# Securing the Internet Economy

*An Executive Guide To Managing Online Risk*

Prepared for *InfoWorld*, an IDG publication, and Internet Security Systems by Bill Laberis Associates, Holliston, Mass. Published by *InfoWorld*. 

# Security: The Business Imperative

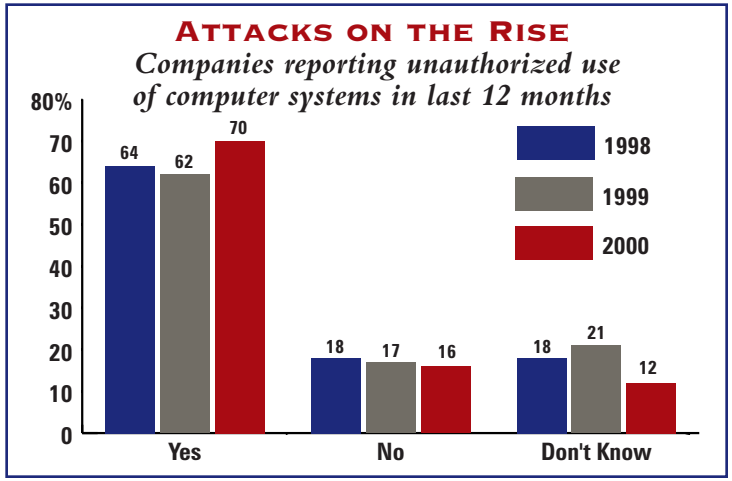
*You manage risk in your physical environment. Are you taking similar steps to protect your online business?*

Security has become an important part of our daily lives. We lock the house when we leave in the morning, and we lock our cars when we get to the office. We take care that our wallets or handbags are reasonably protected, and we make sure no one is looking over our shoulders when we use a phone card or an ATM. We keep sensitive documents locked in a drawer, and we keep easily purloined items such as cell phones out of plain view. Without realizing it, we have adopted a security routine that dictates certain behaviors for certain situations.

Why, then, haven't we taken the same approach to information security? Sure, we may keep the passwords to our office PCs secret—unless we're like the thousands of workers who leave their passwords on sticky notes stuck to their PC monitors. But surprisingly few organizations have developed a complete, overarching security policy and applied that policy such that it becomes second nature to all members of the organization, and an integral part of doing business.

The problem, in part, is that we expect technology to do the

## Inside




Source: 2000 CSI/FBI Survey

work of protecting our computer resources. Whether it's anti-virus software or an Internet firewall, we assume technology tools monitor the network and keep intruders at bay.

But studies tell a different story. Among large corporations and government agencies, 90 percent have detected a breach in computer security in the past 12 months, according to a recent survey by the FBI and San Francisco-based Computer Security Institute. And 70 percent of those breaches were considered serious, involving theft of proprietary information, sabotage of data, or financial fraud. Computer security is a constant challenge, and efforts to address this problem are falling short.

Herein lies one of the important messages of this booklet. Security is not a technology problem; it is a business problem. Securing your business is a key ingredient of overall business success. Correspondingly, failing to secure your business is a recipe for business disaster. Good security allows you to achieve a primary goal of the e-business era: reaching a greater number of customers with enhanced products and services.





## THE BUSINESS THREAT

The security challenge is escalating with the rise of Internet commerce. As more and more organizations realize that e-business *is* their business, they also realize that their computer and network resources are among the critical assets that enable them to become more competitive and successful. They realize that the information stored in their systems is often inventory to be reduced to cash. And then they discover (at times only after their systems have been compromised) that the security measures they have in place—if any—still leave them vulnerable to a range of potentially debilitating attacks. B2B e-commerce alone will generate $7.3 trillion in transactions in 2004, says GartnerGroup of Stamford, Conn. All those transactions will take place over systems and networks that require comprehensive security.

"In the rush to build e-business strategies, organizations' security efforts have not kept pace," says John Pescatore, an analyst who covers computer security for GartnerGroup.

> *"In the rush to build e-business strategies, organizations' security efforts have not kept pace."*
>
> —JOHN PESCATORE, ANALYST COVERING COMPUTER SECURITY FOR GARTNERGROUP

"Security groups are accustomed to a slow pace of change, because in general, change isn't secure. E-business groups, on the other hand, need to move quickly to respond to the market. These two groups will have to get in alignment, because simply put, there is no e-business without security."

In fact, just as e-business makes computer resources more mission-critical, it also opens them to greater threat. After all,

*Security is not a technology problem; it is a business problem.*

e-business is about giving customers and partners access to your networks and databases—information assets that were once kept under lock and key. However, the more open your network, the greater the chance that someone with malicious intent can break in and wreak havoc on the systems that run your business.

The challenges multiply: Customers want to know that they can count on your systems to keep their personal information protected. Partners need to feel confident that weaknesses in your security infrastructure won't compromise their own systems as supply chains become integrated. Stakeholders look for assurances that security breaches won't impact your ability to grow profits. These days, both the business and the mainstream media are quick to jump all over stories of data security breaches, as the media did with the big denial-of-service attacks in February, 2000. No doubt, a media feeding frenzy over stories like this can contribute to a decline, potentially a sharp one, in the stock price of the company whose security has been breached. Perhaps security isn't a core competency for your business. It isn't for most businesses. But security is certainly fundamental to your ability to compete.

## Securing the Future

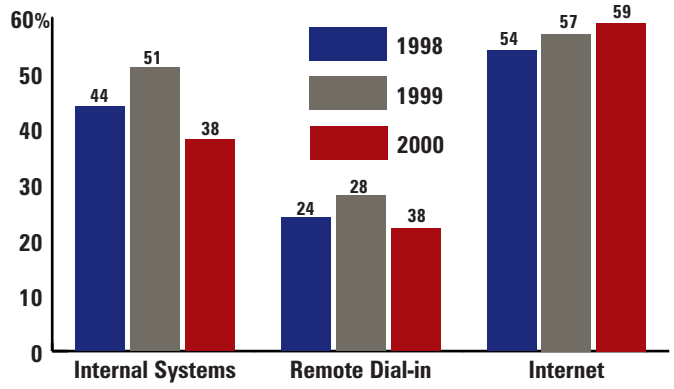
Organizations require a comprehensive, holistic approach to security that addresses the challenges and opportunities of the Internet Economy. This booklet provides a complete view of cyber risks and security management. It is designed to help organizations recognize security needs that relate to their business objectives and to identify the security solutions that will help them achieve their strategic goals.

**Part 1, "Security at Internet Speed,"** assesses the changing security requirements of the Internet Economy, providing an overview of the growing number of security threats and the impact they can have on your business.

**Part 2, "The Trouble with Technology,"** analyzes the traditional tools and techniques for providing Internet security, offering a look at both their strengths and their shortcomings. This section also looks at promising new methods of protecting information assets, including insurance policies that protect against loss resulting from security breaches. As you will learn, system security is a requirement for the smallest to the very largest of companies, and security solutions do vary with the size of the client. What remains constant is the need for system security in all sizes of organizations, from small businesses and emerging technology companies, to the middle-tier companies, to the Global 2000 largest companies in the world.

### The Threat from the Net

*Sources of computer attacks*




Source: 2000 CSI/FBI Survey

*Organizations require a comprehensive, holistic approach to security that addresses the challenges and opportunities of the Internet Economy.*

**Part 3, "Passing the Baton,"** examines emerging trends in security outsourcing, and shows you how to determine when and why outsourcing can be right for your organization.

This booklet is intended for anyone for whom computer security is important—and in the Information Age, that applies to virtually everyone. From knowledge workers sharing information assets to front-line salespeople accessing the network from far-flung locations … from the finance department focused on risk management to the legal eagles guarding against liability … from the IT management and staff charged with protecting your systems and networks to the executive management team providing strategic vision … everyone has a stake in computer security. And no one is absolved from responsibility for it.

Internet security is the number-one concern among IT executives, according to a recent study by the analyst firm International Data Corp. (IDC). But for organizations to implement a workable security plan that will protect their computer resources over the long term, all stakeholders must recognize security's significance and act accordingly. To do any less would be to risk your company's future at the very threshold of the Internet Era.





# SECURITY AT INTERNET SPEED

*As cyber threats proliferate, so do the ways security breaches can derail your organization's long-term success.*

Computer security has been an issue since the days of punch cards and room-sized computers. So apart from the occasional new virus, you wouldn't think there was much new to talk about when it comes to protecting information assets. But the rise of Internet commerce is proving that nothing could be further from the truth.

Consider the current state of affairs:

- The number of computer attacks more than doubled last year, according to reports filed with the Computer Emergency Response Team at Carnegie Mellon University.
- The number of cyber crimes being investigated by the FBI also doubled in the past year. "Even though we have markedly improved our capabilities to fight cyber intrusions, the problem is growing even faster," FBI Director Louis Freeh told a Senate subcommittee in March.
- Fortune 1000 companies lost $45 billion to theft of proprietary information last year, according to a study by the American Society for Industrial Security (ASIS) and PricewaterhouseCoopers.

