

# ESO - Security Trends Report

01/09

## *Report: IT, Security Departments Not Seeing Eye To Eye On Threats To The Business*

### **While 92 percent of security professionals in new Ponemon-Lumension study say their organization suffered a cyberattack, only 55 percent of IT staffers said the same**

Dec 07, 2008 |

**By Kelly Jackson Higgins**  
*DarkReading*

A new report underscores a major disconnect between IT and security groups when it comes to what most threatens their organizations.

[The Ponemon Institute's](#) 2008 Security Mega Trends Survey, which was commissioned by [Lumension](#), reveals just how far apart IT departments and security groups are when it comes to what they perceive as the biggest threats to their data today and in the next 12 to 24 months. While outsourcing risks are at the top of IT managers' worries, data breaches and cybercrime are the biggest worries for security.

More specifically, half of the IT managers said that outsourcing was a high or very high security risk to their organizations today and in the next one to two years; 44 percent also pointed to data breaches as a comparable risk today, while 40 percent expect them to be so in the next one to two years. Security professionals, meanwhile, ranked data breaches and cybercrime higher: Sixty-six percent consider data breaches high or very high risks today, while 65 percent rank them as such for the next year to two years. In addition, 65 percent say cybercrime is a high or very high risk to their organizations today, while 77 percent say it will be in the next 12 to 24 months. That's in contrast to the IT side, where 47 percent consider it a high risk today, and 49 percent expect that it will be in the next year to two years.

"We see a big disconnect between IT and security in their thoughts about data breaches and how risky that is to a business," says Pat Clawson, CEO of Lumension.

But the most disturbing disconnect was in actual breaches. While 92 percent of security professionals say their organizations had suffered a cyberattack, only 55 percent of IT staffers said the same, while 32 percent said they were uncertain. "That just floored me," Clawson says. "That shows the silos" that still exist, he says.

The two groups were far apart on Web 2.0 threats as well, with only 34 percent of IT saying the use of Web 2.0 will result in the loss of business information (including trade secrets), while 64 percent of IT security said it will. "That's a big delta -- IT is not 'getting' the risk," Clawson says.

Mobile devices is one area where both sides are on the same page, however, with nearly half of each group ranking them as a high or very high risk to the business. "We also think that mobility is dramatically contributing to data loss...mobility and mobile devices were the only area where IT and security got close" in their perceptions, Clawson says.

"The key for both IT operations and IT security is to find the common ground necessary to better wage this security battle together," says Larry Ponemon, chairman and founder of the Ponemon Institute.

Interestingly, both IT and security departments don't rate virtualization as high risk. But about half of each said the biggest danger with virtualization is not being able to identify and authenticate users to multiple systems "and third parties' access to private files without authorization," according to the report.

## Cisco: Cyberattacks growing, looking more legit

Sees 90% growth in threats originating from legitimate domains, report says

By Jim Duffy

December 15, 2008 (Network World) Internet-based [cyberattacks](#) are becoming increasingly sophisticated and specialized as profit-driven criminals continue to hone their approaches to stealing data from businesses, employees and consumers, according to a report [Cisco Systems Inc.](#) released this week.

The 2008 Cisco Annual Security Report found that the overall number of disclosed vulnerabilities grew by 11.5% over 2007. Vulnerabilities in virtualization technology nearly tripled, from 35 to 103 year-over-year, and attacks are becoming increasingly blended, cross-vector and targeted, according to the report.

Cisco says its researchers saw 90% growth in threats originating from legitimate domains, nearly double what was seen in 2007. And the volume of [malware](#) successfully propagated via e-mail attachments is declining. Over the past two years, the number of attachment-based attacks decreased by 50% from 2005 and 2006 levels.

This is at least the fourth study on security released this year by Cisco. Three others, conducted by an external research firm but commissioned by Cisco, assessed [insider threats](#), [data leakage](#) and [security policies](#).

According to Cisco, spam accounts for nearly 200 billion messages each day, approximately 90% of worldwide e-mail. The U.S. is the biggest source, at 17.2%, ahead of Turkey (9.2%), Russia (8%), Canada (4.7%), Brazil (4.1%), India (3.5%), Poland (3.4%), South Korea (3.3%), Germany (2.9%) and the U.K. (2.9%).

More online attackers are using real e-mail accounts with legitimate Web mail providers to send spam, which makes it harder to detect and block, Cisco says. The company estimates that in 2008, spam resulting from e-mail reputation hijacking of the top three Web mail providers accounted for less than 1% of all spam worldwide but made up 7.6% of the providers' mail traffic.

Botnets have become a nexus of criminal activity on the Internet, according to Cisco. This year, numerous legitimate Web sites were infected with IFrames, malicious code injected by botnets that redirects visitors to malware-downloading sites, the company says.

The use of social engineering to entice victims to open a file or click links continues to grow. Cisco expects that in 2009, social engineering techniques will increase in number, vector and sophistication.

And targeted phishing -- spear phishing -- is also expected to become more prevalent as attackers personalize spam and make messages appear more credible, Cisco says.

The follow are some 2009 trends to look for, according to Cisco:

- **Insider threats:** The global economic downturn may prompt more security incidents involving employees.
- **Data loss:** Companies will adopt technology, education and clear, well-enforced data security policies to make compliance easier and reduce incidents of data loss due to carelessness, breaches by hackers, or malicious insiders.
- **Mobility, remote working and new tools as risk factors:** The trend of working remotely and the related use of Web-based tools, mobile devices, virtualization, cloud computing and similar technologies will be a [challenge](#) for security personnel, as the increasing number of devices and applications in use can make the expanding network more susceptible to new threats.

The free report is available on [Cisco's Web site](#). Data sources for the report came from multiple Cisco divisions continuously assessing and correlating Internet threats and vulnerabilities.

## Businesses 'fail to learn' from HMRC data loss disaster

By Leo King

December 15, 2008 (Computerworld UK) Businesses appear to have failed to learn lessons from HM Revenue & Customs' loss last year of 25 million records during transport, according to the results of a new survey.

The survey found that employees are still sending sensitive data on CDs in the mail, just as an HMRC employee did.

But according to the research commissioned by collaborative software supplier Axway, some employers are at fault. While staffers often look for a method of sending data over networks, a quarter of businesses do not have a proper system in place.

Some 72% of the employees who send sensitive files by CD, and 51% of those who send such files by e-mail, said they would rather use a secure system. One thousand office workers and 100 IT decision-makers were interviewed for the research by Vanson Bourne and ICM.

This means that users are aware of the security issues but are often forced to take a risk because of the lack of safe systems, the report said.

Alarming, only a third of IT professionals expressed a serious concern that staffs are using CDs, USB sticks and laptops to transport files.

Dave Bennett, chief technology officer at Axway, said, "The issue is that secure alternative methods are not there and as a result, business are putting themselves at risk of data breaches. "As with any investment, it is important to see how the benefits will outweigh the initial cost, and protecting customer and employee data, trade secrets and brand image should be reason enough."

Businesses needed to consider managed file transfer and data loss prevention systems to secure files and improve tracking, Axway said.

## Auditor: IRS doesn't check cyberaudit logs

By Grant Gross

December 16, 2008 (IDG News Service) The [Internal Revenue Service](#)'s IT staff hasn't routinely checked its cybersecurity audit logs, according to a report released this week by the agency's inspector general's office.

The IRS has effectively deployed intrusion-detection systems at its Internet gateways, and it has used access controls for firewalls and routers, said the report, completed in July and released Monday. But the agency's IT staffers weren't always saving or reviewing system audit logs, and clock settings on some firewalls and routers did not comply with IRS rules, the report said.

"These weaknesses increase the likelihood that intruders from the Internet could gain access to sensitive taxpayer data residing on the IRS network without being detected," [the report](#) said.

One IRS employee, the database administrator for routers, had access to router audit logs, even though IRS rules require that a worker outside the immediate IT staff responsible for routers have access for independent review, the report said. In addition, IRS IT staffers did not save audit logs on two separate servers, as recommended in IRS guidelines.

The report, with large chunks redacted, recommends that the IRS allow independent review of audit logs and establish procedures for saving audit logs. It also recommended that the IRS regularly test its Internet gateways for compliance with standard security configurations. The IRS agreed with the recommendations, saying it planned to do bi-weekly compliance testing.

The report also said the IRS had unnecessary services enabled on routers, although the public version of the report does not tell what those services were.

"We have corrected many of the findings outlined in your report and are aggressively implementing additional changes to further protect our Internet gateways," IRS CIO Arthur Gonzalez wrote in response to the report. "Your suggested recommendations are in adherence with standards that will further improve our security posture."

The IRS's parent agency, the [U.S. Department of Treasury](#), received a failing grade for its 2007 cybersecurity efforts, according to a [report card](#) released in May. The annual report, released by Congress, grades federal agencies' compliance with the Federal Information Security Management Act, or FISMA.

The IRS review was performed at the IRS Computer Security Incident Response Center. It covered the period from February 2007 to March of this year.

## 5 ways to secure your BlackBerry

By Joan Goodchild

December 17, 2008 (CSO) It seems we can't go a day lately without a new story about some security screw-up involving a lost or misplaced [BlackBerry](#). This week, officials with [John McCain's](#) campaign mistakenly sold a BlackBerry to a Fox television reporter for \$20 in a fire sale. The device contained confidential campaign information. And many Hollywood gossip publications were abuzz earlier this month with news that Tom Cruise had lost his BlackBerry while promoting a movie in Toronto. (Mixed reports now peg the device as either "found," or "never lost in the first place.")

In light of all of the slip-ups making headlines, it's no wonder that White House officials want [President-elect Barack Obama](#) to relinquish his BlackBerry before taking office. At this time of heightened concern about the security of mobile devices, CSO asked [Dan Hoffman](#), author, mobile security expert and CTO at [SMobile Systems](#), for his advice on ways to keep your BlackBerry safe.

**Treat your BlackBerry like a PC.** You wouldn't shop online, open e-mail attachments and check your bank account on your PC without having the proper firewalls and anti-virus and anti-malware protections in place, would you? So why are you doing it with your BlackBerry? A BlackBerry is a mini computer, said Hoffman.

"The perception [that viruses and malware](#) are not a problem on BlackBerries is outdated," said Hoffman. "The reason we don't hear about widespread infections is because the nature of malware has changed. Infections used to be done for fun and notoriety. Now these crimes are financially motivated."

Without software that can scan for problems and update virus definitions, BlackBerries can be quietly infected without their owners even knowing it, said Hoffman. And the creepiest part of that news is that the most popular type of malware currently seen on BlackBerries is spyware, according to [SMobile](#) research.

"Spyware can intercept every e-mail and text message that goes in and out of the device. And it can remotely turn on the phone and listen in on conversations," said Hoffman.

**Watch your back.** Does this sound familiar? You're killing time during a layover in Dallas by doing some housekeeping on your BlackBerry -- checking and responding to work e-mails, making important work-related calls, maybe even checking your bank account.

"I can't even tell you [how much personal and sensitive information](#) I've inadvertently seen or heard over the years because of what people were doing with their mobile devices," said Hoffman.

