

## Strategy Session

Presented in conjunction with

**SECURITY**  
**darkREADING**

Protect The Business  Enable Access

# Small Businesses, Big Losses: How SMBs Can Fight Cybercrime

Small and midsize businesses are falling prey to cyberattacks that cost them sensitive data, productivity and corporate accounts cleaned out by sophisticated banking Trojans. SMBs are typically on the hook for these losses and lack effective means to prevent them. In this report, we explain what makes these threats so menacing, and share best practices to defend against them.

**By Neil Roiter**



T  
A  
B  
L  
E  
O  
F  
**CONTENTS**

- 4 Author's Bio
- 5 Executive Summary
- 6 SMBs at Risk
- 8 Low Risk, High Profit...for the Criminals
- 10 Detection: Tougher Than Ever
- 14 Work With Your Bank to Protect Your Business
- 18 Best Practices to Secure Your SMB
- 21 Related Reports



T  
A  
B  
L  
E  
O  
F  
  
C  
O  
N  
T  
E  
N  
T  
S

- 6 Figure 1 Incidence of SMB and Consumer Fraud
- 8 Figure 2: What Sources of Breaches or Espionage Pose the Greatest Threat to Your Company?
- 9 Figure 3: Data Lost
- 11 Figure 4: Cost of Cyberattacks
- 13 Figure 5: Constructing a Download Drive-By Attack
- 15 Figure 6: A Complex Problem
- 17 Figure 7: Most Effective Security Practices
- 19 Figure 8: What Small Businesses Did After Discovering Fraud

**ABOUT US** | *InformationWeek Analytics'* experienced analysts arm business technology decision-makers with real-world perspective based on a combination of qualitative and quantitative research, business and technology assessment and planning tools, and technology adoption best practices gleaned from experience.

If you'd like to contact us, write to managing director **Art Wittmann** at [awittmann@techweb.com](mailto:awittmann@techweb.com), content director **Lorna Garey** at [lgarey@techweb.com](mailto:lgarey@techweb.com) and research managing editor **Heather Vallis** at [hvallis@techweb.com](mailto:hvallis@techweb.com). Find all of our reports at [www.analytics.informationweek.com](http://www.analytics.informationweek.com).



**Neil Roiter**  
*Dark Reading*



**Neil Roiter** is a freelance technology writer and contributing editor to *Dark Reading*, with a strong background in information security, risk and compliance, and the role of technology in business. Neil is best known in the industry for his work over nine years as a writer and editor for *Information Security* magazine and *SearchSecurity.com*.

Neil's background includes daily newspaper reporting, editing and management and five years of IT project management for a newspaper company and then a publishing software firm.



# EXECUTIVE SUMMARY



**Small and midsize businesses** are suffering substantial, sometimes crippling losses to cyberattacks that are becoming increasingly difficult to detect and prevent. Automated botnets use polished, highly convincing phishing and social engineering techniques, and sophisticated malware that requires no special skills on the part of attackers, thanks to the proliferation of relatively inexpensive malware kits on the criminal market.

SMBs often fall prey to the same attacks as individual consumers, but the repercussions are typically far worse: Business as well as personal accounts are compromised; corporate accounts, credit cards and sensitive data are exposed through employees as well as owners; and banks are under no obligation to make good on losses even if a business account is drained of tens of thousands of dollars. Midmarket companies should not feel safe because the big attacks on major companies—SONY, Epsilon, RSA, Google, Adobe—make the headlines. You may assume your company's size and obscurity puts it below the radar, but while you may not be singled out for targeting, you may well be a target of opportunity.

In this report, we explain why SMBs are at great risk, discuss measures you can take to reduce chances of a successful attack and suggest ways to cut your losses if your business does become a victim.



## SMBs at Risk

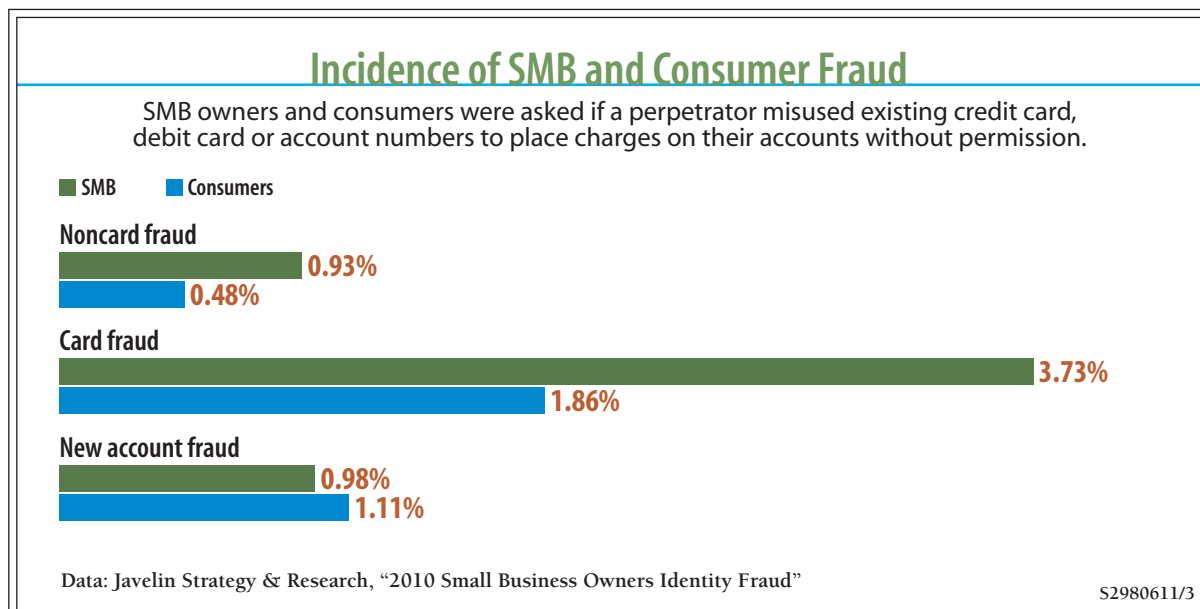
Small companies are suffering big losses. A recent survey by Javelin Strategy & Research pegged the cost of SMB computer fraud in the U.S. at \$8 billion in 2010. The victim companies were on the hook for \$2.61 billion of that loss, with the balance absorbed by financial institutions, credit card issuers, merchant partners or insurance firms.