The same study found that 90 percent of proprietary data exists in digital form.

- Fully 90 percent of large businesses and government agencies detected computer security breaches in the past year, according to the fifth-annual Computer Crime and Security Survey conducted by the Computer Security Institute (CSI). For the 273 respondents who were able to calculate financial loss, the price tag for those breaches totaled $266 million.

Of course, these numbers don't tell the whole story. Experts agree that most security breaches go unreported. And although "estimates of the annual worldwide cost of security breaches range to the billions of dollars, it is very difficult to get an accurate picture [of the problem]," says Chris Christiansen, a security analyst for IDC. "Few companies are willing to report security breaches, for fear of legal reprisals and financial or reputation repercussions. But it's safe to say the numbers are huge."

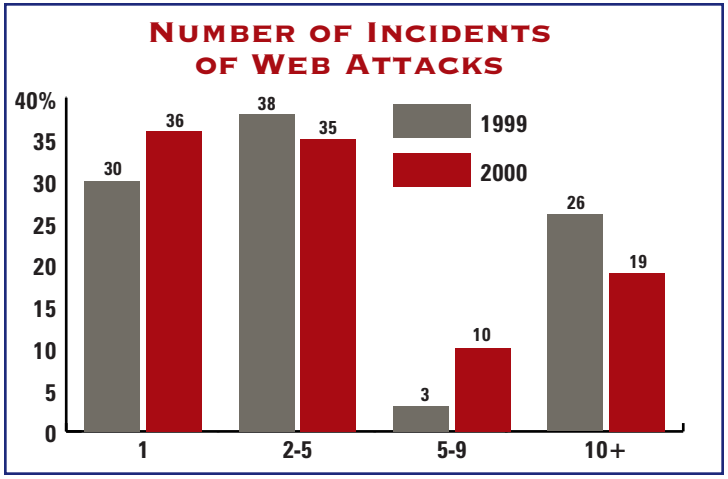
## Friend or Foe?

What's driving the growing security threat, experts say, is the Internet. The Internet presents companies with tremendous opportunities to enter new markets, to integrate disparate operations and to streamline processes. As a result, organizations are pursuing e-business with abandon. B2C e-commerce jumped from $11.2 billion in 1998 to $31.2 billion last year, according to Dataquest/GartnerGroup of San Jose, Calif. And B2B e-commerce is expected to mushroom from $145 billion last year to $7.3 trillion in 2004, composing 7 percent of worldwide sales transactions, says GartnerGroup.

But the same connectedness that makes the Internet valuable also makes it dangerous. "The Internet has had a significant impact on computer security," says Frank Prince, senior e-business infrastructure analyst with Forrester Research of Cambridge, Mass. "As commerce and collaboration take








Source: 2000 CSI/FBI Survey

place over the Internet, there is an opportunity to exploit those interconnections and the greater complexity they introduce."

In fact, in the CSI study, 59 percent of respondents cited their Internet connection as a frequent point of attack—compared with 38 percent who cited their internal systems. And 19 percent suffered unauthorized access to or misuse of their Web sites within the past 12 months. Perhaps even more worrisome, 32 percent said they didn't know if there had been unauthorized access or misuse of their Web sites.

Why is the Internet, the foundation of e-business, so vulnerable to attack? The reason is that the basic rules guiding it, the so-called Internet protocols, were drafted 30 years ago with the goal of creating a global information-sharing and messaging infrastructure. The protocols were not designed to be secure from attack, lest they impede the free flow of information they were designed to facilitate. So while the Internet is indeed the information superhighway it was intended to be, it is not the secure environment that e-business architects have come to demand.

And despite efforts to build products and services to shore up the Internet's inherent security problems, new technologies are being developed so rapidly that all security issues may not be addressed during application development and deployment.

Of course, e-business goes beyond simple Internet connections, affecting how companies go to market, the way they are organized and even what they consider their most important assets. Increasingly, an organization's value lies not in physical assets such as real estate and equipment, but in electronic assets such as customer databases and network infrastructures. This represents a fundamental shift from the bricks-and-mortar economy of just a few years ago and places a new premium on avoiding the potential downsides of a security breach.

"For e-businesses, the network is the business," points out Christopher Klaus, founder and chief technology officer of Internet Security Systems (ISS). "A simple denial-of-service attack, for example, can bring operations to a standstill. And it's easy to calculate the financial downside of that. If you're doing a million dollars of business a day on your Web site, then you know exactly how much a security breach can cost you."

However, these dollar losses do not include intangible but perhaps even more costly losses, the most critical of which may be the loss of consumer confidence and a corresponding loss of brand equity.

## Not Just a Problem for Emerging Businesses

It's no longer only dot-coms for whom the network is the business. Just ask Chris Parsons, senior vice president of strategy and business planning for the $25-billion telecommunications firm BellSouth. "Our telecommunications infrastructure is everything to us," says Parsons. "So a network compromise is simply unacceptable. That means we spend a lot of time on security detection and on taking other steps to protect our business."

Parsons points out that even



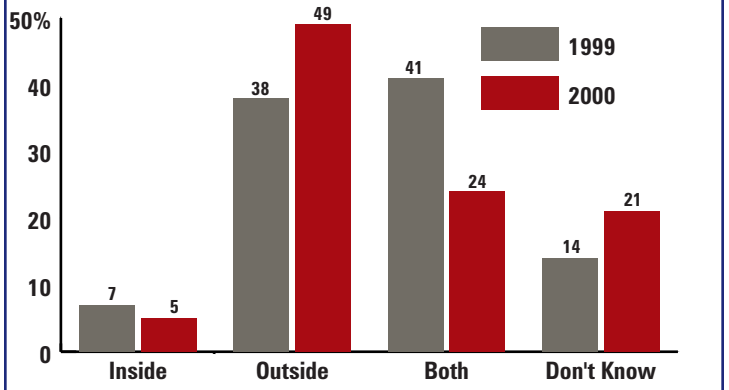


though the network isn't a core competency for most companies the way it is for BellSouth, it's still vital to many firms' operations. And like BellSouth, many traditional enterprises are pursuing e-business initiatives. Whether that means electronically delivering services to customers or integrating supply chains with partners, more data is traveling the network and more transactions are taking place in cyber space. In short, more business is at risk. "When you go online and expose yourself to the world as you do in e-business, the downside of a security breach is huge," says Parsons. "In fact, you may never recover."

Exposures can occur in a variety of places, Parsons notes, from intranets, to online exchanges, to new communications tools such as personal digital assistants (PDAs). Forrester's Prince agrees: "When you extend business processes to the network and depend on people to remotely carry out important operations," he says, "it creates a situation where your security is only as strong as the weakest link."

As a result, organizations need to protect themselves

### Sources of Web Attacks




Source: 2000 CSI/FBI Survey

wherever and whenever their e-business activities open the doors to their networks:

**Intranets and extranets:** Intranets grew as a natural extension of the Internet, allowing organizations to apply Web-based technology to their internal networks. But as much as intranets promote streamlined processes and knowledge sharing, they also expose the enterprise to greater risk. An intruder who breaks through your primary line of defense suddenly has the same convenient access to your rich stores of proprietary data as your employees do.

Extranets extend the intranet to select partners and customers, allowing key stakeholders access to corporate information and even to critical internal infrastructure. This only increases the risk, because you're purposefully allowing external parties access to your mission-critical business networks.

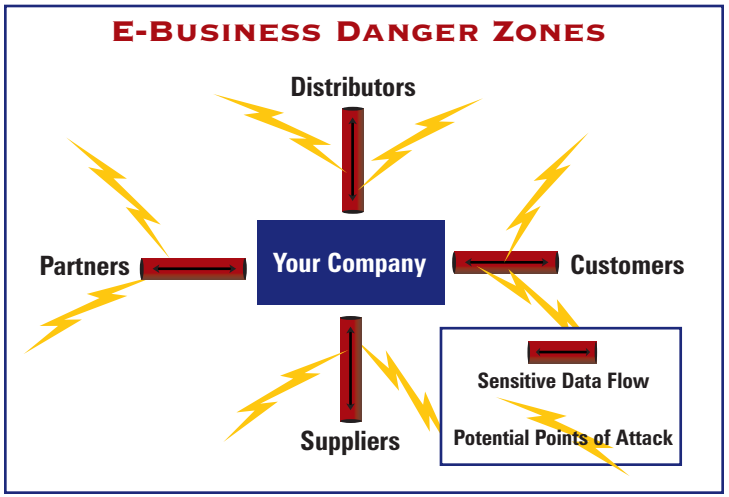
**Supply-chain integration:** After the early rush of B2C e-commerce, it's becoming clear that the real promise of Internet transactions lies in B2B initiatives. From relatively straightforward activities such as online procurement, to electronic collaboration up and down the supply chain, B2B e-commerce promises to streamline processes, to reduce costs and to help organizations pursue new, collaborative business opportunities.

