

# Security Trends Report

05/09

## Cyber Intruders Claim to Hold Personal Health Data Hostage

(May 4, 2009) A posting on Wikileaks.org claims that cyber attackers stole data of about eight million patients from the Virginia Department of Health Professionals' Virginia Prescription Monitoring Program website; they are demanding US \$10 million in ransom for their return. The intruders claim to have encrypted the database and protected it with a password.

That particular site is presently unavailable as are several others related to the Virginia Department of Health Professionals. The ransom note says that if the money is not paid within seven days, the data will be offered for sale. Federal and state authorities are investigating.

## Survey: 7 of 10 IT pros have found sexual, other inappropriate material on employees' laptops

Finding points to behavior that heightens risk of data breaches, researcher says

By Eric Lai

April 16, 2009 (Computerworld) Nearly three-quarters of corporate security and IT professionals in the U.S. have found "inappropriate" pictures, videos or browser cache links on employee laptops, a survey released Wednesday shows.

Two-thirds of the 3,100 IT pros anonymously surveyed by the Ponemon Institute had found "evidence of inappropriate interactions with other employees" of an adult nature on company-issued laptops. A slightly smaller percentage, 63%, found resumes and other evidence of job searches.

Larry Ponemon, chairman of the research group behind the study, said the findings pointed to risky behavior by employees that heightened the potential for data security breaches.

These risks were expected to rise, according to the Web-based survey, which queried IT and security pros from six countries, including the U.S., U.K., Germany, France, Mexico and Brazil.

Those surveyed said that between 23% and 33% of employees' main devices were currently laptops. In five years, they said, that figure is expected to nearly double, to 55% of users in Mexico and as many as 65% of users in Germany. Use of laptops in the U.S. is expected to reach 64%.

The [survey](#) found some interesting, significant cultural differences in how laptops were lost, stolen or otherwise put at risk.

In most countries, losing a laptop in a hotel was the greatest risk. But in Brazil and Mexico, the risk of losing a laptop in a rental car or the airport -- usually the second and third most common locations for loss in the U.S., France, Germany and the U.K. -- was practically nonexistent. About half of the IT pros in Brazil and Mexico reported laptops were commonly stolen from users' homes.

Among U.S. and European workers, laptops were more often damaged during travel. In Brazil and Mexico, more than a third of the IT pros said laptops were damaged mostly due to "employee inflicted damage because of anger or frustration" or from "dropping the laptop accidentally."

The information that posed the greatest potential risk if a laptop was lost or stolen varied by country, the survey found. In Germany and France, it was employee records. In the U.S., it was customer information such as contact lists. In Brazil and Mexico, it was confidential financial information.

Despite the anonymous nature of the Web survey, Ponemon said the results probably understated the true scope of the problems, as respondents with serious breaches or losses were probably too embarrassed to respond.

The survey was sponsored by Dell Inc., which announced Thursday that it would offer solid-state drives (SSD) with full-disk encryption on its Latitude E line of business laptops.

Ponemon said full-disk encryption would "make a big difference" because companies are not doing "such a great" job otherwise to reduce the security risks of laptops.

## With Budgets Tight, US Companies Still Plan to Spend on IT Security

(April 13, 2009) The results of a survey from Robert Half Technology indicate that a majority of companies plan to invest in IT security projects despite the tough economy. Seventy percent of chief information officers responding to the survey said their organizations plan to spend funds on IT security initiatives. The survey includes responses from 1,400 CIOs at US companies with 100 or more employees. Other IT areas in which the CIOs expected to invest include virtualization, data center efficiency, VoIP and social networking.

[http://www.csoonline.com/article/489109/Report\\_Security\\_Tops\\_IT\\_Budget\\_Priorities](http://www.csoonline.com/article/489109/Report_Security_Tops_IT_Budget_Priorities)

[Editor's Note (Pescatore): Threat-facing security spending is usually pretty recession-proof. However, spending that is tied to business expansion obviously does get hit, so there is slowdown in desktop and branch-office related security spending.

(Skoudis): I was surprised to see social networking as an investment area for enterprise CIOs. Yes, I know it's a hot area, but I didn't expect one-fifth of CIOs would mention it as an area to invest their precious resources in. Given the security issues that are rampant in social networking and money flowing into that space, it's going to keep us security professionals busy for quite some time, no doubt.]

## Despite downturn, IT security spending to increase

[Angela Moscaritolo](#) April 13, 2009

Management increasingly is recognizing security as a top business priority, which is resulting in higher budgets for some organizations despite the economic slowdown, according to a new survey.

The survey from the Computer Technology Industry Association (CompTIA), an IT trade group, compiled the responses of 1,538 organizations of varying sizes in the United, Canada, India, UK and China.

According to the survey, regardless of region, the mean spending for security-related technologies now is \$719,930, an increase of 20 percent compared to last year.

Forty percent of organizations said they will spend more on security technologies this year and 32 percent will spend more on security training, the survey concluded. Another 33 percent will increase spending on security-related processes and 21 percent will allocate more cash for certifications, according to the survey. Spending decreases in these areas are only expected to happen in about four percent of organizations.

But concessions still need to be made in light of the economy. The survey showed that fewer companies -- 45 percent compared to 53 percent -- in the United States are providing security training for non-IT employees this year compared to last.

Still, there is good reason that management is earmarking more funds toward security budgets. Breaches remain an issue and have increased slightly over last year. Twenty-nine percent of U.S. respondents said they experienced at least one to three data-loss incidents.

The primary cause of breaches was human error, followed by a failure to follow security policies -- which are rising in prevalence, according to the survey.

Written IT security policies were adopted in more than 63 percent of U.S. organizations in 2008, but only in about 40 percent of small firms, defined as having 99 employees or fewer, the survey found.

Across the threat landscape, spyware is the most prevalent danger facing organizations, followed by viruses and worms, and a lack of user awareness.

But Scott Crawford, research director at research firm Enterprise Management Associates, told SCMagazineUS.com Monday that there seems to be an "awareness gap" between the threats organizations are concerned about and what actually is happening.

"It is a little surprising that I didn't see more about web application security concerns given that major vendor research reports have talked about web app vulnerabilities being the majority of vulnerabilities they see," Crawford said.

Web application vulnerabilities "unquestionably" are the most prevalent flaw affecting servers today, according to an IBM report released this January. In addition, vulnerabilities in web applications made up [80 percent of all web-related flaws](#), according to report released last month from security vendor Cenxic.

## **Privacy rules hamper adoption of electronic medical records, study says**

Choice for policy-makers may be between tough patient privacy rules and speedy EMR deployments, researchers claim

**By Jaikumar Vijayan**

April 14, 2009 (Computerworld) In a study that is unlikely to find favor among [privacy advocates](#), researchers from two academic institutions warned that increased efforts to protect the privacy of health data will hamper the adoption of [electronic medical records](#) systems.

The [study](#), conducted by researchers at MIT and the University of Virginia, said EMR adoption is often slowest in states with strong regulations for safeguarding the privacy of medical records.

On average, the number of hospitals deploying EMR systems was up to 30% lower in states where health care providers are forced to comply with strong privacy laws than it was in states with less stringent privacy requirements. That's because privacy rules often made it harder and more expensive for hospitals to exchange and transfer patient information, thereby reducing the value of an EMR system, the study found.

"Despite EMR's effectiveness at reducing medical errors and improving baseline indicators of patient health, hospitals are deterred from adopting it by strong health care privacy laws," the study states.

The results of the research, which looked at EMR adoption in 19 states over a 10-year period, was originally presented at a Federal Trade Commission workshop in April 2008. It was publicly released only this week following its acceptance in the journal *Management Science*, an MIT spokesman said.

The research suggests that there's a trade-off between achieving fast adoption of EMR technology and strong health care privacy laws, said Catherine Tucker, an assistant professor of marketing at MIT's Sloan School of Management and one of the report's authors. In general, while medical privacy is a good thing, it doesn't always allow for quick adoption of EMR systems, she said.

"What we found was that privacy laws are getting in the way of hospitals" trying to exchange information with one another, Tucker said. "Policy-makers are going to have to choose how much EMR adoption they want and at what cost to patient privacy."

It's a viewpoint that is unlikely to sit well with privacy advocates, who are already nervous about the accelerated move to a nationwide EMR system under a [health care modernization program](#) announced by President Obama earlier this year. The Health Information Technology for Economic and Clinical Health Act was introduced by Obama as part of the economic stimulus package earlier this year. It provides \$20 billion for the creation of a

[national electronic health records system](#) that would fundamentally improve the way health information is electronically accessed, stored and shared.

Health care security experts and privacy advocates cautiously lauded the bill for the many provisions it includes for protecting patient health care data. However, they claimed it doesn't go far enough in addressing all the privacy concerns raised by the use of EMR systems, although they have acknowledged the bill is a step in the right direction.

Among the welcomed provisions are those that require health care organizations and professionals to implement better controls over who can access and share different categories of medical information. Also seen as long overdue is a provision that prohibits health care providers from selling protected health information in electronic medical records and imposes limitations on the marketing of such data.

Such requirements have been considered long overdue in the health care sector. "However, if the end result of Obama's new privacy legislation is to add extra layers of complexity and necessitate hospital-specific customization of privacy filters, then there is the potential for there to be a negative effect," Tucker said.

Hospitals and other health care entities are often reluctant to implement an EMR system if it requires a lot of customization in order to accommodate privacy requirements, she said. For example, if a state law allows only specific groups of people within an organization to access specific kinds of medical information, a hospital might need to implement filters and access controls to comply with the requirement, she said. Such customization also can be costly, which is another factor that results in slower adoption of EMR in states with stringent privacy requirements, Tucker said.