Hoffman recalls a recent flight where he sat directly behind a BlackBerry user who was organizing all of his passwords and entry codes.

"I could see everything through the seats," said Hoffman.

His point? Be discreet. Keep your private information private by taking care of business in a place where prying eyes can't see. And keep the conversations in front of people to a minimum. Besides risking a potential breach, you also risk annoying your neighbor.

**Keep it on you at all times.** This may sound like the most obvious piece of advice, but Hoffman says that most BlackBerry-related security problems begin with the owner misplacing his device.

"They are small and just left everywhere," he said.

Popular places for slip-ups and loss include bars and restaurants, where people place the gadget on a table or a bar, get into conversation and forget about it. This opens up not only the possibility that it will get left behind, but also the possibility that it will get stolen. Even a temporary theft can be damaging; the bad guy can obtain sensitive data or install a Trojan horse within a matter of seconds, said Hoffman.

**Have backup.** OK, so you didn't follow the last step and now you have no idea where your BlackBerry is. What can you do? It depends on whether you've prepared for this scenario.

If it's a corporate device and you work for a company with an enterprise BlackBerry server, contact IT immediately. They can remotely lock or wipe the device. If it is your personal BlackBerry, or if your company doesn't have that kind of support, you should have installed software that gives you that kind of capability. Investing in a program that gives you remote access means you can lock the device so others can't get into it. You can also back up the information you have stored on the BlackBerry and wipe it clean if you think it's gone for good.

If you invest in a remote access security system, said Hoffman, a lost device is simply a lost device, a piece of hardware. If you act quickly enough, you won't lose sensitive corporate data.

**Utilize encryption.** On devices from Research In Motion Ltd., [encryption is there](#), said Hoffman. Users simply need to activate it. But many, unfortunately, do not.

## Cybercrime: The 2009 megathreat

By Larry Ponemon

December 16, 2008 (CSO) The 2009 Security Mega Trends Survey was conducted by [Ponemon Institute](#) and sponsored by Lumension Security Inc. to better understand if certain publicized IT risks to personal and confidential data are, or should be, more or less of a concern for companies. We asked 577 IT security practitioners to consider how 10 security megatrends affect companies today and to predict their impact during the next 12 to 24 months. The opinions of these experts, we believe, will be helpful to companies that are struggling to understand how they should allocate resources to the protection of data during these difficult economic times.

We selected the following megatrends for this study based on input from a panel of experts in IT security. They are cloud computing, virtualization, mobility and mobile devices, [cybercrime](#), outsourcing to third parties, [data breaches](#) and the risk of identity theft, peer-to-peer file sharing, and [Web 2.0](#).

The study examined the risks posed by megatrends that exist today and how the risk will change over the next 12 to 24 months. According to an overwhelming 77% of experts in IT security responding to our survey, [cybercrime](#) will become a "high" or "very high" risk over the next 12 to 24 months.

The selection of [cybercrime as the megatrend](#) most likely to be a high or very high risk in the next 12 to 24 months can be partly based on the fact that 92% of respondents to our study reported that their companies have experienced a cyberattack. The biggest security risk associated with cybercrime is that such an attack will cause a business interruption followed by the theft of customer and employee data.

Other megatrends becoming more risky are cloud computing, malware, Web 2.0 and mobile devices. In the case of cloud computing, it is the inability to assess or verify the security of data centers in the cloud and protect sensitive and confidential information. IT security practitioners see the risk of malware and Web 2.0 as resulting in the loss of sensitive or confidential business information including trade secrets.

It is interesting to note that in our study, IT security respondents perceive the risk of a mobile workforce as decreasing but mobile devices remaining a high or very high risk for many companies. According to respondents, the most risky mobile device is the laptop computer, and the No. 1 concern is the inability to properly identify and authenticate remote users.

### **Data Breaches and Outsourcing Risks Continue**

Data breaches and outsourcing are forecast to remain at the same level of risk. IT security practitioners continue to worry about data breaches because, according to our study, only 16% are very confident or confident that current security practices are able to prevent customer and employee data from being lost or stolen. Therefore, it is understandable why the majority of respondents in IT security believe that data breaches will continue to pose a high and very high security threat to their organizations.

Because IT security professionals don't see the outsourcing of sensitive and confidential information to third parties as decreasing, it will remain a serious risk to an organizations' information assets. The concern expressed by IT security practitioners in our study is about the difficulty in protecting sensitive or confidential information when unauthorized parties might be able to access private files.

### **Certain Risks Are Considered More Manageable**

Becoming less of a concern are risks associated with a mobile workforce, virtualization and peer-to-peer file sharing. Although it seems that the mobile workforce will pose less of a risk, respondents believe the most significant security threat is the inability to properly identify and authenticate remote users. With respect to P2P, it is the concern that inadvertent transfers and disclosures of documents that reside on an organization's computers and laptops will occur. The most significant risk associated with virtualization technology is the inability to properly identify and authenticate users to multiple systems and to prevent third-party access to private files without authorization.

Organizations are faced with a plethora of security threats to their confidential and sensitive data assets. Forecasting the areas that pose the highest risk will help companies create an IT security strategy that is as cost-effective as possible in times of tightening budgets.

## **3 ways to protect yourself from social networking malware**

Spammers and virus creators have found a new path into your PC: social networks such as Facebook and MySpace.

### **By C.G. Lynch**

December 17, 2008 (CIO) As social networking tools change the way we communicate, spammers have begun turning their attention to services such as [Facebook](#) and [MySpace](#), tricking users into installing viruses, launching fraudulent Web sites and deploying malware throughout their computers and networks, according to [a new report by MessageLabs](#).

While spamming via e-mail services remains prevalent, "spammers see social networks as the new horizon," says Matt Sergeant, senior anti-spam technologist at [MessageLabs](#). Spammers have managed to set up phony social networking accounts, according to MessageLabs, by breaking the protections set in place by a safeguard known as [CAPTCHA](#) (Completely Automated Public Turing test to tell Computers and Humans Apart), the letters you normally have to type in when you register for a Web site in a box that says "Are you a human?"

Luckily, if you're wading in the social networking pool, you can revisit some core security principles in order to protect yourself from spammers and other characters on Facebook who can ruin your computer or identity, Sergeant says.

### **1. Re-do your password: It's probably not strong enough.**

Some cyber criminals have become remarkably good at obtaining social networking passwords through phishing schemes. Sergeant cites the case of a spammer in Canada who lured Facebook users into offering up their personal information to sign up for products offered by a fake company selling "male enhancement drugs."

In a lawsuit, which [Facebook won for an amount just shy of \\$900 million](#), the social network alleged that the spammer sent out four million spam messages from accounts in which he had obtained the passwords.

Sergeant says not only should users be wary of phishing schemes, but also of the fact that research indicates spammers are able to guess passwords. He suggests beefing up your password with unpredictable letters, phrases and numbers. At CIO, we recommend checking out [this helpful password how-to](#) from our sister site, [CSO Online](#).

### **2. Watch those third-party applications.**

Facebook has built an ecosystem of third-party applications, from games to widgets. But some apps have been shown to be completely fraudulent. Applications have been created to install malware on your computer and access your personal information (a right that third-party apps typically reserve to do on Facebook).

While Facebook does a good job of policing the site and dealing with app problems once they learn of them, the ecosystem is so big that it's hard to stop poor players, Sergeant says. So users must be educated and cautious about installing apps. In general, Sergeant says, watch for apps that bait you with learning a piece of information by clicking on a button (since this generally will initiate an install).

These apps tend to pander to basic human curiosities. A common example: "Jane has written some personal information about you! Click here to find how what she said!"

Remember that when you click to install an app like that, it not only puts your computer and network at risk, but also potentially sends the same invite out to everyone on your friend list.

### **3. Beware of user-generated spam.**

Social networks like Facebook rely on users to enrich the experience by posting content such as pictures and video (as well as links) and then sharing the content with their contacts. Spam-based social networkers will go to other people's comment threads, for instance, and chime in with links that, if clicked on, will install malware.

For example, if you post a news story, a spammer might comment, "I blogged about this and check out this link." This can be trickier to decipher than a spam-based e-mail, since the participant looks fairly genuine about participating in the discussion on the surface. In fact, the comment might be left with your friend's name on it if his or her account was hijacked.

"It enables spammers to post blog comments on the pages of other contacts and allows them to send messages from the phished accounts to other contacts," the MessageLabs report says.

In other words, if it doesn't sound like your friend who left the comment, it very well might not have been. Check with that person directly before you click on the link (especially if you don't recognize the URL as a household name).

## **Leaders Call for Bolder Security Agenda** **Government Computer News (12/12/08) ; Kash, Wyatt**

More needs to be done to improve federal IT security, said attendees at the recent Armed Forces Electronics and Communications Association conference on cyberspace challenges. Melissa Hathaway, the senior advisor and cyber coordination executive for the Director of National Intelligence, said the attention that is being paid to cyberattacks has resulted in more cooperation between the public and private sectors and more support for finding ways to deal with threats. However, Hathaway noted that there is still a long way to go to develop greater situational awareness, defend against cyberattacks, manage risks in the global supply chain, educate the public, and work with the private sector to protect against future attacks. Crucial Point CTO Bob Gourley said there are a number of existing strategies that the federal government can use to boost IT security, including improving

identity management, authentication, and insider threat modeling and analysis. But new tools, new tactics, and new techniques also need to be used "to detect, to mitigate, and then reflect" on the nature of attacks on federal IT networks, said Mischel Kwon, the director of operations for the U.S. Computer Emergency Readiness Team at the Department of Homeland Security. Bob Lentz, the deputy assistant secretary of Defense for information and identity assurance, said the security of federal IT systems also can be improved by fixing the government's "broken" acquisition process and improving the architecture of government systems.

## **CISOs Ponder New FISMA Requirements**

**Federal Computer Week (12/09/08) ; Bain, Ben**

Information security leaders are concerned that changes to the Federal Information Security Management Act (FISMA) might entail security departments to incorporate more compliance measures. The legislation, passed by the Senate Homeland Security and Governmental Affairs Committee in 2008, would revise how federal agencies' data security practices are judged and would place different criteria on CISOs. At the recent Government Technology Research Alliance conference of CISOs, participants discussed potential changes that could occur if the revised bill is passed, including mandatory annual third-party audits in place of a yearly evaluation; greater job demands for CISOs; involuntary operational evaluations; forming a CISO panel; requiring uniform contract language across all federal agencies; and requiring the Department of Homeland Security to prepare an annual report for Congress. One especially onerous aspect of the FISMA revision would require CISOs to oversee the IT security programs at all subordinate agencies and offices. "At a large department, I don't see how that would be effective or doable," says CISO Richard Prentiss of the Treasury Department's Office of Thrift Supervision.