But if there were ever a situation in which security is compromised by a weak link, it's in supply-chain integration. As sensitive data moves from supplier to manufacturer to distributor to retailer, that information is at risk at every stop along the way. Even more crucial, if suppliers are integrated with your back-end systems, you need to be certain that their networks aren't a hacker's back door into your enterprise.

**E-marketplaces:** More business is taking place over e-marketplaces, also called online exchanges. From ChemDex to MetalSite to PlasticsNet, these sites allow firms to buy and sell goods and services, to integrate operations and to reach new markets. Just how prevalent are








**When data flows freely among business partners and customers, sensitive data is susceptible at more points of attack and intrusion than ever before.**

e-marketplaces? "We believe the total number is close to 800 or 900," says Arthur Sculley, co-author of *B2B Exchanges* (ISI Publications). "New exchanges are being added at a rate of five per day, and we expect the [total] number to grow to 3,000 within the next 18 months."

But surprisingly, few of these marketplaces make security a priority, say experts. "We don't see the security processes of these exchanges being considered an important selling point," says Prince. "That's a problem. Marketplaces should be able to ensure best practices when it comes to security. And organizations doing business over these exchanges should be able to ensure an appropriate level of security as well."

**Online sales/procurement:** For many organizations, online sales are where the e-business rubber meets the road. But few realize that online transactions are rife with potential security problems. Simple breaches can range from defaced Web sites to fraudulently lowered prices when orders are submitted. More serious attacks can crip-

ple an e-business Web server—and the more revenue you're pulling in on the site, the more you stand to lose if your e-tail store is temporarily out of business.

Far more insidious is theft of customer information such as credit-card data. "Our research shows that rates of credit-card fraud are 11 times higher for e-tailers than for their bricks-and-mortar counterparts," says GartnerGroup's Pescatore. Statistics like that will do little to build consumer confidence in online sales.

"Web servers tend to offer an abysmal level of security," Pescatore explains. "Plus, Webmasters tend to operate at a much faster speed than security people, so often the security doesn't keep up with changes on the site." As a result, he says, "two out of three Web servers are hackable."

**Globalization:** One aspect of e-business security that may be overlooked is the global nature of the Net. As the Internet enables organizations to push into remote corners of the world, the security threats multiply. "Globalization is increasingly an issue for every organization," says BellSouth's Parsons. "And it introduces a number of new factors in terms of threats."

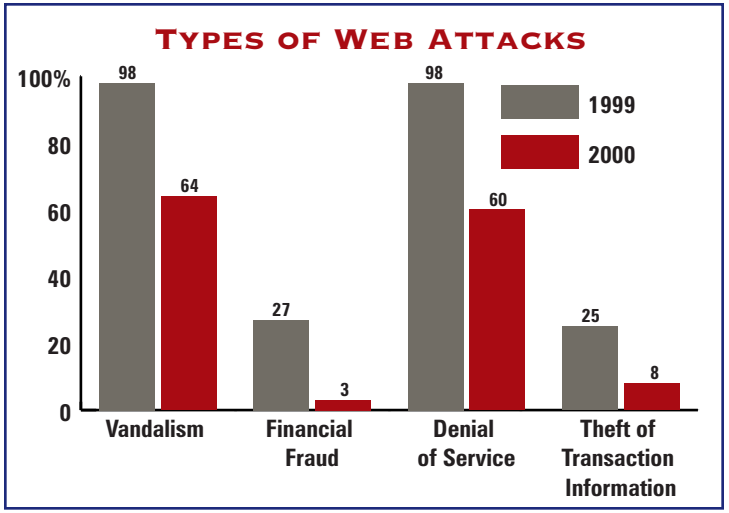
For starters, a more broadly distributed network means more potential points of attack. And the better integrated your organization, the more trouble that can spell. "It doesn't matter where someone breaks into the network," Parsons points out. "Once they do, they have access to the entire organization."

Likewise, security capabilities may not be at the same levels in all regions. "Global organizations do better with security in geographies where they have a strong concentration of security professionals," notes Parsons. "In certain parts of the world, you might not be as prepared as you would hope to be, even though the threats are just as significant."

**New threats:** Another often-overlooked threat is ubiquitous technologies such as e-mail. Not only is e-mail a common way to spread computer viruses, but it's also a place








Source: 2000 CSI/FBI Survey

proprietary data frequently leaks out of the organization. "It's too easy for employees to leak sensitive information to the outside world, either knowingly or inadvertently," says IDC's Christiansen. "Many people don't realize it's a violation of most security policies [if they even have one]—and also potentially illegal—to post company financial information in a chat room, for example."

And what about new technology tools, so-called digital appliances such as PDAs and other cellular devices? These are a security manager's worst nightmare, allowing sensitive corporate data to escape the network with little or no control. Likewise, Internet-enabled cell phones are a growing risk. In early June, the first virus targeted at cell phones hit customers of Spain's Telefonica. As more front-line employees take advantage of these tools, the security risks will only increase.

### WHAT DO YOU HAVE TO LOSE?

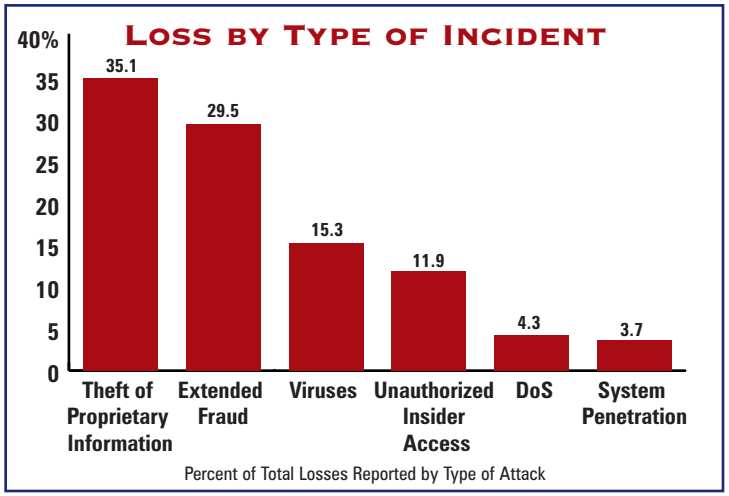
The broad spectrum of potential attacks, combined with new vulnerabilities introduced by

e-business, means that security is a bigger problem now than ever. But what is the net result when security is violated? What are the short- and long-term business impacts?

The primary concern is financial loss. Compromises to your computer infrastructure can mean lost revenue when transactional systems crash, lost productivity when operational systems or networks go down, high costs to locate and resolve security problems, costs for unbudgeted security enhancements—in general, major interruptions of your business processes.

"Security breaches carry with them a broad range of financial impacts," says Richard Macchia, chief financial officer of ISS. "CFOs can no longer say that this is the responsibility of the CIO. Security is a business issue, and financial people have to consider themselves accountable and be aware of the risks."

In fact, in the ASIS study, the average company reported 2.45 incidents in 1999, with estimated losses per incident of $500,000. That's not pocket change. But security breaches can have many other unexpected financial and less-tangible business impacts:




Source: Derived from 2000 CSI/FBI Survey





**Proprietary data:** In the Information Age, intellectual capital is among a company's chief assets. Losing proprietary information—anything from CAD drawings to sales data to details on future strategies—can be devastating. Once this information is in the hands of competitors, it becomes their competitive advantage, and even legal remedies won't necessarily shift the balance back in your favor. In fact, according to the CSI study, "the most serious financial losses [occur] through theft of proprietary information."

Interestingly, it's not competitors themselves who most commonly pilfer proprietary data, say experts. "Most theft of proprietary information is from insiders," says GartnerGroup's Pescatore.

**Legal liabilities:** Security breaches open a Pandora's box of legal repercussions, exposing organizations to legal action by partners concerned with contractual obligations, shareholders concerned with changes in stock valuations and consumers concerned with privacy issues.

"Security is an increasingly important legal issue, particularly as it relates to privacy," says Lisa Norton, an associate with King & Spalding of Washington, D.C., which is among the top 50 law firms in the world. "Consumers are concerned about privacy, and we may see class-action and shareholder lawsuits over privacy in the near future."

In particular, others may try to hold organizations liable if the organizations' security measures don't conform to best practices, suggests Norton. Forrester's Prince sees the same trend, adding that even if firms are only indirectly involved in a security breach, they could still be held legally responsible. "If your server is hijacked and used in a denial-of-service attack against someone else, you may be liable," he says.

**Shareholder equity:** Security breaches can have a direct impact on a company's stock valuation, particularly for volatile dot-coms—as witnessed by price fluctuations for several firms following February's denial-of-service attacks. Increasingly, sharehold-

ers will react strongly to threats against information assets. And no wonder: 50 to 70 percent of a company's value is derived from its proprietary data and trade secrets, according to the ASIS study.

As a result, hackers are mounting attacks for the specific purpose of manipulating stock prices, says Pescatore. Early this year, for example, a hacker broke into the Web site of Aastrom Biosciences of Ann Arbor, Mich., and posted a bogus press release announcing the company's merger with biopharmaceutical firm Geron Corp. of Menlo Park, Calif. Before the firms discovered the prank and notified the Nasdaq index where they are traded, Aastrom shares had climbed 10 percent, while Geron shares had risen 8 percent.

