

# Security Trends Report

08/08

## 10 Key Information Security and Compliance Activities for 2010

by [CarlHerberger](#), Evolve IP

Aug 5, 2009 10:00:12 AM

Managing the security of critical information has proven a challenge for businesses and organizations of all sizes. Even companies that invest in the latest security infrastructure and tools soon discover that these technology-based “solutions” are short-lived.

From antivirus software to firewalls and intrusion detection systems, these solutions are, in fact, merely the most effective strategies at the time of implementation. In other words, as soon as businesses build or strengthen a protective barrier, the “bad guys” find another way to get in. Attackers are constantly changing their tactics and strategies to make their attacks and scams as damaging as possible.

The following areas are of particular concern as you begin planning for 2010:

1. **Pandemic Continuity Planning.** Planning for an epidemic is very different from typical business continuity or technical [recovery planning exercises](#). In fact, in an advisory issued last year by the Federal Financial Institutions Examiner’s Council (FFIEC), it stressed the need for these planning exercises, and detailed the differences between these efforts. Lending more credibility, in April of this year, The Gartner Group weighed in with an advisory of its own and said enterprises shouldn’t overreact to media reports about the swine flu, but should take the event as a wake-up call for reviewing and testing their pandemic response plans.
2. **Readdressing Malware Variants.** Malware is morphing in scale, scope and delivery payloads. Attackers have shifted away from mass distribution of a small number of threats and moved toward micro distribution of large families of threats. These new strains of malware consist of millions of distinct threats that mutate as they spread rapidly.
3. **Addressing Social Networking and Web 2.0 Threats.** Trusted Web sites are the focus of a large portion of malicious activity. As more and more users go online to take advantage of Web 2.0 applications, such as social-networking sites, blogs and wikis, malware authors are right behind them, opening yet another front in the constant cat-and-mouse game between security defenses and hackers. These threats will become increasingly important and relevant to younger workforces who are proficient with these tools.
4. **Re-Architecting the Technical Security Perimeter.** The continued high volume of data breaches underscores the importance of internal data loss prevention technologies, and exposes business’ over-reliance on the perimeter model. The “layered approach” to information security is a term used by professionals to describe the practice of weaving together comprehensive policies and manual procedures to several different point security solutions, filtering systems, and monitoring strategies to protect information technology resources and data. As [data loss prevention](#) becomes increasingly important in these layered defense models, the more likely a risk-adjusted re-deployment of security perimeter resources will occur.
5. **Incident Response/”Get to the Bottom of It.”** When a compromise of information security is suspected, it’s important that steps are taken immediately to ensure the protection of data. Virtually every organization faces the ongoing risk of security incidents, data handling breaches, disasters, or other events. Meanwhile, most have too few human resources, tools, and too little time to develop and maintain an effective incident response program. 2010 will be the year to improve on these capabilities.
6. **Unmanaged Mobile Devices (cell phones/iPods/USBs, etc).** Mobile devices used by employees for business without IT oversight can expose employers to unacceptable risk. From sloppy configuration to dangerous connections, many unmanaged devices — and the business assets they contain — are ripe

for attack. Numerous businesses are rushing to reengineer solutions to solve the risks associated with the huge number of unmanaged mobile devices.

7. **Growth of Social Engineering Techniques.** Always bear in mind that security does not stop or start with the technology alone. The simple reality of the world in which we live is that it is and always will be we humans who use, control, implement, regulate, maintain, modify, repair or add to the technology's base functionalities and capabilities. As an example, phishing continued to be an incredibly active threat in 2008 and 2009. Today, attackers are using current events such as the mortgage crisis, stimulus spending packages, and various "bailout" schemes to make their "bait" more convincing, and are employing more efficient attacking techniques and automations. Moreover, social engineering fraud techniques, such as phishing and pharming, are expanding, highlighting the need for companies to be proactive in addressing these vulnerabilities.
8. **Cryptographic Key Management.** In the rush to encrypt a variety of confidential information, businesses have generated heaps of cryptographic keys that need to be managed and controlled. The resulting management issue is a daunting task and one that should not be taken lightly. Successful key management is critical to the security of a cryptosystem and, arguably, is the most difficult protection to deploy because it involves system policy, user training, organizational and departmental interactions, and coordination.
9. **Virtual Machine (VM) Security.** To date, virtualization technology has been a relatively secure platform. However, the huge adoption and deployment rate of this technology has spurred numerous efforts to learn how to subvert and otherwise uncover configuration vulnerabilities. In fact, there recently have been a number of formally published vulnerabilities and acknowledgements by major VM vendors that lab-hacking scenarios are plausible in the "real world." Moreover, there are many insurmountable management concerns of how to properly remedy detected vulnerabilities because visibility of where this technology actually resides within an organization is often poor.
10. **The Ability to "Prove" Appropriate Levels of Deployed Security.** Evaluating security risks is further complicated by the growing practice of outsourcing. Knowledge of your business partners' security is paramount to a successful relationship. In fact, numerous regulations such as GLBA and [HIPAA](#) require every covered organization to evaluate their key business partners and outsourcing risks. However, the release of too much information on internal security controls can also be a liability. Balancing this mix appropriately will be a crucial skill in 2010.

Budgets might be tight moving into 2010, but businesses still will have to comply to regulations, react to new and low-cost virtualization technologies, and adapt to the growing trend of using outsourced business partners to accomplish key business tasks.

Keeping things secure will be an ever-daunting task, and many will seek external expertise to augment their internal staff. Those who have established an efficient system will reap the rewards, while others will find an ad-hoc method of system security to be nearly impossible to maintain

## 5 Lessons from Dark Side of Cloud Computing

By Robert Lemos

August 6, 2009 03:28 PM ET

CIO - While many companies are considering moving applications to the cloud, the security of the third-party services still leaves much to be desired, security experts warned attendees at last week's Black Hat Security Conference.

