

ESO - Security Trends Report

10/08

Cloud computing could prompt government action

Issues involving privacy and data security are likely to emerge

By Grant Gross

September 12, 2008 (IDG News Service) Cloud computing will soon become a hot topic in Washington, with policy makers debating issues such as the privacy and security of data in the cloud, a panel of technology experts said Friday.

There are "huge challenges" facing policy makers in the next year or two as cloud computing becomes increasingly popular, said [Mike Nelson](#), visiting professor for the Center for Communication, Culture and Technology at Georgetown University and a former technology policy adviser to [President Bill Clinton](#).

The major policy questions to be worked out include: Who owns the data that consumers store on the network? Should law enforcement agencies have easier access to personal information in the cloud than data on a personal computer? Do government procurement regulations need to change to allow agencies to embrace cloud computing?

Cloud computing is "as important as the Web was 15 years ago," said Nelson, speaking at a [Google Inc.](#) forum on the policy implications of hosted applications and services. "We don't have any idea of how important it is, and we don't really have any clue as to how it's going to be used."

Despite the growing number of people using cloud services such as hosted e-mail and online photo storage, many consumers don't understand the privacy and security implications, said [Ari Schwartz](#), vice president and chief operating officer of the [Center for Democracy and Technology](#) (CDT), an advocacy group focused on online privacy and civil rights. So far, U.S. courts have generally ruled that private data stored in the cloud doesn't enjoy the same level of protection from law enforcement searches that data stored on a personal computer does, he said.

"Consumers expect their information will be treated the same on the cloud as it is if it were stored at home on their own computers," Schwartz said.

Forty-nine percent of U.S. residents who use cloud-computing services would be very concerned if the cloud vendors shared their files with law enforcement agencies, according to a survey released Friday by the Pew Internet and American Life Project. Another 15% of respondents said they'd be somewhat concerned, according to the survey, which was released to coincide with the Google policy event.

Sixty-nine percent of U.S. residents who are online use at least one of six popular cloud services, the survey said. Fifty-six percent of survey respondents use Web mail services, 34% store personal photos online, and 29% use online applications such as Google Documents or Adobe Photoshop Express, according to the survey.

Among the concerns about cloud computing: 80% of respondents said they'd be very concerned if a vendor used their photos and other information in marketing campaigns. Another 68% said they'd be very concerned if the vendor used their personal information stored in the cloud to deliver personalized ads to them, and 63% said they'd be very concerned if the vendor kept their data after they tried to delete it.

Asked why they use cloud-computing services, 51% said convenience was the major reason. Another 41% said the major factor was being able to access their information from multiple computers and devices.

One audience member suggested that consumers' growing use of cloud services doesn't match their concerns about the privacy of their data. Schwartz said consumers would embrace privacy protections if they were made easy to use.

"People are obviously making trade-offs in privacy when they use these services," added John Horrigan, Pew's associate director for research.

Asked what policy recommendations they'd make to the U.S. government, Nelson and Schwartz suggested that procurement regulations must change for federal agencies to embrace cloud computing. But questions about data privacy and ownership are also important to address, Schwartz said.

The U.S. government should encourage the free flow of information around the globe, said Dan Burton, senior vice president for global public policy at cloud computing vendor Salesforce.com Inc. The benefits of cloud computing could be hampered by laws that prevent the sharing of data across national borders, he said.

The government should avoid formulating specific policies for cloud computing, according to Nelson. The government's role should be to ensure competition and allow vendors to work out details, he said.

"I do think government has an almost infinite ability to screw up things when they can't see the future," Nelson said. "We have to have leadership that believes in empowering users and empowering citizens."

Open phones are more vulnerable, security execs say

Vendors need to find the right balance between openness and security

By Stephen Lawson

September 12, 2008 (Computerworld) SAN FRANCISCO -- The opening up of the mobile industry is great news for application developers but not so good for IT security professionals who want to sleep at night, executives from the security industry said yesterday.

Mobile phone operating systems have been highly fragmented, and carriers have tightly controlled the applications that can easily be used on phones, but that approach is giving way to open-software platforms and easy-to-use application stores. In addition to [Apple Inc.](#)'s recently introduced [iPhone SDK](#) (software development kit), Google Inc.'s [open-source Android platform](#) is due on phones soon and an open-source [version of Symbian](#) is on the way.

"Everyone has now decided that the developers are very important for the future of this business. If a developer can load software on a device, a hacker can load software on a device," said Mark Kominsky, CEO of Bluefire Security Technologies, during a panel discussion at the CTIA Wireless I.T. & Entertainment show. "I think we're probably 12 to 18 months away from something big happening," he added.

Mobile devices are beginning to have high-bandwidth, open platforms and the ability to load new software, Kominsky said. "Those are the critical elements that occurred in the notebook when viruses took off about 20 years ago," he said.

[Symbian](#), the single most widely used mobile software platform, has already wrestled with the dangers of openness to third-party developers, said [Khoi Nguyen](#), group product manager in mobile security at [Symantec Corp.](#) Symbian 7 and 8 were fairly open and allowed almost any application to be installed and run. This led to a few hundred viruses being introduced within a couple of years, so Symbian 9 was locked down significantly, he said.

That made it much harder and more expensive to develop applications for the operating system, even for a big company such as Symantec, Nguyen said.

Symbian and other platform vendors will have to find a balance between security and openness, he said.

By the same token, the fragmentation of the mobile world that has hobbled software developers still insulates phones from the onslaught of attacks on PCs.

Symbian has less than 70% of the market, Nguyen said. "It makes it very hard for a hacker to develop a single threat ... that can run on all these different platforms," he said.

Nevertheless, there are some new types of malware for enterprises to look out for, as well.

"Snoopware" is a form of spyware that can activate the microphone or camera without the user's knowledge, listen in on calls, and collect text messages and call logs. Another type of threat, which Nguyen called "pranking4profit," can trick the user into allowing actions that will cost money. In one case, a hacker advertised a free Web browser for Symbian phones and persuaded many users to download code that caused their phones to send thousands of premium SMS (Short Message Service) messages to a hacker's phone. Each one cost the sender \$2 or so, Nguyen said.

Although malware may make headlines, the greatest danger to enterprises with mobile phones is loss or theft of data, the panelists agreed.

Enterprises should protect their employees' mobile phones just as they do any other endpoint, with the same security policies, requirements and software, and with an eye to compliance as well, Nguyen said. Companies should also maintain an inventory of their mobile devices and regularly push out software updates. To protect data, they should use password protection, encryption of data and remote data wipe capability, he said.

They should also disable features not required for business use, he said.