Will shareholders respond to such breaches with lawsuits? "We haven't seen much of that happening yet," says Norton. "But if the courts start awarding for something like this, there could be a lot of suits."

**Partner relationships:** As Internet technologies enable partners to integrate supply chains and to conduct business electronically, security will become a key part of the business relationship. If a security lapse on your part allows a hacker access to your partners' systems, you could be held accountable. And even if your partners aren't affected, vulnerabilities in your systems may make them hesitate to do business with you. Many organizations partner in one area but compete in another. Thus, relationships may not be as stable as they once were.

Minimum security levels will increasingly be a price of entry into partner relationships, say experts, particularly in electronic environments such as online exchanges. That also applies to merger-and-acquisition activity, which continues at a brisk pace. "M&A activity around the world is continuing to increase at a rapid pace," notes Patrick Schul, director of sales for New York-based Marsh Inc., a provider of risk solutions and services. "And it's becoming increasingly common for companies to incorporate the potential risks associated with





Internet security into the due diligence process."

**Customer confidence:** Partners and shareholders aren't the only ones concerned with security; customers will increasingly evaluate firms on the basis of how confident consumers feel doing business with them. As privacy becomes a larger issue and rates of online fraud rise, consumers will refuse to buy from firms that can't guarantee security. And remember, in the online world, your competitors are just a click away. "One of the results of disintermediation is that the cost and difficulty of switching drops dramatically," says Pescatore. "So if a customer loses confidence in you because of a security breach, it's quite easy for them to switch to someone else."

How bad has it gotten? The world awoke the morning of February 7, 2000, to hear breaking news of what would be the first of a week's worth of denial-of-service attacks on some of the most venerable names in the e-business world. First it was Yahoo's site that was hit with massive, hacker-induced outages. That was followed by assaults on the sites of Buy.com and eBay, then Amazon.com and even CNN.com. Then on the last day of that month, the FBI's Web site was the victim of a denial-of-service attack that lasted several hours.

Such high-profile attacks got everyone thinking that if such major sites could be struck, then virtually any size e-business could be successfully targeted, given that the mega-sites typically invest most heavily in Internet security. For dot-coms struggling to grab market share quickly, the repercussions of a security breach can be severe indeed. The combination of crashed systems, lost revenue, lower stock prices, angry stakeholders, loss of access to trading partners, lost customers and negative publicity can damage a fragile e-business brand beyond redemption.

## STRIKING A BALANCE

In the final analysis, e-business security is about balancing the need to open the network to customers and partners with

the need to protect the information assets that are the lifeblood of the organization. "The marketing people see complete access as a requirement, while the security people see it as the worst possible scenario," says BellSouth's Parsons. "There has to be a meeting of these two minds. So it's a people issue as much as a technology issue." Fortunately, minds are beginning to change. "E-business is transforming the way organizations view security," says Klaus of ISS. "They understand now that security isn't a technology, but a process. It's an entire methodology that has a full life cycle."

In the e-business realm, what does that life cycle entail? "The three things e-business requires are availability, data integrity and privacy," says Pescatore. "Web sites must be available, data must be available, and systems must be available. You must have data integrity and the ability to ensure that transaction information has not been altered. Most important, you need to be able to guarantee privacy, to keep customer data away from intruders."

Security strategies themselves will be different for different sized companies. Specifically, each size segment will require a different mix of security services, with some developed, deployed and maintained by in-house staff and others provided by outside vendors or outsourcers of managed services. The common theme across all companies is the absolute, mission-critical imperative of securing the e-business, regardless of how big or small the company may be.

Availability, integrity and privacy are what solid security protects. The vulnerabilities are many, the threats abound and the stakes are high. But awareness of the issues, the right technology tools or services, and a comprehensive security strategy can enable organizations of any size to conduct business at Internet speed.





# The Trouble with Technology

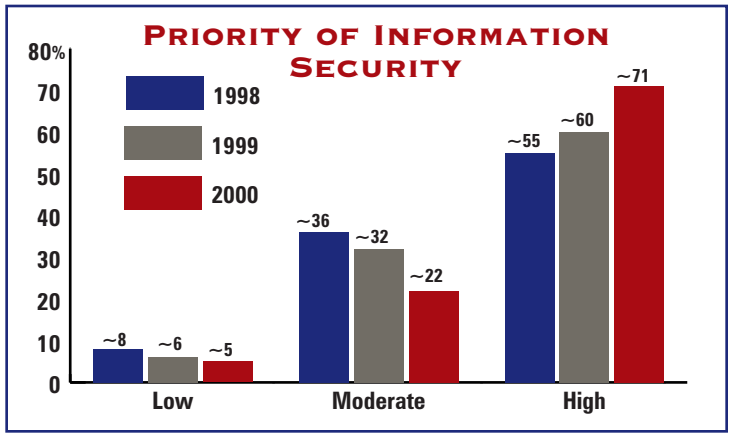
*Most companies deal with security by throwing technology at it. While technology tools are absolutely necessary for keeping information assets safe, they're only part of a complete security solution.*

Deb Rich knows how important technology tools are in protecting an organization's computer infrastructure. As a senior network engineer who manages security for the University of Colorado Hospital, she uses a range of security solutions to protect highly sensitive patient data as it traverses a large, complex network.

But Rich also knows technology's limitations. That's why the hospital has developed a security policy that not only dictates what hardware and software components will keep intruders at bay, but also describes how security supports the organization's core business.

"Security is very important to us from a patient-privacy perspective," says Rich, "even more important than for other organizations. We also have increasing pressure in the form of government regulations. So we are constantly evaluating our security situation to anticipate potential problems and to prepare for new demands. That requires more than just technology; it requires a security strategy."

"Security needs to be governed by an overall policy, and that policy needs to be holistically aligned with business strategy," agrees ISS' Christopher Klaus. "You can't practice security for security's sake. Instead, you need to identify the business objectives you want to accomplish, and then




Source: *InformationWeek* Global Information Security Survey of 4,900 security professionals

wrap your security policy around that."

The trouble is, few organizations heed that sound advice. A recent *InformationWeek* survey of 4,900 executives, security professionals and technology managers reveals that 71 percent of organizations rank security as a high priority, up from 60 percent last year. But only 38 percent say security policies are well aligned with business goals, and 17 percent say security and business goals don't mesh at all. Small and mid-sized organizations, in particular, often feel that they don't have the resources to invest in developing and enforcing a comprehensive security policy.

"Just throwing technology at a security problem isn't the solution," says Frank Prince, of Forrester Research. "You need to determine what you want to protect and how important it is to protect it. Only then can you decide which security solutions are most appropriate to achieving your goals."

## Addressing Business Needs

The fact is, security isn't a technology problem, but a business problem. Approached this way, security takes on an entirely different aspect. It's no longer a method of mitigating





disaster but a means of achieving business success. "Organizations must move beyond looking at security as a way to deal with fear and look at it as a business enabler and a growth mechanism," says IDC's Chris Christiansen. An appropriate security policy can enable you to "reach a larger number of customers and business partners with a higher level of trust. That's a lot more meaningful than talking about how many hours of downtime you can avoid."

Approaching security as a business issue means creating a policy that specifies how security will support your business, establishing the value of your information resources, identifying their level of vulnerability and determining how you will respond if those resources are compromised:

**Creating a security policy:** Effective security starts with the development of an overarching policy. A good policy unifies all aspects of your security measures into a single strategy. It deals with broad issues such as the value of information assets, and it addresses specific questions such as who has access to what. It embodies the work you do to analyze risk and to develop a response plan, and it specifies which technology tools are applied to which resources.

However, few organizations take the time or have the internal human technical resources to develop such a policy. In fact, only about 30 percent of companies that consider security a high priority have a written security policy that outlines objectives, according to the *InformationWeek* study. It's safe to assume the number is lower for organizations that don't consider security a high priority.

That could spell disaster. "Security tends to deal with what we know," points out BellSouth's Chris Parsons. "We address known threats to make sure they don't happen again. But when threats appear for the first time, they can go undetected. That's why it's necessary to have a policy in place, to have your infrastructure ready, to have your people ready and to have partners who

can help you respond quickly."

Small and mid-sized organizations may believe they don't require a security policy, or they may feel that they lack the wherewithal to design one—after all, many firms don't even have dedicated security personnel. But experts emphasize that a policy is still essential, even if it's rudimentary. Even a very big-picture approach to describing your information assets, the threats they face, the tools and techniques you will use to protect them, and how those mechanisms will be enforced will go a long way toward keeping your security on track.

As important as developing a policy is how you develop it. "Most policies approach security with a mandate of 'Keep us safe,'" says Forrester's Prince. "But security threats can't be judged in the light of a broad mandate. You need to first identify your needs and then figure out how to meet them. So instead of saying, 'We need to apply this patch to the accounting system,' you should start with your need, such as 'We need to close the books at the end of the month.'"