The current economic downturn has made cloud computing a hot issue, with startups and smaller firms rushing to save money using virtual machines on the Internet and larger firms pushing applications such as customer relationship management to the likes of Salesforce.com. Yet, companies need to be more wary of the security pitfalls in moving their infrastructure to the cloud, experts say.

"Guys at the low end are using (cloud infrastructure) to save money, but the danger is that the guys at the top end start to use it without any auditing," says Haroon Meer, technical director at security firm SensePost, who discussed his team's research into some aspects of Amazon's Elastic Compute Cloud (EC2) at the Black Hat security conference.

[ For timely data center news and expert advice on data center strategy, see CIO.com's [Data Center Drilldown](#) section. ]

Their experiments showed that companies frequently do not scan the third-party machine instances available from some providers. A malicious instance could easily be created as a Trojan horse to gain access to a company's internal network, Meer said.

With those pitfalls in mind, here are five lessons from the presentations at Black Hat.

1. Cloud offers less legal protection Companies need to realize that data in the cloud is subject to a lower legal standard in terms of search and seizure. The government, or an attorney focused on discovery, may be able to subpoena the data without a search warrant.

Cloud providers are more concerned with protecting themselves and not the client, says Alex Stamos, a principal security consultant at iSec Partners, so don't expect the legalese in service agreements to favor your company.

"All of these (cloud-services) companies have very active and very well-trained legal departments," Stamos said. "And as a result, the agreements you agree to when you sign up for these services, basically promise you absolutely nothing."

If someone breaks in because of the provider's mistake, the client agrees not to hold the firm responsible. If there is a data loss because of a data center failure, the provider are not obligated to do anything for you, Stamos says.

It would be nice, he adds, if there were language that said they will attempt to help you.

"It would be nice if they had language in there that said if there is a security breach, we will try to give you a hand up," he says. "This seems to be where there is a disconnect between the cold heartless world of the lawyers, and the nice warm security (ethics) of the company."

2. You don't own the hardware Companies who want to audit their providers and do their own testing need to remember that they don't own the hardware. Conducting a vulnerability scan or a penetration test requires the explicit permission of the cloud-service provider, Stamos warns. Otherwise, the client is hacking the providers' systems.

While some service agreements, such as Amazon's, specify that the client can conduct testing of their software running on the provider's systems, getting explicit permission is key, he says.

"The recommendation ... is that, if you are asked to pen-test applications in the cloud, they (the legal experts) recommend that you get permission from someone at the company," he said. "Because certainly, by the letter of the law the legal ownership of those machines is very important."

3. Strong policies and user education required While cloud computing offers companies immense benefits, such as allow access to data from anywhere and removing maintenance headaches from the IT staff, the always-on service also means that phishing attacks that hit workers at home could threaten the company.

Thus, educating users about the dangers, not only to themselves but to their company, is key, said iSEC's Stamos.

"It is very difficult to teach all the non-technical users in your company about how to not be phished, but the fact of the matter is, with software-as-a-service, phishing attacks are going to be something that stops being a personal issue and starts becoming a enterprise-wide security issues," he said.

4. Don't trust machine instances When using a virtual machine from a provider, such as the third-party instances created on Amazon's Elastic Cloud Computing (EC2) infrastructure, companies should never trust the system, says SensePost's Meer.

The company's researchers scanned a number of pre-configured instances and found authentication keys in the caches, credit-card data and the potential for malicious code to be hidden within the system. Yet, they found most of their customers did not consider the security implications of using a machine image created by the third-party developer.

"Some customers have based an entire authentication server off of pre-configured images," SensePost's Meer said.

Companies should either create their own images for internal use, or protect themselves technically and legally from potentially malicious third-party developers, Meer says.

5. Rethink your assumptions In all cases, when considering security, corporate information-technology managers need to reconsider their assumptions in the cloud.

For example, when deploying an application to run on a computing instance in a virtualized data center, features that rely on random number generation will not necessarily work as expected. The problem is that virtual systems have much less entropy than physical ones, so random numbers could be guessable, iSEC's Stamos says.

"You need to consider the non-obvious," he says.

## Net Attacks Triple in Two Years

Federal Times (08/03/09) Vol. 45, No. 22, P. 1 ; Carlstrom, Gregg

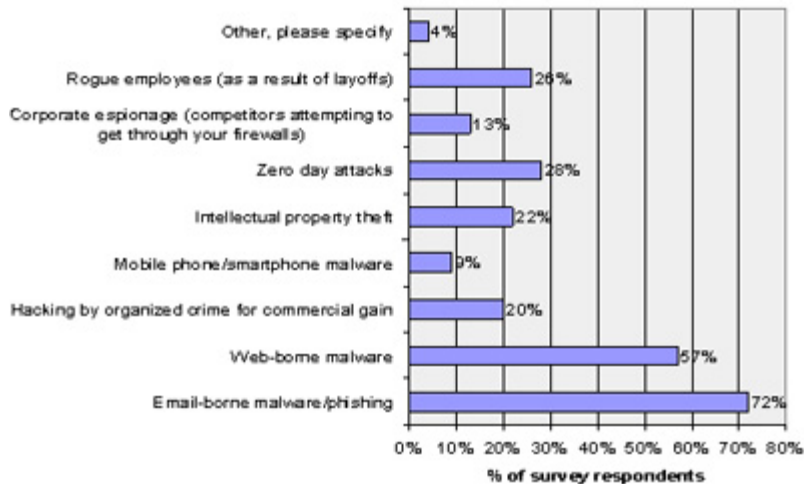
There were more than 18,000 cyberattacks on civilian federal agencies' computer networks last year—a number that is more than 250 percent higher than it was in 2006, according to data from the Department of Homeland Security. However, the problem is likely worse, since the figures do not take into account attacks on Defense Department and intelligence agency networks, which are tracked by the Defense Information Systems Agency. In addition, federal agencies cannot monitor every intrusion on their networks. Nevertheless, experts say the data is a fairly representative sample of the cybersecurity threats facing the federal government. Among the most common threats are "improper usage" incidents, which include such things as copying sensitive information to a home computer or logging onto a secure government Web site from a device that is not secure. There were 3,762 such incidents in 2008, a 490 percent increase compared with 2006. Malicious code attacks, or attacks involving worms, viruses, and Trojans, rose roughly 50 percent between 2006 and 2008. Experts say that these and other common types of attack could be prevented if the federal government made several basic management changes, including centrally managing information technology systems, providing employees with better education and training, and implementing stricter access control.