Senators Introduce 2008 Federal Information Security Management Act

September 12, 2008) US Senators Tom Carper (D-Delaware) and Joseph Lieberman (I-Connecticut) have introduced Senate bill 3474, the 2008 Federal Information Security Management Act. Among the bill's provisions is a requirement that federal agencies appoint chief information security officers; the CISOs would have the authority to block network access if established security policies are not being adhered to. The bill would also require that the Department of Homeland Security (DHS) conduct annual tests to determine if attackers could access sensitive government data. Senator Carper noted that the current Federal Information Security Management Act is an exercise in paperwork rather than an effective means of determining the security of federal computer networks.

http://www.nextgov.com/nextgov/ng_20080912_7543.php

<http://www.fcw.com/online/news/153773-1.html?type=pf>

[Editor's Note (Schultz): Hopefully, the 2002 version of FISMA will soon become a thing of the past. I suppose that this version of FISMA was at least a start towards achieving better cybersecurity within US government agencies and departments. Anyone who has gone through the exercise of trying to achieve FISMA compliance knows, however, that it is indeed a paperwork game, one that has little relevance to countering real-world security risks.

(Pescatore): CISO's with authority is a very good thing, as long as that authority includes some influence over budgets *and* that the government actually starts making security funds be included as part of all budget requests. Having DHS compete with private industry to do security audits is *not* a good thing - there is a thriving commercial market for security audits and penetration testing that will be more effective and more efficient than any government agency.

(Paller): John Pescatore's comment illuminates one of the dirtiest little secrets of federal cyber security - that federal agencies promise, in writing, to spend a specific percentage of each IT project budget on cyber security (usually 4-8%). My best guess, based on interviews with a lot of federal folks, is that only 35-45% of the promised funds are spent on security - the rest go for other uses. That means that when a CIO testifies before Congress that he or she is spending a certain percent of the IT budget on cyber security (a number derived from those promised percentages in the budget documents) that CIO is almost certainly lying to Congress.

On the other hand, the new FISMA 2008 bill solves three of the most difficult problems caused by OMB and NIST's implementation of the old law and should be a breath of fresh air to any cyber security professional who wants to see federal cyber security funds spent on securing systems rather than on consultants who write reports that do not improve security.]

House Subcommittee Hears Testimony on DHS Cybersecurity Shortcomings

(September 17, 2008) The US House Subcommittee on Emerging Threats, Cybersecurity, Science and Technology heard testimony critical of the Bush administration's cyber preparedness efforts. Members of the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th President said that the Department of Homeland Security (DHS) has not established relationships of trust or even partnerships with private sector organizations and other countries. The commission has proposed a solution that includes establishing a high level administration cyber security position that would include necessary security clearances and access to the president - in essence, shifting the responsibility for cyber security from DHS to the White House. The Government Accountability Office (GAO) released a report at the hearing with similar findings. The GAO's report specifically mentioned the shortcomings of the US Computer Emergency Readiness Team (US-CERT), saying it "lacks a comprehensive baseline understanding of the nation's critical infrastructure operations, does not monitor all critical infrastructure information systems, does not consistently provide actionable and timely warnings, and lacks the capacity to assist in mitigation and recovery in the event of multiple, simultaneous incidents of national significance." The DHS discounted the findings presented at the hearing, calling the criticism politics as usual.

US Focusing Cybersecurity on Backdoors in Tech Products **IDG News Service (09/15/08) ; Gross, Grant**

Officials from the Department of Homeland Security (DHS), the White House, and the Office of the Director of National Intelligence unveiled new details about President Bush's National Cybersecurity Initiative at a recent cybersecurity conference. Among the officials in attendance at the conference was DHS deputy secretary Paul Schneider, who noted that the U.S. government needs to better protect its supply chain from hidden vulnerabilities and Trojan horses in some commercial technology products made overseas. Some credit-card point-of-sale machines, for example, have stolen credit card numbers and passwords. Schneider noted that the government plans to work with private vendors to protect its supply chain, and will implement stringent acquisition rules for commercial technology products. In addition to addressing concerns about the supply chain, Schneider noted that the government is also planning to upgrade its perimeter defense scanner, Einstein. The system is largely a passive monitoring system that alerts the government that it has been attacked after the fact. The new version of the system will allow the government to anticipate where threats will come from and prevent cyber criminals from launching attacks. Officials at the conference also noted that the National Cybersecurity Initiative will focus on other issues as well, including improving the sharing of information about cyberattacks and sharing government defense capabilities with private companies.

Enterprises Struggle to Identify Sources of Risk **Dark Reading (09/11/08) ; Wilson, Tim**

Although enterprises are more concerned than ever about security, they still disagree about how to measure risks, reveals a new BT study. The yearly security study, which examines corporate security priorities and preemptive risk management, found that 83 percent of enterprises ranked "improving security" as one of their top priorities for the next year. Twenty-two percent said this is their most urgent task. Yet pinpointing the source of the risk, and making a case to executives for more investment in security technology, are evasive goals for many companies, say BT researchers. Three out of 10 respondents implicated poorly trained end users as the main threat to network security. Despite these concerns, many organizations are not following through with regular security audits. Fewer than half of the companies--about 48 percent--examine their security platforms on a quarterly basis, according to the report. Security professionals must quantify the possible cost of attack-related downtime in order to make a strong business case, experts say. "These costs should take into account financial damages (outright theft), recovery costs (notification of affected parties, etc.), and loss of reputation (leading to loss of business)," the report said.

United Nations Agency Eyes Curbs on Internet Anonymity

CNet (09/12/08) ; McCullagh, Declan

Technologists and privacy advocates are very concerned by the United Nations' (UN's) International Telecommunication Union's (ITU's) drafting of technical standards proposed by the Chinese government to define techniques of tracing the original source of Internet communications and potentially restricting the ability of users to maintain anonymity. "What's distressing is that it doesn't appear that there's been any real consideration of how this type of capability could be misused," says Electronic Privacy Information Center director Marc Rotenberg. One of the most disturbing aspects of the initiative is that it could institutionalize a means for governments to suppress their opposition, which conflicts with the UN's Universal Declaration of Human Rights, notes Columbia University computer scientist Steve Bellovin in a recent blog post. Countering distributed denial of service (DDoS) attacks is the most commonly cited rationale for IP tracebacks, but Bellovin says the method's usefulness in this regard has waned because few attacks employ spoofed addresses, there are too many sources in a DDoS attack to be useful, and the source computer inevitably would turn out to be compromised anyway. Technologist Jacob Appelbaum warns that a traceback system would offer malevolent hackers the ability to commit wrongdoing without being caught, thus abusing the very system that is designed to trace them. The official charter of the ITU's Q6/17 group states that it will work "in collaboration" with the Internet Engineering Task Force and the U.S. Computer Emergency Response Team Coordination Center, which could supply a route toward widespread acceptance. A formal legal mandate to adopt IP traceback would likely be blocked by the First Amendment in the United States.