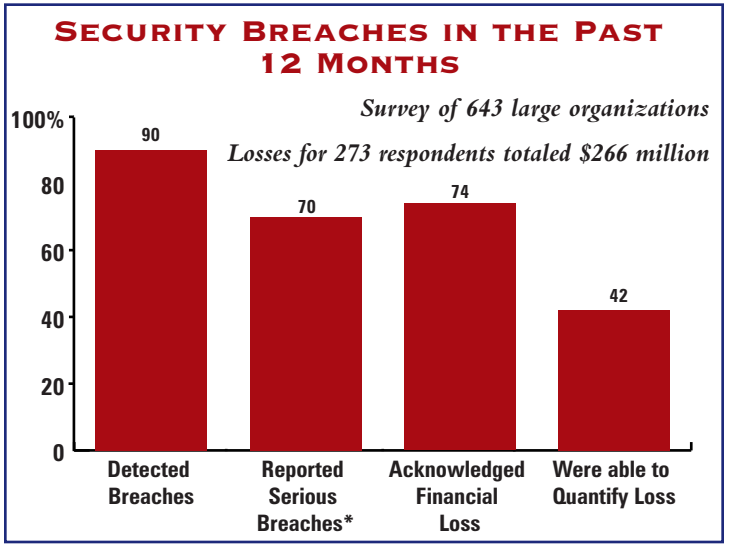
Ideally, a security policy should also deal with specifics. How do employees authenticate themselves? How often must they change passwords? How do you authorize access? How do you determine authorization levels, and how do you change them once they're established? What are your rules for e-mail usage, Web access, instant messaging, MP3, online gaming and streaming video? The Internet introduces a host of such issues, and all have an impact on your security policy.

Finally, your security policy must address people issues. All employees must view security as their responsibility, and safe practices must become second nature. That involves education, from regular reminders that help employees avoid viruses to workshops that help key personnel align security measures with business requirements. But ultimately it involves a culture that recognizes the value of its information assets and is committed to protecting them.

"If you do it right, creating a security policy is difficult








Source: 2000 CSI/FBI Survey

* Serious breaches include theft of proprietary information, financial fraud, system penetration, etc.

and painful," says IDC's Christiansen. "At its heart is a change in behavior. And before you can achieve that, you have to gain consensus. You have to meet with lots of people and convince them to agree to a new set of behaviors. If people don't buy into the policy, they'll use all kinds of ingenuity to get around it."

**Classifying your resources:** If you're applying the same level of security to all systems, then you certainly aren't spending your security dollars wisely, and you're probably leaving key systems open to attack. Classification involves looking at your computer resources and determining how important security issues such as availability, integrity and privacy are for each of them. If a particular system is critical to your success, then you must invest accordingly in the security measures that will protect it.

That seems reasonable enough, but a relatively small percentage of organizations

## Know Thine Enemy

What are the predominant security risks in the Internet Economy? "The threats are largely the same ones that have always been there," says Frank Prince, of Forrester Research. "It's just that e-business has lowered the [access] threshold." Here are some of the most common security risks:

**Denial-of-Service (DoS) attacks:** In a DoS attack, a hacker gains access to several computers connected to the Internet and installs code on those systems. At the hacker's signal, the systems start sending data to targeted Web sites. The sudden burst of network traffic overloads the Web servers and the networks they're connected to, slowing performance and eventually crashing the site. In February, DoS attacks knocked out service for five of the 10 most popular Web sites, including Amazon, Yahoo and eBay. Financial repercussions rang in at $1.2 billion in lost revenue and subsequent losses in market capitalization, according to Yankee Group of Boston.

**Hackers:** A hacker is anyone who gains unauthorized access to computer resources for the purpose of stealing information or sabotaging systems. The Internet only makes a hacker's task easier, which means that the number of hackers will grow. Hackers may be employees stealing proprietary information to sell to competitors, pranksters defacing your Web site, or criminals capturing credit-card data or illegally transferring funds. "There will be an increase in online criminal activity," says IDC's Chris Christiansen. "Money is no longer in banks, but in bits. And it's easy to steal bits and quickly move them around the world."

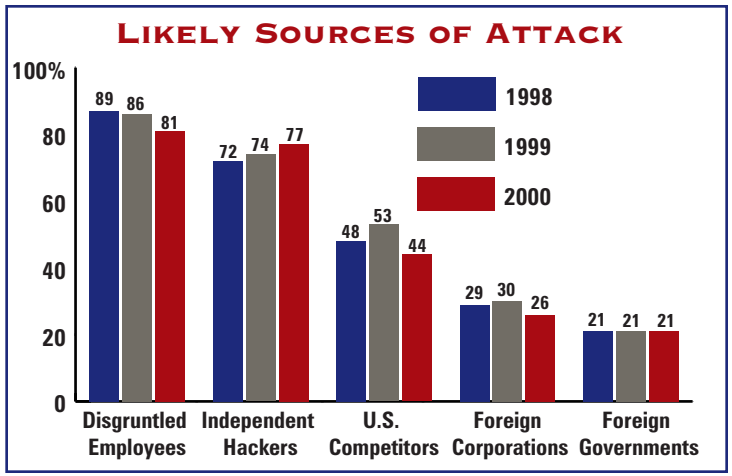
**Insiders:** Between 70 and 90 percent of attacks come from inside the organization, reports Hurwitz Group of Framingham, Mass. And although an annual study by San Francisco-based Computer Security Institute indicates that the rate of insider attacks is falling—only 38 percent of respondents cited internal systems as a "frequent" point of attack last year—experts point out that internal breaches can be the most pernicious. "The majority of high-value breaches—those costing $250,000 or more—are perpetrated from the inside," says Forrester's Prince. "That's because insiders often know how to access the most valuable data."

**Physical break-ins:** One often-overlooked threat is physical security breaches—when intruders actually gain access to a data center or steal equipment. Data-center security goes beyond a simple lock and key, informing the overall way the facility is designed and operated. Are personnel monitored as they come and go from the data center? Are power switches that turn on and off mission-critical servers within easy reach? Can a simple tug on a power cord or cable knock out your network? Likewise, stolen laptops and PDAs are a common and costly problem, not only because they're expensive to replace but also because of the proprietary information that may be stored on them.

**Viruses:** The most common form of security breach, a virus is a program or piece of code that is loaded onto an organization's computers without the organization's knowledge and runs against its wishes. Viruses attach themselves to programs or files on your system; when a program runs, so does the virus. Most can self-replicate, quickly using all available computer memory, and many can transmit themselves across networks. Just how destructive are viruses? The May, 2000, "I Love You" virus cost businesses an astonishing $6.7 billion in lost productivity and repairs, says research firm Computer Economics of Carlsbad, Calif.

actually evaluate their systems this way. In fact, only 33 percent of companies have classified what information is most valuable, according to the *InformationWeek* study. Likewise, "consistent mechanisms and processes for determining the value of proprietary information are not in place at most Fortune 1000 companies," confirms a recent report by the American Society for Industrial Security (ASIS) and PricewaterhouseCoopers. The same situation is likely to be found in smaller companies as well.

**Analyzing your risk:** Another prerequisite for effective security is having a sense of your vulnerabilities. That's where risk analysis comes in. By using an established methodology for assessing your systems, data and networks, you can determine which computer resources are most at risk and




Source: 2000 CSI/FBI Survey

which technology tools and practices will best protect them.

Many organizations turn to outside firms for risk analysis. Experts agree that organizations hire security consultants for security audits for the same reason they use outside accounting firms for financial audits: they need an independent, impartial third party. Common issues such consultants and specialists look for include misconfigured systems, poorly designed e-business infrastructures, and back doors into networks through partner connections. Internal IT staff might lack the expertise to locate such trouble spots, and they may also lack the objectivity to find flaws in systems they designed.

**Developing a response plan:** What happens if a breach takes place? The wee hours of the morning following an attack are no time to be deciding how to respond. Incident preparedness starts with identifying who should respond to an incident and what their roles should be. It often makes sense to designate a single person as the response coordinator. Then develop a team of representatives from all appropriate departments, including IT, legal, human resources and public relations. Educate team members thoroughly and conduct regular fire drills.

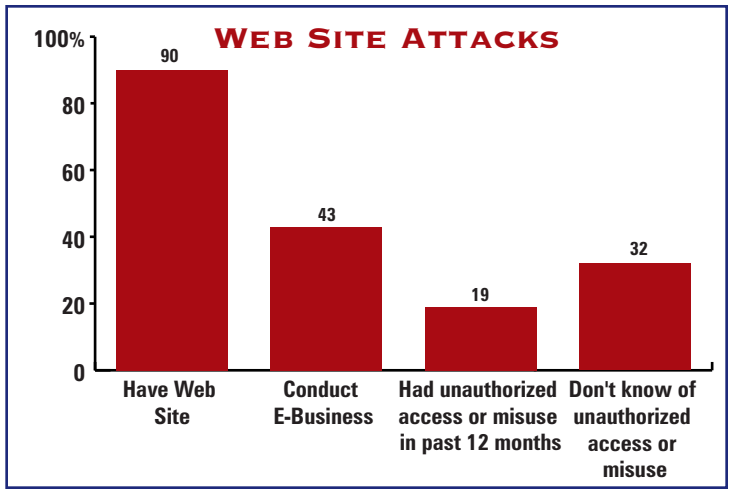
Also establish procedures for determining the seriousness of the breach and what actions team members should take given the severity of the breach-in. The IT department will likely take steps to contain the breach, while the legal department might initiate actions to identify the perpetrator. If the breach affects employees, HR might inform them of what actions they should take. If customers are affected, the PR department might take steps to manage public perception.