Deven McGraw, director of the health privacy project at the [Center for Democracy and Technology](#), blasted the study's conclusions. She said the study was based on old data and didn't consider all of the factors that a health care organization would typically look at when deciding whether to adopt an EMR system.

The study simply looked at whether a state has a medical privacy law and then looked at EMR adoption in that state to draw its conclusions, McGraw said. What it doesn't appear to have done is to examine whether other important factors, such as funding and business value, might have also had an impact on EMR adoption. Often health care providers point to those two issues as being the two most important considerations when making decisions on EMR systems, she said. As a result, the study is "not of much value," she said.

"We just had \$19 billion put on the table by the federal government to spur adoption of electronic medical records," McGraw said. "There's been an acknowledgment by this Congress that you need privacy protections," for people to begin trusting their health care data to EMR systems. Trying to suggest at this stage that policy-makers might have to choose between privacy and speedy adoption of EMR technology is disingenuous, she said.

Deborah Peel, who founded and chairs the Patient Privacy Rights Foundation in Austin, also slammed the study. Suggesting that privacy protections could hamper adoption of e-health systems is "preposterous," Peel said. The fact that only about 5% of hospitals nationwide have implemented EMR systems thus far has nothing to do with privacy issues, she added.

"There are many reasons why there is low adoption, but privacy is not one of them," Peel said. EMR systems are costly and can be "prone to errors and glitches," she added. "A lot of them don't work well, so hospitals and physicians don't like them."

## 'Mafiaboy' spills the beans at IT360 on underground hackers

Social engineering plays a major part in computer hacking

**By Jennifer Kavur**

April 14, 2009 (ITWorldCanada) Attending IT360 last week didn't guarantee you a seat at Michael Calce's keynote with Craig Silverman. The conference room reached full capacity and left a crowd of onlookers spilling into the hall outside the doors.

Calce -- a.k.a. Mafiaboy, the Montreal teen hacker who was the subject of an international manhunt after bringing down some of the highest-profile Web sites on the Internet -- delivered on his promise to provide insight into underground hacker communities.

Social engineering is a much larger aspect of hacking than people think it is, said Calce. "Hackers rely on you to be naïve. They are counting on it," he said.

Internal IT hackers in your company are still more of a threat than remote exploits or denial-of-service attacks, he pointed out. Calce suggested securing your organization before worrying about outside threats.

"You have to integrate some type of security awareness program and training for your employees, because people are still being socially engineered and it's still a very viable threat," he said.

Calce delved further into the hacker mindset in a postconference interview. "They're all about people manipulation skills," he said. "One way or another, you have to manipulate someone."

Hackers can just dress up in a telephone company uniform and walk into your office, Calce explained. Some will print documents saying they work with the phone company or carry order and supply forms.

"As long as you look like you're there for what you're supposed to be doing, they don't really question why you're there -- especially if you do it well. If you're good and you keep a solid face and you have paperwork or a hat that goes with your façade, it's very effective," he said.

"People aren't expecting that angle," Calce explained. "They think that they secure their networks and they're not vulnerable. It doesn't necessarily operate like that. Hackers always think outside the box."

Keeping all angles in mind is an important part of evaluating a company's risk factor, according to Calce, who is forming his own penetration testing company. "I will be doing a lot of technical work and verifying their networks, but a huge portion of it is also social engineering -- how can I get in at the front desk," he said.

Even with the proper training and education, employees might continue to be the weak link in an organization. "They don't really care what happens to the company as a whole. They care about the paycheck they get, they do their job and they go home. But people need to take it to heart and realize that there is a lot at risk," he said.

Calce pointed out the benefits of hiring an ex-hacker during the keynote, which took the form of an interview with Silverman on stage. "You know the ins and outs, you know the way the community works, you may have leaks of information on zero-day exploits that aren't public," he said.

But former hackers have to work hard to gain respect and rebuild credibility with the industry, he explained. "You really have to show that your motivations are on the right side and hopefully people will see that, because there's no 100% definitive way to know if someone has been completely reformed," said Calce.

There are ways to explore technology and satisfy your curiosity without participating in illegal hacker practices, he noted. "You can set up your own network and infiltrate it like that. Set up an operating system and go ahead and see what you can do with it. You don't need to illegally access [a] computer."

Calce addressed further issues during a question-and-answer period with the audience, which included a query about whether or not he had a valid passport.

One attendee asked whether Calce believes there is a way to get ahead of hackers or if IT will always be playing catch-up. "Unless we rebuild the Internet and various protocols, it's always going to be them striking first and us answering back with patches," he replied.

Hacking the hackers would solve a lot of problems, but it's illegal to do so, Calce pointed out. "You need a government institution with the rights to do that," he said.

Calce said his own systems have never been compromised. "I run Unix servers, so I'm constantly maintaining. I'm always watching the logs. Unless there is someone in my systems who is very undetectable, to my knowledge, nothing has been tampered with."

Zero-day exploits are among the biggest threats, according to Calce. They are normally effective because they haven't been out for long, so people don't know about them and there aren't patches out there yet, he said.

Calce suggested a government-level certification process for software releases. "Not one individual in here sees every piece of code that's going out there," he said. "We need some type of hierarchy that monitors what is being released. Obviously, there is not enough debugging and there's not enough bug checks out there."

Another question focused on Calce's distrust of online banking systems. "Down the line in the future, I believe... all these wonderful things will be safe. But as it stands today, I don't have confidence in them," he said.

"We are advancing too quickly for our own good.... We are constantly creating new technology without fixing predecessor technology and making sure that is secure before moving on.... We need to secure things before we move down the line. We're just jumping ahead and we're not stopping. We're not even looking back," Calce said.

## Report: Cyberspace remains a dangerous frontier

---

### Rise in botnet activity in 2008 reverses gains made from aggressive law enforcement in 2007

By [William Jackson](#)

The number of compromised computers actively being used in botnets to launch attacks on any given day last year was about 75,000, according to a new report on Internet threats from security firm Symantec Corp.

"That number actually went up about 31 percent from 2007," said Zulsikar Ramzan, technical director for Symantec. That was due largely to aggressive action against botnet operators by the FBI in 2007, he added. "What we're seeing is a long-term game of whack-a-mole," in which operators knocked down in one place quickly reappear somewhere else.

The figures [appear](#) in Symantec's *2008 Government Internet Security Threat Report*, culled from the company's broader annual Internet threat report. Data for the reports were gathered from Symantec's global network of 250,000 network sensors.

The report paints a picture of a fluid world in which people who launch attacks — which can include hackers, as well as organized criminal syndicates and possibly even nation-states using their services — adapt to changing conditions to stay at least a step ahead of security companies and law enforcement.

Law enforcement is becoming better educated in dealing with online crime and international cooperation appears to be improving, Ramzan said. However, there still is room for improvement; better public awareness also is needed as attacks become stealthier.

"The threats we're seeing today are much more silent but much more deadly," he said. Persons whose computers are being exploited often are not aware of the compromise.

The overall number of threats is increasing quickly. Ramzan said that the number of signatures for malicious code maintained by Symantec for more than 20 years doubled in 2008. Surprisingly, only 3 percent of code

exploits identified in 2008 exploited vulnerabilities in IT systems, down sharply from 2007. Most malicious code relied on social engineering or was downloaded from a command-and-control server onto an already compromised computer.

Malicious online activity usually is being driven now by an increasingly sophisticated underground economy in which specialized services, malware and botnets of compromised computers are offered for sale, and the resulting stolen information is wholesaled and retailed on underground servers. Credit card information is the most common commodity being offered for sale, accounting for 32 percent of the total last year, up from 21 percent the year before. Two-thirds of the stolen accounts were from the United States.

Government networks accounted for 20 percent of breaches of personally identifiable information in 2008, in second place behind the educational community with 27 percent. The average cost of a data breach was estimated at \$6.7 million, and by the end of the year 44 states and the District of Columbia, Puerto Rico and the U.S. Virgin Islands had data breach notification laws.

Despite the profit motives, the most common attack against government systems last year was denial of service, accounting for 48 percent. Attacks against e-mail servers accounted for 18 percent and against Web servers 11 percent. The Domain Name System accounted for just 4 percent of attacks, but because DNS underlies so much Internet activity that is a particularly sensitive area. The U.S. government is in the process of implementing DNSSEC within the .gov top level domain this year.

China was identified as the top source of attacks against government systems in 2008, accounting for 22 percent of the total, up from just 8 percent in 2007.

“The United States ranked second in 2008 for attacks targeting government, with 12 percent of the total, a decrease from 20 percent in 2007,” the report said. “This drop is likely due to the shutdown of two ISPs in September and November 2008, which resulted in a dramatic drop in both bot [command and control] servers and bot-infected computers.”

The origin of attack is determined by the IP address of the computers being used to deliver the attacks, Ramzan said. Because the person controlling those computers could be anywhere in the world, it is difficult to know how much importance to give to country-of-origin figures.

“The origin of the attacks might not be the same as the origin of the attacker,” Ramzan said, and source figures might say more about the country as a victim of attacks rather than as a perpetrator.

## **Botnets: 4 Reasons It's Getting Harder to Find and Fight Them**

***Researchers say vulnerable Web 2.0 applications and peer-to-peer architecture are making it easy for hackers to maintain armies of hijacked computers***

By [Bill Brenner](#), Senior Editor

April 15, 2009 — [CSO](#) —

The perpetual proliferation of botnets is hardly surprising when one considers just how easy it is for the bad guys to hijack computers without tipping off the users.