## **Will Malware 2.0 Replace Web 2.0 in 2009?**

**ITPro (12/11/08) ; Wattanajantra, Asavin**

The new wave of online networking and sharing known as Web 2.0 has ushered in an accompanying batch of security threats experts are referring to as malware 2.0. The European Union's ENISA says that cross-site scripting and other Web 2.0 vulnerabilities have enabled the rise of new forms of malware that can attack a user's computer without the user having to perform any action. One reason so many security holes are springing up is because businesses are moving quickly to update their Web offerings to meet demands, says ENISA analyst Giles Hogben. "Web 2.0 applications are pushing existing Web technologies to their limits--as a result, even the best developers have had to resort to 'hacks' and loopholes in the system to make their applications work," Hogben says. He adds that malware installations have become so popular as to spawn an underground market of "malware as a service."

## **The Web Is More Dangerous, and the U.S. Is Biggest Culprit**

**Government Computer News (12/10/08) ; Jackson, William**

The United States is the world's biggest source of cyberthreats, concludes a recent Sophos report. The report says that the U.S. was the source of 37 percent of the world's online malware and more than 17 percent of the world's spam. China was the second largest source of online malware, accounting for roughly 30 percent of the world's total, the report says. In addition, the report notes that the increased use of automated hacking is making it easier for cybercriminals to take advantage of the vulnerabilities in Web sites. A separate report from WhiteHat Security found that 82 percent of Web sites contain at least one security vulnerability, and noted that 63 percent of Web sites have vulnerabilities rated at high, critical, or urgent severity. Sophos' Graham Clulely says that more and more cybercriminals will try to exploit these vulnerabilities as the economy worsens. "As we enter 2009, we are not expecting to see these assaults diminish," he says. "As economies begin to enter recession, it will be more important than ever for individuals and businesses to ensure that they are on guard against Internet attack."

## Critical security projects escape the budget ax

Old notion: In tight times, table or trim back all projects. New order: Move forward. To delay is to lose out on savings and innovation.

By Stacy Collett

December 30, 2008 (Computerworld) Leslie Lambert, vice president and chief information security officer at [Sun Microsystems Inc.](#), returned from a three-week business trip to India with a few souvenirs and a whole new set of IT security priorities for 2009.

India is home to 29 of Sun's 250 managed services providers. Economic troubles there have made it harder for those providers to build out their data centers, so they're procuring services from other providers around the globe.

"I'm going to be shifting focus," Lambert says. In 2009, projects like server security, metrics, application security and Web security will likely take a back seat to new data-protection measures and deeper enhancement of user-access and identity management systems. "Those are the big hitters now," she adds. In a steadier economy, all of the projects would likely have gone ahead, she says.

Indeed, security remains a top priority for all companies -- with antivirus, encryption and identity management topping the list for *Computerworld's* Forecast survey respondents. But with economic uncertainty overshadowing most IT budgets, managers will have to pick and choose the projects that are most important.

The U.S. Tennis Association (USTA) is a prime example. The organization generates 85% of its revenue in just two weeks in late summer during the U.S. Open tennis tournament, and with so much riding on one event, the IT staff can't afford any security snafus. So when CIO Larry Bonfante decided the USTA would need to upgrade its network access control system to protect the network from contaminants brought in by 800 media members using its Web site, the project got a green light, despite a flat budget.

"Anything that can impact revenue, the fan or customer experience, or the game of tennis is considered business-critical," Bonfante says. Still, "all projects are certainly under significant scrutiny to make sure there's a tangible return on investment before we get funding for them. Security projects are no different in that regard."

Law firm Nexsen Pruet LLC plans to overhaul its intranet in 2009. Among other things, the upgrade will enable the system to grant users access to financials and reports according to their security levels. Despite the tough economy, the project will move forward, but at a slower pace than originally planned. "Increasing overall organizational efficiency and productivity sometimes means increasing spending for technology infrastructure and key applications," says Technology Director John E.C. Davis.

### Keeping your guard up

Projects that "keep the bad guys out" are usually the most recession-proof, says [John Pescatore](#), an analyst at [Gartner Inc.](#) But spending for projects that "let the good guys in" is often tied to business cycles.

### Bright Spot

Gartner's John Pescatore sees coming IT security challenges as an opportunity. "In these tough cycles, we have a chance to change the way we're doing things -- not just take chances, but change everything and try to reduce how much you're spending on security."

"If there's a new business project to open up new services and products, there's a lot of security spending in identity and access management," says Pescatore. "But in 2009, that's probably the area we'll see get hit," creating a growing potential for security leaks.

Worst-case scenario: Companies could stop allowing employees to use their home PCs, laptops or iPhones for business use if identity and access management systems aren't in place. But Pescatore says that's not likely, again because of the economy.

"Some will reverse the privilege," most likely in government and financial sectors, he says. "But the majority of companies may say, 'If you use your home PC, we don't have to buy you one, and that will save us money.'" Some businesses might even consider letting workers use their own software, such as Google Apps.

"In businesses that are really under cost pressure, they may be very tempted to take the security risk to use these cheaper consumer alternatives," Pescatore adds.

The financial meltdown may also spark more regulations to address financial wrongdoing this year, which could in turn drive spending on reporting tools. While the new regulations may affect only financial firms, as opposed to every publicly traded company, "there may be a push for new risk reporting directly to the government," Pescatore says.

## **Getting Compliant**

In the meantime, companies in many industries will be working to comply with legal and regulatory mandates that protect private, sensitive information.

For instance, utilities have mandates from several regulatory bodies requiring them to secure SCADA -- supervisory control and data acquisition -- systems and industrial control tools that monitor processes. In the financial services sector, smaller banks are moving toward dual authentication to meet [FDIC](#), Federal Financial Institutions Examination Council and Basell II standards. And retailers must meet payment-card industry requirements.

"Information security is non-negotiable for these organizations," says Jeff Bernstein, senior director of information assurance at Asero Worldwide Inc. in Washington. "For IT purchases such as hardware and software, there will probably be some suffering. But meeting internal and external security requirements" won't be compromised, he adds.

Industry-watchers worry that postponing some IT security projects could lead to risky business behaviors -- especially with pesky new botnets infecting the most secure enterprises. "If I don't look for [malware], I'm not going to incur the expense of doing anything about them," Pescatore says.

[The Procter & Gamble Co.](#) has invested heavily in IT security, yet in 2007 it found that 4% of its PCs were compromised by botnets, according to a [Gartner case study](#). To fix the problem, P&G had to reimage most of the 3,000 PCs -- an expensive task.

But dealing with a breach is more expensive than preventing one, Pescatore says. An incident where information on 100,000 customers is exposed typically costs an enterprise \$10 million to \$15 million to fix, excluding damage to the brand name. But preventing a data leak costs \$3 million to \$5 million.

And with layoffs looming in all sectors, Gartner expects more companies to consider outsourcing some security functions. Also expect companies to turn to "security as a service" to help reduce software, management and maintenance costs and lower in-house power and cooling costs.

"Over five years, it may cost you more," Pescatore says, "but in 2009, it will cost you less."

## What can you afford NOT to do on IT security?

There may be some security projects you can put off because of the recession -- without risking your company's data or reputation.

**By Jaikumar Vijayan**

December 22, 2008 (Computerworld) With the [ailing economy](#) putting a crimp in IT budgets, information security managers -- like just about everyone else in the tech world -- are feeling pressure to keep their costs in line.

Few expect to be hit with outright budget reductions, at least in the short term; regulatory requirements and the ever-expanding list of external and internal threats make it hard to devote less money to [security efforts](#). But there is a growing push to curb or defer spending increases, according to IT managers and security analysts.

"It's imperative to squeeze every penny of value out of everything you do," said Jim Kirby, senior network engineer at DataWare Services, an IT services firm in Sioux Falls, S.D. This is a good time to stop working on "marginal" projects and redirect resources to security capabilities that are absolutely necessary, Kirby said.

[Matt Kesner](#), chief technology officer at [Fenwick & West LLP](#) in San Francisco, said the law firm's security strategy for next year is to "focus on basics." Its 2009 IT budget doesn't call for reduced spending on security -- but neither does it include a funding increase.

And Fenwick & West is taking some steps to cut costs. The firm is deferring an earlier plan to hire a full-time networking and security expert because of the recession, Kesner said. It is also looking for opportunities to use open-source alternatives to some of its security tools.

One of the few new IT projects approved for next year is a replacement of the antivirus software installed on all of the law firm's PCs -- an upgrade that Kesner said is being driven by the increased threats to corporate data from malware and phishing attacks. Fenwick & West also plans to train end users more intensively on how to secure their PCs and mobile devices, and on the importance of creating strong passwords.

Even in an economy gone sour, a growing number of government and industry regulations impose security compliance costs that there is simply no getting away from. For instance, new data-protection laws in states such as Massachusetts, Connecticut and Nevada require companies to use data encryption tools and implement other security controls to safeguard the personal information of state residents.

Similarly, the Payment Card Industry Data Security Standard, created by the major credit card companies, requires all businesses that accept credit and debit transactions to adopt a broad set of data protection controls. And the federal HIPAA law includes data security and privacy rules for health care providers in order to protect patient information.

Meanwhile, [cybercrooks](#) are targeting companies with increasingly sophisticated -- and successful -- attacks. For example, Symantec Corp. said in a report last month that at least \$1.7 billion worth of bank accounts were compromised in the U.S. during the 12-month period that started in July 2007.

In light of all that, not making cutbacks in antivirus subscriptions and purchases of frontline security tools such as firewalls and network intrusion-detection systems is a no-brainer, security managers said.

Kirby said investments in outbound-traffic inspection tools and controls for locking down portable media devices also are worthwhile because of the heightened risk of insider attacks at a time of increased layoffs. In addition, he thinks that cutting back on disaster recovery and business continuity projects wouldn't be wise.

Whittling away at risk management and compliance oversight functions is another bad idea, said the chief privacy officer (CPO) at a large financial services firm. That could leave companies facing potentially serious consequences for not complying with security requirements, he said.

## What to Cut

But there are other areas in which IT and security managers may be able ease up on spending. Kirby said that although intrusion-detection systems are a must-have item, many companies can live without intrusion-prevention tools, which are more sophisticated but also more expensive and harder to manage. He added that biometric security projects can often be postponed.

Paring back on third-party security education and training programs can also yield some extra dollars that can be used for other purposes, said the CPO, who asked not to be identified. "Companies have a lot of vendor-hosted or vendor-provided education programs -- kind of, 'Here's how you do data security if you're covered by HIPAA or by PCI,' " he said. According to the CPO, the cost of individual programs can sometimes top \$200,000 annually, depending on the number of employees being trained.

Marcin Czabanski, director of IT at LifeSecure Insurance Co. in Brighton, Mich., said companies should also look for ways to move applications -- and their security functions -- into the [computing clouds](#) offered by vendors such as [Google](#), Microsoft and Amazon.com.

By doing so, Czabanski said, "you can outsource a lot of the headache" of managing and securing desktop applications -- and do so for less money than keeping the work in-house.

E-mail is another application that can move to the cloud. The Henssler Financial Group in Kennesaw, Ga., is a user of Google's Postini e-mail security and archiving services. Tim O'Pry, Henssler's chief technology officer, said the arrangement has enabled the financial services firm to offload to Google the hassle and expense of securing its e-mail system.