The cost to a particular company can be very high. While the average cost absorbed by the SMB was \$1,574 per incident, according to the Javelin report, the median cost was only \$21. That means while many of the incidents were trivial, others cost small businesses thousands of dollars they could ill afford.

Findings of a global survey of companies with fewer than 500 employees by Symantec were even more alarming: Three-quarters of the responding companies suffered cyberattacks in 2009, at an average direct annual cost of \$188,242.

SMBs are twice as likely as individual consumers to suffer non-credit card fraud (see Figure 1, below). The figures can be numbing, but the individual cases will hit home to every small business owner. Brian Krebs, author of the popular Krebs on Security blog, has reported (in his

Figure 1





blog and previously in *The Washington Post*) on some 75 cases of SMBs that have lost many thousands of dollars to cyberfraud; he says he has interviewed twice that number.

For example, thieves used the infamous Zeus banking Trojan to steal log-in credentials from the controller of an Abilene, Kan., car dealership and run a phony payroll batch for employees totaling \$63,000. The attackers were able to monitor the controller's activity as he ran a legitimate payroll batch an hour earlier. In another case, thieves stole \$465,000 from a California escrow company's online bank account.

And it's not just small businesses. Hackers stole \$600,000 from the online account of the town of Brigantine, N.J. A college of the University of Virginia lost nearly \$1,000,000 to hackers, and the Catholic Diocese of Des Moines, Iowa, was taken for \$600,000. The numbers may be small compared with what attacks cost TJX or Heartland Payment Systems, but the impact on a small business can be catastrophic.

Does this mean small businesses are being targeted? For the most part, no, says Krebs.

"The criminals I have been tracking tend to be opportunistic," he says. "They spam out a ton of Trojans via email and go after what sticks." But, while businesses are no more likely to be victimized than individual consumers, "the stakes are much, much higher."

This is because consumers have zero liability if their online accounts are robbed—the banks will make good. But businesses have no such guarantee. Moreover, banks and credit card companies are far more likely to spot suspicious activity around consumer accounts, where very large transfers are unlikely, but a business transfer or withdrawal of \$50,000 or \$100,000 would appear more or less normal.

That's not to say small businesses cannot be targeted. Small banks, in particular, have been known to be singled out. It isn't hard for criminals to learn enough to launch a spear-phishing attack directed at a small company or an individual in that company.

"The malware propagation campaigns we see are indiscriminate in nature," says Paul Royal, research scientist at the Georgia Tech Information Security Center, "but it wouldn't take a lot of effort to do a small amount of research on the company you want to target, do a little social engineering and get account credentials."



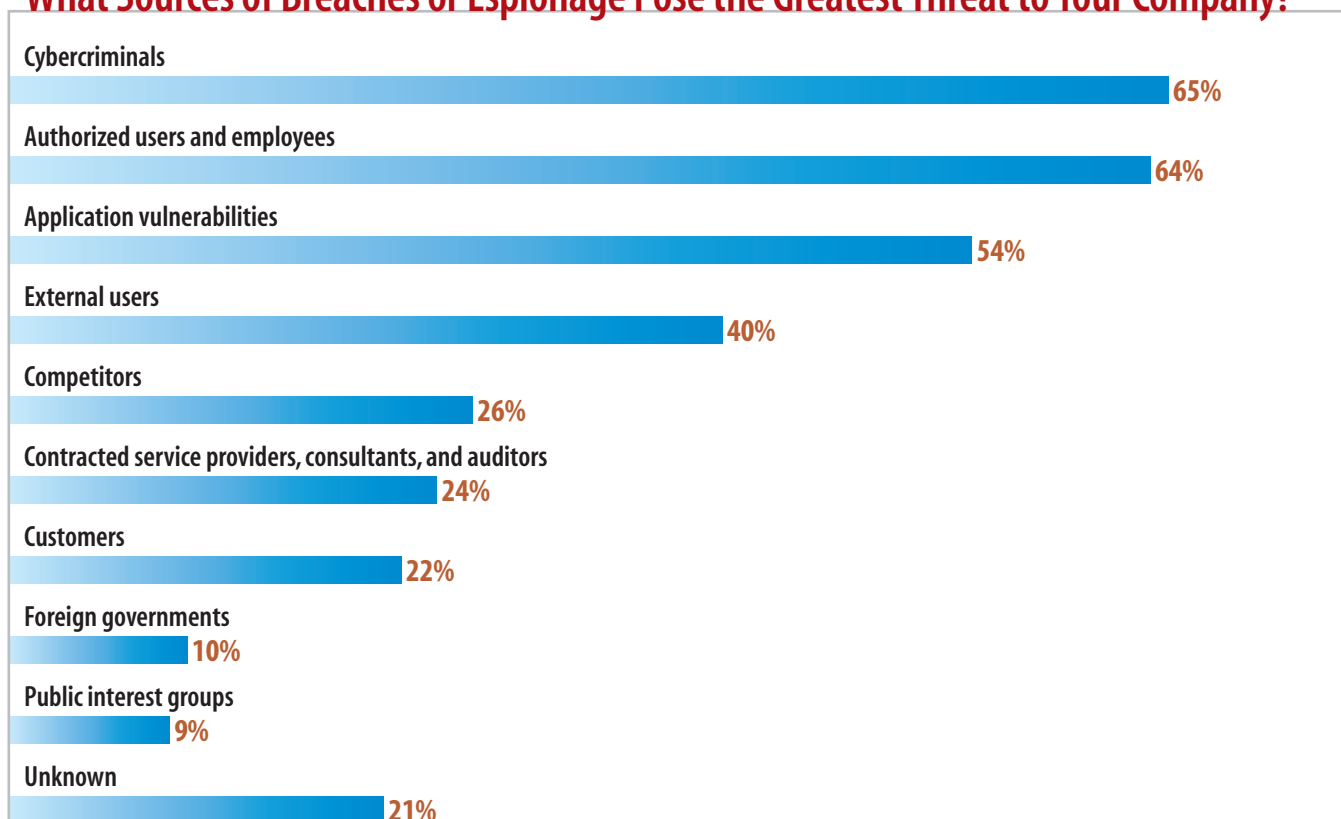
For example, companies make far too much information available on their websites, such as controller's name and email address, and they're careless about what specifics they post and who they respond to on Facebook.