Five Trends Driving the Need for Better Mobile Security

Mformation Chief Marketing Officer Matt Bancroft outlines five mobile security trends keeping CSOs up at night

By Matt Bancroft - September 19, 2008

The pace of mobilization within many enterprises is increasing rapidly. Enterprises of all sizes and types are finding that going mobile can significantly increase the productivity of their employees, bringing added flexibility and cost reductions and helping many companies gain a competitive edge in their market.

In a survey of CIOs of top-500 companies undertaken by independent research firm Coleman Parkes, 81 percent of the CIOs interviewed reported that they have seen significant productivity increases from their mobile investments, and the same percentage expect further significant productivity increases from new mobile products over the next five years.

It comes as no surprise, then, that enterprises are providing a growing number of management and staff with mobile devices equipped to access corporate data and applications.

In addition, enterprises are embarking on initiatives that will significantly increase their use of mobile applications. As mobile and wireless solutions become increasingly important to an organization's overall business strategy, they are also becoming increasingly important in an organization's IT strategy. Security issues consistently top the list of IT concerns - nearly eight out of 10 of the CIOs surveyed indicated concerns about the security implications for their company's corporate data of the proliferation of sophisticated mobile devices among employees.

A number of trends are driving the need for better mobile device management and security. The combination of an increasingly varied set of mobile devices with increasing memory, power and portability, combined with a trend toward more powerful, IP-based network infrastructures, is creating a fertile ground for the migration of Internet-based threats into the mobile space. At the same time, new and powerful mobile applications are being launched and security threats are becoming increasingly sophisticated. These are among the issues keeping CIOs and CSOs up at night.

Trend 1: More powerful and less expensive mobile devices are becoming ubiquitous and are as irreplaceable as any PC or laptop, significantly increasing the risks from loss and theft. Mobile handsets are becoming more

powerful with each new release, to the point where the newest and smartest mobile devices are more like handheld computers than cellular phones. And with every product release, the devices have more capabilities and cost less. As an example, the 8 GB [iPhone 3G](#) coming out this month will cost a mere \$199, compared to the original 8 GB [iPhone](#) that cost \$599 when it was first introduced last year and \$399 just a few months ago. The same trend is playing out with other smart devices, including [BlackBerry](#), [Windows Mobile](#) and [Symbian](#) devices.

Network providers have made their pricing models more attractive to enterprises as well. Rather than per-minute, per-transaction or per-byte pricing, which is difficult to budget for and therefore very unattractive to enterprises, data services are being offered in attractive pricing bundles, including "all-you-can-eat" packages.

With this sort of power in such a small and portable package, many executives and managers are finding their mobile handset to be as irreplaceable as any PC or laptop. Unlike PCs and laptops, however, mobile devices carry an equally significant amount of information in a much smaller and more portable package that is incredibly easy to misplace, lose or steal, significantly increasing the risk to the enterprise.

Trend 2: A move toward more powerful, IP-based network infrastructures is leading to increased use of data-heavy mobile services, which need more sophisticated management. Wide-area networks are continually being enhanced to deliver the bandwidth necessary to support new data-heavy mobile services and applications. These enhanced networks offer improved breadth of coverage and reliability - key objectives for most mobile operators. UMTS (Universal Mobile Telecommunications System) in GSM-based networks, and EV-DO (Evolution-Data Optimized) in CDMA-based networks, both represent significant improvements in these areas.

4G networks such as WiMAX (Worldwide Interoperability for Microwave Access) are now being rolled out, enabling ever more sophisticated, data-heavy mobile services and applications. 3G LTE (Long Term Evolution) and other all-IP variants are shortly to follow.

More than a decade of R&D has gone into securing PCs and laptops connected to the Internet and corporate intranets. These technologies are now commonplace in enterprise networks. The same level of attention needs to be paid to these highly portable wireless devices if they are to succeed in the enterprise. However, simply porting PC-style security and management systems to the wireless arena ignores the very small form factor, extreme portability and vastly different usability expectations that are unique to mobile devices and wireless connections. IT organizations are finding that they need to find a middle ground, leveraging some of the R&D done in the PC/laptop arena while keeping the unique needs and the requirements of the mobile device in mind to ensure the mobile experience is not negatively affected in any way.

Trend 3: Increased numbers of corporate users of mobile devices accessing company applications and data at all levels of the enterprise are creating a huge headache for IT departments. Not only are more company executives than ever before beginning to depend on their smart mobile devices, but also staff at all levels are increasingly "going mobile." Smartphone use is rapidly driving down into the ranks of middle management and staff workers. Sixty-seven percent of CIOs responding to the Coleman Parkes survey reported that the proportion of non-managerial staff with access to advanced corporate mobile devices will increase, with fully one third of them indicating that the proportion would increase significantly. And in many cases, when the enterprise doesn't supply mobile devices to employees, they are simply using their personal mobile devices to transact company business and run company applications, with or without the knowledge of the IT organization.

This proliferation of devices that can access company applications and data is creating a huge headache for IT departments. Not only do they need to minimize the risk associated with the possible loss, theft or misuse of a growing population of devices, but they also need to find ways to manage and secure everything from company-issued mobile devices to a host of different personal and partly personal mobile devices.

Trend 4: More advanced and data-heavy mobile applications and services on employees' mobile devices require more sophisticated monitoring and management.

Over the past several years many industries have come to rely upon mobile enterprise applications. BlackBerry devices, for example, have become de rigueur among investment bankers and lawyers who need always-on access to e-mail, calendar and market information. Government organizations are using mobile devices to capture information from remote government employees for a wide range of tasks, including Emergency Medical

Services (EMS), traffic management and even animal control and tracking. In the health-care industry, physicians and case workers can now capture and access health information at point of care using their mobile devices. Popular mobile enterprise applications used across all industries include sales-force automation, field-force automation, fleet management, inventory management, mobile tech and wireless CRM.

Employee mobile devices often contain a wide range of applications and data files, both company-issued and personal. However, according to the Coleman Parkes survey, 63 percent of CIOs interviewed do not actively monitor the types of data that employees are storing on their devices. Nothing prevents employees from installing data and applications onto their devices that could cause problems for the company - from unknowingly circulating viruses to not playing well with corporate systems or not adhering to corporate security policies.

Trend 5: More and more sophisticated security threats are appearing as new devices provide richer targets.

Although, so far, infestation of wireless handsets by Internet-based security threats has been relatively low, new threats to mobile devices, including malicious programs (viruses, worms and Trojan horses) continue to appear. In just the last few months, two new Trojan horse viruses, one targeting Symbian SMS messages and another targeting specific Windows Mobile programs; two new worms, one targeting particular Symbian phones and one targeting multimedia cards; and a new spy-ware application have shown up in the market. Thankfully, none of these malicious bits of code have caused widespread damage. However, despite the fact that the current threat is not particularly high, most industry experts are saying that the iPhone, Android, and mobile devices with WiFi and other broadband capabilities will undoubtedly be rich targets for malware and viruses in the coming years.