Botnets have long used a variety of configurations, in part to disguise their control mechanisms. But as user-friendly but insecure applications continue to become available -- especially [social networking programs used by the non-tech-savvy](#) -- hackers have an ever growing number of security holes to choose from. They're also getting smarter about building resilient architectures, according to botnet hunters who have monitored recent activity.

Here are four reasons the botnet fight is getting harder, and what to do about it:

## 1. Operating below the radar

While much of the attention lately has been on botnet activity related to the Conficker worm researchers say some of the largest botnets have largely escaped media attention. And that's how the bad guys like it.

Alex Lanstein, senior security researcher at FireEye Inc., a security vendor based in the San Francisco Bay area, said this is because their overlords don't want to make news and let people know their machines are infected. Cimbot, for example, is a piece of malware that has been used to create a botnet that now accounts for about 15 percent of the world's spam, he said.

Paul Royal, principal researcher at Atlanta-based security vendor Purewire Inc., has found several other examples of botnet herders operating below the radar. In one experiment he participated in, Project ZeroPack, he found that automated obfuscation techniques allow the bad guys to engage in such activities as server-side polymorphism. With malware morphing regularly, traditional antivirus vendors have more trouble keeping up with the right AV signatures. The Waledac botnet has used this method with much success.

Meanwhile, he said, hackers are moving away from the centralized command-and-control botnet structure in favor of a more peer-to-peer-based architecture. This is unfortunate because with the more centralized structure, security researchers at least have one large target to aim at. The P2P approach means more smaller targets that are tougher to aim at, he said.

"Conficker.C, Storm and Waledac have all moved from centralized architecture to peer-to-peer-based architecture," Royal said.

## 2. Malware can shield itself

Among the problems security researchers have encountered when trying to track and shut down botnets is that the newer worms used to build botnets are using strong cryptography to protect the command-and-control centers, said Paul Kocher, president and chief scientist at Cryptography Research.

"It used to be you could track how a botnet was getting its commands and send out fake commands to take it out," he said. "It's getting a lot harder to do that."

The newer botnets are also better at snuffing out a machine's security controls.

"We're also watching more sophisticated efforts among botnet-building worms to evade detection," Kocher said. "They're more polymorphic, changing from copy to copy. It makes it more difficult for an antivirus author to craft a signature to block it."

## 3. Popular apps are beyond IT's control

Researchers continue to find that the path of least resistance for bot herders is the variety of applications people use on company machines but outside the control of IT. They use these to pass a variety of sensitive data back and forth, including medical records, financial data and so on.

Security vendor Palo Alto Networks recently released its Spring 2009 Application Usage and Risk Report that reviewed enterprise application use and traffic from more than 60 large organizations across financial services, manufacturing, healthcare, government, retail and education. The assessments, conducted between August and December 2008, represented the behavior of nearly 900,000 users. Among the findings:

- More than half (57 percent) of the 494 applications found can bypass security infrastructure -- hopping from port to port, using port 80 or port 443. Some examples of these applications include Microsoft SharePoint, Microsoft Groove and a host of software update services (Microsoft Update, Apple Update, Adobe Update), along with end-user applications such as Pandora and Yoics!
- Proxies that are typically not endorsed by corporate IT (CGIProxy, PHPProxy, Hopster) and remote desktop access applications (LogMeIn!, RDP, PCAnywhere) were found 81 percent and 95 percent of time, respectively. Encrypted tunnel applications such as SSH, TOR, GPass, Gbridge, and SwIPe were also found.
- P2P was found 92 percent of the time, with BitTorrent and Gnutella as the most common of 21 variants found. Browser-based file sharing was found 76 percent of the time with YouSendit! And MediaFire among the most common of the 22 variants.

Collectively, the report said, enterprises spend more than \$6 billion annually on firewall, IPS, proxy and URL filtering products. All of these products claim to perform some level of application control. The analysis showed

that 100% of the organizations had firewalls and 87 percent also had one or more of these firewall helpers (a proxy, an IPS, URL filtering) -- yet they were unable to exercise control over the application traffic traversing the network.

As a result, malware pushers have a relatively easy time using these applications for foul play, including botnet building.

#### **4. Social networking has widened the attack surface**

Then there's the growing use of social networking programs like Facebook, Twitter and Myspace, which are easy for the non-tech savvy to use and also hard for enterprise IT shops to monitor.

At the ShmooCon security conference in Washington D.C. in February, for example, researchers Nathan Hamiel and Shawn Moyer guided attendees through attacks made easy because of the very nature of these sites, where users can upload and exchange pictures, text, music and other content with little effort. Among the attacks targeting these programs, hackers use social networking tricks to dupe users into opening links that in turn drop malware onto the computer, effectively turning it into another zombie machine in a monster botnet.

#### **User education still a key defense**

Gunter Ollmann, vice president of research at Atlanta-based security vendor Damballa, Inc., said enterprise IT shops would do well to ramp up efforts to detect the lesser known malware being used to such devastating effect these days. In the last 2 years, he said, IT shops have deployed a broad range of detection and prevention technologies. Each layer of defense has gotten better at fending off certain attacks.

"The more common the threat, the better the protection," he said. "But the bad guys are very much aware of how these defenses work, so they're using more sophisticated, targeted social engineering attacks. Looking at the malware used, a high percentage is IDS and AV proxy aware."

Ollmann and others offer the same advice: Since attackers are so successful at [using social engineering tricks](#) -- luring users with fake headlines that play on current events and duping them into clicking on malicious links -- one of the best defenses remains user education.

Show the average user what they're up against every time they go online and they are less likely to be duped into downloading the bot-building code, experts say.

## **Study: Mistakes, Not Malicious Insiders, to Blame for Most Breaches**

***285 million records breached, most attacks came from external sources, according to Verizon study***

By [Joan Goodchild](#), Senior Editor

April 16, 2009 — [CSO](#) —

2008 was a banner year for security breaches, according to new research from Verizon. And while many security vendors have been banging the drum about the threat of malicious insiders, this report indicates organizations should be more wary of outside attacks.

The "2009 Verizon Business Data Breach Investigations Report," released this week finds that hackers continue to intensify and sharpen their efforts to steal sensitive data. In fact, more electronic records were breached in 2008 than the previous four years combined. The study's authors said the upswing is fueled by a targeting of the financial services industry and a strong involvement of organized crime. Corporations fell victim to some of the largest cybercrimes ever during 2008, noted the report .

The findings debunk the motion that insiders account for the biggest threat to security in most organizations and instead finds that 74 percent resulted from external sources. Only 20 percent were caused by insiders.

"Outsiders are going to exceed insiders in number. There are more of them. It makes sense that that attack ratio would be there," said Wade Baker, a Research and Intelligence Principal with Verizon.

The study, the second annual conducted by Verizon, is based on data analyzed from Verizon Business' actual caseload comprising 285 million compromised records from 90 confirmed breaches. The financial sector accounted for 93 percent of breaches, and a staggering 90 percent of these records involved groups identified by law enforcement as engaged in organized crime.

"The world of cybercrime has definitely moved away from the teenage hacker in the basement motif to it's a business now," said Baker. "It really does have an effect. When you gather a group together and they all share this purpose of compromising data, then they leverage their collaborative resources and can do attacks one person would not have the time, resources or computing power to do."

Baker also noted that the investigation found most breaches were avoidable. Nearly nine out of 10, 87 percent, were considered avoidable through simple or intermediate controls.

"If you look at the top three types of hacking, the ways criminals get in the door, it is default credentials, it is SQL injection and poor access control," said Baker. "From that standpoint the method of entry into the corporate network, they aren't using very sophisticated methods. If you did things well, you would be able to prevent that."

Additionally, 81 percent of victims were not Payment Card Industry (PCI) compliant. A statistic Baker said study authors interpreted as testimony to the effectiveness of PCI DSS.

The study found that highly sophisticated attacks account for only 17 percent of breaches and 83 percent of attacks were considered to be what Verizon termed as "not highly difficult" to pull off. However, the study authors also note that while the percentage of sophisticated attacks was small, they accounted for 95 percent of the total records breached. The numbers, according to Baker, once again point to the sophistication and power of today's organized cybercriminal networks.

## Verizon Business's 2009 Data Breach Investigations Report

(April 14 & 16, 2009) According to Verizon Business's "2009 Data Breach Investigations Report," the number of records compromised in the breaches it examined in the last year is greater than the totals of the four previous years combined. Of those breaches detailed in the report, 90 percent have ties to organized crime rings. Only one third of the incidents Verizon investigated were publicly disclosed. Attacks now target personal identification numbers (PINs) along with other payment card account information. Eighty seven percent of the security breaches occurred on systems that were not compliant with the Payment Card Industry Data Security Standard (PCI DSS) at the time of the incident.

Approximately 75 percent of the breaches investigated were launched from external sources.

[Editor's Note (Weatherford): Good report with a couple of interesting take-aways. First, taking into account the perfidious nature of statistics in general, we've read for years that somewhere between zero and 100% of data breaches were the result of the "insider threat." That makes a good quote but not much else. This report confirms from the survey group that 74% of all breaches are caused by external sources.

Second, there has been a lot of discussion lately about PCI and that it may not be the silver bullet for preventing breaches. Maybe, maybe not but this report found that over 80% of organizations who had a payment card breach were either not compliant with PCI or had never been audited. ]

## Western Australia State Government IT Systems' Security Found Wanting

(April 15, 2009) A report from Western Australia's Auditor General Colin Murphy says the state government's IT systems have serious security shortcomings. The report takes a detailed look at five unidentified agencies, all of which collect sensitive personal information about residents. In the report, Murphy says that there are "fundamental weaknesses in all of the key areas of information security at the agencies examined," and that other agencies exhibit problems as well. Among the security concerns listed in the report are a lack of IT

security policies; accounts remaining active after employees have left the agencies; a failure to install security patches and updates; and use of default passwords.