### Low Risk, High Profit...for the Criminals

SMBs are attractive to cybercriminals, says Serge Jorgensen, VP and CTO at security consultancy Sylint Group. Nearly two-thirds of midmarket companies cite cybercrime as the greatest threat to their companies, according to the *InformationWeek Analytics 2011 Strategic Security Survey: Midmarket* (see Figure 2, below).

Figure 2

## What Sources of Breaches or Espionage Pose the Greatest Threat to Your Company?



Data: *InformationWeek Analytics 2011 Strategic Security Survey* of 699 business technology and security professionals at companies with fewer than 1,000 employees, March 2011



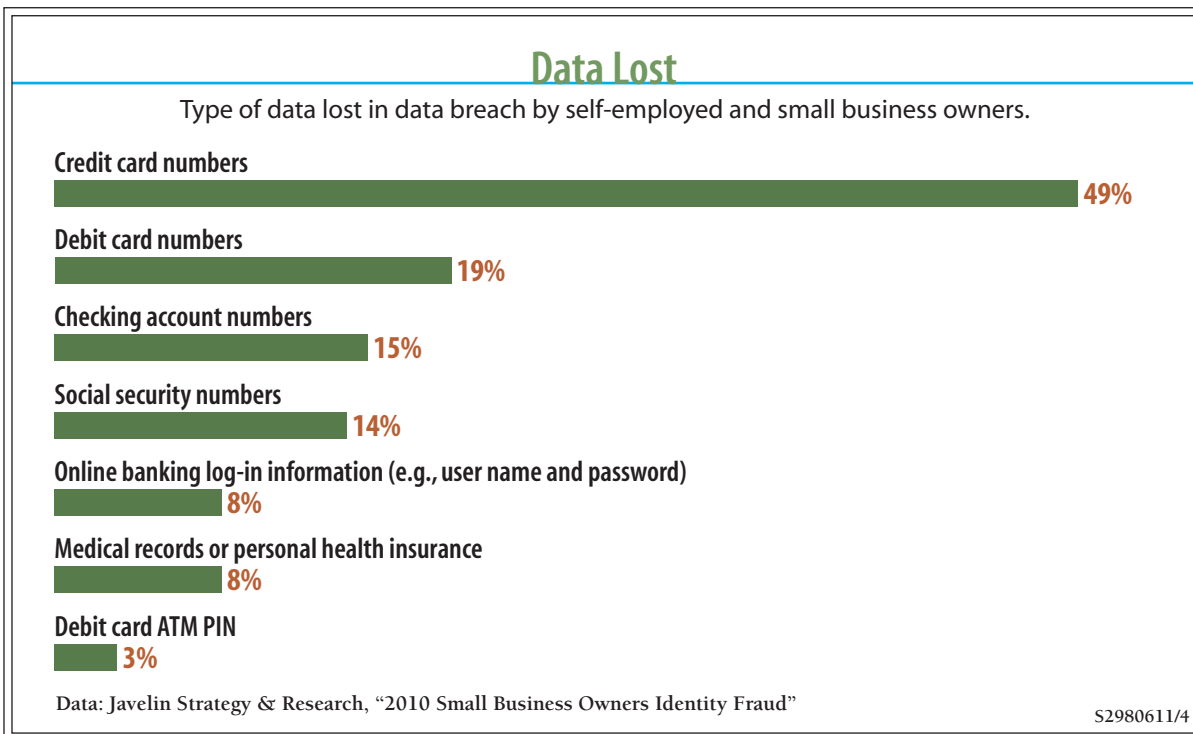
Enterprises yield a big payoff in sensitive information, but are getting increasingly tough to crack, while the payoff for infecting a consumer PC is not very high. Credit card numbers are by far the most common type of data stolen, according to Javelin (see Figure 3, below), but thefts of online banking log-in information, while relatively small in number, can be devastating, as Krebs and others can attest.

“SMBs are low-hanging fruit, much like consumers,” Jorgensen says. “But the bang for buck for attacking and penetrating them is a lot higher.”

The fruit is even juicier if the small business is responsible for handling a lot of money—often many times more than the amount of its own cash—for clients.

“We’ve seen an uptick in the last year on attacks against law firms, CPAs, accounting firms, other collections of professionals that deal with large amounts of money,” Jorgensen says. “For example, a law firm may do real estate transactions, so its net worth is significantly less than

Figure 3





the money that flows through it. A 100- to 200-person law firm may be worth \$50 million, but handle 10 or 20 times that amount because it is handling mergers and acquisitions.”

Fraud is even tougher to detect in that kind of environment. History has shown that banks have enough trouble spotting anomalies when there are predictable, routine transfers, such as the payroll for the unfortunate car dealership mentioned above. But in cases such as the law firms, the amounts are large and unpredictable. These transactions can occur anywhere in the world and involve multiple banks and other entities.

Compromised small businesses also can be a risk to larger partners. Enterprises depend on small businesses for all sorts of supplies and services. Typically, the SMBs have a tunnel connection to their partners, requiring no more than user name and password authentication.

Enterprises are locking down their environments, but remain vulnerable through smaller companies that have access.

“It’s a hole in the enterprise,” says Jorgensen. “We’ve seen it in defense contractors, critical infrastructure, research and development firms. It’s an authorized access path that very few companies are monitoring.

“We’ve seen a number [of SMBs] collapse because they were penetrated, either because of financial pressure or because they’d lost the confidence of their partners.”

### **Detection: Tougher Than Ever**

SMBs report all kinds of loss as a result of cyberattacks (see Figure 4, next page), according to the Symantec survey, starting with lost productivity, followed by lost revenue and direct financial loss, which, as we’ve seen, can be devastating. Why is this happening? And why aren’t SMBs better protected?