## From Security to Risk Management

You've created a security policy, classified systems, assessed risk and developed a response plan. Have you achieved 100 percent security? In short, no. Experts agree that despite the best efforts, organizations will always be vulnerable to the latest virus, the cleverest hacker or the most insidious insider break-in. In fact, even the largest organizations with the deepest IT pockets eventually reach a point of diminishing returns on their security investments.

At this point, security enters the realm of risk management. Traditionally, risk management was concerned with protecting physical assets such as equipment, inventory and physical plant. But in the Internet Economy, the assets and processes that are critical to business success reside in databases and traverse the network. So increasingly, say experts, organizations will consider insurance policies to manage the gap between the real and the ideal in computer security.

"Even with the best controls and mitigation strategies, there is still risk. And this is a business risk," says Emily Q. Freeman, senior vice president and national practice leader, e-business risk solutions at Marsh Inc. of New York, a provider of risk solutions and services. "Without the ability to contractually transfer that risk to someone else, those losses




Source: 2000 CSI/FBI Survey

come out of your balance sheet. Insurance is a way for you to manage that risk. It transfers the risk to an insurance company in exchange for a premium."

As recent history has shown, there is no computer system that is 100 percent secure. And to some extent, the more complex distributed, networked systems become, the more vulnerable they are. Thus, experts see insurance as a logical component of a complete security program.

"Security is one area in which organizations cannot afford to operate in the dark," says former U.S. Senator Sam Nunn, who has been instrumental in raising awareness of security issues within the federal government. "How vulnerable are your information networks? Could a computer-based attack cripple them and erode consumer confidence in your company? Organizations need a uniform policy for protecting their networks, responding to incidents and assessing the risk of such computer attacks."

In fact, new offerings from several leading insurers are specifically targeted at protecting information and reputation assets against security breaches. This is an important development, because "traditional insurance protects physical assets against things like earthquakes and hurricanes," says Marsh's Freeman. "It doesn't deal well with information."

Security insurance covers things such as security breaches, computer theft, errors or omissions that cause financial damage to others, and "content injury"—things like infringement of copyrights and privacy violations. A good policy will protect against cyber attacks, viruses and programmer errors, and against lost income and extra expenses associated with the disruption of electronic activities.

Insurance can also help justify the cost of security in business terms. "It can be hard to justify a budget for security without being able to quantify the risk," says Matthew Kovar, an analyst with Boston-based Yankee Group. "An insurance policy creates balance between what you are protecting and what you're spending to protect it."

In any case, there's no question that computer security and overall risk management are becoming intertwined. "Information security is central to risk management in the Internet Economy," concludes Freeman. "You can't do risk management in the Internet Economy without doing information security. It's not the entire risk management program, but it's an essential component."

## Enabling E-Business

At the University of Colorado Hospital, Deb Rich has watched computer security become crucial to the organization's business. "Fifteen years ago there was no security," she says. "But you can't operate like that anymore." As more patient information is captured, stored and communicated electronically, as more hospital operations rely on electronic processes, security becomes either an obstacle or an enabler. "If you're going to have data flying around the network," says Rich, "then you have to protect it. It's that simple."

Protecting data goes beyond hardware and software, beyond tools and techniques, beyond even policies and procedures. Security is a business imperative. It allows you to collect the information that builds customer relationships, to share the information that enables collaborative partnerships, and to take advantage of the information that makes you more competitive. It means that customers can trust you with their personal data, that partners can trust you won't expose their trade secrets to competitors, and that shareholders can trust you are taking the steps necessary to ensure your long-term success.

In short, security enables e-business. "Any time you can avoid turning bits into atoms and back into bits again, you realize enormous advantages," says Tom Noonan, CEO of Internet Security Systems. "Any time you can reduce latency or eliminate intermediary steps, you decrease costs, you improve customer satisfaction, and you have the opportunity to increase revenue. That's the promise of secure systems."





# PASSING THE BATON

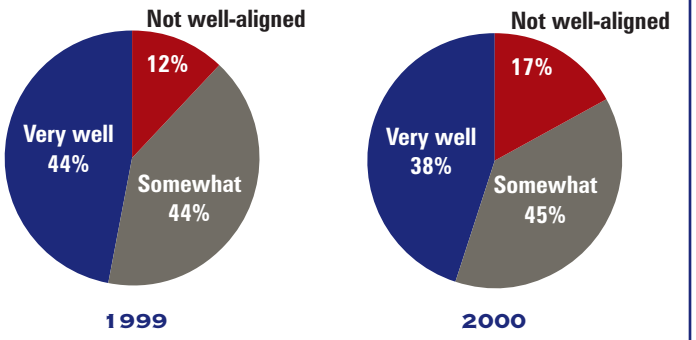
*For most organizations, security isn't a core competency. But it is mission-critical. That means a growing number of firms will turn to outsourcing to meet some or most of their security needs.*

As the upsurge in e-business activity makes protecting networks crucial, as the growing concern over consumer privacy makes guarding databases essential, as the increasing reliance on information assets makes securing the IT infrastructure an imperative, organizations large and small are struggling to develop and to deploy optimal security solutions. They assess their security needs. They invest in security measures. They develop broad-based security policies. They buy an extra measure of protection through security insurance.

Still the risks multiply—and with them, the challenges of securing the business. Many of these challenges are a product of the Internet Economy. The open nature of e-business networks means that more people have access to your systems, and that protecting them is far more difficult than it was in the past. The unprecedented pace of e-business opportunities means organizations often have little time to take security concerns into consideration. And rapid development of e-business technology means the IT infrastructure is growing ever more complex.

Then there's the continuing shortage of tech talent. There are nearly 60,000 more IT jobs in the United States than

## ARE SECURITY POLICIES ALIGNED WITH BUSINESS GOALS?




Source: *InformationWeek*

there are qualified candidates, and turnover rates are soaring past 20 percent, reports Philadelphia-based Hay Group, an HR consultancy. In fact, the Department of Commerce says the country will require 1.3 million new highly skilled IT workers in the years leading up to 2006. It's no wonder more than 60 percent of CIOs list IT staffing among their top three day-to-day issues, according to Forrester Research.

In *Computerworld*'s 14th Annual Salary Survey, released in September 2000, security managers and administrators netted the largest salary increases, a trend likely to continue. The same survey found that entry-level salaries for security specialists are among the highest in IT, with entry-level security staff being hired at an average annual salary of $44,439, higher even than the salary of entry-level network administrators.

Meanwhile, earlier in 2000, the UK firm Xephon PLC found that 43 out of 90 companies it surveyed decided to outsource security needs because they either didn't have the right skills in-house or they wanted internal staff to work on more strategic projects.

The shortage of information security professionals is acute. "The sheer volume of potential vulnerabilities and threats, combined with the complexity of security technology, means that it is virtually impossible for an organization to find staff with the knowledge and capabilities to respond effectively," says Yankee Group's Matthew Kovar.

### THE EXTERNAL ANSWER

Organizations are looking for a solution. They need a cost-efficient, effective way to maintain high levels of security while focusing on their e-business initiatives and on their core competencies. Increasingly, say experts, that solution will be security outsourcing.

"Outsourcing will become a necessity," predicts IDC's Chris Christiansen. "The complexity of environments, the increasing demands on the network, and the scarcity of trained security professionals will mean that organizations will have to look to outsourcing. The fact is that security is not a core competency for most organizations."

Even organizations for whom security is a key part of the business are partnering with external providers. At the $25-billion telecommunications firm BellSouth, for example, the network is, literally, the business. And that means BellSouth requires the highest levels of network security. "We consider security a core competency," says BellSouth's Chris Parsons. "But we still partner with security providers to be sure we have the best skills and solutions."

BellSouth is in good company. Investment in network security services in general will grow from $512 million in 1998 to $2.24 billion in 2003, IDC anticipates, a compound annual rate of about 34 percent. And the move to security outsourcing in particular is part of an overall trend toward offloading crucial but non-core IT functions. In fact, companies worldwide will invest in IT outsourcing to the tune of $123 billion by 2002, predicts Dataquest/GartnerGroup of San Jose, Calif.

"Security outsourcing holds a lot of promise," agrees Forrester's Frank Prince. "It allows organizations to retain the responsibility of managing security without actually doing it themselves. A lot of day-to-day security activities are difficult and expensive because of the technical knowledge required, the rapid pace of changing threats and the difficulty in hiring knowledgeable staff. These things can be offloaded to a company that can handle them. For the vast majority of companies, [security] doesn't need to be done in-house."