Effective management of a company's mobile devices, data and applications will mean faster mobilization of enterprise applications, which, in turn, will lead to increased employee productivity at all levels of the enterprise. Recognition of the trends driving mobile adoption and the unique challenges associated with managing and securing mobile devices is a good first step in ensuring that corporate data is protected and the business is kept safe while it moves forward with mobilization initiatives. The next step is to make sure policies and systems are in place to effectively manage and protect mobile devices, data and applications while supporting the people who increasingly depend on them.

[Nevada Deadline on E-Mail Encryption Looming](#)

What happens in Vegas, may stay locked down in Vegas.

On Oct. 1, the state of Nevada will be requiring the encryption of all transmissions, such as e-mail, for all businesses that send personal, identifiable information over the Internet. The statute was signed into law in 2005 and is about to kick in as an enforceable law next month. Three years flies when you're raking in chips at casinos and enjoying the rising popularity of poker.

The [Nevada law](#) is stated as such:

NRS 597.970 Restrictions on transfer of personal information through electronic transmission.
[Effective October 1, 2008.]

1. A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.

As with any law about to go in effect, this one could be bound to catch many Nevada businesses off guard. In parallel, a few IT security vendors that sell encryption software and hardware are lining up to tell the technology media about it.

Think about all the hotels, resorts, golf courses, pawn shops, nightclubs, check cashing, ski lodges and

small businesses this is going to effect. Not to mention all the businesses--the vice-ridden ones legal to Nevada only and otherwise--that incorporate in the tax-friendly state. Nevada is the West's version of Delaware (albeit a much sexier state, sorry Delaware).

Beyond the infrastructure impact, the statute itself looks like swiss cheese. [Bryce K. Earl](#), a Las Vegas-based attorney with Santoro, Driggs, Walch, Kearney, Holley & Thompson, has been following the issue closely and believes there are some problems with the statute as it is on the books right now, namely the broad definition of encryption, the lack of coordination with industry standards and the unclear nature of penalties both criminal and civil.

"The statute's lack of specificity with regard to penalties will perhaps create the unintended consequence of opening up more liability," said Earl. That doesn't sound good, but again, nothing has happened just yet.

Earl explained why the broad definition of "encryption" by the state is potentially problematic. Here is the [definition from the state's Web site](#):

NRS 205.4742 "Encryption" defined. "Encryption" means the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to:

1. Prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound;
2. Cause or make any data, information, image, program, signal or sound unintelligible or unusable; or
3. Prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network.

Earl said an argument could be made that a password-protected document sent in an e-mail might be good enough to hold up with the state's broad definition of encryption here. Is that good enough?

Moreover, how the heck will Nevada enforce this?

Earl said at this time it was unclear, but he thinks that the state--which holds legislative session every other year--could address the statute for more clarity next year when the Nevada state government reconvenes. A possible-pending lawsuit may also help to better define the law for clearer interpretation, but as Earl hinted, that doesn't necessarily mean it will help that potential lawsuit.

The challenge for Nevada is that its intentions were good in trying to stem the tide of identity theft and criminal behavior online. But once again, the legal system and the IT industry are faced with potentially bigger compliance and liability issues than they probably intended. The disconnection is real.

Following is another provision in the law to consider:

NRS 193.170 Prohibited act is misdemeanor when no penalty imposed. Whenever the performance of any act is prohibited by any statute, and no penalty for the violation of such statute is imposed, the committing of such act shall be a misdemeanor.

Two-thirds of firms hit by cybercrime

Published: 2008-09-22

The Department of Justice released data from its 2005 National Computer Security Survey last week, finding that two-thirds of firms detected at least one cybercrime during that year.

More than 7,800 companies responded to the survey ([pdf](#)), which classified cybercrime into cyber attacks, cyber theft, and other incidents. The survey found that three-quarters of cyber attacks came from external sources, while insiders accounted for the same proportion of cyber thefts. More than half of companies reported a cyber theft to law-enforcement authorities, but only 6 percent of cyber attacks were reported. Computer viruses made up more than half of all cyber attacks.

"A nationally representative sample of 35,600 businesses representing 36 economic sectors received the survey," the DOJ said in [a statement](#) summarizing the survey. "Twenty-three percent of the selected businesses responded. Though the responses are not nationally representative, the NCSS is the largest survey conducted to date. Detailed findings for each of the 36 sectors are provided in this report."

The survey, which was developed by the DOJ's Bureau of Justice Statistics and the U.S. Department of Homeland Security, found that telecommunications companies and computer-system design businesses were hardest hit by cybercrime. About 90 percent of businesses that suffered an incident sustained monetary loss, and cyber theft accounted for half of the loss, according to the summary.

Some surveys of companies have found that damages due to cybercrime have fallen. In 2006, the Computer Security Institute [released their annual survey](#) finding that corporate losses due to cybersecurity incidents had fallen for the fifth straight year. Critics questioned, however, whether the survey had enough data to make that conclusion. Last year, [a survey of identity-theft prosecutions](#) found that the suspected thieves were often first-time offenders and did not know their victims.

In the recently-released NCSS, about two-thirds of all victims lost \$10,000 or more.

Plugging the Holes

Government Executive (09/01/08) Vol. 40, No. 12, P. 34 ; Aitoro, Jill R.

The federal government's computer security issues are due to poor security policies, not a lack of funding, experts say. In fiscal year 2008, federal agencies allocated more than \$6.6 billion to information security, which represented 10 percent of the \$68.3 billion that the government spent on IT as a whole, according to statistics released by the Office of Management and Budget. By comparison, the health care and financial services industries--which are generally regarded as having the best IT security practices--spend only 7 percent of their IT budgets on security, IT research firm Gartner reports. Instead, the problem with federal computer networks lies with the fact that agencies must spend much of their IT budgets complying with the 2002 Federal Information Security Management Act (FISMA), which requires agencies to identify and inventory IT systems, determine how sensitive the information stored on those systems is, find vulnerabilities that hackers can use to access their networks, and implement security controls. Federal CISOs say it is difficult if not impossible to develop plans to develop security technologies and processes that go beyond FISMA's requirements in part because most of their IT budgets are spent complying with the law. As a result, federal agencies have limited abilities to adopt information security strategies that aim to mitigate their specific weaknesses. Security managers say that a better federal security strategy would allow agencies to develop information security plans that reflect their priorities and address their specific security needs, with FISMA supporting those strategies.

