



IT Security: The Data Theft Time Bomb

While viruses and worms remain the most pesky security problems, data theft concerns simmer beneath the surface, according to InformationWeek's 10th annual Global Information Security survey.

By Larry Greenemeier, [InformationWeek](#)

July 14, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=201001203>

Despite the billions of dollars spent on information security products, the aggressive patching and repairing of [operating systems](#) and applications, and the heightened awareness of the need for [computer](#) users to guard against identity theft, most organizations aren't feeling any more secure than they were a year ago. InformationWeek Research's 10th annual [Global Information Security](#) survey, conducted with consulting firm Accenture, shows that two-thirds of 1,101 survey respondents in the United States and 89% of 1,991 respondents in China are feeling just as vulnerable to security attacks as last year, or more so.

Contributing to this unease is the perception that security technology has grown overly complex, to the point where it's contributing to the problem. The No. 1 security challenge identified by almost half of U.S. respondents is "managing the complexity of security." So-called "defense-in-depth" is just another way of saying "you've got a bunch of technologies that overlap and that don't handle security in a straightforward manner," says Alastair MacWillson, global managing director of Accenture's security practice. "It's like putting 20 locks on your door because you're not comfortable that any of them works."

Yet a case can be made that respondents aren't worried enough, particularly about lost and stolen company and customer data. Only one-third of U.S. survey respondents and less than half of those in China cite "preventing breaches" as their biggest security challenge. Only one-quarter of U.S. respondents rank either unauthorized employee access to files and data or theft of customer data by outsiders in their top three security priorities, and even fewer put the loss or theft of mobile devices containing corporate data or the theft of intellectual property in that category. This lack of urgency persists despite highly publicized--and highly embarrassing--data-loss incidents in the last year and a half involving retailer TJX, the Department of Veterans Affairs, and the Georgia Community Health Department, among many, many others.

Instead, as with last year, the top three security priorities are viruses or worms (65% of U.S. respondents, 75% in China), [spyware](#) and [malware](#) (56% and 61%), and [spam](#) (40% in both countries).

THE LIGHT'S BETTER OVER HERE

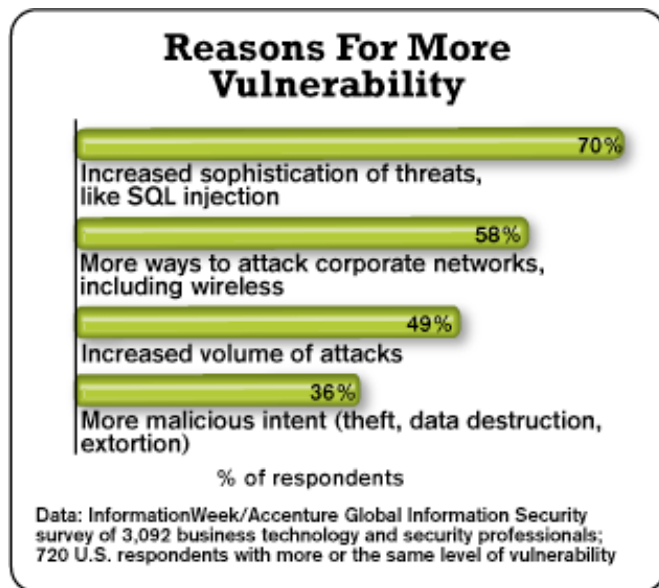
So are security pros focusing on the wrong things? Yes, says Jerry Dixon, director of Homeland Security's National Cyber Security Division. "You need to know where your data resides and who has access to it," Dixon says. "This speaks to the



[integrity](#) of the data that resides in your databases, the data that you use to carry out your business."

When asked what security pros should be worried about, security researcher Bruce Schneier, CTO of service provider BT Counterpane, puts it this way: "Crime, crime, crime, and compliance."

It seems as though security pros are missing the point, choosing to focus on the security threats with which they're most familiar as opposed to emerging threats designed to cash in on the value of customer data and intellectual property. A careful reading of our survey's results, however, indicates that organizations are waking up to just how vulnerable their customer information and intellectual property are to data thieves.