In addition, using the [hosted services](#) has "dramatically" reduced Henssler's e-mail archiving costs while making it easier for employees to search for and retrieve old messages, O'Pry said.

Moving e-mail to a cloud infrastructure such as Google's can also help organizations lower the costs of complying with e-discovery rules in legal cases, said David Jordan, chief information security officer for Virginia's Arlington County.

For instance, Google earlier this year launched a Postini service called Message Discovery that is designed to help businesses comply with e-mail retention regulations and speed up the process of retrieving messages in response to lawsuits or other legal matters. Such setups can also help customers trim their e-mail hardware, software, management and security costs, Jordan said.

Another possible cost-saving option, he noted, is deploying virtualization and thin-client technologies that let employees access a set of centralized applications. Jordan said he thinks that thin-client architectures are inherently more secure -- and thus less costly to manage and control -- than traditional client/server computing models.

Any cutbacks should be carefully weighed, though.

Phil Hochmuth, an analyst at Yankee Group Research Inc., said it's understandable that companies might want to rein in their security spending. But on a longer-term basis, "it would probably be a mistake if they backed off strategic initiatives" just to cut costs now, Hochmuth said.

O'Pry agreed. "Trying to scrimp and save on security in this economy would be a penny-wise, pound-foolish thing to do," he said. O'Pry noted that as a financial services firm, Henssler is "affected more than anyone else" by the downturn. Even so, there's little talk within the company about cutting security spending. "Your most valuable nontangible asset is your reputation," O'Pry said. "You can't risk taking any hits to that."

## Small laptops pose a big security threat

Ultraportables forgo size, weight, power -- and security.

**By John Edwards**

December 22, 2008 (Computerworld) They're highly portable, inexpensive, very popular -- and a potential security nightmare. Running against the trend of mobile computers featuring progressively larger processors, memory, storage, screens and price tags, [ultraportable laptops](#) promise to streamline and simplify their users' lives. [Easy to carry](#), capable of running only a handful of modest applications and affordably priced, ultraportables have emerged over the past year or so to become one of the [hottest mobile computing trends](#).

Pioneered by Taiwanese PC maker [Asustek Computer Inc.](#) with its [Eee PC](#) and now also available from vendors such as [Dell](#), [Hewlett-Packard](#) and Fujitsu, ultraportables are designed to appeal to users who need portable systems with more power and functionality than a smart phone but don't want to lug a conventional laptop through offices, hotels and airports.

"It's a technology with great appeal to many people," observes Gabriel Vitus, IT director at the Certified General Accountants' Association of Canada, a trade organization in Vancouver, British Columbia.

That small package comes with built-in compromises, however. Ultraportables typically feature a processor that lags at least a generation or two behind the CPUs included in traditional laptops, a few gigabytes of solid-state memory and storage, a squeezed-down display and a cramped keyboard. But another characteristic of the new portable pipsqueaks is striking fear into the hearts of a growing number of IT managers: security weaknesses that are directly attributable to the machines' diminished technology.

"This is a threat that IT managers are just beginning to recognize," says Brian Wolfe, a security analyst at Lazarus Technologies Inc., an IT consulting service in Itasca, Ill.

### Reduced Resources

Minimized hardware resources force ultraportables -- and their users -- to cope with weakened system software. Most models ship with a stripped-down Linux operating system or, in some cases, Microsoft Corp.'s previous-generation operating system, Windows XP. Newer and more capable operating systems, which also tend to have the latest internal security safeguards, demand processing and storage power that ultraportables typically lack, Wolfe notes.

"The machines are often sent out into the world with little or no protection. "

Brian Wolfe, security analyst, Lazarus Technologies

Ultraportables' reduced resources also limit their ability to run add-on security software, such as data encryption and anti-malware tools. With processing power, internal memory and storage space all at a premium, it can be difficult -- sometimes impossible -- to squeeze security software onto an ultraportable. "As a result, the machines are often sent out into the world with little or no protection," Wolfe says.

Vendors' use of dated software can also make ultraportables more susceptible to various malware. Earlier this year, for example, Brazilian security firm Rise Security released an alert that showed that old, unpatched Samba code found on the [Eee PC](#) allowed the machine to be subverted ("rooted") right out of the box. Such vulnerabilities allow hackers to remotely gain complete control over the systems.

Other key security features are often absent on ultraportables. "Many, if not most, [ultraportables] are sold without Trusted Platform Modules because they are targeted at the consumer market," says [Rob Enderle](#), an analyst at Enderle Group in San Jose. "This means they either don't have encryption solutions or the solutions aren't that robust."

Enderle also notes that most ultraportables aren't designed to be managed centrally and therefore can't have their solid-state drives remotely wiped clean of data in the event of loss or theft.

## Ultra Invaders

The number of ultraportables acquired by enterprises remains small, at least compared with conventional laptops, notes Wolfe. Still, many IT managers are discovering that some employees are starting to take their machines into the office and along on business trips. This trend is raising security concerns, he says.

Ultraportables' built-in Wi-Fi and USB connectivity makes moving data from enterprise systems onto the machines relatively simple, says Christopher Ciabarra, founder and president of Los Angeles-based security software firm Network Intercept LLC.

Ultraportables' wireless capabilities also make it easy for them to disgorge stored data to unauthorized parties. Ciabarra believes that Wi-Fi vulnerabilities are a potentially big problem. "Everywhere an ultraportable goes, it can be logging into networks and exposing its data," he says. "The user often isn't even aware this is happening."

To protect against this kind of exposure, he recommends that IT secure Wi-Fi networks and enforce password access to the devices.

Christine Leja, CIO at Southwestern Illinois College in Belleville, Ill., says her school's students are always experimenting with new gadgets, including ultraportables, forcing her to keep a step ahead of potential threats. "Every year brings something new, it seems," she says.

Students don't have access to enterprise data, so the biggest perils Leja faces are from Wi-Fi intruders and malware, which ultraportable users can inadvertently introduce into the university's system. "We protect against this by operating a secure, closed network that students and employees have to log into," she says.

### Small Notebooks Growing

Worldwide ultra-low-cost notebook shipments forecast:

2008: 11 million

2009: 21 million

2010: 29 million

2011: 36 million

2012: 41 million

Source: IDC, 2008

The network is also compartmentalized into virtual LANs that serve various classroom, business and general-purpose applications, helping to limit any breaches. Furthermore, employees transmitting sensitive data are required to use cellular 3G networks, which Leja says are more secure than Wi-Fi connections. "We think that's a smart move when dealing with all types of mobile devices," she says.

Ultraportables' toylike appearance and size may cause some users, at least on a subliminal level, to let down their guard when it comes to security. "In some ways, the machines don't look like a 'real' computer, so it may lead to people being less protective of them," Ciabarra says.

Moreover, a smaller laptop may be easier to misplace than a full-scale laptop. "Look at the number of people who leave their cell phones in taxis and airport lounges," Vitus says. "An ultraportable isn't all that much larger."

The systems' compact size may also appeal to thieves, Enderle says. "This class of product is particularly easy to steal because it is very easy to conceal," he says. "It is also very desirable, which suggests it will be easy to sell as well."

## Building a Strategy

Although ultraportables pose a variety of unique security challenges, the risks can be contained and managed by extending and expanding existing laptop security practices. On the wireless front, conventional Wi-Fi security protocols and access controls should be adequate to deal with threats to enterprise data from ultraportables and other emerging wireless-enabled devices, Vitus says. "It doesn't matter what device they're using; they can't get into our network unless we want them to," he says.

When ultraportables are used off-premises as an extension of a company's technology, however, the challenge grows more serious. If storage encryption can't be used, an alternate data-protection technique should be adopted. Enderle says that critical data should never be stored inside an ultraportable. Instead, any data should be accessed from a secure remote repository to avoid the possibility of infecting enterprise systems.

Another option for protecting sensitive documents, Enderle says, is to use a secure flash drive, such as IronKey, that is itself protected and stays with the employee. That way, if the laptop is stolen, the sensitive data doesn't go with it -- the data always remains on the secured flash drive.

But the best protection of all, Enderle notes, is prevention. "Most [enterprise] data should not be on a device in this class anyway," he says.

Employee education in acceptable-usage practices is a must, regardless of the IT security systems used, Enderle says.

### **Have your say**

Leja agrees. "You have to count on continual security awareness," she says. "Make sure that [students or employees are] being conscientious, and then use the few tools that do exist to help."

The worst approach any IT manager can take is to ignore the threat ultraportables pose. "Even if you haven't yet encountered any of these machines," Wolfe says, "you probably eventually will."

## **Social Engineering: Eight Common Tactics**

***Stealing your company's 'hold' music, spoofing caller ID, pumping up penny stocks - social engineers blend old and new methods to grab passwords or profits. Being aware of their tricks is the first line of defense.***

By [Joan Goodchild](#), Senior Editor

November 06, 2008 — [CSO](#) — Famous hacker Kevin Mitnick helped popularize the term 'social engineering' in the '90s, but the simple idea itself (tricking someone into doing something or divulging sensitive information) has been around for ages. And experts say hackers today continue to steal [password](#), install [malware](#) or grab profits by employing a mix of old and new tactics.

Here's a refresher course on some of the most prevalent social engineering tricks used by phone, email and Web.

### **1. Ten degrees of separation**

The number one goal of a social engineer who uses the telephone as his modus operandi is to convince his target that he is either 1) a fellow employee or 2) a trusted outside authority (such as law enforcement or an auditor). But if his ultimate goal is to gain information from or about employee X, his first calls or emails might go to a different person.

The old game of six degrees of separation has a few more layers when it comes to crime. According to Sal Lifrieri, a 20-year veteran of the New York City Police Department who now educates companies on social engineering tactics through an organization called Protective Operations, there might be ten steps between a criminal's target and the person he or she can start with in the organization.

"In my educational sessions, I tell people you always need to be slightly paranoid and anal because you never really know what a person wants out of you," said Lifrieri. The targeting of employees "starts with the receptionist, the guard at the gate who is watching a parking lot. That's why training has to get to the staff. The secretary or receptionist criminals start with might be ten moves away from the person they want to get to."

Lifrieri says criminals use simple ideas to cozy up to more accessible people in an organization in order to get information about people higher up in the hierarchy.

"The common technique [for the criminal] is to be friendly," said Lifrieri. "To act like: 'I want to get to know you. I want to get to know stuff that is going on in your life.' Pretty soon they are getting information you wouldn't have volunteered a few weeks earlier."

## **2. Learning your corporate language**

Every industry has a short hand, according to Lifrieri. A social engineering criminal will study that language and be able to rattle it off with the best of them.

"It's all about surrounding cues," he said. "If I'm speaking a language you recognize, you trust me. You are more willing to give me that information I'm looking to get out of you if I can use the acronyms and terms you are used to hearing."

## **3. Borrowing your 'hold' music**

Successful scammers need, time, persistence and patience, said Lifrieri. Attacks are often done slowly and methodically. The build-up not only includes collecting personal tidbits about people, but also collecting other "social cues" to build trust and even fool other into thinking they are an employee when they are not.

Another successful technique involves recording the "hold" music a company uses when callers are left waiting on the phone.