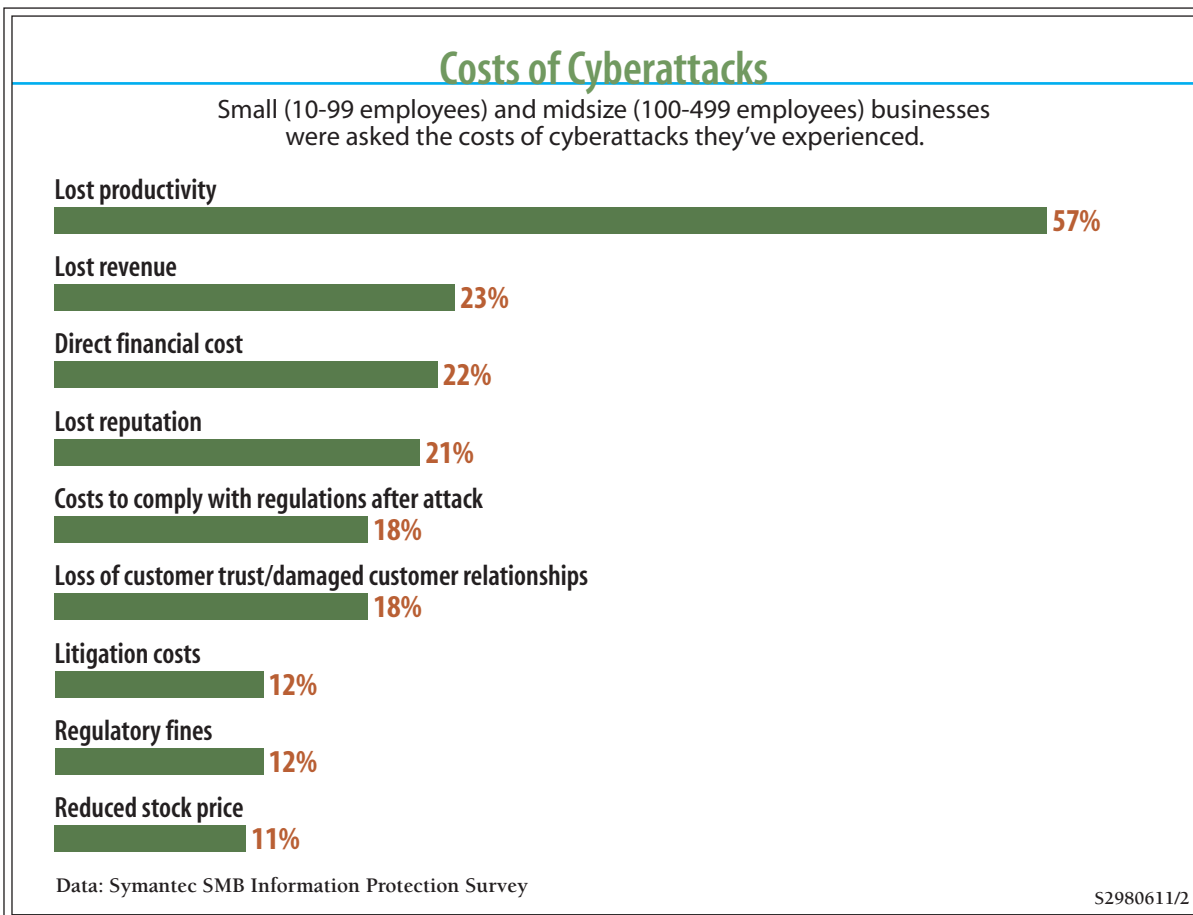
The answer is, in large part, that contemporary malware attacks are slick and hard to detect, either by careful business owners and their employees or even up-to-date antivirus protection. Most (85%) of SMBs consider malware the type of breach they’re most likely to suffer, according to *InformationWeek Analytics* research.



Botnets can blast out millions of seemingly legitimate, well-crafted email messages. The clumsy, misspelled phishing attacks addressed to “valued customer” are history. Messages appear to be addressed personally, and the social engineering, though generic, is realistic enough to convince even the most alert users the messages are directed at them. Remember the assurances in the aftermath of the Epsilon breach that only user email addresses had been stolen? That’s precious information for attackers who can use it to send you a phishing message, knowing you are a customer of JPMorgan Chase, Capital One, Marriott Rewards, U.S. Bank, Citi, Ritz-Carlton Rewards, Walgreens, Home Shopping Network or any of some 50 other companies.

Phishing attacks, social engineering, malware are all rolled up into attacks designed to lure users to inadvertently download Trojans and other malicious software designed to steal information.

Figure 4





Banking Trojans, such as Zeus, are insidious. Not only can they be spread by phishing, but by drive-by downloads (see Figure 5, next page) of malicious links during simple searches of legitimate websites that have been unknowingly compromised—attackers have become adept at search engine optimization—or social networks such as Facebook and Twitter. Bogus online ads are another source of infection. Georgia Tech’s Royal cited a hack of the USA Today website, in which visitors could be infected even if they didn’t click on the compromised ad. In that case, users were taken to a rogue antivirus site, but attackers can harvest information from a wide demographic of users this way and decide what to do with it later.

Banking Trojans such as Zeus capture authentication credentials when a user logs into an account. They can generate forms and false websites, and even take screenshots to capture not only credentials but account numbers, addresses, signatures and check images. They can “learn” a lot.

They are also good at hiding themselves. URLZone, for example, uses techniques to evade fraud detection technologies designed to flag anomalous transactions: It allows criminals to rewrite account balances to hide thefts, preset the percentage of money to be transferred, and detect security researcher programs and send false information. The popular Clampi Trojan uses encryption.

“They not only get passwords; they get to control the victim’s computer,” says Krebs. “This means they cannot only log in to bank accounts using the victim’s own IP address and computer, they control what the victim sees in the browser.”

SMBs can reduce their exposure by maintaining up-to-date antivirus protection and keeping their PCs patched, but don’t assume that will prevent infections. Far from it.

“I’ve interviewed more than 150 victims,” says Krebs. “All had AV, but very, very few had detections before they lost all the money.

“Is it a good idea to run AV? Yes. Should you assume it will protect you from this type of attack? Absolutely not.”