For example, the No. 1 reason for feeling more vulnerable to attack this year, according to 70% of U.S. respondents, is the increased sophistication of threats, including SQL injections. A programming technique applied to [Web site](#) requests, [SQL](#) injections have one purpose: to steal information from [databases](#) accessed by Web applications.

The next three reasons for feeling vulnerable: more ways for corporate networks to be attacked (including [wireless](#) access points); increased volume of attacks; and more malicious intent on the part of attackers (i.e., theft, data destruction, and extortion). Our survey suggests that companies think they're being attacked less to bring down their networks--though that remains the primary outcome of cyberattacks--and more to have their assets (customer or enterprise data) stolen. Only 13% of U.S. respondents see denial-of-service or other network-impairing attacks as a top three priority, down from 26% a year ago. Chinese respondents were only marginally more concerned about denial-of-service attacks.

Some security pros may be blissfully ignorant. Botnets, which can take control of IT resources remotely and can be used to launch attacks or steal information, debut as a concern in this year's survey, though only 10% of U.S. respondents and 13% of Chinese respondents rank them as a top three problem. This may be because companies are often unaware that they've been infiltrated by botnets, which is exactly what [bot](#) herders are counting on.

Similarly, viruses, worms, and [phishing](#) are the top three types of security breaches reported by U.S. respondents. Seventh on the list: identity theft. But that doesn't mean that identity theft isn't a greater threat. Identity theft and fraud are worst-case scenarios for a company whose data has been compromised, but not having experienced them could be as much about luck as it is security. TJX was extremely unlucky in that some of the 45.7 million customer records stolen from its IT systems over the past few years surfaced earlier this year in Florida, where they were used to create fake credit cards and defraud several Wal-Mart stores of millions of dollars. By contrast, the VA, last year's poster child for data insecurity, lost 27 million records when a laptop was stolen from an employee's house, but so far no [identity theft](#) or fraud activities have been traced back to that security breach.

Here's another sign that data security is a growing concern: While U.S. respondents measure the value of their security investments first for their ability to cut the number of hours workers spend on security-related issues (43% of respondents), second in priority is how well these measures protect customer records (35%), and third is a decline in the number of breaches (33%).

Perhaps the most surprising stat of the entire survey is that nearly a quarter of U.S. respondents don't measure the value of their security investments at all.

THE LUCKY ONES

As already mentioned, the most significant impact of cyberattacks is network downtime, followed by business apps, including e-mail, being rendered unavailable. Third on the impact list, as reported by a quarter of U.S. respondents and 41% in China, is information confidentiality being compromised. Fourth is "minor" financial losses, reported by 18% in the United States and 21% in China. They were the lucky ones.

The financial impact of security lapses is difficult to calculate in the short term, particularly when it involves the loss of data. In fact, the highest percentage of respondents admitting to a breach, 35% in the United States and 31% in China, say they

don't know the total value of the loss they suffered.

In the long run, though, the security losses can be painfully obvious. TJX reported a \$20 million computer intrusion-related charge for its third quarter, ended April 28. The loss to the Florida Wal-Marts: about \$8 million in merchandise.

The shadowy underground of malicious hackers and cyberthieves has been responsible for some high-profile breaches over the past 12 months, and concerns over the next strike occupy most security pros' time. More than half of those surveyed cited computer hackers as the source of breaches or espionage at their companies within the past year, and more than a third suspect that malicious coders were responsible. Just as significant, though, breaches by unauthorized users rose in 2007, to 34% from 28% in 2006.

At BryanLGH Medical Center in Lincoln, Neb., CIO Rich Marreel's main security concern is protect- ing the organization's patient data, not just from malicious hackers but from employee misuse, whether intentional or not. "We're always concerned about people sharing their [authentication](#) credentials with someone else or with information leaving the organization via laptops or [memory](#) sticks," Marreel says. The solution: a combination of employee education and security technology, including encryption.