## Prime Opportunity

That's exactly what Robert Enslein discovered. As CEO of New York-based Prime Office Centers, Enslein knows real estate, not security. But he also knows that a secure network is crucial to his business.

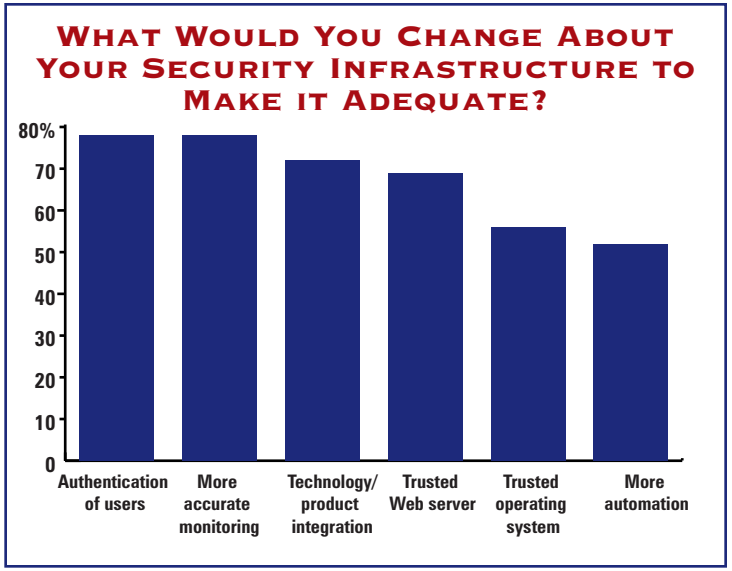
Prime Office Centers operates 250 office suites at three locations in lower and midtown Manhattan. The offices come fully furnished and offer a complete complement of business services, including a preinstalled telephone and network infrastructure. Clients can literally sign a lease today and move in tomorrow. "Companies know that the innermost circle of hell is to negotiate a lease with a New York landlord," jokes Enslein. "So if they want to move into their space tomorrow and have a phone on the desk and a complete infrastructure already in place, they turn to us."

The organizations that lease space from Prime Office Centers range from consultants and insurance brokers to major firms such as Gateway and Intel. These companies come to Prime Office Centers for the prestigious address and for the range of services—including a secure T1 Internet connection. "That is a competitive advantage, something I believe attracts people to do business with us," says Enslein. "Anyone can offer raw bandwidth. What we're offering is a truly secure network."

But Prime Office Centers doesn't rely on internal resources to protect that network. Instead, it outsources administration of its security








Source: *NetworkWorld*

needs to an external provider. "We can manage most of our IT needs in-house," Enslein explains. "But we don't have the expertise to handle security. It requires a high level of knowledge and skill that probably isn't in our best interest to invest in."

Outsourcing enables Prime Office Centers to focus on its core business. It also gives Enslein a level of confidence that a key competitive advantage—the secure network it offers its clients—is being properly managed. "If someone were to hack into our network and disrupt the activities of our clients, that would be extremely detrimental to our business," says Enslein. "So we wouldn't outsource our security unless we felt 100 percent confident it was the right business decision."

A year into the contract, Enslein is convinced now more than ever that he made the right choice. "Outsourcing

offers a lot of benefits, there's no question about that," he says. "We wouldn't have been able to achieve this level of security if we had tried to do it ourselves."

## Business Benefits

What are the primary advantages of security outsourcing? "The benefits are largely the same as for any outsourcing situation," says Forrester's Prince. "You outsource to gain better quality of service and more predictable costs. Over time, organizations that use best-of-breed service providers for their non-core operations will outperform those that do it themselves."

That quality of service is probably the key advantage to organizations using outsourcers. Security outsourcers have implemented best practices and developed proven methodologies that they can apply to your organization. They have access to state-of-the-art solutions and the expertise to deploy them most effectively. They can offer sophisticated strategies, comprehensive disaster recovery plans, and arcane but important advantages such as forensics services to help you track down cyber criminals.

Outsourcing can also yield less-tangible benefits such as avoiding political conflicts. "Security can be a constant source of battles, and security decisions are often unpopular among users," says Prince. "The outsourcer can be the one to recommend an unpopular course of action, or to give objective support to the decisions of internal technical or security staff." Because the directives are coming from an outside expert, employees and other stakeholders may be more likely to conform to them.

Another important benefit of outsourcing is that security services providers can attract and retain the best tech talent, and can invest in the training and development that the vast majority of firms simply can't cost-justify. In today's tight job market, security professionals can easily command six-figure salaries. Few organizations can afford to keep a staff of such experts monitoring the network around the clock. As the





table on page 41 shows, the costs of in-house security provisioning are indeed steep.

With outsourcing, costs will certainly become more predictable: You get a specific level of service for a pre-established fee. You can also shift security costs from your capital budget to your operational budget. Finally, there's no need for you to invest directly in security enhancements—that becomes your outsourcer's problem.

"If you look at outsourcing purely in terms of cost, it will probably seem expensive," says Enslein of Prime Office Centers. "But if you look at it in terms of time saved or the ability to focus on your core business, the value more than makes up for the cost."

## Knowing When to Look Outside

You can outsource a broad range of security measures. Candidates include virus protection (think "inoculation"), intrusion detection (think "burglar alarm") and vulnerability assessment (think "internal audit"). Outsourcing can take the form of onsite security management, remote network monitoring or "proxy-based solutions" such as routing e-mail traffic through the outsourcer's systems for real-time evaluation.

Prince suggests that organizations consider some or all of the following security categories for outsourcing:

1. **Authentication and authorization:** While functions like password administration are often handled by human resources or by individual departments, the underlying infrastructure can be successfully outsourced.
2. **Security operations:** Day-to-day management of tools such as firewalls and intrusion detection systems are ideal for either onsite or remote outsourcing.
3. **Incident management:** Outsourcers are often better prepared than internal security staff to respond to emergencies and to get your network back up and running.

IDC's Christiansen recommends that companies outsource functions that require

constant vigilance, such as virus protection and intrusion detection. "Your security is only as good as its last update," he notes, since new viruses are always being developed. And new technology always introduces potential new vulnerabilities. "By paying someone else to manage that, you have some degree of assurance that updates are current. You also have legal recourse should a breach occur, and you may find it easier to obtain security insurance."

What should you look for in a security outsourcer? Most important are reputation and experience. "Look for an outsourcer with a strong track record," says Prince. "Get references, and look into them. There's no substitute for references." Beyond that, be sure the outsourcer can demonstrate that it understands your security and business requirements, can provide the level of protection you require, and has the resources in place to scale as your needs grow.

Outsourcing also places a premium on ensuring that you have a solid security policy that specifies who is responsible for what. As in any outsourcing relationship, make sure both you and your provider agree on service levels and response times—before an incident occurs. And even if you're outsourcing large portions of your security, it's wise to retain or assign internal staff to oversee the relationship and to ensure that the outsourcer delivers the appropriate level of service.

Most important, perhaps, is to approach outsourcing knowing what you hope to achieve by offloading management of your security. Organizations that perform due diligence are more likely to succeed in their outsourcing initiatives, according to a recent study by IDC and Technology & Business Integrators of Woodcliff Lake, N.J. In fact, only 13 percent of outsourcing arrangements were successful without due diligence. It helps the provider understand how outsourcing contributes to your business objectives, and lets both parties set realistic expectations for success.

Overall, experts believe that security outsourcing holds





## THE ECONOMIES OF OUTSOURCING

### Year 1 costs

| Component | In-house Costs | Outsourced solution |
|---|---|---|
| Hardware/software | $ 60,000 | $ 50,000 |
| 1-time setup/install | N/A | $ 18,000 |
| Monthly management | N/A | $ 75,000 |
| Employee salaries | $ 180,000 | N/A |
| Employee training | $ 24,000 | N/A |
| Total | $ 264,000 | $ 143,000 |
| **Estimated Year 1 savings** | | **$ 121,000** |

### Year 2+ costs (annual)

| Component | In-house Costs | Outsourced solution |
|---|---|---|
| HW/SW maintenance | $ 8,000 | $ 7,000 |
| Monthly management | N/A | $ 75,000 |
| Employee salaries | $ 180,000 | N/A |
| Employee training | $ 24,000 | N/A |
| Total | $ 212,000 | $ 82,000 |
| **Estimated Year 2+ annual savings** | | **$ 130,000** |

### Assumptions

Based on a 250-user network using a single T1 Internet gateway. Security elements include single Check Point Firewall-1™ 250-user license running ona Nokia IP330 device, and two Sun Netra T1 servers running Internet Security Systems RealSecure™ intrusion protection software.

Employee salaries are based on three salaried employees, each working an 8-hour shift daily and earning $60K per year while devoting 100% of their on-duty time to managing/monitoring security devices.

Employee training includes 2 courses per year for each employee mentioned above, as well as travel expenses.