[Editor's Note (Honan): These findings tie in closely with an interesting fact from the Verizon Business's 2009 Data Breach Investigations Report (see "Top of the News") that "87 percent of breaches could have been avoided through the implementation of simple or intermediate controls".]

## Glut of Stolen Banking Data Trims Profits for Thieves

A massive glut in the number of credit and debit cards stolen in data breaches at financial institutions last year has flooded criminal underground markets that trade in this material, driving prices for the illicit goods to the lowest levels seen in years, experts have found.

For a glimpse of just how many financial records were lost to hackers last year, consider [the stats released this week by Verizon Business](#). The company said it responded to at least 90 confirmed data breaches last year involving roughly 285 million consumer records, a number that exceeded the combined total number of breached records from cases the company investigated from 2004 to 2007. Breaches at banks and financial institutions were responsible for 93 percent of all such records compromised last year, Verizon found.

As a result, the stolen identities and credit and debit cards for sale in the underground markets is outpacing demand for the product, said Bryan Sartin, director of investigative response at Verizon Business.

Verizon found that profit margins associated with selling stolen credit card data have dropped from \$10 to \$16 per record in mid-2007 to less than \$0.50 per record today.

According to a study released last week by **Symantec Corp.**, the price for each card can be sold for as low as 6 cents when they are purchased in bulk.

"[Cyber thieves] now have their hands on a tremendous amount of data, and there's certainly no scarcity of it out there right now," said **Alfred Huger**, vice president of development at Symantec. "Given all that we've seen in the past year, we're not sure why we haven't seen even more of a drop in pricing, but it could be that the people doing the selling have sewn up the market and no longer have to worry about being undercut by other sellers."

**Steve Santorelli**, director of investigations at the private security research firm **Team Cymru**, said his group's monitoring of cyber criminal forums appear to support Huger's hunch: Many forums are simply restricting the registration of new "verified" members. Getting verified involves successfully conducting a number of transactions with other members to demonstrate that the new entrant is not merely a "ripper," someone who will abscond with the money or goods before a transaction is completed.

"The rate of new additions allowed into the miscreant verified lists is very low," Santorelli said.

What's more, Santorelli said, thieves in possession of huge troves of stolen credit and debit card data appear to be hoarding the credentials, releasing them onto the market in smaller chunks in an effort to control the overall supply of card data available at any one time.

"This results in lower average prices for buyers and some sellers stockpiling products to restrict supply in a bid to keep prices inflated," he said.

### Sorting Good Stolen Cards From Bad Stolen Cards

Crooks who deal in stolen credit and debit cards and hacked online banking credentials have long used shadowy online forums and chat rooms to broker sales with other thieves who try to convert those goods into cash.

But recently, several commercial Web sites have sprung up and created a brisk business helping thieves check the balances and limits on stolen cards, with discounts for customers who check hundreds or even thousands of card numbers at a time.

The services are advertised on Internet forums that facilitate identity theft, and cater to criminals who wish to buy large numbers of stolen credit and debit cards. Using such services, the would-be buyers can quickly verify whether a random sampling of the cards is still active, and -- for an additional fee -- the available balance on each card. In

most cases, the only barrier to new customers signing up at these services is the ability to speak and read Russian, and the ability to pay with one of several virtual currencies, such as Webmoney.

**Lawrence Baldwin**, a security consultant in Alpharetta, Ga., has been working with several financial institutions to help infiltrate illegal card-checking services. Baldwin estimates that at least 25,000 credit and debit cards are checked each day at three separate illegal card-checking Web sites he is monitoring. That translates to about 800,000 cards per month or nearly 10 million cards each year.

"And those are estimates just for the card-checking sites we know about," Baldwin said. "There are almost certainly many other services exactly like these."

Baldwin said the checker sites take advantage of authentication weaknesses in the card processing system that allow merchants to conduct so-called "pre-authorization requests," which merchants use to place a temporary charge on the account to make sure that the cardholder has sufficient funds to pay for the promised goods or services.

Pre-authorization requests are quite common. When a waiter at a restaurant swipes a customer's card and brings the receipt to the table so the customer can add a tip, for example, that initial charge is essentially a pre-authorization.

With these card-checking services, however, in most cases the charge initiated by the pre-authorization check is never consummated. As a result, unless a consumer is monitoring their accounts online in real-time, they may never notice a pre-authorization initiated by a card-checking site against their card number, because that query won't show up as a charge on the customer's monthly statement.

In fact, in most cases when banks are alerted to the card-checking activity, it is because a credit card customer is regularly checking their online statement or has signed up with their bank to receive e-mail alerts each time a charge is initiated against their account.

The crooks have designed their card-checking sites so that each check is submitted into the card processing network using a legitimate, hijacked merchant account number combined with a completely unrelated merchant name, Baldwin discovered.

One of the many innocent companies caught up in one of these card-checking services is Wild Birds Unlimited, a franchise pet store outside of Buffalo, N.Y. Baldwin said a fraudulent card-checking service is running pre-authorization requests using Wild Bird's store name and phone number in combination with another merchant's ID number.

**Danielle Pecoraro**, the store's manager, said the bogus charges started in January 2008. Since then, she said, her store has received an average of three to four phone calls each day from people who had never shopped there, wondering why small, \$1-\$10 charges from her store were showing up on their monthly statements. Some of the charges were for as little as 24 cents, and a few were for as much as \$1,900.

"They're for different, random amounts every time," she said.

Pecoraro said that after a few months of this, she complained to her state attorney general, but was told that the state could do nothing for her because she had not experienced a financial loss from the incidents. What's more, the people who do notice the bogus charges on their online statements find the pending transactions expire after a few days, and eventually dropping off of their statements completely.

"Most people I talk to are understanding when I tell them we're just as much of a victim as they are, but some people get really irate and accuse us of stealing their money," Pecoraro said.

Baldwin said the thieves running the card-checking sites are counting on the fact that companies that operate different parts of the financial processing system -- including issuing and acquiring banks, and the merchant -- traditionally do not share fraud data with one another, or even signs of unusual activity.

"The problem is that the detail of each individual entity's perspective at a transaction level is restricted or filtered," Baldwin said. "But if everyone involved shared this pre-authorization transaction information, these guys would not be able to do these card checks, because the patterns are ridiculously obvious when you can see all of the components at once."

## **Industry Group Gives Government a Failing Grade in E-Mail Authentication** **Government Computer News (04/14/09) ; Jackson, William**

Online Trust Alliance's study of the public DNS records of 25 government domains and 20 million emails that claim to have come from those domains has found that less than half of the 25 government agencies are using email authentication technology. The study found that only 11 of the 25 government domains were using the technology, which allows servers to verify that email traffic is coming from the domain or sender that it appears to be coming from and that the email's sender is allowed to use that domain. Among the agencies who were found to be using the technology are the U.S. Census Bureau, the Central Intelligence Agency, and the Social Security Administration. The White House, the Department of Homeland Security, and the FBI were among those who were not using email authentication. A similar study of commercial sites found that 55 percent were using some type of email authentication.

## **Report: State Computer Systems a Hacking Risk** **Star Tribune (Minn.) (04/10/09) ; Brunswick, Mark**

A recent report issued by Minnesota's legislative auditor found that small state agencies typically do not have enough security measures in place to protect their computer systems. The report looked at 12 small state agencies, including the Board of Nursing and the Public Utilities Commission, and found that seven did not have dedicated information-technology or security staffs. In addition, the report found that the majority of the 12 agencies had not conducted risk assessments of their IT systems. Another agency was found to have neglected changing four default passwords to database accounts on a software product it purchased. The report concluded that these security gaps makes it possible for unauthorized individuals to access nonpublic information or disrupt state functions. Minnesota's Office of Enterprise Technology acknowledges many of the concerns raised in the report. The agency, which oversees the state's IT systems, notes that it is trying to consolidate its data centers into a high-security facility with a secondary backup for disaster recovery.

## **IRS to Boost Oversight of Security, Accuracy of E-Filings** **Washington Post (04/11/09) P. A9 ; Kang, Cecilia**

The Internal Revenue Service (IRS) has responded to a report from the Government Accountability Office that raised concerns about the lack of a clear system to monitor the electronic tax filings prepared by applications such as Intuit's TurboTax. The report, which was given to the IRS in February, noted that although the agency does provide some oversight of the tax software industry, it does not fully monitor compliance with security and privacy standards. The report also found that tax software providers are not required to meet the IRS standards that deal with the privacy of tax programs. As a result, the IRS does not know whether taxpayers' information is

at an increased risk of being poorly protected from fraudsters and identity thieves, the report said. The report added that while there have been no problems with the security of electronic tax filings, the IRS still needed to adopt a system to ensure that software providers are complying with security and privacy standards. The IRS said that it agreed with the GAO's recommendations and that it would begin to improve its oversight of the security and accuracy of electronic tax filings.