## Shrinking budgets tie hands of security professionals

Posted on 27 July 2009.

RSA Conference released the results of a recent survey of security professionals regarding the critical security threats and infrastructure issues they currently face, including those exacerbated by the current economic climate.

**What type of attacks have you seen an increase in?**



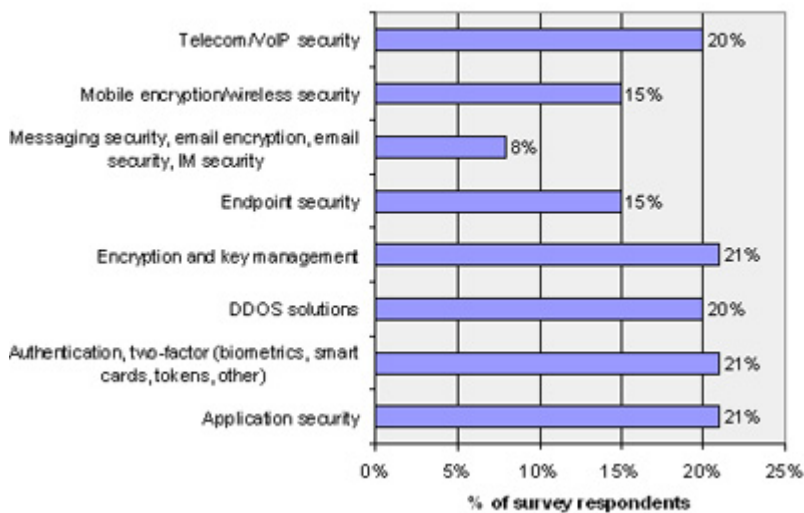
The study, "What Security Issues Are You Currently Facing?," includes responses from nearly 150 C-level executives and professionals charged with directing, managing and engineering security infrastructures within their respective organizations.

The study indicates that even though practitioners are most concerned about email phishing and securing mobile devices, technologies addressing these needs are at risk of being cut from IT budgets. Seventy-two percent of respondents indicated a rise in email-borne malware and phishing attempts since fall 2008, with 57% stating they have seen an increase in Web-borne malware. Concerns about zero-day attacks and rogue employees as a result of layoffs were cited by 28% and 26% of survey respondents, respectively.

When asked about the top security and organizational challenges they expect to face in the next 12 months, 57% of respondents cited budgetary constraints; 44% cited employee education as a major concern and 40% called out lost or stolen devices.

The survey also asked what technology investments will likely be bypassed or curtailed due to spending freezes and budget cuts. Given the above information, however, the survey illustrates that even though employees are seeing increases in email- and Web-borne malware and phishing, IT budgets are not being sufficiently allocated to defend against these issues.

**What technology investments will you likely have to bypass or curtail in the coming year?**



Specifically, the survey demonstrates that even though 72% of respondents have seen a rise in email-borne

malware and phishing, 8% still plan on cutting money that would previously be earmarked to attempt to mitigate those risks. Even more alarmingly is that 40% of respondents admitted that securing lost or stolen devices – like the iPhone or Blackberry – is a top concern in the coming year, yet 15% of those surveyed will be reducing spending in this area.

In an attempt to uncover the impact of the recent Twitter and [Facebook phishing attacks](#) that have received extensive media coverage over the last several months, RSA Conference asked respondents how their organizations were affected. The survey found that while 84% of respondents allow the use of these tools, only a mere 3% were seriously affected by the attacks. Conversely, 73% said that their organization was not impacted at all and 24% indicated they were somewhat affected.

“We rely on the real world experiences of security practitioners to develop the educational programming and the agenda at RSA Conference,” said [Sandra Toms LaPedis](#), Area Vice President and General Manager of RSA Conference. “This survey not only serves as a benchmark for the industry and a vehicle to learn from one another, but also provides insight into the issues that may become the content focus of RSA Conference 2010.”

## A year after Terry Childs case, privileged user problem grows

### Managing those who manage the keys is hard

By Jaikumar Vijayan

July 20, 2009 06:00 AM ET

Computerworld - One year after former network administrator [Terry Childs made national headlines](#) for locking up access to a crucial San Francisco city network, the issue of how to protect corporate systems against the very people who manage and administer them remains as thorny as ever.

Just yesterday, Lesmany Nunez, a former computer support technician at Quantum Technology Partners (QTP) in Miami, was sentenced to a year in jail for illegally using his administrator account and password to shut down the company's servers from his home computer. Nunez also changed the passwords of all the IT systems administrators at the company and deleted certain files that would have made data restoration from backup tapes easier. His actions resulted in more than \$30,000 in damages to QTP.

Numerous similar cases, including ones involving [Fannie Mae](#) and [Pacific Energy Resources Ltd.](#) have been reported over the past few months, each one causing considerable damage and disruption to the companies involved.

Childs is [awaiting trial after being jailed last July on a \\$5 million bond](#) for resetting administrative passwords to switches and routers on San Francisco's FibreWAN network, and later refusing to divulge the new passwords thereby locking up the network.