Cyber Attack Data Sharing Is Lacking, Congress Told

Washington Post (09/19/08) P. D2 ; Nakashima, Ellen

U.S. intelligence agencies are unable to share information on foreign cyberattacks against companies due to a fear of jeopardizing intelligence-gathering sources and methods, testified Paul B. Kurtz at the first open hearing on cybersecurity held by the House Permanent Select Committee on Intelligence. Kurtz and other cybersecurity

experts discussed the Bush administration's Comprehensive National Cybersecurity Initiative, which focuses on cybersecurity espionage against government systems but, according to the experts, does not adequately address the private sector. The panelists, members of the Center for Strategic and International Studies commission on cybersecurity, say there is no coordinated strategy or mechanism for sharing intelligence about intrusions with companies, nor is there a systematic way for companies to share information with the government. Although certain information must be kept classified, the government needs to be better at sharing unclassified information on cyberattacks, says Rep. Silvestre Reyes (D-Tex.), who chairs the intelligence committee. Office of the Director of National Intelligence's Ross Feinstein says the intelligence community works very closely with law enforcement on cyberattacks to share knowledge that might assist with investigations, and with the Department of Homeland Security to assist with infrastructure protection efforts. Kurtz also says the United States is heavily investing in technologies that are being stolen at little to no cost by the country's adversaries.

Report: Unauthorized Apps Run Rampant on Many Enterprise Networks

Dark Reading (09/15/08) ; Wilson, Tim

Many enterprises are supporting traffic on their networks from applications that they do not know they have and do not allow, concludes a Palo Alto Networks report. The report, which is based on data collected from evaluations of live traffic at 60 enterprises that use Palo Alto Networks' firewall, found that these companies were running a total of 290 unauthorized applications. Some of these programs were applications that most companies do not use for business, such as Google applications. However, others were applications that most IT departments do not allow because they are security vulnerabilities, such as peer-to-peer applications. The study also found that some of the extra applications traffic was from malware such as iFrame attacks, which were found in 86 percent of the enterprises, as well as various forms of spyware and attacks hidden in audio or video content. In an effort to root out these unauthorized applications, some of the companies involved in the study installed blocking or filtering software on their networks. But after receiving complaints from users, the companies decided to allow the applications and talk to the users about how to use them securely. Although this is sometimes the right tactic to take, blocking does make sense in cases where users are using applications that are big security risks and have little business value, says Palo Alto's Steve Mullaney.

Every Piece of Data Lengthens a Digital Shadow

Financial Times Digital Business (09/17/08) P. 8 ; Pritchard, Stephen

As individuals use the Internet and post personal information on blogs or on Web sites such as MySpace, Facebook, and LinkedIn, they create what London School of Economics professor Jannis Kallinikos calls a digital shadow. The need to control this digital shadow has become more urgent in the wake of reports that cybercriminals are accessing personal information from social networking sites and genealogy sites. Compounding the problem is the fact that banks and other organizations often use this same information to verify individuals' identities when they open new accounts or when they have forgotten the password needed to access an existing account online. As a result, cybercriminals who access individuals' personal information from the Web have been able to use it to commit identity theft and other types of fraud. One possible solution to this problem could be to move to using forms of authentication that do not require personal information to verify an individual's identity, such as tokens that generate one-time codes or biometric systems. Companies also could use outsourced authentication services to make it more cost effective and convenient for them to deploy large-scale authentication systems. However, only a few of these shared authentication services currently exist. If more of these services came into existence and more companies adopted stronger authentication systems, it would free Internet users to divulge whatever information they wanted without fear that it would be used by cybercriminals to steal their identities or hijack their credit card accounts.

Companies Can Learn from Hacking of Palin's E-Mail

USA Today (09/19/08) P. 6B ; Acohido, Byron

The recent hack of vice presidential candidate Sarah Palin's email account highlights the risks companies take when they allow employees to conduct business over free, Web-based platforms such as email, instant messaging, and toolbars. A recent survey of 60 companies by Palo Alto Network found all of them using a

variety of Web mail providers. The most popular were Hotmail, Yahoo Mail, Gmail, and AOL Mail. Most companies have policies allowing moderate use of free Web-based email, but unfortunately many employees ignore suggested best practices such as choosing an obscure password and using only secure connections, says Palo Alto's Chris King. The Palin hacker reportedly used Google searches to find Palin's ZIP code, birth date, and other information needed to answer password security questions on her Yahoo account.

Limbo malware grabs personal banking data

Trojan horse program adds data fields to legitimate online bank sites to trick consumers

By Stephen Lawson

September 26, 2008 (IDG News Service) A Trojan horse program now available to a growing number of fraudsters can add data entry fields to legitimate online banking sites and entice consumers to give up sensitive information such as bank card numbers and personal identification numbers.

The malware, Limbo, integrates itself into a Web browser using a technique called HTML injection, said Uri Rivner, head of new technologies at RSA Consumer Solutions. Because it's so closely integrated in the browser, it can operate even while the user is at the real bank site and can actually change the layout of that site, he said.

"Nothing tells you that something is wrong here, with one exception: You're being asked to provide some information that you were never asked to do before," Rivner said during a briefing for reporters and analysts earlier this week. "If you are convinced that you are now communicating with the bank, the fraudsters can get away with anything they like."

Limbo can get onto a user's computer through many paths, including both pop-up messages that ask you to download an add-on program and methods that are invisible to the user, he said. They sometimes get on to PCs in conjunction with other phishing attacks.

And like other malware programs, Limbo is becoming available to more fraudsters through an underground market that includes a complex supply chain and falling prices, according to Rivner. Limbo costs about \$350 (U.S.), down from about \$1,000 a year ago and \$5,000 two years ago, he said.

"The big trend here is that it's becoming affordable," Rivner said.

The online fraud marketplace consists of so-called harvesters, who collect user information and "cash-out" operations that use the information to do whatever has to be done to translate that information into money. For example, harvesters may capture credit card numbers and cash-out operations may use those cards to buy products online, have them delivered to an address and sell them on the black market, Rivner said. The two classes of fraudsters typically meet and do business with each other in IRC chatrooms and dedicated Web forums, where the most successful fraudsters are the ones who develop a reputation for working reliably and honestly with other participants, Rivner said.

Now, some fraudsters are taking a software-as-a-service approach, selling malware, access to botnets and everything else a person needs to become a harvester of data on unsuspecting consumers, according to Rivner. Having paid the price for this service, the harvesters can then take the identities stolen with it and sell them at a profit. The ease of going into business with this model may dramatically increase the volume of online fraud, he said.

"If phishing were a stock, I would invest in it," Rivner said.

At RSA, the encryption giant that became [EMC](#)'s security business through a \$2.1 billion acquisition in 2006, the target for combating online banking fraud is the cashing-out step. The company sells software that looks at every transaction a customer makes and assesses the level of risk, Rivner said. It may look at the IP address from which the site is being accessed, as well as that user's typical pattern of transactions. If the risk level is high, the bank can block the transaction and contact the customer directly, he said.

This approach is increasingly being used by banks because of the difficulty of tracking down and eradicating malware and phishing, Rivner said. There may be numerous Trojans on a customer's computer, but the bank isn't hurt by any of them until a fraudster tries to use them to divert money from an account, he said.