## **McAfee Looks at Spam's Damage to Environment**

**eWeek (04/16/09) ; Eddy, Nathan**

The global annual energy used to transmit, process, and filter spam is 33 billion kilowatt-hours (kWh), which is equivalent to the electricity used in 2.4 million homes, concludes McAfee's "Carbon Footprint of Spam" study. The study found that spam produces the same level of green house gas (GHG) emissions as 3.1 million passenger cars using 2 billion gallons of gasoline. The study found that an estimated 62 trillion spam emails were sent in 2008, and that most of the energy consumption related to spam, 80 percent, comes from end users deleting spam and searching for legitimate email. Spam filtering accounts for 16 percent of spam-related energy consumption. "As the world faces the growing problem of climate change, this study highlights that spam has an immense financial, personal, and environmental impact on businesses and individuals," says McAfee's Jeff Green. "Stopping spam at its source, as well investing in state-of-the-art spam filtering technology, will save time and money, and will pay dividends to the planet by reducing carbon emissions as well." The report says if state-of-the-art spam filters were used to protect every inbox, organizations and individuals could reduce spam's energy consumption by 75 percent. However, the researchers note that although spam filtering is helpful, fighting spam at its source is even better.

## **Data Security: Whose Job Is It Really?**

**CSO Online (03/30/09) ; Jaquith, Andrew**

Chief information security officers (CISOs) often have a difficult time securing corporate data, despite the large investments that have been made in technology and processes over the last several years. There are several reasons why protecting enterprise-wide data is still an unattainable goal for many CISOs, including the fact that software-as-a-service, Web 2.0 technologies, and computerized hardware open up more avenues for data thieves to use to steal sensitive information. In addition, trends such as increased amounts of available bandwidth and the growing number of vendor point products has made it harder for CISOs to secure data. CIOs and CSOs often respond to these challenges by trying to assume full control over data security. However, CIOs and CSOs could do more for the security of their organization's data by making business units more accountable for protecting the information they store, Forrester Research says. The firm notes that this strategy can be implemented in three steps. For starters, IT should take ownership for basic data security tools, particularly the ones that do not require customization. IT security also should offer data flow monitoring services to all business units. Next, IT security should allow business units to take the lead on data protection initiatives while it plays an advisory role in efforts to implement technologies such as database encryption and port/URL blocking. Finally, IT should make controls no-load/no-think and inescapable, instead of relying on educating employees about data security.

## **Study: Lost Notebooks Cost Corporations \$50K Apiece**

04.22.09

by [Mark Hachman](#)

The average value of a lost corporate laptop is about \$50,000, according to a study of lost or stolen notebooks released by the Ponemon Institute, and released on Thursday.

The study, sponsored by [Intel](#), focused on a voluntary survey of companies by Ponemon, and covered 138 thefts or lost notebooks. The value of the notebook was assessed by estimating the cost of the data, the loss of [productivity](#), costs associated with replacing the notebook, and other factors.

The maximum value reported was almost a million dollars, Larry Ponemon, founder of the Ponemon Institute said during a Wednesday [teleconference](#).

The study complements a [somewhat similar report from Verizon Business](#) that found that financial services information was targeted by hackers seeking to breach a company's defenses and extract its [data](#). But according to the report, the services industry (which includes legal firms and consulting companies) generated an estimated cost of \$112,853 per lost or stolen laptop, versus \$71,820 for one owned by a financial services employee.

Healthcare, pharmaceutical companies, education, and technology firms also ranked at the top of the list of industries which would be the most financially affected by a lost notebook. But technology topped the list of notebooks containing the most intellectual property, with an assessed value of \$18,205.

So, in dollars, who is the biggest risk of [losing data](#) in a corporation? Not the chief executive, the study found. Mid-level managers responsible for keeping the company up, running, and moving ahead, and their directors, would cost their companies \$60,000 or so in lost data and hardware costs. A CEO's lost laptop would cost just \$28,449, the study found.

Intel loses, on average, hundreds of notebooks a year, according to Rex Rountree, an [encryption](#) manager for Intel's information risk and security group, "somewhat more than smaller shops," he said during a teleconference.

Intel's goal is to make sure that every notebook has hardware antitheft technology in it, part of its vPro line of platform technology, added George Thangadurai, director of strategic planning and general manager of Intel's anti-theft program.

## **Hathaway advocates for direct White House role on cybersecurity**

Says federal government isn't 'organized appropriately' to address cyberthreats

**By Jaikumar Vijayan**

April 23, 2009 (Computerworld) SAN FRANCISCO -- Endorsing a viewpoint that's been gaining currency in the security industry, President Obama's acting senior director for cyberspace Wednesday called for a [more direct White House role](#) in coordinating national cybersecurity efforts.

Melissa Hathaway, who just completed [a 60-day review of the government's cybersecurity preparedness](#) at the president's behest, said that while cybersecurity needs to be a shared private and public sector effort, the task of leading it "is the fundamental responsibility of our government."

In arguing for a bigger White House role, Hathaway said the government's responsibility "transcends" the purviews of individual departments and agencies, none of which has a broad enough perspective to match the "sweep of the challenges."

"Protecting cyberspace requires strong vision and leadership and will require changes in policy, technology, education, and perhaps law," she said.

Hathaway is a former Bush administration aide who has been working as a cybercoordination executive for the Office of the Director of National Intelligence. She headed a multiagency group called the National Cyber Study

Group that was instrumental in developing the [Comprehensive National CyberSecurity Initiative](#) which was approved by former President George W. Bush early last year.

In February, Obama asked her to conduct a review of federal cybersecurity programs to see what needed to be done to better align them with the threats they are designed to mitigate. She completed the review last Friday and her report was handed over to the president. It isn't known what if any recommendations might result from it.

Speaking at the RSA conference, Hathaway said that what she was offering was only a preview of what's contained in the report.

Based on her review, it's clear that the federal government is not "organized appropriately" to address threats in cyberspace, Hathaway said. Responsibilities for cyberspace are scattered across too many departments, many with overlapping missions and authorities.

"We need an agreed way forward based on common understanding and acceptance of the problem," she said.

Hathaway also stressed the need for greater collaboration between the private and public sector on cybersecurity matters because such a large portion of the critical infrastructure is owned by private companies.

"The public and private sector's interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government services depend," she said. Going forward, the U.S. also needs to find a way to collaborate with other countries to secure cyberspace effectively, she said.

Though there were no surprises in Hathaway's speech, her remarks add to the growing chorus of voices calling for a substantial overhaul of federal cybersecurity practices. In December, the [Center for Strategic and International Studies](#) (CSIS) delivered a set of cybersecurity recommendations to the president, many of which are identical to those being suggested by Hathaway.

Two lawmakers, Sens. Olympia Snowe (R-Maine) and Jay Rockefeller (D-W.Va) [introduced legislation](#) seeking to give the federal government sweeping new authority to develop and enforce cybersecurity policies across the government and the private sector. Among the provisions in the bill is one that would give the president the authority to disconnect government or private entities from the Internet if necessary for national security purposes. A companion bill seeks to create a new cybersecurity office within the White House.

In addition to such efforts, there is also a move to create a [new military cybercommand](#) under the control of the Pentagon for addressing cyberthreats against military networks and systems.

Such moves are seen as signals of the heightened concern among lawmakers and those within the security community about the scale of cyberthreats facing the nation. The concerns have been heightened by news of a reported [compromise of the U.S. electric grid by foreign cyberspies](#) and the [theft of terabytes of data relating to an advanced fighter aircraft](#) under development by the military.

What's crucial now is for government to act on these recommendations, said Tom Kellerman, vice president of security awareness at Core Security Technologies in Boston and a member of the CSIS committee that prepared the cybersecurity recommendations for the president.

"Leadership from within the White House is paramount to the success of the national campaign against cybercrime and espionage," Kellerman said.

He also said it would make sense to confirm Hathaway's role as senior director for cyberspace and vest her with the authority needed to enforce cybersecurity practices across the government and the private sector.

"Hathaway called this a marathon," Kellerman said. "It's very important that they not change runners," in the middle of it.

## Cloud computing a 'security nightmare,' says Cisco CEO

'Swamp computing' might be a more appropriate name, says one security expert

By Robert McMillan

April 22, 2009 (IDG News Service) If anyone has the right to be excited about cloud computing, it's John Chambers. But on Wednesday, the Cisco Systems Inc. chairman and CEO conceded that the computing industry's move to sell pay-as-you-go computing cycles available as a service on the Internet was also "a security nightmare."

Speaking during a keynote address at the annual RSA security conference, Chambers said cloud computing was inevitable, but that it would shake up the way that networks are secured.

"You'll have no idea what's in the corporate data center," he said. "That is exciting to me as a network player. Boy, am I going to sell a lot of stuff to tie that together."

However, he added, "It is a security nightmare and it can't be handled in traditional ways."

Cloud computing is a hot topic here at the security conference in San Francisco this week. Big computing companies like Cisco and IBM are eager to talk about it, but security experts see a lot of work ahead.

"I think it's really going to be a focal point of a lot of our work in the cybersecurity area," said Ronald Rivest, an MIT computer science professor and noted cryptographer, speaking during a conference panel Tuesday. "Cloud computing sounds so sweet and wonderful and safe ... we should just be aware of the terminology, if we go around for a week calling it swamp computing I think you might have the right mind-set."

Rivest added that he was optimistic about cloud computing's future, but that it was going to take "a lot of hard work" to make it secure.

Show attendees haven't bought into the concept either.

"I'm not seeing a huge benefit in the cloud for us," said Bruce Jones, chief information security officer at Kodak, speaking in an interview.

One of the main problems is that Jones doesn't want to give up control of sensitive data to a nebulous cloud-based computing architecture. For long-term computing projects, it's probably cheaper to simply buy the hardware, he said, although cloud computing could work on a small scale at Kodak.