"The criminal gets put on hold, records the music and then uses it to their advantage. When he or she calls the intended victim, they talk for a minute and then say "Oh, my other line is ringing, hold on," and put them on hold. "The person being scammed hears that familiar company music and thinks: 'Oh, he must work here at the company. That is our music.' It is just another psychological cue."

## **4. Phone-number spoofing**

Criminals often use phone-number spoofing to [make a different number show up on the target's caller ID](#).

"The criminal could be sitting in an apartment calling you, but the number that shows up on the caller ID appears to come from within the company," said Lifrieri.

Of course, unsuspecting victims are more than likely to give private information, like passwords, over the phone if the caller ID legitimizes it. And, of course, the crime is often undetectable after because if you dial the number back, it goes to an internal company number.

## **5. Using the news against you**

"Whatever is going on in the headlines, the bad guys are using that information as social engineering lures for spam, phishing and other scams," said Dave Marcus, director of security research and communications for McAfee Avert Labs.

Marcus said Avert has seen a rise in the number of [presidential campaign-related](#) and economic crunch-based spam emails lately.

"There have been a bunch of phishing attacks related to banks being bought by others," said Marcus. "The email will say 'Your bank is being bought by this bank. Click here to make sure you update information before the sale closes.' It's an attempt to get you to release your information so they can log into your account to either steal your money or sell your information to someone else."

## **6. Abusing faith in social networking sites**

Facebook, Myspace and Linked In are hugely popular social networking sites. And people have a lot of faith in them, according to Marcus. A recent spear-phishing incident targeted Linked In users, and the attack was surprising to many. Marcus said, increasingly, social networking devotees are being fooled by emails that claim to be from sites like Facebook, but are really from scammers.

"They will get an email that says: 'The site is doing maintenance, click here to update your information.' Of course, when you click on the link, you go to the bad guys' site." Marcus recommends advising employees to type Web addresses in manually to avoid malicious links. And also to keep in mind that it is very rare for a site to send out a request for a password change or an account update.

## 7. Typo Squatting

On the Web, bad guys also bank on the common mistakes people make when they type, according to Marcus. When you type in a URL that's just one letter off, suddenly you can end up with unintended consequences.

"Bad guys prepare for typing mistakes and the site they prepare is going to look a lot like the site you thought you were going to, like Google."

Instead of going where they wanted, unsuspecting users who make typing mistakes end up on a fake site that either intends to sell something, steal something, or push out malware.

**8. Using FUD to affect the stock market** The security and vulnerabilities of products, and even entire companies, can make an impact on the equities market, according to new research from Avert. Researchers studied the impact of events such as Microsoft's Patch Tuesday on the company's stock and found a noticeable swing each month after vulnerability information was released.

"Publicly-released information has an effect on stock prices," said Marcus. "Another recent example is the fake information that was circulated a few weeks ago about Steve Jobs' health. Apple stock took a dive on that. That is a clear example of someone inserting FUD and [a resulting effect on a stock](#)." Presumably the culprits held a 'short' position which allowed them to profit from this trick.

The converse approach is to use email to execute the ancient 'pump-and-dump' tactic. A scammer can buy a large volume of a penny stock, the blast out emails under the guise of an investment advisor touting that stock's great potential (that's the 'pump'). If enough recipients of this spam email rush to buy the stock, the price will spike upward. The scammer then quickly 'dumps' his shares at a great profit.

## Hacking US is Big Business in Russia

**December 26, 2008**

Chicago Tribune

MOSCOW -- Not long ago, the simple, anonymous thrill of exposing chinks in American software was enough of a payoff for a Russian hacker.

Today it's cash. And almost all the targets are in the United States and Europe, where Russia's notorious hackers pilfer online bank accounts, swipe social security numbers, steal credit card data and peek at e-mail log-ins and passwords as part of what some estimate to be a \$100 billion-a-year global cyber-crime business.

And when it's not money that drives Russian hackers, it's politics -- with the aim of accessing or disabling the computers, Web sites and security systems of governments opposed to Russian interests. That may have been the motive behind a recent attack on Pentagon computers.

A new generation of Russian hacker is behind America's latest criminal scourge. Young, intelligent and wealthy enough to zip down Moscow's boulevards in shiny BMWs, they make their money in cyber-cubbyholes that police have found impossible to ferret out.

From behind the partition of anonymous online hacking forums, they boast about why they use their programming savvy to spam and steal, mostly from the West.

Other times it's politics, with the goal of accessing or disabling the computers, Web sites and security systems of governments opposed to Russian interests -- the possible motive behind a worrisome hacking of Pentagon computers recently.

A new generation of Russian hacker is behind America's latest criminal scourge. They are intelligent, talented twentysomethings who make their money in cyber cubbyholes almost impossible for the police to ferret out, and who zip down Moscow's boulevards in shiny BMWs.

However elusive, they can be heard from behind the partition of online hacking forums boasting of why they use

their programming savvy to spam and steal, mostly from the West.

"Why should I take a regular job after graduating and exert myself to earn just \$2,000 a month, rather than grab this chance to make money?" says a Russian hacker on a cyber-crime forum that specializes in credit card fraud. "It makes sense to get as much as you can, as quickly as possible, rather than wasting time working for someone else."

Cyber-crime, by some estimates, has outpaced the amount of illicit cash raked in by global drug trafficking. Hackers from Russia and China are among the chief culprits, and the threat they pose now extends far beyond spam, identity theft and bank heists.

Besides the recent attack on computers at the U.S. Defense Department, which may have originated in Russia, according to military leaders in Washington, Russian hackers also are believed to be behind highly coordinated attacks that brought down government Web sites in Estonia in 2007 and in U.S.-allied Georgia when war broke out between Russian and Georgian forces in August.

They're even suspected of hacking into the computer systems of Barack Obama and John McCain during the presidential campaign; technical experts hired by Obama's campaign suspected the attacks may have come from Russia or China, according to Newsweek.

So far there has been no evidence of a link between the Russian government and any of the attacks on American, Georgian and Estonian Web sites and computers. Russian authorities denied any involvement in the Georgian and Estonian attacks, and they recently said that speculation about a Russian link to the attack on U.S. Defense Department computers was "groundless" and "irresponsible."

Nevertheless, the need to ramp up security of American cyberspace is being discussed with greater urgency in Washington. Earlier this month, a commission on cyber-security delivered a report to Congress calling for the creation of a new White House office that would gird the United States against computer attacks from hackers and foreign governments.

According to the commission, "unknown foreign entities" in 2007 hacked computers at the Departments of Defense, Homeland Security and Commerce, as well as NASA. Hackers broke into Defense Secretary Robert Gates' unclassified e-mail and probe Defense Department computers "hundreds of thousands of times each day," said the commission, a panel of leading government and computer industry experts.

A senior State Department official told the commission that the department had lost thousands of gigabytes of data due to computer attacks, and among the Homeland Security divisions reporting computer break-ins was the Transportation Security Administration, which provides airport security. Hacking attacks compromising intellectual property have cost U.S. companies billions of dollars, the report stated.

"The damage from cyber attack is real," the report continued. "Ineffective cybersecurity, and attacks on our informational infrastructure in an increasingly competitive international environment, undercut U.S. strength and put the nation at risk."

After the Soviet collapse in 1991, Russian hackers were primarily motivated by mischief. They crafted viruses and worms simply for the delight of revealing weaknesses in security systems and software.

"Back then, it was simple hooliganism," said Vladimir Dubrovin, a hacker in the late 1990s and now a Russian computer security expert.

Today, however, most hackers in Russia are in it strictly for the money. Cyber-crime gangs approach computer programming graduates from Moscow's technical universities with offers of making sums of \$5,000 to \$7,000 a month, a far cry from Russia's average monthly salary of \$640, says Nikita Kislitsyn, editor of Hacker, a glossy Russian magazine with how-to information for budding hackers.

Yevgeny Kaspersky, chief executive of Moscow-based Kaspersky Lab, one of the world's leading computer security firms, says Russian hacking flourishes as "a cyber-criminal ecosystem" of spammers, identity thieves and "botnets," vast networks of infected computers controlled remotely and used to spread spam, denial-of-service attacks or other malicious programs. A denial-of-service attack floods a Web site with inquiries, forcing its shutdown.

To pry online bank accounts, Russian hackers rely on viruses that record keystrokes as customers type log-ins and passwords. Russian-made viruses are believed to be behind several major online heists, including the theft of \$1 million from Nordea Bank in Sweden in 2007 and \$6 million from banks in the United States and Europe that same year.

The huge amount of money cyber-crime generates has created a vast underworld market that so far has proved to be virtually impregnable by Russian police. Viruses and other types of so-called "malware" are bought and sold for as much as \$15,000, Kislitsyn says. Rogue Internet service providers charge cyber-criminals \$1,000 a month for police-proof server access.

Botnets relied on for cybercrime can also be used to lash out at political enemies, computer security experts say. Most analysts agree that criminal botnets were used by Russian hackers to shut down Estonian government and banking Web sites after the tiny Baltic republic angered Russians by moving a Soviet war memorial from downtown Tallinn in 2007.

In countries such as Russia and China, where criminal botnets are highly developed, such a resource could evolve into a potent cyber-warfare weapon, experts say.

"The Internet can now be used to attack small countries," Kaspersky said. "There are Russian and Chinese hackers that have the power to do that."

Russian police departments have cyber-crime divisions, but arrests of major cyber-criminals are rare.

"It comes down to a question of volume," said Steve Santorelli, investigations director at Team Cymru, a Burr Ridge, Ill.-based Internet security research firm. "In Russia, there simply aren't the resources."

## **Survey: Collaboration Applications Inadequately Secured** **SC Magazine (12/18/08) ; Moscaritolo, Angela**

Many of the collaboration applications businesses use to facilitate communication and activity among workers, including Web-based intranet portals, Microsoft SharePoint, and common Internet file systems (CIFS) lack sophisticated security features, concludes Rohati in its recent survey of 117 CISOs, CIOs, and IT leaders. More than 50 percent of the security leaders surveyed said their businesses rely on collaboration applications. Of those, 71 percent said they are not proactively securing information that passes through these platforms. Rohati's Shane Buckley says almost every organization is likely to have at least one application that does not meet regulatory compliance requirements. "The question is if your risk profile is increasing as you go forward," he notes. "As the collaborative devices are being rolled out, the risk profile is increasing." About 40 percent of those surveyed said the risk of malicious users accessing sensitive data was the chief concern pertaining to collaboration applications. Twenty-nine percent were worried that application vulnerabilities would lead to a data breach, and 14 percent said they were most concerned about the internal abuse of data found on collaboration applications.