Such sabotage can be extremely difficult to stop because it involves users with legitimate administrative access to critical systems. But contributing to the problem is the continuing failure by many companies to adequately manage the numerous user accounts and passwords that control privileged access to critical corporate networks and systems.

Although the issue is well recognized by security experts, far too many companies continue to overlook it, said Sarah Cortes, an analyst with Inman TechnologyIT. The threat is "highly underestimated," Cortes said.

"It's not a sexy issue but it's a fundamental security issue," said Cortes, a former tech executive at several financial services companies.

Large companies can have thousands of account names and passwords that provide root access to applications, databases, networks and operating systems. While not all of them are critical to the enterprise, there are numerous accounts that if abused can cause serious disruptions enterprise wide.

Some companies can have anywhere between 10 and 70 people with root-level access to such critical systems, Cortes said. These could be staff who require access for system or database maintenance purposes, for

patching or upgrading applications, and other valid reasons. The number of people with such access is usually far greater than managers might know about or track, Cortes said.

The situation is worse in environments with older legacy systems that are no longer being actively supported but need to be maintained all the same. There can be numerous individuals in such situations who have been provided emergency, or temporary, root-access to a system in response to a specific need, but whose access is then never later revoked, she said.

Many companies today do not have adequate termination controls for quickly removing access rights when a person leaves a company.

Another problem is the fact that privileged passwords are often shared among multiple staff who might need access to the same system for various reasons. "When you are talking about a shared password you might not even know who has access to the password [over time]," said Boaz Gelbord, executive director of information security at Wireless Generation Inc., a technology services provider to the educational market.

Because such passwords are shared by people across multiple functional groups, they are seldom changed and, over time, end up being used by numerous individuals.

Many companies are still failing to adequately log and audit the use of such shared passwords to gain access to critical systems, Gelbord said. "There is a fundamental difference between a regular password and a shared password," he said.

While companies have fairly mature processes for forcing changes for regular passwords, few have the same processes for privileged passwords, he said.

More tools are becoming available to companies to help better manage privileged access accounts. Though such tools can do little to stop a really determined insider from abusing his or her privileged access, they do make it harder, Gelbord said.

His company is using a password management tool from Cyber-Ark Inc. to centralize privileged user accounts, apply policies to them, as well as log and audit their use.

"I think the real benefit of having such tools is not so much about preventing a particular person from hitting a particular system," Gelbord said. Rather it's more about instituting a process for controlling access to privileged accounts, he said. "You want to know exactly who has access to your critical systems at all times".

Cyber-Ark's products are designed to help companies centralize and securely manage privileged accounts, and can be used to automatically change passwords, as well as audit and log use.

The technology can be used to enforce privileged account policies on UNIX/Linux, Windows, Cisco, Oracle, SAP and other environments. The company is one among a handful of others, including Symark International Inc. and e-DMZ to offer tools designed to help companies better manage privileged accounts.

While such tools can be useful, it's vital that companies monitor the alerts generated by them, and sift through the false-positives, Cortes said.

Security managers need to do a daily audit and control report looking at all of those who have access to critical systems and ensuring that they have them for a legitimate reason, she said.

"I wouldn't expect to see more than one or two names for any application," Cortes said. "When you start to see the number grow, it's time to look into the matter."

# Agencies riddled with security holes, GAO says

---

## A performance audit shows that agencies are putting data at risk

By [Ben Bain](#)  
Jul 17, 2009

A continued lack of sufficient information security controls at major federal agencies puts sensitive data at risk, the Government Accountability Office said today. GAO also said the process agencies use to report progress on information security needs to be improved.

In [a report](#) released today, GAO said agencies have persistent weaknesses in the controls they place on information systems and insufficient information security policies. The GAO's auditors said a recent audit that examined how well agencies were protecting information and complying with the Federal Information Security Management Act (FISMA) found significant problems.

"These persistent weaknesses expose sensitive data to significant risk, as illustrated by recent incidents at various agencies," GAO said. "Further, our work and reviews by inspectors general note significant information security control deficiencies that place a broad array of federal operations and assets at risk."

GAO said that according to its previous findings and those from agency inspectors general, agencies have persistent weaknesses in the access controls, configuration management controls they use to protect data. In addition, problems also existed with their segregation of duties, continuity of operations planning and agencywide information security programs. GAO said almost all 24 major federal agencies had weaknesses in information security controls.

Meanwhile, the auditors said the current FISMA reporting process doesn't produce data to accurately gauge the effectiveness of agencies' information security activities. In addition, GAO said OMB annual reporting instructions to agency for FISMA reports weren't always clear and OMB didn't put key information about problems identified by the IGs in its report to Congress. GAO also said OMB didn't approve or disapprove agency information security programs.

To correct the problems, the auditors recommended that OMB:

- Update annual reporting instructions to request inspectors general to report on the effectiveness of agencies' processes for developing inventories, keeping track of contractor operations, and providing specialized security training.
- Clarify and improve reporting instructions to inspectors general for certification and accreditation evaluations.
- Include in the report to Congress a summary of the findings from the annual independent evaluations and significant deficiencies in information security practices.
- Approve or disapprove agency information security programs after review.

Vivek Kundra, the federal chief information officer, said in response to the report that OMB was working to clarify FISMA reporting guidance and improve performance metrics. He also said OMB was planning to move FISMA reporting to an Internet-enabled database for fiscal 2009 reporting.

Kundra also responded that each year OMB reviews all FISMA reports from agencies and IGs year and uses that information to evaluate agencies' security management programs.

## Cops swoop on e-crime gangs after banks pool intelligence Early success for new task force

By [Chris Williams](#)

8th July 2009

Two London-based cybercrime gangs have been busted, following an agreement by banks and credit card companies to share intelligence on network attacks and malware.