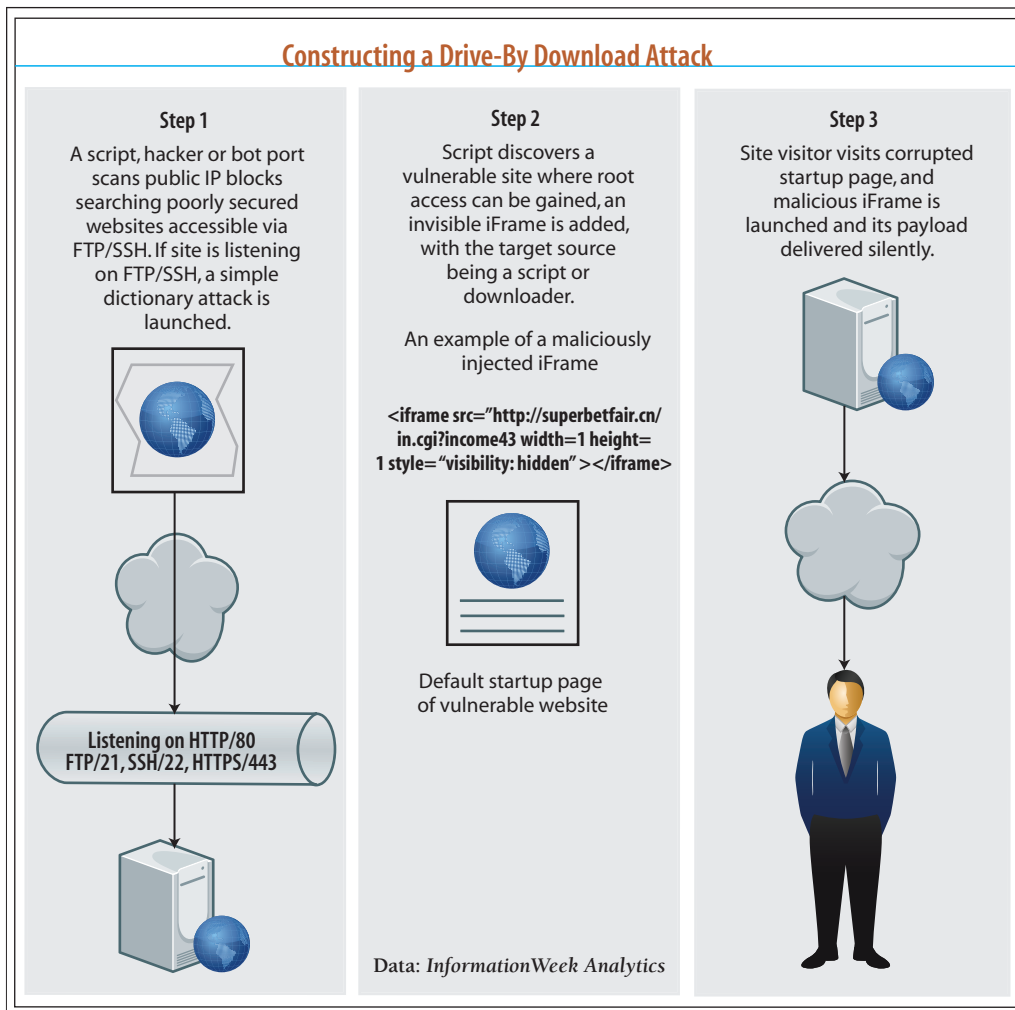
Malware variants are being spawned at remarkable rates and use obfuscation techniques that make them look like legitimate programs. It’s increasingly difficult for antivirus vendors to



detect malware and keep pace. Often, Royal says, they are already out of date, as the malware on a PC has downloaded several updates from its command-and-control server by the time a signature is available. A report by Georgia Tech, for example, showed that a Waledac malware sample was detected by 38 out of 39 antimalware tools. Another, updated sample was detected by only 11.

“Criminals have capable software engineers studying AV and finding ways to evade it,” says Royal. “They perform QA tests to see what AV does and how to avoid it. They create novel obfuscations and automate mutations and transformations.”

Figure 5





In addition, modern malware is almost impossible for the typical user to detect, Royal says. In the past, a user might notice that a computer had slowed to a crawl and call the help desk. But dual- or quad-core CPUs and 4MB to 8MB of RAM “creates quite a playground for malicious software,” and most malware doesn’t consume much CPU time. Most SMB networks have excess bandwidth, so additional traffic typically goes unnoticed, he adds.

What’s more, with streaming audio and video at the desktop, users are unlikely to attribute slowdown to malware.

### **Partner With Banks to Protect Your Business**

The bank can be your new best friend in dealing with computer fraud, but you need to understand the limits of the bank’s liabilities and take the initiative to ensure you get the best protection services available.

As discussed earlier, banks are not liable to make good on losses if money is stolen from a business account. Banks need only demonstrate that they have followed the “commercially reasonable” security protocols they have put in place and agreed to by the customer, according to David Navetta, founding partner of the Information Law Group. So, for instance, even if a hacker steals credentials and makes what appear to be authorized transactions, the bank is off the hook.

“There has to be agreement at the outset,” Navetta says. “But if the customer knows and is comfortable with what the security procedures are, if there’s a breach, the risk shifts back to the customer as long as the bank does what it is supposed to.”

Look at your contract—you do have a contract, right?—to determine if the security procedures and controls meet your requirements. If not, start shopping for a different bank. Some banks are offering various forms of two-factor authentication to make it tougher for criminals to get into your accounts. That’s not a sure thing, as some banking Trojans have found ways to overcome two-factor authentication, and, if they have control of your PC, they may execute fraudulent transactions during your session, after you have authenticated.

Make sure your bank will alert you by phone if it detects anomalous behavior. In some instances, you can ask the bank to hold up certain transactions until it gets your explicit authorization. Work with the bank to define what is—and isn’t—normal banking behavior for



your business. For example: How often do you process payroll? What is the maximum size of a given type of transaction? Do you do business with companies or individuals in other countries? Which countries? There are no guarantees; cybercriminals will often break up their thefts into a series of smaller transfers, for example, typically to money “mules” they have hired to accept transfers and then send the money to another account.