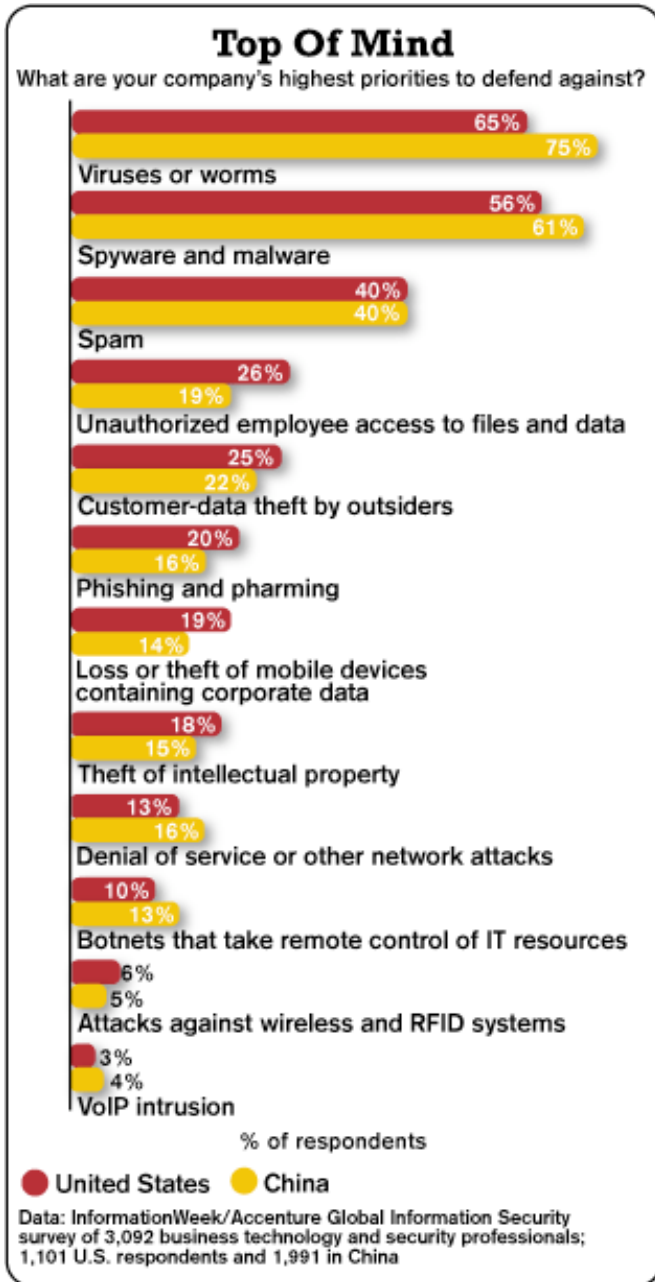
Without carefully managing user access rights, and demanding that users protect their [login](#) and password information, companies introduce "a hidden threat," Marreel says. At the hospital, for example, "a lot of people were writing down logins and passwords and carrying them around or even posting them on their PCs," he says. Haven't we heard this before?

THE CHINA FACTOR

U.S. and Chinese survey responses are similar, but different in many ways. For instance, exploiting known [operating system](#) vulnerabilities is the leading method of attack in both countries--43% of respondents in the United States and a whopping two-thirds in China say so. The same disproportionate response applies to the second leading attack method--known application vulnerabilities--where 41% of Chinese respondents' systems were compromised that way, as compared with less than a quarter in the United States. This could be the result of the large amount of pirated [software](#) used in China, says Accenture's MacWillson. "They don't have access to the patches," he points out (see story, "[China's Evolutionary Leap](#)").

Other popular methods of attack cited by respondents include falsified information in [e-mail](#) attachments (26% and 25%) and exploiting unknown operating system vulnerabilities (24% and 31%). Such intrusions, however, aren't the only concerns. Of the 804 U.S. respondents admitting to having experienced breaches or espionage in the past 12 months, 18% [attribute](#) the problem to unauthorized employees, and 16% suspect authorized users and employees.





But that's down from nearly 25% of companies reporting breaches in 2006. And that's surprising, because there's no getting around the fact that employees are a weak link in the security chain. Gary Min's attempted fleeing of his former employer, chemical company DuPont, included about \$400 million worth of company trade secrets that he tried to turn over to a DuPont competitor before that company alerted the FBI. Hiding in plain sight, Min accessed an unusually high volume of abstracts and full-text .pdf documents off DuPont's Electronic Data [Library](#) server, one of the company's main databases for storing confidential and proprietary information. Min downloaded about 22,000 abstracts from the EDL and accessed about 16,706 documents--15 times the number of abstracts and reports accessed by the next highest user of the EDL for that period. Min pleaded guilty and faces up to 10 years in prison, a fine of \$250,000, and restitution.