Early success for the new "virtual task force", which is set for public launch next week, comes after years of pressure from investigators frustrated at the lack of intelligence on the activities of cybercrime gangs.

The first swoop, dubbed "Operation Poplin" netted an Eastern European group working in South East London. Bank security staff detected them attempting to use trojans to steal money. The gang of 13 were arrested in April and face charges including money laundering and fraud.

In June an investigation using intelligence from the task force by the new Police Central e-Crime Unit, with FBI cooperation, saw nine arrests. "Operation Lumpfish" targeted a fraudulent music sales website which collected banking information for the gang.

Speaking at the Association of Chief Police Officers conference in Manchester today, Janet Williams, Deputy Assistant Commissioner of the Met's specialist crime directorate, said she expected the task force to allow a 15 and 30-fold increase in such targeted police activity.

"We have proved we can do this," she said.

"It's like a crime and disorder partnership, only one that actually works."

Researchers at Queen's University in Belfast and Chatham House in London will assist in the analysis of information shared via the virtual task force. ISPs are also cooperating, Williams said.

Banks and credit card companies have historically been very reluctant to share details of attacks against them, frustrating investigators and the security industry. Their secrecy stemmed from fears that widespread knowledge of their vulnerabilities could be exploited by criminals or competitors, and increase anxiety about online services among customers.

Financial services companies will not share all their security secrets via the virtual task force, but its forthcoming launch marks a significant step towards cooperation, Williams said. ®

## Oz cops turn to wardriving to fight Wi-Fi 'jackers

By [Tony Smith](#)

17th July 2009

Police in the Australian state of Queensland are to go on the hunt for unsecured wireless networks.

Claiming that "the crooks are out there driving around trying to identify these [open] networks", Queensland Police Detective Superintendent Brian Hay [told](#) local site ITnews that the Boys in Blue will now do the same.

Folk found to be in possession of an un-WEPed WLAN will be warned of the dangers they face, as will wireless router owners who enabled security but retained the default password.

"Look, lads, there's *another* 'Belkin54g'!..."

Some might argue that Queensland's cops have better things to do than war-drive around the state's 'burbs. But Hay compares the scheme to any other crime prevention activity, from warning home owners to secure their property and telling car owners not to leave their vehicles unlocked when unattended. ®

## City of Los Angeles Considering Move to Google-Provided Cloud Computing

(July 16 & 17, 2009) The city of Los Angeles has proposed moving its government e-mail, police records and other information management to Google's cloud computing services. If the proposal is approved, Los Angeles

will become the second US city, after Washington DC, to migrate data storage to Google's services. The plan has the mayor's support, but police officials have some concerns. Los Angeles Police Protective League president Paul Weber expressed concern about the security of data stored on Google systems. Last week, internal Twitter documents were accessed through Google Apps and leaked to the Internet.

[Editor's Note (Schultz): I like Google, but Google should by no means be considered a leader when it comes to information security practices.

Until Google achieves this reputation, users of Google's so-called (and misnamed) "cloud services" should not be very trusting concerning Google's email and file storage services. The city of Los Angeles should have heeded Paul Weber's word of caution. ]

## Consumer Devices with Embedded Web Interfaces are Vulnerable to Attacks

(July 16, 2009) Stanford University researchers tested 21 devices with embedded web interfaces, such as webcams, printers, network switches, and photo frames, and found that none was immune to attack. The researchers subjected the devices to several types of attacks including cross-channel scripting, cross-site request forgeries and unauthorized access of files or device resources. The devices posing the greatest overall security risk were network-attached storage, or NAS units. The researchers plan to share their findings at the Black Hat security conference in Las Vegas.

## The United States Tops the Spam Table

(July 20, 2009) A recent study by Sophos shows that the United States is responsible for relaying more spam than any other country in the world. In the report published on Monday, 15.6% of all spam email in the second quarter of 2009 was relayed from the United States. The other countries that make up the global top three are Brazil at 11.1% and Turkey at 5.2%. The top three countries and their rankings remain unchanged from the first quarter of 2009. The large percentage figure attributed to the United States can be explained by the number of infected PCs with access to broadband networks and that are part of large botnets.

## Analysts see alarming development in mobile malware

**By Jeremy Kirk**

July 16, 2009 09:35 AM ET

IDG News Service - The first worm that spreads between mobile devices by spamming text messages has developed a new communications capability that one security vendor says signals the arrival of mobile botnets.

Trend Micro has analyzed a piece of mobile malware known as "Sexy Space," which is a variant of another piece of mobile malware called Sexy View, which targets devices running the Symbian S60 OS.

Sexy View, which was detected by vendors such as F-Secure six months ago, is significant because it is the first known malware sample that spreads by SMS (Short Message Service). It appeared initially in China.

Infected phones would send SMSes to everyone in the phone's contact list with a link to a Web site. If someone clicked the link, they would then be prompted to install Sexy View, which purports to offer pornography-related content.

In another advancement, those who wrote Sexy View were able to get the application approved and signed by Symbian. The OS manufacturer, now owned by Nokia, vets applications for security using both manual and automated processes, said Mikko Hypponen, chief research officer for F-Secure.

Sexy View's creators were somehow able to subvert that automated vetting process, allowing the application to access functions such as SMS, Hypponen said. The latest variant, Sexy Space, is also signed by Symbian.

But in the latest alarming development, Trend Micro analysts have found that Sexy Space is capable of downloading new SMS templates from a remote server in order to send out new SMS spam, said Rik Ferguson, senior security advisor for Trend.

No malware for a mobile device has been known to do that before. Analysts at Trend had "heated internal discussions" about whether Sexy Space qualified as botnet code, Ferguson said.

Sexy Space is also capable of stealing subscriber and network information from the device and sending it to a remote server, Ferguson said.