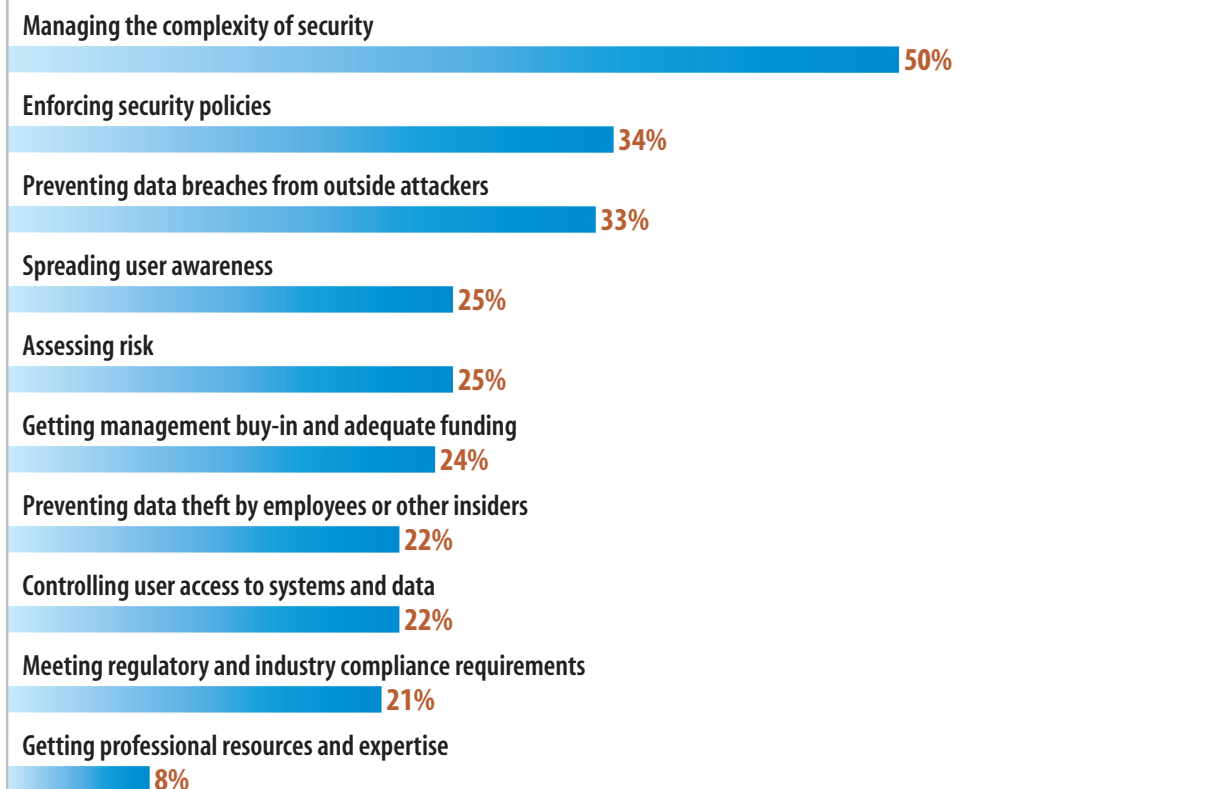
Ideally your bank is watching for this kind of activity, but don’t assume anything.

“Every attack I’ve written about, there are no-brainer red flags—time and again banks let these things go through,” says Krebs. “They were very, very unusual. The victim organizations had never done anything like that.”

Figure 6

### A Complex Problem

What are the biggest information and network security challenges facing your company?



Data: InformationWeek Analytics 2011 Strategic Security Survey of 699 business technology and security professionals at companies than 1,000 employees, March 2011



Many banks are employing antifraud services and technologies to detect potentially criminal behavior. Make sure your bank is among these, and take further steps to make sure it tailors its monitoring to your business practices. If the bank charges a premium for these services, again, shop around.

“SMBs shouldn’t have to pay a premium for any of that now,” says Syllint’s Jorgensen. “Most of the larger banks have implemented some of these services for free.”

Does that mean you should choose a large, international bank over a small regional one? Yes and no. Big banks can be successfully attacked, but sometimes they quash potential bad publicity by making good on a business customer’s losses even if they are not obligated to do so. Many of the SMBs Krebs has written about were at small banks that are less able to absorb losses and “make victims whole” after an incident. But small banks know their business customers and their business practices, which can pay off in other ways.

“One business avoided a big problem because someone at the bank knew the customer by name and activity,” says Krebs. The bank rep knew the company didn’t process payroll on Tuesdays. The rep “gave the customer a call and saved them a bundle of money.”

Larger banks can compensate for their lack of this kind of personal knowledge by developing accurate business profiles of each customer.

Of course, if all else fails, you can sue your bank. A number of small businesses have done this, in some cases claiming the banks failed to follow their established security procedures. For example, Louisiana-based JM Test Systems sued Capital One, claiming it failed to take action even after the firm had notified the bank of the first of two fraudulent money transfers a week apart that cost the company \$97,000.

Legal action can be a viable option, says the Information Law Group’s Navetta. Banks are obligated to institute security protocols that are “commercially reasonable,” he says, but “what’s commercially reasonable is not necessarily a settled proposition. For example, one bank did not have two-factor authentication in place, and the FFIEC [Federal Financial Institutions Examination Council] has some guidance on two-factor.” The bank settled that case after a judge rejected an early motion to dismiss.