"It's a pilot or an R&D project where they want to do something and they need some kind of on-demand scalability; it's good for that as long as you don't care about the confidentiality of the data," Jones said.

As data moves onto the cloud, Cisco's security services will become even more important, and the company's ability to dig in and inspect data moving on and off corporate networks will become even more critical, said Tom Gillis, vice president of marketing with Cisco's security technology business unit.

"The move to collaboration, whether it be video or the use of Web 2.0 technologies or mobile devices is really dissolving the corporate perimeter," Gillis said. "This notion of security as a line that you draw in the sand ... that notion is just gone."

And it's not going to come back. Chambers said that his company's use of Web 2.0 technologies such as video blogging and conferencing has mushroomed in the past year. In the first quarter of 2009, Chambers held 262 meetings, he said. Two hundred of them were virtual, using Cisco's TelePresence system. "It's got to be secure as we do this," he said. "This is our lives."

## Windows bugs never really die

Because some PCs are never patched, pool of victims persists, says researcher

By Gregg Keizer

April 23, 2009 (Computerworld) Hackers can successfully attack Windows PCs months -- even years -- after Microsoft Corp. fixes a flaw, a security expert said today, because there's always a pool of unpatched systems.

According to data that Qualys Inc. culled from scans of more than 80 million machines, between 5% and 20% of all systems are never patched for any vulnerabilities, including those disclosed by Microsoft in its monthly security updates.

Qualys, a provider of on-demand IT security systems, tracked four vulnerability bulletins issued by Microsoft in 2008 and in each case found that a sizable fraction of the PCs it scanned had not been patched, even though in some cases more than a year had passed since Microsoft issued fixes.

The four updates, all labeled "critical" by Microsoft when they were released, included the following:

- MS01-001, a two-patch update in January 2008 that plugged holes in [three Windows TCP/IP protocols](#).
- [MS08-007](#), a single February 2008 patch for Windows' WebDAV Mini-Redirector, which defines how basic file functions such as Copy, Move, Delete and Create are performed using HTTP.
- [MS08-015](#), a one-fix update in March 2008 for a bug in Outlook, Microsoft's mail client, that could be exploited by tricking a user into visiting a malicious Web site.
- MS08-021, a two-patch update released in April 2008 for [Windows GDI](#), or graphics device interface, a frequently-fixed core component of the operating system.

Even as late as this year, MS08-021 had not been applied to 20% of the PCs that Qualys scanned. The percentage of machines lacking the MS08-015 update, on the other hand, dipped at times to about 5%.

"It's difficult to say why they haven't been patched," said Wolfgang Kandek, Qualys' chief technology officer. Kandek presented his findings at the RSA security conference in San Francisco. "It just baffles me. Some administrators are just doing their worst possible job patching."

Qualys' scans are conducted on machines owned by its clients, which are exclusively businesses -- predominantly large companies.

"Either they don't care, or they don't have enough resources to patch every machine," Kandek speculated.

Because some machines are never patched, there is always a ready reserve of potential victims, even for aging malware, Kandek continued. "Even very old worms can be successful," he said.

The notorious Conficker worm is a case in point. Though it's not old by any definition -- it debuted in November 2008 and just came to prominence in January 2009 -- Conficker's makers prey on PCs that have not been patched with an emergency update Microsoft issued last October. Last week, even after a media blitz about the worm's [April 1 trigger](#), [nearly 20%](#) of the PCs Qualys scanned were without the MS08-067 update.

As if to flaunt that fact, the newest version of Conficker [reactivated](#) its ability to spread by exploiting the Windows bug.

Microsoft's products are not the only ones that never get completely patched, Kandek warned. Some of Adobe Systems Inc.'s applications are in the same boat. "There are always stragglers," Kandek said. "Microsoft Office is one of the biggest stragglers for patching, and Adobe Reader is another. They're just not on the map for many companies."

## IRS Awards Payment Processing Contract to RBS WorldPay

(April 23, 2009)

RBS WorldPay, the payment processor that recently acknowledged a security breach that compromised an estimated 1.5 million payroll card accounts and 1.1 million Social Security numbers (SSNs), has been awarded a contract to process US Internal Revenue Service (IRS) tax return payments. Last month, Visa declared RBS was not in compliance with the Payment Card Industry Data Security Standards (PCI DSS); a spokesperson for the Atlanta-based payment processor says the company expects to be compliant once again "within the next few weeks." RBS will not process payments taxpayer credit card payments until January 20, 2010; before that date, the company must show that its IT systems are PCI-DSS compliant and it must pass an IRS-required security audit.

[Editor's Note (Schultz): Lamentably, the IRS's decision poignantly shows just how little regard this agency has for information security.

Hopefully, the IRS's extremely questionable judgment in this case will be subjected to Congressional and GAO oversight.

## House Committee Seeks Information on P2P Data Theft, Briefing on Fighter Jet Data Theft

(April 22 & 23, 2009)

The US House Committee on Oversight and Government Reform has sent letters to Attorney General Eric Holder and Federal Trade Commission

(FTC) chairman Jon Leibowitz asking what the Justice Department and the FTC have done to prevent illegal use of peer-to-peer (P2P) filesharing applications. Specifically, the committee is concerned about the applications being used to steal financial account information, health data and other sensitive information. Security experts would like to see the committee focus on encouraging agencies to prevent workers from downloading P2P applications. In a separate story, the same House committee is seeking a cyber security briefing following allegations that cyber intruders stole information about the Joint Strike Fighter.

[Editor's Note (Liston): While technical means for controlling P2P use exist, they're certainly not foolproof. From my perspective, nothing works better than making the installation of an unapproved application a fireable offense AND monitoring your networks and following through on the threat.]

## Most Businesses Don't Have Their Heads Around Cloud Security: Survey Network World (04/20/09) ; Greene, Tim

More than four in five businesses that contract with cloud computing service providers say they are not actively gauging the effectiveness of cloud security, according to a recent Deloitte survey. It is unclear whether the 82.6 percent of businesses that do not have formal assessment programs lack the capabilities or the money to carry out such evaluations, Deloitte notes in the study. The consultancy says the lack of enforcement is a major problem for companies that are trusting in good faith in the security and privacy provisions of a third-party provider. "You cannot put out in a third-party cloud data storage, email, and financial applications and say I am obliged to meet data laws, regulations, and contractual agreements and not have some mechanism of assurance in place," says Deloitte's Rena Mears. Companies may neglect to test and audit providers' security measures because the concept is still new and foreign to them, or because the process is too onerous. The report notes that whichever the case, it is ultimately the responsibility of the business, not the third-party storage provider, to ensure security.

## Cloud Computing's Inherent Security Risks CIO Insight (04/13/09) ; Parkinson, John

Despite advances in platforms and technological security, cyberattackers still have the upper hand over businesses and consumers, writes John Parkinson. He says cybercriminals can acquire the same tools and technologies as everyday users, have more computer savvy than most users, and run operations that are backed by profits from online extortionary schemes. Because of this three-pronged attack strategy, the crooks over time will win against security, Parkinson says. He says cloud-based storage still has too many areas of vulnerability to be considered safe. The risks of data storage are always high when an administrator cannot physically see and control where the information is being stored, and ironically vendors that offer management and monitoring capabilities only expose the data more. If the security-as-a-service market continues to gain

momentum, vendors and administrators can expect to see more frequent and more devastating data breaches, Parkinson predicts.

## Companies still dragging their feet with patches

By Jeremy Kirk

April 28, 2009 (IDG News Service) A study from security vendor Qualys has found that companies are patching just a hair faster than they were five years ago.

Qualys has conducted a research project for the last six years in which it collects data on software vulnerabilities from its customers' computers. Qualys provides Web-based services that can detect vulnerabilities in software, Web applications and can also perform compliance audits.

The latest data was collected throughout 2008, said Wolfgang Kandek, Qualys' CTO. Qualys scanned 80 million IP (Internet Protocol) addresses using 200 scanners that looked at Internet-facing PCs and 5,000 internal scanners behind firewalls on company intranets.

Kandek said 680 million vulnerabilities were found, with 72 million constituting critical ones, meaning the software problem could allow a hacker to take control of a computer remotely and install malicious software.

Qualys has created its own measurement, called "half life," for how fast companies patch. The measurement is the number of days it takes a companies in a certain industry to patch 50% of the vulnerabilities that have been publicly released.

The figures have barely changed since Qualys released its last study in 2004. Then, it took an average of 30 days to hit the half-patched mark. For 2008, that figure has only moved up to 29.5 days, Kandek said.

"The patch cycle hasn't really accelerated," Kandek said during the InfoSecurity conference on Tuesday in London.

By industry, the figures vary: The service sector takes 21 days; finance industry, 23 days; and wholesale and retail, 24 days. The laggards are the health industry at 38 days and manufacturing at 51 days.

The problem with putting off patching is that hackers are creating exploits faster than companies are patching them, Kandek said. "The attackers are getting much faster than before," he said.

Of the 21 fixes issues by Microsoft on Patch Tuesday this month, exploits for 10 of those problems were already in circulation, Kandek said.

Computer administrators also take too long to patch what should be higher-priority applications, such as Web browsers, Kandek said.

Also, long-known vulnerabilities in software including Microsoft Office, Adobe System's Acrobat and Microsoft's Windows Server 2003 SP2 continue to be found on systems after patches are available, Kandek said.

Adobe Acrobat seems to be particularly low on the patch list. That's dangerous since hackers have created malicious PDF (portable document format) files that can exploit vulnerabilities and infect a computer. Acrobat can be a "major source of malware infections."

"We have to patch these vulnerabilities as soon as possible," Kandek said.

