge your electronics before you begin a trip so that you don't have to charge them in an airport lounge or waiting area. Charging in a public place increases your risk of forgetting an item, or having it taken when you look away for a moment.

- If you carry your cell phone, mp3 player, electronic planner, or other small item in your pocket, always check the area when you get up from a seat. Devices can easily slip from a pocket when you're sitting down.

- Take extra care at security checkpoints to make sure you've retrieved all your important possessions. Don't feel you have to rush to get out of someone else's way, especially if rushing will increase your risk of forgetting something.

productivity, costs associated with replacing the notebook, and other factors.

The maximum value reported was almost a million dollars. Analysts said this number is hardly surprising, given the value of proprietary information such as customer lists and product plans.

According to another report from Verizon Business, the services industry (which includes legal firms and consulting companies) generated an estimated cost of $112,853 per lost or stolen laptop, versus $71,820 for one owned by a financial services employee.

Healthcare, pharmaceutical companies, education, and technology firms also ranked near the top of the list of industries that would be most financially affected by a lost laptop.

So, in dollars, who's at the biggest risk of losing data in a corporation? Not the chief executive, the study found. Mid-level managers responsible for keeping the company up, running, and moving ahead, and their directors, would cost their companies $60,000 or so in lost data and hardware costs. A CEO's lost laptop would cost just $28,449, the study found.

For the first time, insiders have overtaken computer viruses as the most frequently reported type of security incident.

Data breach costs

It costs $6.6 million on average when an organization suffers a data breach and more than $200 per compromised record, according to research from Ponemon Institute.

Researchers looked at 43 organizations that reported a data breach last year and found that roughly $202 was spent on each consumer record compromised. The average number of consumer records exposed in each breach was about 33,000.

More than 84% of the companies surveyed had at least one data breach or loss prior to 2008. The cost of a breach in 2007 was $6.3 million, up from $4.7 million in 2006.

The annual study measured the direct costs of a data breach, including the following:

- Hiring forensic experts.
- Notifying consumers.
- Setting up telephone hotlines to field queries from customers.
- Offering free credit monitoring subscriptions.
- Discounts for future products and services.

The survey also sought to measure more intangible costs of a breach, such as the loss of business from increased customer turnover and decreases in consumer trust. Following a data breach disclosure, the percentage of customers who leave one brand for another was highest among health care and financial services companies.

The experts who conducted the study said breaches truly do cost businesses customers; people really do care when organizations compromise their data.

The survey did not include the effect of a breach on the company's stock price, which in some cases can be substantial. Recently when Heartland Payment Systems, the nation's sixth-largest credit and debit card processor, disclosed a breach that could affect millions of customers, the company's stock lost 42% of its value.

The study also didn't measure the cost of intellectual property that is lost or stolen after a data breach. At least 44 states have enacted laws that require companies that experience a breach of personal information to notify those affected.

The accidental enemy

The potential for both accidental and deliberate breaches of personal information and intellectual property by workers is a growing concern, security experts say. Sometimes, employees just get careless, or perhaps they don't know all they should about their security-related responsibilities.

Indeed, many experts say the top security challenge facing business is to plug these accidental breaches. The enemy, in such cases, is ignorance. For example, an employee in the human resources department might email a contractor a spreadsheet that appears to contain only specific, unclassified material.

But if that employee is unfamiliar with the spreadsheet program, he or she may miss the fact that the document includes another tab that's full of sensitive data on company workers.

Other times, though, the breaches are intentional, perpetrated by disgruntled workers or contractors.

Gaping security hole

Every day, organizations deal with proprietary information containing everything from company trade secrets and marketing research to Social Security numbers and addresses belonging to employees, customers, and others.

For the first time, insiders have overtaken computer viruses as the most frequently reported type of security incident. The financial implications stemming from the theft of proprietary information in the workplace are startling, as the average hit to U.S. businesses recently soared to about $350,000.

As long as security budgets focus on technology, the more worrisome threat – human beings – will continue to go unaddressed.

What organizations need to understand is that money spent on technology-based security solutions has its limits; insiders, after all, by definition already have access to the network. As long as security budgets focus on technology, the more worrisome threat – human beings – will continue to go unaddressed.

Analysts say they've seen hundreds of cases in which a large organization devotes virtually its entire security budget to software and network solutions – but doesn't take such basic steps as issuing employee badges, training workers

about security responsibilities, or even locking the back door!

And workers needn't be tech-savvy to spill company secrets; often, information about processes, executive changes, and product plans is what rival businesses truly want to learn.

The number one root cause of security breaches continues to be the human factor: an organization's employees, customers, third parties, and business partners.

There's a famous saying that "amateurs hack systems, while professionals hack people." The point is that defense systems designed to stop hackers, spies, phishers, and frauds are always compromised by timeless human weaknesses: inattention, incompetence and complacency.

Numerous information security surveys and reports indicate that awareness training is falling short with many organizations consigning it to a once a year activity or even ignoring it altogether. Experts warn that organizations that fail to train their workers in security fundamentals do so at their own peril. Interestingly, nearly 90 percent of organizations that have implemented awareness training believe that the number of security breaches they've encountered has been reduced, according to a CompTIA study.

The bottom line: Cyber security is a team sport involving every employee in the organization. It's not just about having the right technology and security policies in place — it's about teaching users how to act securely and responsibly whether they are at their desks or on the road. ❑

Data Security Checklist

Sometimes, the key to data security is … well, an old-fashioned lock and key. Here are some expert tips on securing sensitive data, both physically and electronically.

✔ Lock, stock — or peril. Computer defenses can be critical, but when it comes to protecting personal information, don't forget old-school physical security. Discourage light-fingered passersby by locking sensitive information in a cabinet or drawer.

✔ Barbarians at the gate. Viruses, spyware, and other invaders will attack an unprotected computer in just seconds. Remember, electronic security is everybody's business. Be sure to use strong passwords, and change them regularly.

✔ We have met the enemy and he is us. Hackers certainly pose a threat, but sometimes the biggest risk to a company's security is an otherwise conscientious employee who hasn't learned the basics about protecting personal information.

Trust, but verify. That Cold War phrase should describe your approach to the security practices of your contractors and service providers.

NSI's SECURITYsense Solution

Whether it's protecting the nation's most sensitive secrets or your company's proprietary information, the National Security Institute helps you – and your employees – defend against a growing array of threats from inside and outside your organization.

Since 1985, NSI has been recognized as a leader in innovative and proven employee security awareness training and awareness programs – providing an array of services for both government and private sector. Our client list includes many of the top names in corporate America as well as virtually every government agency involved in protecting the nation's secrets.

NSI's **SECURITYsense** awareness program addresses the critical human dimension of information security and gives employees the tools and information they need to make security second nature. To learn more about how this valuable resource can help you turn your weakest security link into your greatest security asset, contact NSI at 508-533-9099 or visit us on the Web at http://nsi.org/SECURITY-sense.html.

National Security Institute
165 Main St., Ste. 215
Medway, MA 02053
Tel. 508-533-9099
Email: InfoCtr@nsi.org
Internet: http://nsi.org

FREE! e-newsletter

exclusively for the corporate and government security professional.

Every week **NSI's Security NewsWatch** brings news summaries and links to more information on vital issues of concern to help security professionals stay one step ahead of ever-changing threats. This weekly e-newsletter is provided to you free of charge by the National Security Institute as a professional courtesy. To start your free service, register at http://nsi.org/Newsletter.html.