Gartner: Security risks rise as smart phones get smarter

Growing use of handhelds in business apps increases potential for attacks, analyst says

By Jeremy Kirk

- September 29, 2008 (IDG News Service) As wireless devices become more numerous [within businesses](#), their convenience will be counterbalanced by an increasing potential for [security problems](#), according to a [Gartner Inc.](#) analyst who spoke at the consulting firm's IT Security Summit in London today. New trends in the wireless industry are making it easier for hackers to launch [attacks targeting handhelds](#), Gartner analyst [John Girard](#) said. A few years ago, there wasn't much standardization across smart phones and other wireless devices, he noted. Differing operating systems and implementations of mobile Java — even varying configurations among devices with the same operating system — made it hard to write malicious code that ran on a wide array of devices, Girard said.

But that's changing, he added, saying that the process of writing malware that can run on a variety of handheld devices has been simplified. "The more your phone gets like a PC," Girard said, "the more it can [host malicious code](#)."

Many of the security threats that traditionally have plagued PCs, such as phishing attacks, will increasingly [move to mobile platforms](#), Girard predicted. That could cause problems, he said, when companies begin installing business applications on mobile phones, which will house data that is potentially valuable to attackers. "We're very quickly moving to the point where people really can [do business](#) on smart phones," Girard said.

Gartner forecasts that wireless identity theft and phishing attempts targeting mobile devices will become more and more prevalent next year. Girard said that before buying large quantities of handhelds for their workers, companies need to be sure that the devices meet a minimum set of security specifications, based on what kind of data the devices will handle and the regulations that businesses need to comply with under data protection laws.

Having the mobile hardware and software arrive in a secure state is a lot easier for IT managers than trying to fix devices after they've been deployed in the field, he added.

Girard laid out a few key [security pointers](#): Data should be encrypted on handhelds, proper identity and access controls should be implemented, and intrusion-prevention systems should be used to ensure that rogue devices don't access sensitive information, he said.

Are Employees Really to Blame?

A New Look at Who is at Fault For Breaches of Personal Information

ARLINGTON, Va.--([BUSINESS WIRE](#))--More than 244 million private records have been lost by companies and government agencies since 2005 with almost all of these losses being blamed on employees' risky behavior. However, before assigning blame, organizations might want to take a look in the mirror, according to a new, first-of-its-kind study by the Information Risk Executive Council (IREC), a program of the Corporate Executive Board (NASDAQ: EXBD).

“The irony here is that employees actually want to do the right thing, they just need a little help,” says Jeremy Bergsman, Ph.D., the lead author of the study. “Our study shows that most companies either don’t do much to educate employees about information security, or the training is not based on what actually works to help employees do the right thing.”

This study shows that more than a third of risky employee behavior is caused by security guidelines and procedures that are too hard to follow according to the 57,000 employees from 60 global corporations included in the survey. Moreover, 46% of risky behavior can be addressed with proper training and incentives – something companies rarely do effectively, wasting millions of dollars in training costs.

The research identifies three key insights to consider when designing information security “awareness” efforts. First, do not focus on scare tactics or technical explanations, but instead provide clear instructions about what employees should do in a way that is relevant to employees’ actual jobs. Second, incentives—as simple as token gifts or a word from a manager—are just as effective as more costly training efforts. Third, while security professionals tend to think first about punishments for misbehavior, rewards for good behavior are just as effective. Positive incentives allow companies to reach the majority of employees that tend to do the right thing, rather than waiting for something bad to happen before they can act.

IREC, the leading consultancy for Chief Information Security Officers and other senior Information Risk executives, took this research beyond measuring employee behavior related to security, to include the psychology behind those behaviors and what companies should do to change risky behavior. This unique focus and the large sample size make it the best information available to guide information security awareness efforts.

The survey used in the study is available on an ongoing basis to organizations that would like to assess their current awareness efforts and learn how best to create a culture of security. It is available in English, Spanish, French, and other languages.

Dr. Bergsman says, “Our work allows companies to take an understanding of employee psychology and turn it into a huge reduction in risky employee behavior -- often without increasing spending. In fact, in most cases spending on employee behavior gets you more bang for the buck than the technology solutions that IT people usually gravitate to.”

Firms ignoring risk of security breaches

Logica survey uncovers alarming complacency at UK companies

Written by David Neal
[Computing](#), 24 Sep 2008

A new survey from business services firm Logica has found a remarkable lack of awareness about how to manage data and respond to the risks of security weaknesses in enterprise systems.

The study, released today, found that a minority of firms educate staff on how to cope with data breaches, or even how to handle information in the first place.

Logica said that just 30 per cent of firms educate staff in IT security, and roughly the same amount have an in-house team with the specific remit of handling security incidents.

Alarmingly, in this compliance-centric enterprise environment, only a quarter of firms are complying with ISO 27001/2, an international standard that covers security procedures when storing personal data.

Perhaps worse is the fact that firms are not reporting breaches to their clients. Logica said that 60 per cent of companies that have experienced a data breach did not tell their clients, and half failed to tell the police or authorities.

Tim Best, director of enterprise security solutions at Logica, said: "Data losses put customers at risk and can lead to large contracts being withdrawn.

"With some organisations failing to disclose security breaches, this complacent attitude not only increases the likelihood of financial and reputational consequences, but highlights inadequate security policies and protocols at UK organisations."

Overall the study found that 57 per cent of those firms surveyed had no understanding of the impact of a security breach on their organisation.

Mobile workers are leaking your data

Blurred lines between business and home cause risky behaviors, study says.

By Jim Duffy

October 1, 2008 (Network World) Numerous behavioral risks taken by employees in increasingly distributed and remote locations can lead to the loss of corporate information, [according to a study](#) commissioned by Cisco Systems Inc.

[Cisco](#), which is banking a large chunk of its growth on collaboration, says that as workforces become increasingly mobile, lines are blurring between work life and personal life. This could lead to risky or reckless use of company IT resources, resulting in leakage of sensitive data, the company says.

"Businesses are enabling employees to become increasingly collaborative and mobile," said John Stewart, Cisco's chief security officer, in a statement. "Without modern-day security technologies, policies, awareness and education, information is more vulnerable."

The study, conducted by InsightExpress LLC and commissioned by Cisco, is based on surveys of more than 2,000 employees and IT professionals in 10 countries. It is intended to examine [security](#) and data leakage implications for businesses as employee lifestyles and work environments are becoming increasingly untethered from a fixed location. It also identifies common data leakage mistakes and risk management opportunities among workforces around the world as this new workplace paradigm is increasingly adopted.

The study surveyed 1,000 employees and 1,000 IT professionals from various industries and company sizes in 10 countries: the U.S., the U.K., France, Germany, Italy, Japan, China, India, Australia and Brazil. The countries were chosen because they represent a diverse set of social and business cultures, established and emerging network-dependent economies, and varied levels of Internet adoption, Cisco says.