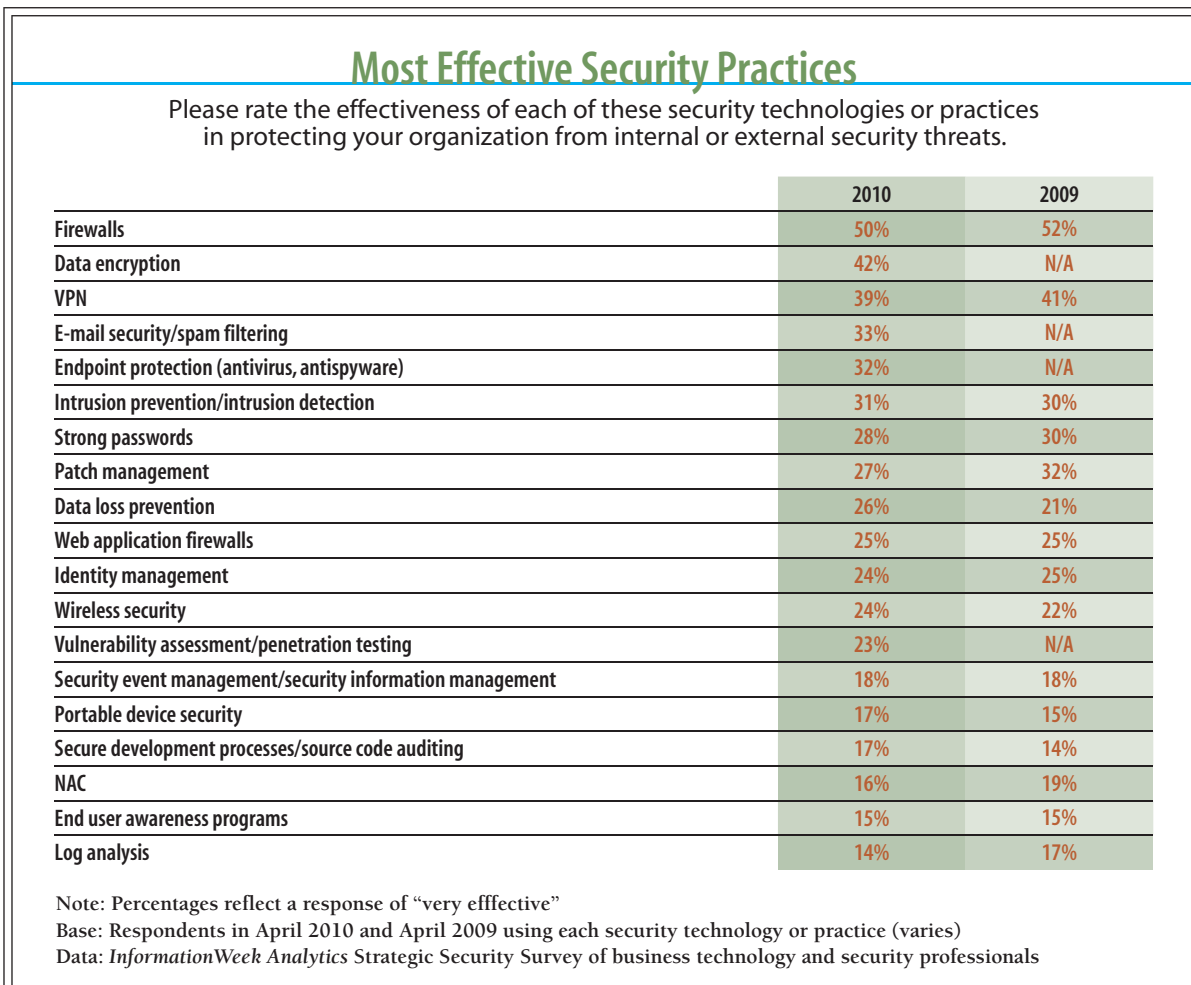


Banks don't want to risk jury trials that could set bad precedents," Navetta says. Filing a lawsuit "might give you leverage to get some sort of settlement from the bank."

### Best Practices to Secure Your SMB

Clearly, the bad guys are skilled, aggressive and have the upper hand. But, in addition to implementing antivirus software and up-to-date patches to reduce the chances of a successful attack, there are numerous steps you can take to help prevent compromise or detect malicious

Figure 7





activity before it damages or even destroys your business. Some of these measures are more technical than others; some require additional expense, most take extra effort. If you don't think they're worthwhile when stacked against the risk of losing \$100,000 or \$500,000 of your money or your customers' money, or the risk of compromising your partners' security, stop reading here. But if you're among the 70% of SMBs that told *InformationWeek Analytics* today's increasingly sophisticated threats are making you feel more vulnerable, keep reading.

Many SMBs made substantial changes in the way they do business after suffering a breach, according to the Javelin survey. Some of these changes may have been knee-jerk reactions (see Figure 8, next page). Three-quarters installed antivirus protection or a firewall; one-third stopped banking online; more than a quarter stopped using social networking sites. Nearly one in five switched banks and another one in five changed credit card companies.

Whether you've been victimized or not, you'll want to consider these measures to safeguard your business:

**>> Restrict employee access according to business need.** Don't share bank accounts with staffers who don't absolutely need to get into them. The more people who have log-in credentials, the more likely the chance of a successful attack. Maintain separate accounts so you can track who is doing what for the business and limit your exposure if there is a breach. Set corporate credit card limits according to each user's needs.

"A lot of small businesses run on trust," says Phil Blank, senior analyst for security, risk and fraud for Javelin. "But friendly fraud is a severe problem, because people know the business patterns and habits and how to get around them."

**>> Limit the information you post on your company website.** Don't include names, email addresses, phone numbers or other specifics about key personnel if there's no business need to make it public. Certainly, don't include personal information attackers can use for social engineering.