Source: Internet Security Systems

great promise. "We know of very few companies that have outsourced their entire IT security function. Yet, we can name very few others whose security organization can operate effectively today given the breadth and depth of knowledge and skills required without augmenting internal resources with external help," says a recent report by Giga Information Group.

While security outsourcing is a relatively new concept, a growing number of organizations will use it to align their security efforts with their business goals. "It was a big jump for us to do this kind of thing," concedes Enslein of Prime Office Centers. "But we've had no regrets. In my view, security outsourcing is the perfect solution."





# The Tools That Protect

An important part of an overall security strategy is the security hardware and sofware that protect your information assets. In fact, the market for security software alone will grow from $3.2 billion in 1998 to $8.3 billion in 2003, predicts International Data Corp. of Framingham, Mass. Here are some common security tools and techniques:

**ANTI-VIRUS SOFTWARE:** Because viruses are the most prevalent security threat, anti-virus software is a key weapon in the security arsenal. There are several types of anti-virus software—from solutions that protect individual PCs to those that protect file and messaging servers—and all are necessary in the fight against viruses. An effective anti-virus strategy also includes regular software updates to protect against the latest threats, as well as ongoing education to ensure that users are aware of the dangers and how to avoid them. Perhaps most important, an anti-virus strategy must specify standards for desktop configurations and usage. By restricting what software employees are permitted to load on their PCs, you can help prevent viruses from being introduced and can solve breaches more quickly if they occur.

**AUTHENTICATION:** Authentication provides a means for identifying an "object"—a user, a system, an application and so on. After being authenticated, the object can be granted access to the services it requires, and its activities can be monitored. Authentication mechanisms vary from the familiar username and password to sophisticated biometrics systems, which authenticate users through physical characteristics such as fingerprints. Authentication is a foundation of any security plan, and is often a key part of other security solu-

## The Tools That Protect

CONTINUED FROM PAGE 43

tions. The authentication technology you use to protect a particular computer resource should be determined by the resource's importance to your business.

**Firewalls:** The job of a firewall is to examine data as it enters the network and to block traffic that doesn't meet specified criteria. There are several types of firewalls, and all can be used in combination. A proxy server intercepts all messages entering and leaving the network and hides the true network address. A packet filter examines data packets entering or leaving the network and accepts or rejects them on the basis of specified criteria. An application gateway secures specific applications. A circuit-level gateway applies security mechanisms when a connection is established; after that, network traffic flows without further checking.

**Intrusion detection systems (IDS):** Applications that actively monitor operating systems and network traffic for attacks and breaches are considered an IDS. Its goal is to provide a near-real-time view of what's happening on the network. There are two approaches to intrusion detection: network-based and host-based. Network-based systems "sniff" the wire, comparing live traffic patterns to a list of known attacks. Host-based systems use software "agents" that are installed on all servers and report activity to a central console. A complete solution involves both types. Both require a regularly updated list of known attacks, just like anti-virus software. But they can also detect an electronic attacker trying different password combinations and alert the operations center or even automatically shut down that part of the network.

**Public key infrastructure (PKI):** PKI is a mechanism for both authentication and encryption, combining software, encryption technologies and services to protect network communications and e-business transactions. PKI involves a system of digital certificates—an attachment to an electronic message that can encrypt data and verify that the sender is who he or she claims to be—as well as certificate authorities, a third party that issues the digital certificate. PKI protects information assets by authenticating identity using a digital certificate, verifying integrity by ensuring that messages have not been altered or data corrupted, and ensuring privacy by protecting information from interception during transit. Its effectiveness has been hampered, however, by the fact that several PKIs are in use, and no standard yet exists.

**Virtual private networks (VPNs):** VPNs allow remote employees to access the corporate network by using the Internet as the transmission medium. Encryption technology and secure protocols make the network "private," even though communication takes place over public phone lines. In effect, the VPN makes possible the secure exchange of information across the Net. And it achieves that at about half the cost of a truly private network such as a leased line. Worldwide expenditures on VPN products will jump from $6.3 billion this year to more than $39.8 billion by 2004, predicts Infonetics Research of San Jose, Calif.

# The Business of Security

*Security no longer exists in a vacuum. Organizations are recognizing that they must apply the same principles of risk management to their information resources as they do to their physical assets.*

The threats against your information assets continue unabated. Studies such as the annual Computer Security Institute survey show that the vast majority of organizations—90 percent in the past 12 months—are experiencing attacks on their computer resources. Existing efforts to protect data and networks are barely keeping pace.

And the threats are only escalating as more transactions take place over the network and as a greater proportion of corporate assets reside in cyber space. From emerging technology startups to established bricks-and-mortar enterprises, organizations understand that increasingly, the network is the business. They recognize that they must apply the same principles of risk management to their information resources that they bring to their physical assets.

That starts with approaching security not as a technology concern but as a business issue. "Organizations that think of security as a necessary evil aren't effectively managing risk," says Peter Cottrell of Cottrell & Maguire, an underwriting syndicate at Lloyds of London. "But organizations





that approach security as a business issue have a firm foundation from which to pursue new opportunities. In the Internet Economy, a secure network means that a greater number of customers, partners and investors will do business with you and become stakeholders with you. I know we certainly feel that way here at Cottrell & Maguire regarding our clients around the globe and the protection of their vital business information assets."

The costs of not managing security risks can be high indeed. Compromises to your computer infrastructure can result in losses on every front—lost revenue, lost data, lost productivity, lost customer confidence and lost shareholder equity. It's not an exaggeration to say that organizations simply can't afford not to invest in security.

Of course, there will always be a gap between the real and the ideal. There is a point at which further investment in security will not yield adequate returns. When they reach that point, organizations are beginning to turn to cyber insurance as a way to manage the risk—the same way they manage risks to physical assets.

Finally, a growing number of companies are concluding that while security is mission-critical, it's not a core competency. That means security becomes a candidate for outsourcing, just like other non-core IT functions. Outsourcing gives organizations access to best security practices, state-of-the-art security technology, and highly trained, knowledgeable security experts, all while rendering security costs predictable and manageable.

Ultimately, computer security is a business enabler. It's less about keeping the network from going down and more about ensuring the availability, integrity and privacy that lets customers trust you to protect their personal information, that lets partners trust you to protect their systems, and that lets stakeholders trust you to protect their investments. That's security in the Internet Economy.

# The Action Plan for Implementing Information Security Management

**1. Publish a policy.**
Set a clear direction and demonstrate your support by issuing an information security policy.
* ***A written policy document should be available to all staff.***

**2. Establish your framework.**
Establish a management framework to implement security. Depending on the size of your organization, you may need forums to approve policy, assign roles and coordinate the implementation of security. You may also need to establish a source of specialist advice within the organization.
* ***Responsibilities for protecting assets and implementing security measures should be explicitly defined.***

**3. Assess your security.**
You will need to balance your expenditures on security against the business value of the assets at risk, and against the consequences of failures. Assess your risks to determine the controls you need and the priorities for implementing them.

**4. Implement security standards.**
When implementing a set of standards, consider the needs of your employees for specific guidance. Each group may have different requirements, problems and priorities, depending on their role and their IT environment. You may wish to build up a portfolio of individual guidelines.
* ***Precautions should be taken to prevent the spread of computer viruses.***
* ***Important organization records should be safeguarded against loss, destruction and falsification.***
* ***Applications handling personal data (on individuals) should comply with data protection legislation and principles.***

**5. Develop business continuity plans.**
Set a clear business plan to develop and to maintain appropriate recovery plans to protect your critical business processes from major failures or disasters.
* ***There should be a managed process in place for business continuity planning across the organization.***

**6. Educate your staff.**
Devise a suitable security education program for your employees, and make sure that all computer users are trained in the correct safe use of IT facilities. They will need to be told how to respond to security incidents.
* ***Users should be given adequate security education and technical training.***
* ***Security incidents should be reported through appropriate channels as quickly as possible.***

**7. Check for compliance.**
Make sure your IT systems and facilities are regularly reviewed against organizational security policy and standards.
* ***Copyrighted material (e.g. software) should not be copied without the owner's consent.***
* ***Systems should be regularly reviewed to ensure compliance with organizational security policy and standards.***

**Now that you've got your house in order, what about your business partners?**

Source: The British Department of Trade and Industry

### Project Manager—Bill Laberis Associates

Bill Laberis was editor in chief of *Computerworld* for ten years (1986-1996). He currently is president of Bill Laberis Associates (www.laberis.com), an IT content and consulting company in Holliston, MA.

### Lead Writer—Eric Schoeniger

Eric Schoeniger is an award-winning writer and communications consultant, based in Lower Gwynedd, Pa. Previously he was founding editor of *ENT Magazine* and editor in chief of *Digital Age, Exec*, and other publications. Contact him at ericschoeniger@aol.com.

### Design—Suzanne Peterman, TopDog Design

Suzanne Peterman has been president of TopDog Design (www.topdogdesign.com) since 1987, and is based in Acton, MA.


An IDG Publication

INTERNET
SECURITY
SYSTEMS™