Sexy Space confirms what analysts such as Hypponen and Ferguson have said since late last year: As mobile devices take on greater functionality and operate like minicomputers, it's likely they will be targeted by malware writers and eventually lassoed into botnets.

Botnets -- arguably one of the biggest security threats facing the Internet -- are networks of hacked computers that can be used to send spam, conduct denial-of-service attacks on Web sites or steal data.

Hypponen said F-Secure analysts had not confirmed that Sexy Space calls on a remote server, and Trend engineers are still studying where the remote server is located.

It's not clear how many phones may be infected. But one Beijing mobile security vendor, NetQin Tech, wrote on its [blog](#) that infections had been widespread in China and Saudi Arabia.

F-Secure informed Symbian about the malware. It is possible for network operators to revoke the certificate that allows an application to run on a Symbian phone, Hypponen said.

But the revocation mechanisms are not automatic, and depending on the operator's setup, it may not work for all phones, Hypponen said.

F-Secure has a [writeup](#) of the malware, also known as "Transmitter." Trend has also posted an [analysis](#).

## Mind Games: How Social Engineers Win Your Confidence

***Brian Brushwood, founder of Scam School, demonstrates the four simple psychological mechanisms underlying social engineering mind games.***

By [Joan Goodchild](#), Senior Editor

July 22, 2009 — [CSO](#) —

Social engineering and mind games expert Brian Brushwood has not come by his knowledge in the traditional manner of school or business training. Brushwood is the host of the Internet video series [Scam School](#), a show he describes as dedicated to social engineering in the bar and on the street.

In addition to his passion for teaching people about social engineering cons, Brushwood is also a touring magician who frequently performs on college campuses and has appeared on the Tonight Show. He first became interested in social engineering years ago as a means to enhance his performance and pull off secret moves successfully. Brushwood said his understanding and use of the term social engineering goes beyond the security industry perception.

"When I use the phrase, I am actually talking about an older version of it. Social engineering just basically means the application of social science to the solution of social problems," he said. "In other words, it's getting people to do what you want by using certain sociological principles."

These days, Brushwood uses social engineering techniques so frequently he admits it is sometime hard to "turn it off." Here Brushwood explains the four basic psychological tactics social engineers use to gain trust and get what they want, and how security pros can arm their staff against this type of deception.

## 1. Social engineers are confident and in control of the conversation

According to Brushwood, one of the first steps to pulling off something deceptive is to act confident. For example, someone trying to get into a secure building might forge a badge or pretend to be from a service company. The key to getting in without being challenged is to simply act like you belong there and that you have nothing to hide. Conveying confidence with body posture puts others at ease.

"People running concert security often aren't even looking for badges," said Brushwood. "They are looking for posture. They can always tell who is a fan trying to sneak back and catch a glimpse of the star and who is working the event because they seem like they belong there." Another way to gain the upper hand is to seem in charge through conversation, said Brushwood.

"The person who asks the questions controls the conversation," he said. "When someone asks you a question, it immediately puts you on defense. You feel a social pressure to give a correct or appropriate response."

Brushwood refers to these types of reactions as fixed action patterns and credits the book [Influence: The Psychology of Persuasion](#) by Robert Cialdini as a major inspiration for his current work.

*Takeaway:* Advise employees not to become too comfortable with allowing outsiders into the building. Visitors (and service providers) should have credentials checked thoroughly -- even if they are familiar faces.

## 2. They give you something

Reciprocation is another fixed action pattern, said Brushwood.

"When people are given something, such as a favor or a gift, even if they actively dislike the person who did it, they feel the need to reciprocate," said Brushwood, who referred to the Hare Krishnas as one of the more well-known employers of this tactic.

"They give out a flower or a copy of the Bhagavad Gita and say 'This is a gift for you. Enjoy. Oh, by the way, would you like to make a donation?' You may be thinking 'I didn't want this flower,' but it's still difficult to turn around and say 'No, go away.'"

Brushwood himself uses this tactic during his many cross-country flights when he is hoping for a free upgrade or perhaps a free drink or two. With a few bags of M&Ms in hand, he boards each flight and hands them to flight attendants on his way in and tells him he wanted to give them something for their hard work.

"Even if they hate M&Ms, they are so moved by the thoughtfulness of the gesture," he noted.

This tactic, like the confident attitude, would be useful for a social engineer trying to gain illegal entry into a secure facility or office building. However, Brushwood noted that the time delay between giving the gift and asking for a favor is also important.

"If you give a gift and then immediately ask for a favor, the odds are that somebody might perceive it as a bribe. If they perceive as a bribe, they react uncomfortably."

Instead, a skilled con artist might give something to a gatekeeping employee early in the day and then come back later, claiming to need access due to a mix up, such as an item left behind after a meeting.

"Chances are they will let you by as reciprocation for how you treated them earlier," said Brushwood.

*Takeaway:* Advise employees to be skeptical of anyone who tries to give them something. Depending on how big the stakes are, an experienced criminal may even spend weeks laying the ground work to form a reciprocal relationship with staff that can result in access to sensitive or secure areas.

## 3. They use humor

People generally enjoy the company of those who have a good sense of humor. The social engineer knows this all too well and uses it to gain information, get past a gatekeeper, or even just to get out of trouble. Brushwood refers to it as the 'liking' fixed action pattern.

"People who we like, or think we like, we are much more likely to grant a favor to because we feel a familiarity to them," he said.

Brushwood has used humor to get out of speeding tickets many times. His trick is to show a funny license picture and then even finds a way to hand the officer a Monopoly "Get out of Jail Free" card as part of his side-of-the-road shtick.

"Police deal all day with the boo-hoo stories," he said. "But my approach is to be upbeat. To give them the impression that I am not worried and would rather hang out and make them laugh."

Brushwood estimates he gets out of speeding tickets 80 to 90 percent of the time with this tactic.