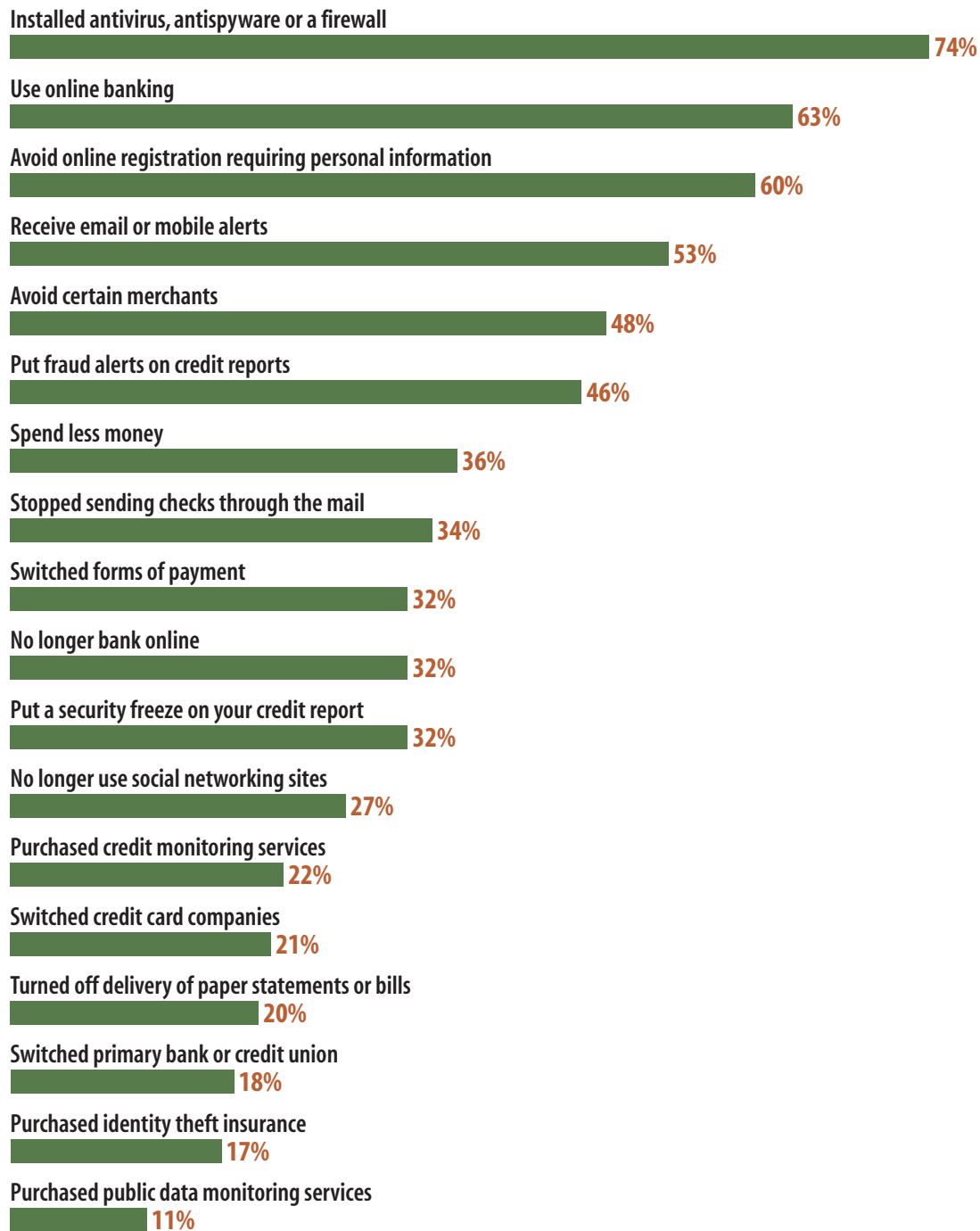
**>> Don't do your banking on the same computers you use for routine business or Web surfing.** If you and your authorized employees use computers designated for online banking only—no surfing, no social networking, no instant messaging, no music or video downloads, no email—chances are pretty good those computers won't get infected. Krebs recommends using



Figure 8

## What Small Businesses Did After Discovering Fraud

Small business owners were asked, "As a result of being a fraud victim, which statements are true?"



Data: Javelin Strategy & Research, "2010 Small Business Owners Identity Fraud"

S2980611/5



Mac or Linux-based computers for banking, since almost all malware is designed to exploit Windows vulnerabilities. Don't get lazy and do a quick Google search or send a personal email on these computers just because you can. Georgia Tech's Royal suggests saving the cost of a dedicated PC by putting two virtual machines on a single computer, dedicating one to banking and one for everything else. He cautions that the host should not be used for any activities.

**>> Restrict employees' online activities, and use basic Web filtering and log monitoring to enforce your policies.** Keeping employees from using P2P applications, visiting certain types of websites, and monitoring for policy violations and indications of malicious activity are standard practices at large enterprises. SMBs tend to adopt a more open approach, because they don't realize the risks or don't have the money or technical expertise to review their logs. Assume your employees' computers are infected, because no doubt they are, says Sylint's Jorgensen, and invest the time to monitor for aberrant activity or pay a security service provider to do it for you. Admonitions to be careful about clicking on links in suspicious emails no longer do any good.

"We're way past that," Jorgensen says. "Any bad guy worth his salt will craft a drive-by download the user won't notice. Emails are so well-crafted a user won't think twice. They look legitimate and the payloads are invisible."

**>> Maximize use of your UTM firewall.** Unified threat management products are SMB and branch office versions of firewalls integrated with other security tools that can be activated for a modest subscription fee. Spend the \$150 a year to turn on the intrusion detection functionality.

**>> Consider two-factor authentication.** This is another approach SMBs avoid because of cost, but you can minimize the expense by limiting deployment to specific employees for specific activities—for example, remote access, online banking and accessing other sensitive business information.



## Want More Like This?

Making the right technology choices is a challenge for IT teams everywhere. Whether it's sorting through vendor claims, justifying new projects or implementing new systems, there's no substitute for experience. And that's what *InformationWeek Analytics* provides—analysis and advice from IT professionals. Our subscription-based site houses more than 800 reports and briefs, and more than 100 new reports are slated for release in 2011. *InformationWeek Analytics* members have access to:

**Research: 2011 Strategic Security Survey:** The 1,084 security pros responding to our 14th annual Strategic Security Survey say CEOs are finally making risk management a priority. They also weigh in on the emerging risk areas of mobile devices and social media, as well as security budgets, software development, compliance and the cloud.

**Informed CIO: Mobile Device Security:** We share four strategies to mitigate risk in companies that allow employees to access corporate data using privately owned mobile devices.

**Strategy: SMBs in the Crosshairs:** Cybercriminals are targeting small and midsize companies, and many business' accounts have been cleaned out. We identify the threats and show you how to shore up your defenses.

**Strategy: Secure Design on a Dime:** Get our five best practices to move to the next level in protecting small and midsize business assets without spending a fortune.

**Strategy: Windows 7 Security:** We evaluate the security Microsoft has built into Win 7 to help you determine if it's sufficient for your company's defense purposes and what, if any, additional tools you'll need for comprehensive protection.

**PLUS:** Signature reports, such as the *InformationWeek Salary Survey*, *InformationWeek 500* and the annual State of Security report; full issues; and much more.

**For more information on our subscription plans, please [CLICK HERE](#)**