According to Cisco, these were the 10 most noteworthy behavioral findings:

1. Altering security settings on computers: One out of five employees altered security settings on work devices to bypass IT policy so they could access unauthorized Web sites. More than half said they simply wanted to access the site while one-third said, "it's no one's business" which sites they access.

2. Using unauthorized [applications](#): Seven out of 10 IT professionals said employee access of unauthorized applications and Web sites ultimately resulted in as many as half of their companies' data loss incidents. This belief was most common in the U.S. (74%) and India (79%).
3. Having unauthorized network/facility access: In the past year, two out of five IT pros dealt with employees accessing unauthorized parts of a network or facility. Of those who reported this issue, two-thirds encountered multiple incidents in the past year and 14% encountered this issue monthly.
4. Sharing sensitive corporate information: One out of four employees admitted verbally sharing sensitive information with nonemployees, 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."
5. Sharing corporate devices: Almost half of the employees surveyed share work devices with others, such as nonemployees, without supervision.
6. Blurring of work and personal devices and communications: Almost two out of three employees admitted using work computers daily for personal use. Activities included music downloads, shopping, banking, blogging and participating in chat groups. Half of the employees use personal e-mail to reach customers and colleagues, but only 40% said this is authorized by IT.
7. Leaving devices unprotected: At least one in three employees leave computers logged on and unlocked when they're away from their desk. These employees also tend to leave laptops on their desks overnight, sometimes without logging off, creating potential theft incidents and access to corporate and personal data.
8. Storing log-ins and passwords: One in five employees store system log-ins and passwords on their computer or write them down and leave them on their desk, in unlocked cabinets or pasted on their computers. In China, 28% of employees reported storing log-ins and passwords to personal financial accounts on their work devices.
9. Losing portable [storage](#) devices: Almost one in four employees carry corporate data on portable storage devices outside of the office.
10. Allowing "tailgating" and unsupervised roaming: More than one in five German employees allow nonemployees to roam around offices unsupervised. The study average was 13%, and 18% have allowed unknown individuals to tailgate behind employees into corporate facilities.

Cisco says these findings can help companies sculpt global risk management plans. To prevent data loss, the company recommends practices such as these for preventing data loss:

- Establish security awareness, education and training.
- Know how/where data is stored, accessed and used.
- Protect data as if it were money. Educate employees about how data protection equates to money earned and data loss equates to money lost.
- Institutionalize standards for safe conduct by determining global policy objectives and creating localized education tailored to a country's culture and threat landscape.
- Foster a culture of trust between employees and IT.

The study's release comes shortly after a Cisco executive noted the security vulnerabilities of virtualization and cloud computing during an industry trade show [keynote address](#). Cisco is also relying heavily on these market trends for its [future growth](#).

Despite Threats, Companies Lag on Web 2.0 Security

Industry Standard (09/24/08) ; Goodchild, Joan

A new study by Colorado-based security software manufacturer Webroot says companies are performing poorly when it comes to protecting against Web 2.0 threats. Out of the 648 organizations surveyed in the United States, Britain, Australia, and Canada, 30 percent have had their corporate Web platforms compromised by employees using Web-based emails, downloading content, and visiting social-networking sites. More than one in three employers believed their employees spent an hour or more each day using the Internet for leisure instead of work. Employers are paying much attention to email-based threats but are still essentially ignoring the largest nemesis: Web-based attacks brought on by employee Internet use, according to the study. Webroot researchers found that 85 percent of malware is now disseminated through Web sites and cited research indicating that 49 percent of employers do not regulate employee access to social-networking sites, which do not filter for malware.

Information of the World, Unite!

Scientific American (09/08) Vol. 299, No. 3, P. 82 ; Garfinkel, Simson L.

Privacy advocates are concerned about the potential ramifications of data fusion, in which databases are linked together, writes Naval Postgraduate School computer scientist Simson L. Garfinkel. However, this integration is a more challenging proposition than many people assume, and appears to be restricted to specific contexts due to a number of factors, including the high incidence of errors and meaningless coincidences in databases. Distinguishing worthless from valuable information is a formidable problem for data fusers, as is correctly identifying people and things when names are shared by multiple individuals or objects. One industry that has fueled a great deal of innovation in identity-resolution systems is Las Vegas gambling, which is striving to exclude cheaters and self-declared problem gamblers from its gaming establishments. Casinos have invested in the development of the nonobvious relationship analysis (NORA) method, which involves the combination of identity resolution with databases of credit companies, public records, and hotel stays. A NORA system is designed to construct hypotheses based on the data, and then update these hypotheses as new data becomes available. Garfinkel speculates that society may be placing unreasonable demands on data fusion, and the failure of data-fusion systems could just as easily stem from flaws in their algorithms as from a lack of data. He adds that a dearth of public information about data-fusion systems in actual use is also a source of frustration to scientists.

Can Security's Human Side Stop Data Breaches?

As human error increasingly becomes the top reason for security breaches, behavior-based strategies are making their way into the workplace to supplement technology

By [Joan Goodchild](#), Senior Editor

October 06, 2008 — [CSO](#) —

Shira Rubinoff was a practicing psychologist in 2004. When it came to technology, her experience was simply as a tech user, certainly not a tech guru. Then one day she was phished.

"After it happened, I was like: "There's got to be a better solution out there. Because once you put security in people's hands, so much can happen."

Rubinoff decided to take her background in human behavior and turn it into a security software firm that taps into how the mind works in order to prevent [phishing](#) attacks. Her New Jersey-based company, Green Armor, provides a product that uses a visual cue on the Web log-in page that is unique to each user of the site. The cue is generated using a mathematical formula based on the user id. It uses a colored box and a short word, a method she developed after extensive research and experimentation about how users memorize and retain information.

The idea, according to Rubinoff, is that users will know if something is amiss much easier than with the usual authentication techniques currently used by many online [banking](#) and other secure sites.

"This approach deals specifically with the humanistic factors of technology," said Rubinoff, who was recently named a "Women of Influence" award winner at the Executive Women's Forum because of her work on the software. "I think other technology out there look for technology problems. They forget there is a person sitting behind the computer that is very easily manipulated."

Human behavior is increasingly becoming a hot area of focus in security. In fact, a new study from networking giant [Cisco](#) says risky behavior tops the list of reasons for security breach. The study, which surveyed 1,000 employees and 1,000 IT professionals from various industries and company sizes in 10 countries, was conducted to examine security and data leakage at a time when [employee lifestyles and work environments are changing dramatically](#).

"We conducted this research in order to understand behavior, not technology per se," said John N. Stewart, chief security officer of Cisco. "Security is ultimately rooted in users behavior, so businesses of all sizes and employees in all professions need to understand how behavior affects the risk and reality of data loss - and what that ultimately means for both the individual and enterprise."