Besides outright fraud, employees fail to protect the data they have stored on their corporate IT assets, mainly their laptops. Laptops and portable storage devices are being stolen from employees' cars and homes in mind-boggling numbers. Last month, a [backup](#) computer storage device with the names and Social Security numbers of every employee in the state of Ohio--more than 64,000 records--was stolen from a state intern's car. Twelve months earlier, a laptop containing names, addresses, and credit and debit card information of 243,000 Hotels.com customers was stolen from an Ernst & Young employee's car in Texas. "Most of this is human error or bad business process," says Rhonda MacLean, CEO of consulting firm MacLean Risk Partners and former chief security officer at Bank of America and Boeing.

Similarly, only 5% of survey respondents cite contract service providers, consultants, or auditors as the source of their breaches. But that doesn't mean they shouldn't be concerned.

In April, the Georgia Department of Community Health reported the loss of 2.9 million records containing personal information, including full names, addresses, birth dates, Medicaid and children's health care recipient identification numbers, and Social Security numbers, when a computer [disk](#) went missing from service provider Affiliated Computer Services, which was contracted to handle health care claims for the state.

"If a partner or service provider has access to any of our data, we want a security paragraph written into our contract that gives us the right to perform a security [audit](#) against them and to perform these audits regularly," says Randy Barr, chief security officer of WebEx, a Web-conferencing company. Barr says that all contractors with access to company systems must undergo background checks, a policy since 2004.

You'd think that simply educating employees and partners about your company's security policies would be sufficient to keep generally honest people from letting customer information leak out through e-mails, instant messages, and peer-to-peer networks--but you'd be wrong. Sure, the No. 1 tactical security priority for U.S. companies in 2007, according to 37% of respondents, is creating and enhancing user awareness of policies. But that's down from 42% in 2006. A smaller percentage of U.S. companies also plan to install better access controls, monitoring software, and secure remote access systems. In China, companies are focusing on installing application firewalls, better access controls, and monitoring software.

Only 19% of respondents say that security technology and policy training will have a significant impact on alleviating employee-based security breaches, the same percentage as last year. "It takes more than showing them a few videos," consultant MacLean says. "You have to track employee training and make sure that employees finish with at least the basic understanding of what you want them to know."

Over the past 12 months, the change at Eisenhower Medical Center in Rancho Mirage, Calif., that's had the greatest impact on security is the health care organization's move from a paper-based to an electronic patient records system. "This put more responsibility on us to make sure the patient's data is secure," says CIO David Perez. "And it's not just the movement of the data online but the volume of that data makes it more challenging. A CAT scan a few years ago would provide 250 to 500 images, but our new system can produce up to 5,000 images."

As more and more physicians and medical staff log on to Eisenhower's [intranet](#) portal to do their work, Perez and his team must increase their monitoring for security problems and ensure that only the appropriate physicians and staff are accessing different medical records, as required by the Health Insurance Portability and [Accountability](#) Act. "Users sign a confidentiality statement when they join the medical center," Perez says. "We'll also post reminders on the employee portal."

THE BIG BROTHER APPROACH

Some companies prefer the Big Brother approach. Of the U.S. respondents who say their companies monitor employee activities, 51% monitor e-mail use, 40% monitor Web use, and 35% monitor phone use, roughly consistent with last year's findings. However, other sources of data leakage are given less attention: Only 29% [monitor instant messaging](#) use, 22% the opening of e-mail attachments, and 20% the contents of outbound e-mail messages. And only a handful keep a close eye on the use of portable [storage](#) devices.

Still, 42% of respondents say data leakage is bad enough that employees should be fined or punished in some way for their role in security breaches, once those employees have been trained. Consultant MacLean takes an even tougher tack: "Termination is pretty severe, but in some cases it's appropriate, as is civil or even criminal prosecution."