## **Spam Trends for 2009; What to Look Out For** **Computerworld Canada (12/16/08) Smith, Briony**

Cisco Systems' 2008 Annual Security Report holds discouraging results for security experts: Virtualization vulnerabilities almost tripled to 103 over a period of 12 months, and threats springing from legitimate Web sites increased by 90 percent, nearly double the growth rate in 2007. The report says nearly 5 percent of the world's

spam originates in Canada, and the volume of reputation hijacks, where one person hacks into another person's account and uses it as a base for attack, is also on the rise. In the upcoming year, the primary IT threats will likely occur on the mobile platform, and internally at the hands of errant employees. Insider threats will increase especially if economic conditions continue to slip, says Cisco's Patrick Peterson. Info-tech Research Group analyst Candice Low suggests applying "the principle of least privileges," or restricting access to sensitive data to certain employees. As more employees being working remotely or on flexible schedules, it will also become vital to protect the network with updated patches, encryption, and antivirus software, Low adds.

## **Wireless VPNs: Protecting the Wireless Wanderer**

**CSO Online (12/15/08) ; Wheatley, Malcolm**

Although laptop users might have the assumption that they are safe from cyberthreats when using virtual private networking (VPN) to log on to their organization's network, the technology does not provide them with as much security as they might think. "People tend to fixate on the word 'private' in virtual private network," says security instructor Jeremy Cioara. "They're sitting in Starbucks working at their laptop, and they think that because they're using a VPN, it's safe. It isn't." However, there are a number of steps CISOs and CSOs can take to make VPNs safer for their employees. For instance, VPN wireless access can be secured by using a combination of tokenless, two-factor authentication systems. In such a system, pass codes can be sent to a wireless device, such as a Blackberry, instead of a token that could get lost. When users want to log on to the organization's network, they enter their username, their log-on password, and their combined personal PIN code and pass code. Other steps that can be taken include switching off the parallel connection in the VPN client so that the only way to access the Internet is through the corporate network.

## **Serious About Security**

**InformationWeek (12/08/08)No. 1214, P. 24 ; Ely, Adam**

Although developers, businesses, and users like the features and benefits of using cloud computing, IT security professionals have several concerns about the use of the technology. For instance, many IT security professionals remain unsure of how to securely move applications and data to the cloud. In addition, some IT security professionals are concerned that using cloud computing could delay efforts to consolidate identity management technologies and processes by a decade. But some cloud vendors are beginning to address some of the concerns IT security professionals have with cloud computing. Nevertheless, analysts say IT security professionals should not rely solely on the security measures taken by cloud vendors. They also should be proactive by asking cloud vendors about how they perform backups, if their backups are tested, and where their backed up data is stored, among other things.

## **U.S. Not Ready for Cyber Attack**

**Reuters (12/19/08) ; Mikkelsen, Randall**

The results of a two-day cyberwar simulation involving 230 representatives from U.S. government defense and security agencies, private companies, and civil groups found that the United States is not prepared to defend itself against a major hostile attack against its computer networks. The war game simulated a surge in computer attacks during a time of economic vulnerability, and challenged participants to find a way to mitigate the attacks using real-life knowledge of tactics and procedures. The exercise took place almost a year after President Bush launched a cybersecurity initiative aimed at improving U.S. computer defenses. "There isn't a response or a game plan," says Mark Gerencser from Booz Allen Hamilton, which ran the simulation. "There isn't really anybody in charge." U.S. Rep. James Langevin (D-R.I.) says that a successful attack could cause the U.S.'s banking or national electrical systems to fail. Both the government and industry need to invest billions of dollars to improve security, says U.S. Rep. Dutch Ruppersberger (D-Md.). Homeland Security secretary Michael Chertoff told participants that cyberattacks will become a routine warfare tactic to damage command systems in preparation for a traditional attack, and that international law and military doctrines need to be updated to address cyberattacks.

## States hope feds will help replace legacy systems

By Patrick Thibodeau

January 5, 2009 (Computerworld) With [President-elect Barack Obama](#) proposing to spend billions of dollars on road and bridge projects as part of his economic stimulus plan, some state CIOs are hoping that their aging IT infrastructures might also qualify for makeovers.

There's a lot that needs to be updated. In an online survey of state CIOs conducted last summer by the [National Association of State Chief Information Officers](#), nearly two-thirds of the 29 respondents said that between 40% and 80% of their IT setups consisted of legacy systems. And many reported that they were still running code written 20 or more years ago.

Kyle Schafer, West Virginia's chief technology officer and co-chairman of a NASCIO working group that wrote a report based on the survey results, plans to replace 92 long-used applications with an ERP system at an estimated cost of \$40 million to \$60 million.

One of the selling points was lower operating costs. Schafer said that based on benchmarking done by a consulting firm, it costs West Virginia \$33 to process an invoice, while states with modern ERP systems have an average processing cost of about \$8.

West Virginia has a budget surplus, but many other states are facing deficits. Schafer said he hopes that as part of any stimulus package, the Obama administration treats IT upgrades the same way as other infrastructure-renewal projects.

## Why policy enforcement is so hard

by [Dan Lohrmann](#),

Sat, 2009-01-03 14:42

A recent Seattle Times article offers an interesting case-study for security professionals. The headline: "After 6 months, drivers ignoring cellphone ban." Can we learn anything from law enforcement's implementation of this new law? I think so.

[The Seattle Times article](#) covers a variety of important policy implementation steps that were used:

1) A PR campaign was initiated and initially worked.

*Cindy Baker-Williams held a "Hang Up and Drive" banner over Aurora Avenue North in Fremont when Washington's handheld cellphone ban for drivers began on the first of July. She and her family hoped the new law would change drivers' behavior. It did at first.*

2) Over time, people started to ignore the ban.

*Sgt. Freddy Williams of the State Patrol (said), "We see about one in three drivers talking on a cellphone. People seem to be ignoring the law."*

3) Enforcement penalties were real, but somewhat limited.

*Statewide, troopers handed out 746 tickets for illegal driving-and-talking through November.... Troopers also issued 1,345 written and verbal warnings.... But driving-and-talking is a secondary offense, meaning the police have to stop a driver for another violation before they can write a \$124 ticket for holding a cellphone.*

4) Metrics were available, but the meaning of the data could be argued.

*The pioneering law — only six states have such a ban — might have contributed to a drop in car crashes on state roads this year. It's impossible to know, though, Williams notes, whether the drop resulted from the cellphone ban or other factors such as high gas prices and less travel.*

5) Next steps are controversial.

*The public appears to support a tougher law. Baker-Williams expects it will take a similarly long time — and lots of statistical evidence and personal tragedies — before the cellphone law is strengthened and drivers change their habits.*

Perhaps you're wondering, what does this cellphone ban law have to do with security or other technology policy enforcement? Can't we just "impose our policies" on corporate or government networks and PCs, laptops and other devices? Can't security policy enforcement be automatically implemented in ways that cell phone bans in cars cannot?

No doubt there are differences, but in some ways the cellphone ban for drivers is a best case scenario. For one, everyone "get's it." They understand the law (policy), and they understand the potential risks and life/death consequences of not complying. Of course, the trouble is that they don't think the bad things (like an accident) will happen to them - which is just the same risk/reward equation that is faced with violating security policies.

In addition, the penalties were real and in place in this case. The metrics were available, and the ways of hiding behavior were somewhat limited. One could easily argue that enforcing a drivers cellphone ban is an easier task than enforcing security policy on work networks.

In my opinion, there are quite a few similarities that CSOs should take note of here. First, policy enforcement requires a look at people, process and technology - NOT JUST TECHNOLOGY.

(Sorry for shouting, but many in the industry just can't seem to understand this fact.)

For example, I've seen staff bring in their own web-enabled cellphones to bypass security measures on government or corporate networks. Strong "built-in" technology controls can't stop users from using personal devices to access external networks and websites that pose risk.

The temptation may be to ban all personal cellphones (or other devices) at work, but after governments and companies take away cellphones from staff to save money, you may face a backlash from such moves. Every action causes an opposite reaction and needs to be weighed carefully.

Bottom line, policy enforcement is hard - but needs to be done. My point in this blog is to illustrate some of the difficult aspects that CSOs and others face after they implement a network or security policy. Oftentimes, this is a long road. Just like cellphone bans for drivers, it takes years to change people's habits.

Ending on a more positive note, there are several examples where we have seen long-term behavioral change after policy change. Two such areas include the use of seat belts and smoking bans. In both cases, we needed to change the public opinion and not just the law/policy. CSOs need to keep the ongoing training/awareness aspects of new policies in mind.

## 2008 Data Breach Totals Soar

*ITRC Reports 47% Increase over 2007*

San Diego, CA (January 6, 2009): Reports of data breaches increased dramatically in 2008. The Identity Theft Resource Center's 2008 breach report reached 656 reported breaches at the end of 2008, reflecting an increase of 47% over last year's total of 446.

In terms of sub-divisions by type of entity, the rankings have not changed between 2007 and 2008 within the five groups that ITRC monitors. The financial, banking and credit industries have remained the most proactive groups in terms of data protection over all three years. The Government/Military category has dropped nearly 50% since 2006, moving from the highest number of breaches to the third highest. As the chart indicates, the business community still needs to enhance and enforce data security measures.

	<b>2008 - # of Breaches</b>	<b>2008</b>	<b>2007</b>	<b>2006</b>
<b>Business</b>	<b>240</b>	36.6%	28.9%	21%
<b>Educational</b>	<b>131</b>	20%	24.8%	28%
<b>Government/Military</b>	<b>110</b>	16.8%	24.6%	30%
<b>Health/Medical</b>	<b>97</b>	14.8%	14.6%	13%
<b>Financial/Credit</b>	<b>78</b>	11.9%	7%	8%

According to ITRC reports, only 2.4% of all breaches had encryption or other strong protection methods in use. Only 8.5% of reported breaches had password protection. It is obvious that the bulk of breached data was unprotected by either encryption or even passwords.

The ITRC tracks five categories of data loss methods: data on the move, accidental exposure, insider theft, subcontractors, and hacking. Subcontractor breaches, while counted as one breach each, in some cases affected dozens of companies. It is important to note that the number of breaches reported does not reflect the number of companies affected.

<b>For 2008</b>	<b>Financial</b>	<b>Business</b>	<b>Education</b>	<b>Gvt/Military</b>	<b>Medical</b>
<b>Insider Theft</b>	2.4%	5.6%	1.8%	3.4%	2.4%
<b>Hacking</b>	3.5%	6.1%	2.7%	0.8%	0.8%
<b>Data on the Move</b>	1.7%	7.3%	3%	4.3%	4.4%
<b>Accidental Exposure</b>	0.8%	3.0%	6.1%	3.0%	1.5%
<b>Subcontractor</b>	0.8%	3.5%	1.5%	2.3%	2.3%

Sadly, these trends continue to plague companies and government alike, despite education on safer information handling, new laws and regulations. Mal-attacks, hacking and insider theft, account for 29.6% of those breaches that reported the causal factor. Insider theft, now at 15.7%, has more than doubled between 2007 and 2008. On the other hand, data on the move and accidental exposure, both human error categories, showed noteworthy improvement, but still account for 35.2% of those breaches that indicate cause.

Electronic breaches (82.3%) continue to outnumber paper breaches (17.7%). While there were 35.7 million records potentially breaches according to the notification letters and information provided by breached entities, 41.9% went unreported or undisclosed making the total number of affected records an unreliable number to use

for any accurate reporting.