The research found one in five surveyed admit to altering security settings on computers. Additionally, one of four employees admitted verbally sharing sensitive information to non-employees. And a whopping seven in ten surveyed said they regularly use unauthorized applications at work.

Similar findings from consulting firm Deloitte earlier this year back up the Cisco research. A Deloitte survey of more than 100 companies found 75 percent cited human error as the leading cause of security failures.

Green Armor is one of several companies with a product that is based on human behavior. A quick [Google](#) search turns up many antivirus and malware solutions that utilize behavior analysis. Most of the major antivirus software makers, such as [Symantec](#) and McAfee, have implemented some kind of behavior-based defense into products.

A California-based consultancy called Security Mentor, which only launched in April, is hoping to find business in an approach that goes right to the source: the user. Security Mentor offers training that, according to founder and President Marie White, takes on a brief, frequent and focused approach. Employees take part in weekly, seven-minute-long informational Web sessions that teach and reinforce good security habits and practices.

"There is wide spread information at this point that employees are one of the greatest threats to an organization," said White. "But the question is: Why do they remain the greatest threat? One can assume they are either intentionally or unintentionally engaging in risky behavior. Most people agree it's unintentional. This training addresses that."

Security Mentor, which launched at the RSA conference, is still in the start-up phase, according to White. While the firm is not working with any customers yet, there is interest from a wide-swath of commercial and government organizations, she said.

White said in developing the sessions, she also took into account how the [typical employee](#) works today. The sessions are short to fit the attention-span criteria of a busy person. They are regular so that retention of information will be more effective.

"We consider how employees multi-task and the training fits in that attention span window," said White. "Also, how often people get interrupted coupled with how they remember. And the frequency of having training weekly makes it a lifestyle difference for employees."

Reported Data Breaches in US on the Rise

(October 6, 2008) According to statistics compiled by the Identity Theft Resource Center, there have been 516 reported consumer data breaches in the first nine months of 2008, exposing 30 million records; in 2007, the total number of reported breaches was 446. Extrapolated from the numbers so far this year, the total number of reported breaches in 2008 could top 680.

Eighty percent of the breaches involved digital media; the remaining 20 percent involved data recorded on paper. Of the incidents this year, 36 percent occurred at businesses, 21 percent occurred at educational institutions, and 16 percent on military or federal government systems. Twenty percent of the reported breaches were due to lost or stolen digital media storage devices, 17 percent were due to insider theft and 13 percent were exposed through hacking.

The Snake Within

Governing (10/08) Vol. 22, No. 1, P. 60 ; Perlman, Ellen

After studying 49 insider cyberattacks, Carnegie Mellon's Software Engineering Institute Computer Emergency Response Team (CERT) developed a model that could help IT managers in state and local governments to understand and mitigate the risk of such threats. CERT's study found that people who perpetrated cyberattacks on their own organization were database or system administrators who often did not get along well with others or were unable to take criticism. The study found that these people were often provoked into launching an attack against their organization when they did not get a raise they felt they deserved or when they were punished in some other way. Once the employees have been provoked, they create "back door" accounts that only they can access. The employee can then use that account to plant a logic bomb or a time bomb that will wreak havoc on the organization's IT systems, days, weeks, or even months after they quit or have been fired. CERT's Dawn Cappelli says employers can diminish the threat of such attacks by demoting or firing such employees when they begin to notice bad behavior. Unfortunately, many organizations leave themselves vulnerable to insider attacks by choosing to ignore such behavior, she says.

Does Patch Management Need Patching?

CSO Online (10/01/08) ; Cook, Rick

Verizon's "2008 Data Breach Investigations Report" found that 90 percent of successful cyberattacks target vulnerabilities for which a patch has been available for at least six months. The report also found that no security breaches occurred when vulnerabilities were patched within a month of an attack. The study's findings indicate that organizations can prevent data breaches more effectively by using a patch deployment strategy that focuses on coverage and consistency, instead of patching systems as soon as patches are released. As part of this strategy, one of the first things organizations need to do is to take a complete inventory on all the systems on their network. This can be done with the help of an inventory program at all but the smallest of organizations. Next, organizations need to develop a process for installing and managing patches. Such a process should be backed up by the appropriate software.

Companies Own Up to Virtual Security Blind Spot

Techworld (10/01/08) ; Jowitt, Tom

Most companies have scant or nonexistent security in place to protect their virtual systems, concludes a Shavlik Technologies survey of 300 IT virtualization and security experts at the recent VMWorld 2008 conference in Las Vegas. Shavlik's Neil Butchart says it is becoming more routine for data centers to deploy virtual machines (VMs). "In general we are finding in talks with customers that at least 99 percent of them plan to add VMs now or in the near future," he says. Nevertheless, Shavlik says many companies are not taking security risks seriously enough. Over 80 percent of survey respondents said that securing their VMs was "very important to critical," but nearly two thirds of those surveyed do not have any protections in place for these systems. Conference attendees also were asked if their IT infrastructure received industry or government audits, and if these audits extended to VMs. About 61 percent responded affirmatively, and nearly all of the delegates said it was critically important to centralize virtual and physical system patch management. Nearly one third said they had no security strategy in place to secure virtual environments, even though it is a requirement, and 37.8 percent were deciding between solutions for virtual security.

Credit-Card Security Standard Issued After Much Debate

Network World (10/01/08) ; Messmer, Ellen

On Oct. 1, the Payment Card Industry Security Standards Council issued the PCI 1.2 data security standard (DSS) after considerable deliberation. The new standard seeks to clear up points that left many people confused. One such point was that all operating systems associated with card processing are required to run antivirus software, not just Microsoft Windows. A hot topic at the council's recent meeting in Orlando, Fla., was how to define "network segmentation" because the PCI standard targets the development of technical methods to shield off the credit card storage area in order that PCI compliance evaluation can concentrate on specific segments of a merchant's network involved with cardholder data, and not the entire organization. The PCI 1.2 standard clarifies that today's network segmentation "is not a requirement," but notes that "without network segmentation the entire network is in the scope of the PCI DSS assessment." The standard recommends the use of network-restricting technologies such as internal firewalls to guarantee internal network segmentation for card-processing purposes, while council general manager Bob Russo says the biggest issue for merchants is a rule requiring that new deployments of Wired Equivalent Privacy (WEP) are banned after March 31, 2009, while by June of the following year all WEP must be jettisoned. Next year the council will focus on the establishment of security guidelines for unattended payment terminals, including ATMs and other kinds of vending machines that process payment cards. End-to-end encryption could emerge as a primary issue as the council seeks advice on how this might best be accomplished in the payment-card space via different technologies, while another issue the council plans to debate is how to ascertain the best method for protecting card data in the virtualization environment.