## Security training 101

### How to build organizational 'cybersafety'

By Lynn Haber

April 28, 2009 (Network World) Installing the latest security hardware and software means nothing if end users don't practice cybersafety. And the best way to get end users to "think security" is to create an ongoing culture of security at your company.

"Security awareness isn't one of those things that organizations do for fun. It's 24/7, and accountability starts with the CEO and is pushed to all corners of the organization," says Larry Ponemon, founder of the Ponemon Institute LLC, a privacy and data protection research firm in Traverse City, Mich.

The stakes are high and getting higher all the time. In January, the Identity Theft Resource Center (ITRC) [reported](#) that the number of data breaches in 2008 increased 47% compared with 2007. The organization also reported that 35.2% of breaches were the result of human error.

And Ponemon recently released a [study](#) showing that the average cost of a data breach grew to \$202 per record compromised in 2008, up from \$197 per record in 2007. And the average security incident cost individual companies \$6.6 million per breach in 2008, up from \$6.43 million in 2007 and \$4.7 million in 2006.

Worse, security breaches result in a loss of consumer confidence, which translates into customers taking their business elsewhere.

So, what are the keys to a successful security awareness program? Creating a culture of security starts at the top, includes individuals from all departments and groups, is based on predetermined policy and subsequent controls, is consistently revisited and updated, and is practiced daily.

### Security is Job 1

Computer security is a fast-moving target. Today, there are more threats, more vulnerabilities, more portable storage devices and increased mobility. There's also less of a wall between one's personal life and work life. The things to protect and protect against are changing.

That means educating end users about security is more difficult, demanding and necessary than ever before.

"Today, users are more aware of existing threats, but threats are more sophisticated, and they migrate faster," says Max Reissmueller, senior manager of IT infrastructure and operations at Pioneer Electronics USA Inc. in Long Beach, Calif.

Reissmueller is responsible for end-user security awareness for approximately 1,600 employees at about 15 locations in North America. Pioneer Electronics has a formal security review board that updates policy annually and disseminates changes to end users.

But one major problem when it comes to end-user training is that security is not the end user's primary job. "The end user doesn't do security for a living, so their focus isn't on how to keep the company secure; it's how to best do their job," Reissmueller says.

In fact, industry experts agree that social engineering makes it difficult for enterprises to keep up with the rapidly changing vulnerability landscape. You can't expect end users to be security experts, but you can teach them how to notice when something looks suspicious and whom to call when a security-related issue arises.

Another key is to put security awareness in the larger context of protecting company assets, company revenue and the company's reputation. "Policy is often written with little or no consultation. End users get e-mails to be aware about threats, but there's no context," says Sam Curry, vice president of product management and strategy at RSA Security Inc., a division of [EMC Corp.](#) in Bedford, Mass.

Curry believes that not only does creating a culture of security require the involvement of all an organization's departments, but it's also paramount that users understand why their actions create a risk for the organization.

What happens when security risk isn't put in context for end users? According to RSA's 2008 Insider Threat Survey, "People will do as they will, regardless of awareness of best security practices."

The survey, which polled 417 people from North America and Latin America, found that 94% were familiar with their organizations' IT security policies, yet 53% have felt the need to work around IT security in order to get their work done.

## **Best practices**

Pioneer's Reissmueller says there's security compliance and there's security awareness, but they're not the same thing. Security awareness is not a check-box item. It's also not a one-time or even two-times-a-year event.

Security awareness must be ongoing, "to keep the knowledge fresh and real in the mind of the end user," he says.

The training often begins by working to get end users to really understand why security awareness is necessary.

"Organizations want users to internalize the problem. They want employees to do the right thing because it's the right thing to do, not because you're watching them," says Mark Rasch, a Bethesda, Md., attorney specializing in computer security and regulatory compliance. Rasch was also the former head of the U.S. Department of Justice computer crimes unit.

A common component of security awareness training is a video or Web-based module. Companies can also require that all employees read and sign Internet and acceptable-use policy and security policy documents.

"Policy must also reflect the culture of the company and its values," Rasch says. Furthermore, policy must be enforced with training. "The longer an organization goes without training, the greater the divergence between the written one [policy] and the unwritten one, or the one users are following," he adds.

Many organizations offer security awareness training. For example, SCIPP International, a global nonprofit organization in Vienna, Va., offers security awareness certification for individuals and organizations.

## **Hands-on training**

In 2005, New York developed an antiphishing exercise with the Anti-Phishing Working Group, AT&T and the SANS Institute. The exercise involved 10,000 state employees who were unaware they were participating in a security exercise.

In the exercise, 15% of employees fell prey to a phishing scheme. After the results were tallied, these individuals got a message informing them that they had fallen for a fraudulent e-mail and directing them to a brief tutorial on how to be more aware of phishing scams.

The organization launched a different online exercise to the same employee population two months later and saw a 50% improvement. Users who failed the second exercise were asked to participate in a feedback survey to determine why they took the actions they did.

The goal of the exercise was to understand how well the state communicates and how well users learn, according to William Pelgrin, chief cybersecurity officer and director of the New York State Office of Cyber Security & Critical Infrastructure Coordination in Albany.

"Just telling people that phishing is out there isn't very effective. It's better for users to have a tactile interactive experience," he says.

## **Changing behavior**

Some low-level activities that organizations use to raise end-user security consciousness include displaying posters, running banners on the company's intranet, hosting a computer awareness day and distributing security training material.

An additional training tool is to run mock scenarios to reinforce what to look for, what action to take and who to contact. "The user has to know, this is what you have to do and why you have to do it," Rasch says.

It's also important for organizations to provide role-based training for workers with specific jobs and responsibilities, says Mark Wilson, an IT specialist, information security at the National Institute of Standards and Technology's Computer Security Division in Gaithersburg, Md.

Reissmueller takes a multipronged approach to security awareness that includes penetration testing, because he finds that policy and education alone aren't enough.

"The goal is to make security awareness a partnership between the end user and the business, something they do without realizing they're thinking about it," he says.

## Can you no longer avoid closely monitoring employees?

By Ellen Messmer

April 28, 2009 (*Network World*) The insider threat has always existed, but in an era of economic upheaval and uncertainty, the problem is only magnified. A recent Ponemon Institute LLC survey of 945 people who were laid off, fired or quit their jobs during the past year found that 59% admitted to stealing company data, and 67% used their former companies' confidential information to leverage a [new job](#).

How far should IT managers go to protect corporate data?

"There's a balance," says Max Reissmueller, senior manager of IT operations and infrastructure at Pioneer Electronics USA Inc. in Long Beach, Calif. "I wouldn't want managers coming to me to keep an eye on a particular employee, wondering what they are doing every minute."

At the same time, Pioneer is determined to protect its intellectual property, customer-service lists and other sensitive data. "I don't want a disgruntled employee trying to take a bunch of information," Reissmueller says. That's a main reason the company has installed [network access-control](#) gear to monitor traffic to the "crown jewels," to keep an eye on whether employees are trying to overstep their authority.

Using a [ConSentry](#) switch and [network access-control product](#), Pioneer will watch for patterns that might reveal wrongful behavior and block it. "But I don't want my security staff to become Big Brother," Reissmueller says.

All it takes is a data-leakage case to compel organizations to beef up their monitoring.

The University of Arizona went through a few data-leak imbroglios in which it had to make public notification about exposed personal data, says Eric Case, information security officer there.

That induced the university's information and security office to kick off a program that involved making sure that faculty and staff there weren't leaving sensitive data lost and forgotten in computers.

To determine that, the university has deployed [data leak prevention](#) freeware called Spider that can look into a targeted machine to see if it's holding data that shouldn't be there in order to either delete it or move it to a more secure server.

Although the security staff did explain in depth what it was up to, "we had a couple of people freaked out because we were looking at their files," Case says, speaking about the topic at the recent Infosec World conference in Orlando. "They were upset."

But after calming people down, the data leak prevention process had to proceed because "we know we have data all over the place," Case says. "Have we reduced our threat surface? Quite a lot."

Rick Haverty, director of IS infrastructure at the University of Rochester Medical Center in New York, says laws and regulations his organization must abide by regarding patient health care information leave no choice but to confront instances in which it appears that employees may have broken rules. One concern is an employee taking a sneak peek at someone's medical records without cause.

"People have been fired for this," he notes, adding that the start of an investigation usually involves a complaint about someone gossiping about a patient's medical circumstances. An investigation would generally involve examining log records to determine whether inappropriate access to records may have occurred.

Gartner Inc. analyst John Pescatore says the key word to think about is how "closely" to monitor employees.

"There is definitely a requirement to monitor critical business data leakage from employees and a requirement to monitor what comes into their PCs to prevent malware," Pescatore says. "However, in the real world, there is less of a need to monitor every action a user takes, block them from every Web site that is not work-related or try to keep them from using their work PC for anything but work, or keep them from using their home PC for work."

The trend toward work/home mixing is under way, he points out, and "security can't stop this any more than it could stop the Internet, wireless LANs or other previous trends."

## **Can You Say for Sure Who Has Access Rights to Your Sensitive Data?**

**Network World (04/27/09) ; Musthaler, Linda**

Many experienced IT public and private sector practitioners say they are not confident that their users have the appropriate rights to access the applications, files, and information they need to do their jobs, according to Ponemon Institute's 2008 National Survey on Access Governance. Of the nearly 700 IT practitioners from business and governmental organizations that participated in the survey, more than half said that they were not confident that the process of assigning access rights is properly performed in their organizations. The survey also found that 73 percent of respondents said their organizations determine risk to information based on the inherent risk of various data types instead of users' roles or functions--a finding that suggests changing business roles and responsibilities may make it too difficult for organizations to manage access rights at the individual level. In addition, the report found that IT practitioners face a number of challenges when implementing an effective access governance framework, including difficulties in enforcing access policies across the enterprise and an inability to keep up with changes to users' roles within the organization.