Based on the breach reports from the past 3 years, the ITRC strongly advises all agencies and companies to:

1. Minimize personal with access to personal identifying information.
2. Require all mobile data storage devices that contain identifying information encrypt sensitive data.
3. Limit the number of people who may take information out of the workplace, and set into policy safe procedures for storage and transport.
4. When sending data or back-up records from one location to another, encrypt all data before it leaves the sender and create secure methods for storage of the information, whether electronic or paper.
5. Properly destroy all paper documents prior to disposal. If they are in a storage unit that is relinquished, ensure that all documents are removed.
6. Verify that your server and/or any PC with sensitive information is secure at all times. In addition to physical security, you must update anti-virus, spyware and malware software at least once a week and allow your software to update as necessary in between regular maintenance dates.
7. Train employees on safe information handling until it becomes second nature.

### ***Internal Controls Vital in Combating Data Loss***

A staggering 280 million people worldwide have lost personal details over the past three years, with human and procedural errors accounting for a significant number of these losses. The risk of such errors is greatly reduced by implementing appropriate and clearly defined procedures around the use and handling of data.

These are just some of the major finding of KPMG's first Data Loss barometer, which has researched recent publicly disclosed incidents of data loss on a worldwide basis and provided a snapshot of the key issues.

The value of implementing and adhering to strict internal controls is clearly evidenced by the fact that between 2007 and 2008 50% of all incidents emanated from internal sources. Such incidents included accidental web or network exposure, human or system errors, improper data disposal and the loss of removable media.

In fact the loss or theft of removable media is a growing concern, though interestingly it is much more likely that such media will be lost internally (62%) than stolen by an outsider. And whilst encryption is the most effective means of protecting the organization against such losses, in only 38% of such instances was the data encrypted or password protected.

The research clearly shows that organizations must plan their incident response carefully. Security policies should be in place to detect, escalate and resolve issues, as well as specifying the appropriate action to be taken in the event of an incident.

From the research it is clear that three incidents accounted for the majority of the victims of data loss between 2007 and 2008, namely:

- The TJX Companies data breach in the US, which threatened the credit/debit card details of over 45 million customers;
- The loss by HM Revenue and Customs in the UK of two CDs containing the details of over 25 million child benefit recipients;
- The exposure in the Netherlands of the details of 15 million people on a legitimate health insurance website.

However, when these three incidents are taken out, we see the following figures:

- 6.2 million victims of PC theft;
- 4.6 million people affected by human or system errors;

- 3.8 million victims of dishonest employees;
- 5.0 million people affected by web exposure.

In terms of the industry sectors that are most likely to be vulnerable to data loss, then the education and healthcare sectors stand out in terms of sheer numbers, possibly because they tend to have restricted security budgets which makes it more difficult to provide adequate protection.

Government organizations also don't fare well, as they were accountable for 19% of the data loss incidents. They were closely followed by financial sector organizations, responsible for 14% of incidents, which is perhaps not unsurprising given that they tend to hold customer data that is particularly attractive for cyber criminals.

What is crystal clear from the research, however, is that data loss is universal and exists across all businesses, sectors and geographical regions. So, it is vital that every organization commits sufficient resources to reduce risks and keep their own and their customers' data secure.

## ***Cyber Insurance – Balance Sheet Protection***

“It will never happen to us” – this is typically the response from many IT security managers, when the subject of Cyber Insurance is raised. However, we are seeing on a regular basis companies suffer from both data privacy breaches and system failures, which result in tarnished reputations and unexpected costs that are hitting the corporate balance sheet.

When high profile system breaches or system failures occur, it is not just the organisation's reputation in question. For IT departments that often walk a tightrope between managing business expectations and supporting the day-to-day operations within budget, a system failure or breach can cost dearly.

### **The Costs of Incidents**

Data privacy alone has gained the attention at the highest level among worldwide regulators, industry associations and the boards of global organisations. The 2008 UK Information Security Breaches Survey stated that for a large company (defined as greater than 500 employees) the average cost for the most serious incidents were between \$1.5m and \$3m. Costs that can have a substantial impact on a company's IT budget and balance sheet, unless proper protection is in place.

### **Benefits and Scope of Cyber Insurance**

Even the most robust IT/DR security is never failsafe. That's why many security vendors have gone on record stating that companies should not rely on technology products alone. Coupled with the threats of operational error and administrative mistakes, Cyber Insurance can be the ideal vehicle to transfer residual risk.

Cyber Insurance generally covers incidents including and not limited to;

- Malicious employees;
- Hacking;
- Malicious code;
- Cyber extortion;
- Denial of service;
- Operational errors;
- Cyber terrorism;
- E-fraud.

The key benefits of Cyber Insurance include coverage for costs ranging from the IT department's internal investigation of an incident and steps to rectify the situation to lost income and wage roll. Cyber Insurance policies also typically include coverage for reputation rehabilitation expenses, such as compensation to customers affected by the incident as well as payment for specialist crisis management consultants to assist in re-establishing the company's brand.

Customer notification and credit monitoring costs may also be included whereby credit monitoring agencies are engaged to write to the customer and provide them with 12 months of credit monitoring surveillance.

To obtain coverage speak with your insurance broker, they should be able to advise you on the types of policy cover available and bespoke coverage to your concerns. The cyber insurance market has opened up over the past few year's, premium's have reduced as more insurer's have built up a loss history.

## **Conclusion**

The world's economy relies heavily on networked computer systems for commerce, communications, energy and transportation distribution and a host of other critical activities.

System failures or beaches, no matter what the cause, are part and parcel of business life. IT/security managers should seek out advice on Cyber Insurance not only to help protect against reputational risk, but also to protect the IT budget from these unforeseen incidents. Managers should not dismiss the prospect of buying Cyber Insurance as a failure in their own abilities to defend their network. Companies take similar precautions in other areas, such as installing smoke detectors and sprinklers within their buildings and making sure they buy property coverage on an annual basis.

Cyber attacks will continue, but with proven risk management and risk transfer mechanisms, there is less and less reason why these incidents should jeopardize corporate IT management and the bottom line.

## ***Employees need more education on risks of online shopping***

A survey has found that whilst employers frequently allow their employees to shop online from their office computer, they do not do not educate them about the associated risks that can expose employees and employers alike to spam, malware, phishing and loss of productivity in the workplace.

The survey, undertaken by ISACA on nearly 1,000 US consumers, found that 63% of employees plan to shop online from their work computer during November and December, but 26% do not know how to, or do not bother to, check whether a website is secure. They also found that nearly half of employees (49%) had clicked on an e-mail link to go to a retailer's website from their workplace computer, potentially exposing their employer to Trojans or malware from infected or unscrupulous websites. Over a fifth of all employees, 22%, had compounded the problem by clicking on a link to order goods while also using their work e-mail address as a contact address for purchases, thereby exposing themselves to a greater risk of attack by spammers.

A similar survey of 251 IT professionals in the UK revealed even more disturbing news. In this case, a mere 21% of respondents said their organization's employees fully understood the risks associated with shopping online from their workplace computers. More than 82% said their organization either does not have, or they are not aware of, a policy that prohibits employees from shopping online (in fact only one in 10 organizations having security measures in place to actually prevent employees from carrying out such shopping). There was also an expectation that there would be more online shopping from the workplace than last year, with over 51% predicting an increase.

Interestingly, the age groups that respondents felt posed the greatest threat to their organizations infrastructure were Millennials (born 1977-94). Confirmation of these worries came with the fact that almost 50% of young workers aged 18 to 25 were more concerned about the security of their own personal computer than their work computer, a figure that was significantly higher than for other age groups.

Lynn Lawton, international president of ISACA and the IT Governance Institute commented: "Shopping from the workplace looks set to continue, especially with the increased pressures inevitable in a recessionary environment. It is clear that more needs to be done to improve employee awareness of the hidden dangers of

shopping online, particularly regarding clicking on links from unsolicited e-mails or making sure that a website is safe before shopping. The challenge for organizations is not only to educate workers about information security, but also to change their behavior."

## The 4 Security Rules Employees Love to Break

### ***Cisco CSO John Stewart gives his take on four security rules employees bend a lot, and what you can do to set them straight***

By [Joan Goodchild](#), Senior Editor

January 06, 2009 — [CSO](#) —

Most CSOs and security managers know [employees are taking risks](#) everyday that could set their company up for a breach. What some of the biggest offenses? And what can be done to nip that [risky behavior](#) in the bud? [John Stewart](#), CSO of [Cisco](#), offers his take on 4 rules people love to break and offers advice on getting them to stop.

#### **Allowing "tailgating" and unsupervised roaming**

According to a recent Cisco survey, more than one in five German employees allow non-employees to roam around offices unsupervised. The study average was 13 percent. And 18 percent have allowed unknown individuals to tailgate behind employees into corporate facilities. The reason, according to Stewart, is that confronting people who may be gaining access illegally is difficult for people.

"Globally, tailgating creates an interesting human problem," said Stewart. "You are walking into building and you may have to challenge someone to prove that they have the right to be there. This is uncomfortable for a great number of people. In certain cultures it's insulting and unacceptable."

Stewart recommends creating an environment that makes it hard for people to tailgate. Consider signage that even states tailgating is not allowed.

"When there are signs posted it makes it easier for a person to ask for identification. They can say: 'The company makes me do this.' It diffuses some of the tension."

Help your user community say in a very obvious way: I don't want to have to do this but I have to do it, said Stewart.

#### **Adding unauthorized wireless access points**

At Cisco, the process of dealing with unauthorized [wireless access](#) points is known as 'whack-a-mole', according to Stewart. That's because they pop up so frequently

Wireless access points can be needed either by employees looking to test things, or when people who don't normally need access suddenly do.

"You could end up in a meeting with people from all over and they all need Ethernet. However, one or two computers might not have authentication credentials to get on corporate wireless and then someone has the great idea to create a wireless environment with USB stick. Wireless is just that easy."

While most employees are just looking to fill a need, said Stewart, the unauthorized access point is an exposure.

"You've got the corporation at risk," he said. "Tailgating and wireless access points are, in many ways, the exact same problem. You are potentially allowing unauthorized or unexpected users on your network."

Stewart advises having a clear and consistent policy with consequences. Consistency is key.

"If the consequences aren't severe, most people won't take you seriously. Get serious about real rules. I know some companies who will charge the department with the person who put the wireless access point on the network. The bill goes to the manager of the person that did it. You can imagine how that plays out."

### **Sharing corporate or sensitive information with unauthorized people**

According to Cisco research, one of four employees (24 percent) admitted verbally sharing sensitive information to non-employees, such as friends, family, or even strangers. When asked why, some of the most common answers included, "I needed to bounce an idea off someone", "I needed to vent", and "I did not see anything wrong with it."

Stewart thinks companies need to educate workers to treat corporate information like it's a personal secret.

"You don't want people know certain things about yourself. If there is something really personal you would rather not have the world know about, that is how company feels, too. You can also equate corporate information with money. Keeping sensitive information secret says 'I'm not going to share my money with you.'"