*Takeaway:* In a breach or criminal scenario, the social engineer might try and chat with an employee to get information out of him. One good example is the fake IT call, where the caller asks for an employee's password. It is much more likely that sensitive information will be volunteered if the conversation is fun, and puts the employee at ease.

#### **4. They make a request and offer a reason**

Brushwood was recently inspired by the results of a recent Harvard study, also included in Cialdini's 'Influence,' which found people are likely to concede to a request if the word 'because' is used when asking. The study looked at groups of people waiting to use a copy machine in a library and how they responded when someone approached and asked to cut in line.

In the first group, the person would say: "Excuse me, I have five pages. May I use the Xerox machine because I'm in a rush?" In that group, 94 percent said yes and allowed the person to skip ahead in line. In another group, the line-cutter asked: "Excuse me, I have five pages. May I use the Xerox machine?" However, only 60 percent said yes to the person looking to cut. In a third group, the question was: "Excuse me, I have five pages. May I use the Xerox machine because I need to make copies?" Even though the reason was seemingly ridiculous, 93 percent still said yes to the line-cutter.

"Turns out magic word is because," said Brushwood. "It didn't matter what she said next. Just like if you see someone marching around like they own the place, it's safe to assume they belong there. Likewise, if someone says 'because' people assume they have some legitimate reason."

Brushwood points out that the fixed action pattern at work in this scenario is the simply the perception of a reason. Even if the reason given is nonsense, hearing the word 'because' prompts people to respond favorably.

*Takeaway:* It's important to slow down and look and listen to what is happening and what is being said in a work environment. During a hectic day, it may seem easier to wave someone by, or give up information when it is requested. But awareness and presence of mind are paramount to prevent a criminal from taking advantage of you.

## **Twitter: A Growing Security Minefield**

***As it explodes in popularity, the micro-blogging site attracts the bad guys.***

***By Robert Vamosi***

July 23, 2009 — [PC World](#) —

In June, the world watched as tweets from the streets of Tehran flooded Twitter. Frequent Twitter users--and people who hadn't even heard of the microblogging service--were suddenly and simultaneously witnessing its potential.

At the same time, antivirus vendors were warning of new phishing attacks that spread via Twitter. Using Twitter accounts, phishers would follow users and then infect them via a link to a fake profile page laden with malware. Like instant messaging, MySpace, and [Facebook](#) before it, Twitter had come of age.

After three years of relatively quiet development and growth, the service's meteoric rise in 2009 has been rough. Aside from scaling issues due to the influx of new users, in January a [Twitter hack](#) compromised the accounts of 33 high-profile users, including President Barack Obama, CNN anchor Rick Sanchez, and entertainer Britney Spears.

In April, a [Twitter worm](#) known as "Mikeyy" or "StalkDaily" reared its head. Similar to the 2005 [Samy worm on MySpace](#), the Mikeyy worm was authored by a 17-year-old who took advantage of a code quirk to gain notoriety for his Web site, StalkDaily.com. Twitter shut it down--plus a few follow-up viruses ("How TO remove new Mikeyy worm!")--fairly quickly. Following the worm attacks, cofounder Biz Stone wrote on the company blog, "Twitter takes security very seriously and we will be following up on all fronts."

### **Shortened-URL Dangers**

Parallel to the growth of Twitter is the expansion of URL-shortening services. Fitting your thoughts into 140 characters takes practice; including full URLs is almost impossible. Usually URLs have to be truncated through services such as Bit.ly and TinyURL.com, which also mask the true destination URL and can present their own security problems as a result.

The first signs of shortened-URL trouble came with a pair of Twitter worms that promised to help users remove the Mikeyy worm. In June, a wave of hidden poisoned URLs swept Twitter, using Bit.ly links to low.cc and myworlds.mp domains where users were asked to download a file called free-stream-player-v\_125.exe to view a video. The file held malware. Bit.ly and TinyURL have been responsive to reports of abuse; Bit.ly, for one, now blocks those low.cc and myworlds.mp domains.

At least one security product, ZoneAlarm, blocks access to TinyURL.com by default, listing it as a potentially malicious site (you can unblock it). You have other ways to protect yourself, too. TinyURL has a preview feature, and Firefox has a Bit.ly preview add-on. Some Twitter apps, such as TweetDeck and Tweetie, also preview the URL before you click.

Aviv Raff of RSA designated July 2009 as "A Month of Twitter Bugs," during which researchers are to disclose a new Twitter vulnerability each day. Citing previous efforts focused on browsers and on Apple Mac OS vulnerabilities, Raff says his goal is not to break Twitter but to improve it and to address all social networking flaws: "I hope that Twitter and other Web 2.0 API providers will work closely with their API consumers to develop more secure products." The first disclosed Twitter bug concerned cross-site scripting flaws in Bit.ly. Within hours of the disclosure, Bit.ly corrected them.

### **Follow Me, Please**

A frequent goal of Twitterers is to build an audience; some people rate their profile a success if it has hundreds or even thousands of followers. A site called [TwitterCut](#) advertised that it would dramatically increase your base of followers--if you gave it your user name and password. Most security vendors deemed it a pay-per-click scam.

People who fell for the scam saw their Twitter accounts later used in the "[Best Video](#)" phishing attack, in which anyone who visited a link in the tweet wound up downloading a malicious PDF that then attempted to install a [fake security product](#) if the PC lacked the latest Adobe security update.

### **Gone Phishing**

Most [Twitter phishing attempts](#), however, are more straightforward. Twitter routinely notifies users of recent followers by e-mail, often with a link to the follower's profile. Recent phishing attacks spoofed that e-mail and held a link to a faux Twitter log-on page.