## **Federal CISOs: Bad economy could create vulnerabilities**

**They worry about retaining workers, cybersecurity issues**

**By Grant Gross**

April 30, 2009 (IDG News Service) Many U.S. government chief information security officers (CISOs) believe the nation's recent recession could hurt their ability to do their jobs, according to a survey released Thursday.

But federal CISOs see some opportunities in the difficult economic times, with 48% of respondents saying the economy will make it easier to retain key security workers. Forty-three percent said the recession will create more vulnerabilities, according to the survey, by Cisco Systems, Government Futures and the International Information Systems Security Certification Consortium, or (ISC)<sup>2</sup>.

The survey didn't ask for details about why CISOs feel the bad economy could create more vulnerabilities, but it seems that federal CISOs are concerned about their budgets and about IT vendors not patching their software as often as in the past, said Lynn McNulty, (ISC)<sup>2</sup>'s director of government affairs.

There seemed to be concern that government cybersecurity efforts "would not be viewed as economic stimulus," McNulty said. "I'm sure there are feelings out there that they're having to compete for resources when the emphasis is being put on financial institutions and money that will ... create jobs."

Thirty-three percent of the respondents said they were concerned that financial pressure could lead vendors to push products to market too quickly, making the products less reliable.

Asked about the biggest threats, 48% of federal CISOs identified outsider threats as their main concern, apparently contrasting with some cybersecurity companies that say insider threats are the biggest problem of

many companies. Just 26% of government CISOs identified insider threats as their biggest threat, and another 26% said vulnerable software was the biggest problem.

Insider threats have also been a major cause for concern among U.S. lawmakers, as federal employees have lost hundreds of laptops, including the high-profile theft of a laptop and hard drive containing the personal information of 26.5 million military veterans and family members from the home of a U.S. Department of Veterans Affairs employee in May 2006.

But federal agencies may have experienced a larger number of attacks from foreign hackers, McNulty said. "I think the numbers reflect what the CISOs are having to deal with," he added. "The people who were surveyed are the ones having to grapple with that on a daily basis."

Federal CISOs may be facing more organized and sophisticated attacks than many private companies, McNulty added.

"My perception is that the threat against the federal government goes far beyond what we see in the financial sector," added David Graziano, manager for federal security solutions at Cisco Systems.

The survey also found CISOs divided about whether the U.S. government has made lasting progress against cyber vulnerabilities. About half said they believe the U.S. government is making progress but is still "not getting ahead of the attackers." The other half said they believe "we are turning the corner."

## **Can the feds buy their way to better cyber security?**

Among the suggestions for improving federal cyber security that were proposed at a hearing by the Senate Homeland Security Committee Tuesday, one that appeared to garner a fair amount of interest from lawmakers had to do with the use of government buying power to boost security.

The suggestion from Alan Paller, director of research at the Bethesda, Md.-based SANS Institute is one that is shared by several others within government and outside it as well. The basic premise is that the government which purchases over \$70 billion worth of IT products a year can use its enormous buying power to force vendors to make their products more secure.

Most often, cyber criminals and foreign adversaries are able to penetrate systems and networks because of common programming errors and insecure configuration issues that are pretty well understood at this point but which vendors keep repeating all the same in their products. So getting them to fix these issues before they are permitted to sell into government is a surefire way to improve security and reduce costs, says Paller.

An example of where this approach has worked is the U.S. Air Force which has deployed over 500,000 desktops with a secure, standard Windows desktop configuration, Paller says. "Dozens of customers had asked Microsoft for more secure configurations and all were refused or were asked to pay large amounts of money for consulting services to develop customized settings," Paller wrote in his testimony for the Senate hearing.

But because the Air Force was about to spend \$500 million on Microsoft software it was able to tell Microsoft what it wanted from a security standpoint and get the vendor to bake it into their products. The result has been much more secure software and substantially lower procurement and operational costs, for the Air Force he says. The Air Force model is now being replicated across other agencies as well and there's no reason why the same approach shouldn't be used for all technology procurement by the U.S. government. The Air Force procurement has also led Microsoft to bake similar security into the products it sells to many other buyers, Paller says.

The idea of using procurement as leverage for better security appeared to appeal to Sen. Susan Collins (R-Maine) who is the ranking member of the Senate Homeland Security Committee and Sen. Joe Lieberman (Ind-Conn.) who is its chair. While Lieberman found the testimony "riveting", Collins found it "very compelling" that a federal official would have to literally beg software vendors such as Microsoft to provide more secure software. She sought specific recommendations on how federal purchasing power could be used to get vendors to incorporate more security into their products and implied that this is a topic

she will be looking into going forward.

That is something that a lot of people are likely going to want no doubt. As security consultant [David Rice](#) says in his book *Geekonomics*, software products in general have had largely detectable and preventable security defects for a long time now. Yet vendors have done little to address the problems, because they have had very little incentive to do so, he says. Unlike the auto industry, there is no formal safety rating system in the software industry which consumers can use when making purchasing decisions. There also isn't a whole lot of choice actually. So consumers and business by and large have had to live with whatever it is the vendors have given them, and then forced to patch and pray later. It's the reason why some are now advocating that the government step in and use its purchasing power as a weapon to get vendors to make more secure products. The question is will it work?

## **Survey: Software flaws account for breaches at 62% of companies**

**By Computerworld UK reporter**

May 1, 2009 (Computerworld UK) More than 62% of companies experienced a security breach in the past 12 months due to insecure software, a survey conducted by Forrester has revealed.

Forrester's "Application Risk Management in Business Survey" research, commissioned by application risk management platform supplier Veracode, surveyed more than 200 respondents from 180 different businesses across various industry sectors. Development, security and risk professionals across the U.K. and U.S. were interviewed.

Most security breaches were due to exploitation of vulnerabilities in their critical software applications.

Insecure software is a top priority for management and developers alike. While companies feel they know the makeup and business criticality of their mixed application portfolios, there is little confidence in the security quality of their applications.

The U.K. uses less open-source and outsourced applications extensively for business critical functions and has a lower ratio of security personnel to developers, but the results in terms of breaches were in essence the same, the review concluded.

Only 34% of companies have a comprehensive software development life cycle (SDLC) that includes application security.

More than half of companies (57%) use outsourcing regularly for business critical applications. Yet only one-third of companies require rigorous security testing before accepting and implementing code from outsourcers.

The recession is also impacting security risk, as 64% of respondents stated that while application security is important to them, they are struggling to meet the challenge on existing budgets.

"The same economic forces driving enterprises to use third-party applications are also increasing the risk of insecure software," said Matt Moynahan, CEO of Veracode. "Given the prolific use of third parties to build business-critical applications, global enterprises need a single flexible and cost-effective solution to seamlessly test the security across their entire application portfolio regardless of whether it was built internally or externally."

## **McAfee reports huge drop in spam**

**By Ellen Messmer**

May 5, 2009 (Network World) Global e-mail spam volumes have dropped 20% for the first quarter this year compared with the same period last year, according to [McAfee's](#) latest research.

McAfee attributes the dramatic reduction in e-mail spam to the November shutdown of the notorious [McColo](#) spam-generating site. In the McAfee Threat Report for the First Quarter 2009, published today, the security company said spam levels are still 30% below their peak seen in the third quarter of last year right before the shutdown of the rogue ISP McColo.

Spam as a total percentage of e-mail volume is now at 86% -- hardly great news, but 90% had been the more common figure and current levels haven't been this low since 2006, according to McAfee. All e-mail, both good and bad combined, is believed to have averaged about 100 billion messages per day worldwide in March, a trend continuing into April, notes Dave Marcus, McAfee director of communications.

However, McAfee is not optimistic that e-mail spam volumes will continue to drop. "The question is not whether spam will return to previous levels but rather when it will return," McAfee says in its report.

The U.S. remains the top country whose computers -- many of them compromised -- generate the most spam worldwide. "The U.S. continues to lead the world with 35% of the globe's spam output," McAfee states in its report.

But in other nations there's also trouble, McAfee points out, asserting that criminals have been attacking Russian banking and government networks in order to use computer resources within them to generate malware-laden e-mail and spam.

McAfee cites Rusfinance Bank, OGO Bank, Tusarbank, Link Capital Investment Bank, Maritime Bank, Vladivostok Alfa Bank, Bank Voronezh and Inter-Svayz Bank as being among the Russian financial institutions inadvertently generating spam.

"This data suggests online criminals are largely indiscriminate about their targets and will attack any organization of financial or other interest to them," McAfee states in its report.

The McAfee report also adds, "Our data suggests that computer systems in the following Russian government offices are controlled by cybergangs. These institutions would include the Ministry of Taxation, Nazran Region; the Russian State Internet Network; Regional Finance and Economy Institute; Joint Institute for Nuclear Research; and Pension Fund of the Russian Federation, among several others.

Marcus says McAfee has notified these institutions of its findings, which were recently made as the company combed through information it was collecting about spam and IP addresses.

When it comes to malicious Web activity from sites with "bad reputations" for [hosting malware](#), the top three countries remain the U.S., China and Russia. But this last quarter saw growth in malicious Web activity from sites in the Netherlands, United Kingdom, Republic of Korea, Japan, France, Canada and Czech Republic, the McAfee report says.