### **Putting sensitive data in the wrong place**

This could mean copying or extracting corporate sensitive information from protected place and putting it on handheld device. It could also mean e-mailing information to an outside, non-corporate e-mail account. Whatever the scenario, it means sensitive information could get in the wrong hands, especially if it's on a portable device [that gets lost](#). Cisco research found 22 percent of employees carry corporate data on portable storage devices outside of the office.

"If you instinctually know that the work environment you have is causing this, figure out a solution," advised Stewart. "If an employee is engaging in this behavior say to them 'Tell me what you've got to do that's forcing you to do this and let us figure out a way to solve it.'"

## **IT Security Spending Up For Some**

### ***Though a new Forrester survey suggests more security spending in 2009 despite the economic downturn, some security professionals see a different story in their own companies. Here's a look at how they're managing***

By [Bill Brenner](#), Senior Editor

January 07, 2009 — [CSO](#) —

The [economy may be in tatters](#), along with legions of [IT security budgets](#). But a new report from [Forrester Research](#) suggests security spending is actually on the rise in some enterprises.

The Cambridge, Mass.-based research firm interviewed nearly 1,000 firms for its [State Of Enterprise IT Security: 2008-2009 report](#) and found, among other things, that the security portion of IT budgets is expected to rise 12.6 percent in 2009, up from 7.2 percent in 2007 and 11.7 percent in 2008.

"Even during challenging economic conditions, IT security remains an integral part of business operations as firms look to maintain their current environment as well as plans for the implementation of new initiatives," wrote Forrester analyst [Jonathan Penn](#), the report's chief author. In a follow-up interview, he told [CSOonline](#) that companies still aren't looking at security as a business enabler. But they now understand that it's at least better to take steps to prevent attacks than to do nothing.

"Security is getting a bigger slice of the IT pie, with the focus less on reactive vulnerability defenses and more on looking at what's necessary to protect the business," Penn said. "More often than not, the focus is on protecting the data itself."

### **Spending not up for all**

[CSOnline](#) conducted its own poll on the subject and found, not surprisingly, security professionals who see a different picture in their own environments.

A security officer who manages IT security operations for a county government on the east coast said he has faced tough budget choices.

"As with all other state/local governments, we are directly impacted by the housing decline, unemployment and a decrease in state funding," said the security officer, who asked to remain anonymous because he isn't authorized to speak to the press. "Because of this, revenue decreases for next fiscal year (beginning in July) are estimated at between 10-25 percent."

His choice was either to cut staff from an already lean team or decrease operating expenses. He decided to reduce existing spending, largely on the technology front.

Zach Lanier, senior network security analyst at [Harvard Business School](#), said overall, security spending at his organization will be down, mainly because it has completed initiatives that started and closed in 2008. Costs for those projects in 2009 will be mostly operational expenditures, he said.

"We're not immune to the economy's poor performance. While Harvard Business School has traditionally been a big spender, the current conditions have caused us to think twice just in case," he added. "I would be inclined to add that it's also caused my organization to think twice about different ways of tackling problems."

For example, he said, the organization has turned to "high-performance" commercial products to get it to that "85 percent" and filled in the rest with free and open source tools. "Also," he said, "we've stepped back a bit and looked at processes and procedures and how those can be improved rather than just throwing money at a vendor."

### **Security not linked to economy**

Others confirm their organizations' plans reflect Forrester's findings. In these cases, security is an ongoing necessity unaffected by economic peaks and valleys.

"In the government, pressures caused by data losses has prompted more spending," said a UK-based IT security specialist who requested anonymity because he isn't authorized to speak to the press.

According to the Forrester report, firms are devoting 11.7 percent of their company's IT operating budget to IT security in 2008 compared with 7.2 percent in 2007, and they plan to continue nudging up IT security budgets in 2009 to 12.6 percent of the IT operating budget. Allocation of budget for new security initiatives mirrors this trend, going from 17.7 percent in 2008 to 18.5 percent in 2009, Penn said.

"There has been a clear and significant shift from what was the widely recognized state of security just a few years ago," the report notes. "Protecting the organization's information assets is the top issue facing security programs: data security (90 percent) is most often cited as an important or very important issue for IT security organizations, followed by application security (86 percent), and business continuity/disaster recovery (84 percent)."

Meanwhile, the report said, areas like threat management (81 percent) and regulatory compliance (80 percent) are cited less frequently. Data security also tops the list of business objectives for security, with 89 percent citing protection of corporate data and 87 percent citing protection of personal data as important or very important business objectives.

### **When security budgets aren't measured**

In some cases, it's hard to figure out how far up or down spending is because the company in question doesn't have a specific line item for security.

"Most companies I have worked with don't even measure any type of security budget," said Nalnees Gaur, chief information security architect and principal at [Diamond Management & Technology Consultants Inc.](#) in the Dallas/Fort Worth area. "As a consultant, I get involved with companies where something bad has happened like

getting hacked. With getting hacked as the driver, I often see a surge in priority for security where the company will spend a lot of money." The trick is if they can sustain the program after the first year, he said.

## **Regulators: Thanks PCI, but we'll take it from here**

The Payment Card Industry Data Security Standard (PCI DSS) being pushed by the major credit card companies has probably done a lot to stave off state and federally mandated controls for protecting customer credit and debit card data up to now. The big question as a new year begins, is for how much longer though?

More than two years after the PCI standard went into broad effect, data breaches involving payment card data continue unabated. Obviously it would have been unrealistic for anyone to have expected them to stop altogether just because of PCI. And it's impossible to know how many compromises were averted because of the standard.

Even so, the number of data compromises involving payment card data being disclosed by businesses is only increasing, not decreasing. One reason is simply that state breach notification laws are forcing companies to disclose compromises that in the past they might not have. Another is the continuing lack of visible enforcement of PCI which has resulted in an environment where many companies, including large ones, are still not fully compliant with the mandate.

And that's a problem for those hoping that a private industry initiative such as PCI alone will be enough to keep lawmakers at bay for much longer.

Already [Massachusetts](#) and [Nevada](#) have passed laws requiring companies to encrypt all sensitive customer data and implement measures for controlling access to it. The Massachusetts law, which seems to have a lot of people anxiously reviewing their security measures, was supposed to have gone into affect Jan 1 but has been [pushed back](#) to May 1. Nevada's law went into effect on October 1.

As far back as May 2007, [Minnesota](#) passed a law known as the Plastic Card Security Act. Under the statute, companies that suffer data breaches and are found to have been storing prohibited credit or debit card data on their systems will have to reimburse banks and credit unions for the costs of blocking and reissuing cards. Attempts at passing similar legislation-most of which are sponsored by financial institutions--have so far failed in places such as [California](#), [Texas](#) and elsewhere. But all its going to take is for another major retail breach or two for them to be revived.

The security requirements spelled out in these statutes are mostly the same as those mandated under PCI though they cover other data classes as well such as Social Security numbers and bank account information. The key difference is that the mandates in Massachusetts and elsewhere are coming from a government agency and carry the full authority of state law. Companies that suffer data breaches and are found to have been noncompliant with the regulations could find themselves exposed to greater legal and financial issues than the PCI standard generally provides for.

Here again, everything will depend on how vigorously these mandates are enforced. But it probably is going to be a whole lot riskier for companies to simply pretend like they are doing something, as at least a few appear to be doing, with PCI.

## Browser bug could allow phishing without e-mail

By Robert McMillan

January 12, 2009 (IDG News Service) A bug found in all major browsers could make it easier for criminals to steal online banking credentials using a new type of attack called "in-session phishing," according to researchers at security vendor Trusteer.

[In-session phishing](#) gives the bad guys a solution to the biggest problem facing phishers these days: how to reach new victims. In a traditional phishing attack, the scammers send out millions of phony e-mail messages disguised to look like they come from legitimate companies, such as banks or online payment companies.

Those messages are often blocked by spam-filtering software, but with in-session phishing, the e-mail message is taken out of the equation, replaced by a pop-up browser window.

Here's how an attack would work: The bad guys would hack a legitimate Web site and plant HTML code that looks like a pop-up security alert window. The pop-up would then ask the victim to enter password and log-in information, and possibly answer other security questions used by the banks to verify the identity of their customers.

For attackers, the hard part would be convincing victims that this pop-up notice is legitimate. But thanks to a bug found in the JavaScript engines of all the most widely used browsers, there is a way to make this type of attack seem more believable, said [Amit Klein](#), Trusteer's chief technology officer.

By studying the way browsers use JavaScript, Klein said he has found a way to identify whether or not someone is logged onto a Web site, provided they use a certain JavaScript function. Klein wouldn't name the function because it would give criminals a way to launch the attack, but he has notified browser makers and expects the bug will eventually get patched.

Until then, criminals who discover the flaw could write code that checks whether Web surfers are logged onto, for example, a predetermined list of 100 banking sites. "Instead of just popping up this random phishing message, an attacker can get more sophisticated by probing and finding out whether the user is currently logged into one of 100 financial institution Web sites," he said.

"The fact that you're currently in-session lends a lot of credibility to the phishing message," he added.

Security researchers have developed [other ways](#) to determine whether a victim is logged onto a certain site, but they are not always reliable. Klein said his technique doesn't always work, but it can be used on many sites including banks, online retailers, gaming and social networking sites.

## Encryption Top IT Security Initiative in 2009

Network World (01/05/09) ; Messmer, Ellen

IT budgets for 2009 are expanding in order to accommodate new encryption technologies and maintain current security technologies, according to a new Forrester Research study of 942 IT managers. The study found that personnel and security maintenance account for more than 50 percent of IT security budgets overall. The study found that for every \$5 spent on IT security, at least \$1 will be set aside for security outsourcing, while another 18.5 percent will go toward new and emerging security solutions. Full-disk encryption is the most popular security technology to be rolled out in 2009, followed by file-level encryption, desktop data-leak prevention, and network-based data-leak prevention. Respondents to the survey also expressed interest in the deployment of identity and access management platforms such as activities monitoring and individual sign-on.

## Four Insider Threats to IT Security

Public CIO (01/09) Vol. 6, No. 6, P. 18 ; Gilbert, Jackie

Organizations can protect themselves from insider threats by using a risk-based identity management strategy. Such a strategy helps organizations identify employees that are most likely to do damage to IT systems, reduces compliance costs and burdens on IT staff, and prioritizes and limits the focus of internal controls and audits. Risk-based identity management strategies help organizations to assess and measure risk over a period of time and enable them to demonstrate that their identity controls are working to reduce their exposure to threats as well as their liability from security breaches. The process of developing a risk-based identity management strategy begins by assessing four areas of risk exposure: The organization's risk from orphan accounts, or accounts remaining on the network after employees quit or are terminated; the access level given to contractors and temporary employees; entitlement creep, which occurs when workers gradually accumulate more and more access privileges over time; and the challenges associated with enforcing separation of duty policies across numerous applications and systems. After an assessment is done, organizations must then create the procedures and technology infrastructure that will be used to support identity risk management as a regular business process. This involves centralizing identity data, performing access reviews on a regular basis, automating the enforcement of separation of duty policies, and identifying users that pose a high security risk to the organization.