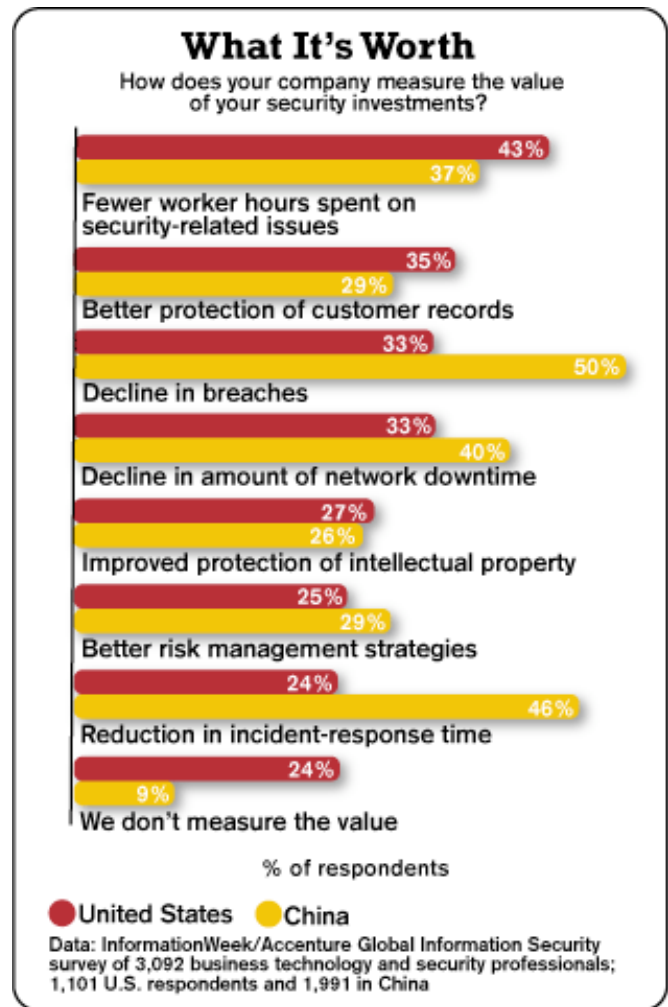
A significant number of respondents want to put the responsibility for porous security on the companies selling them security technology. Forty-five percent of U.S. companies and 47% of companies in China think security vendors should be held legally and financially liable for security vulnerabilities in their products and services.

Some of the unease about corporate IT security may stem from the fact that most companies don't have a centralized security executive assessing risks and threats and then calling the shots to address these concerns. The process for setting security policy in most companies is collaborative, and groups comprising the CIO, CEO, IT management, and security management all have input. Eisenhower Medical Center doesn't have a chief information security officer, instead relying on its general counsel to make regulatory [compliance](#) decisions, and on CIO Perez, working with system administrators, to set security policy. "We gather information from each director in each department to find out what systems and data they need access to," Perez says. "It's an interesting back and forth. The doctors want easy access, and we're trying to make it more secure."

The number of chief information security officers has grown significantly in the last year. Roughly three-quarters of survey respondents say their companies have CISOs, compared with 39% in 2006. CISOs predominantly report to the CEO or the CIO.

When it comes to the ultimate sign-off, however, half of U.S. companies say that the CEO determines security spending. In the United States, the greatest percentage of respondents, 37%, say their companies assess risks and threats without the [input](#) of a CISO, while an astounding 22% say they don't regularly assess security risks and threats at all.

In the United States, the portion of IT budgets devoted to security remains pretty flat; companies plan to spend an average of 12% this year, compared with 13% last year. China, on the other hand, is on a security spending spree: The average percentage of IT budget devoted to security this year is 19%, compared with 16% in 2006. It's interesting to note that 39% of U.S. companies and 55% in China expect 2007 security spending levels to surpass those in 2006.



If it all sounds overwhelming, don't panic. While information security has gotten more complex--as attackers alter both their methods and their targets, and companies layer more and more security products on top of each other--the good news is that the measures required to plug most security holes often come down to common sense, an increasingly important quality to look for in any employee or manager handling sensitive data.

Illustration ©2007 Brian Stauffer c/o theispot.com

Continue to the sidebar:
[China's Evolutionary Leap](#)

View charts:
[IT Security: Still A Daunting Task](#)

Buy the report:
[2007 InformationWeek/Accenture Global Information Security Survey](#)



Copyright © 2007 [CMP Media LLC](#)