Another variation of the [phishing scam](#) sent out a tweet reading, "Hey, check out this funny blog about you." Clicking the URL took the victim to a fake page (at twitter.access-logins.com/login/). No matter how good the site looks, examine the URL, and think twice about entering your info--especially if you are already logged in to Twitter.

Bad guys have tried more-subtle tactics, too, such as the [porn-name game](#). According to the game, to create the name you'll use during your adult-film career, you take the name of your first pet and combine it with the street you grew up on, your mother's maiden name, or the model of your car. Recognize those things? They're common security questions. By tweeting your answers, you could give away access to your Twitter account--or to your bank account.

Some of the emerging security rules for using Twitter are simply common sense. Just as you wouldn't leave a phone message saying you'll be out of town, don't tweet your vacation plans. And please don't share your location if you're a U.S. congressperson going on a confidential overseas trip. Just ask Representative Pete Hoekstra (R-MI), who [tweeted earlier this year](#): "Just landed in Baghdad. I believe it may be [the] first time I've had [BlackBerry] service in Iraq."

## Hackers put social networks such as Twitter in crosshairs

By Jeremy Kirk

August 17, 2009 11:08 AM ET

IDG News Service - Web sites such as Twitter are becoming increasingly favored by hackers as places to plant malicious software in order to infect computers, according to a new study covering Web application security vulnerabilities.

Social-networking sites were the most commonly targeted vertical market according to a study of hacking episodes in the first half of the year. The study is part of the latest Web Hacking Incidents Database (WHID) report, released on Monday. In 2008, government and law enforcement sites were the most hit vertical.

Social networks are "a target-rich environment if you count the number of users there," said Ryan Barnett, director of application security research for Breach Security, one of the report's sponsors, which also includes the [Web Application Security Consortium](#).

Twitter has been attacked by several worms, and other social-networking platforms such as MySpace and Facebook have also been used to distribute malware. That's often done when an infected computer begins posting links on social-networking sites to other Web sites rigged with malicious software. Users click on the links since they trust their friends who posted the links, not knowing their friend has been hacked.

The WHID sample set is small, encompassing 44 hacking incidents. The report only looks at attacks that are publicly reported and those with which have a measurable impact on an organization. The WHID's data set is "statistically insignificant" compared to the actual number of hacking incidents, but shows overall attacker trends, Barnett said.

Other data showed how Web sites were attacked. The most common attack was SQL injection, where hackers try to input code into Web-based forms or URLs (Uniform Resource Locators) in order to get back-end systems such as databases to execute it. If the input is not properly validated -- and malicious code ignored -- it can result in a data breach.

Other methods used include cross-site scripting attacks, where malicious code gets pushed to on a client machine, and cross-site request forgery, in which a malicious command is executed while the victim is logged into a Web site.

The WHID found that defacing Web sites is still the most common motivation for hackers. However, the WHID includes the planting of malware on a Web site as defacement, which also points to a financial motivation. Hacked computers can be used to send spam, conduct distributed denial-of-service attacks and for stealing data.

"Ultimately they [the hackers] want to make money," Barnett said.

## Cisco 2009 Midyear Security Report

(July 14, 2009)

Cyber criminals are taking their cues from the business world, according to a new Cisco report. In addition to creating business and marketing plans, cyber criminals are developing new techniques to pace with emerging technology and exploit the ever-shifting winds of interest in popular culture. Criminals are also turning more frequently to SMS text messages to lure victims, and are increasingly using a technique that has been dubbed

smishing, in which phishing links are sent to smart phones where a user can click on the link. SMS attacks are also being used to send messages that appear to come from financial institutions and ask the recipients to call a number and verify account information.

Cyber criminals have also developed niche services, such as scanning malware to see if it will be blocked, or breaking CAPTCHA tests.

## **Insiders Becoming Source of Hacking and ID Theft Threats**

**Computer Business Review (07/15/09) ; White, Kevin**

A new Cisco report has brought attention to insider hacking and identity theft attempts as legitimate security concerns, which can be expected to escalate this summer and fall. In its most recent audit of global security threats and trends, the firm said that considering the recession during which many workers have lost their jobs or become disillusioned, the increase of insider attacks seems especially likely. Cisco's Maurizio Taffone said that companies need to reexamine their security strategies and vulnerabilities to possible insider thefts. "Data leakage protection technology has a part to play, as do systems that help identify unauthorized access to enterprise resources," he said. The report also verified a resurgence of spam, while social networking attacks are set to persist and attacks on legitimate Web sites are increasing. Cisco noted that cybercrooks are increasingly taking advantage of current events, while spamdexing is expanding, in which cybercrooks load Web sites with keywords to exploit users' trust of search engine rankings.

## **Encryption Reduces Risk of Data Breach: Study**

**Computer Business Review (07/08/09) ; White, Kevin**

Current research indicates that encryption mitigates the risks of an enterprise data theft or penetration attack, but businesses are still not using the technology to its fullest potential. In a recent Ponemon Institute study, 33 percent of those firms reporting no data theft occurrence in the last 12 months alleged to have had implemented a business-wide encryption policy. On the contrary, businesses with the highest volume of data theft incidents were discovered to be the least likely to have implemented a diligently enforced, organization-wide initiative regulating the use of data encryption platforms. Of businesses claiming five or more data-loss incidents, none employed any type of encryption plan. The study found that 57 percent of British businesses are protecting sensitive data with some variety of encryption data, with more than one third having implemented a small-scale strategy to address certain applications. "Encryption is most widely used to protect the data held on file servers, virtual private networks, and databases," the report states. "VOIP and mainframe encryption are the least deployed applications." The study also found that public enterprises experienced the highest volume of data breaches in the past year. "This study underlines the critical importance of implementing an encryption strategy that encompasses all aspects of an organization's data, not to just meet privacy or data security regulations but to also protect against brand damage and loss of customers," says PGP Corp. CEO Phillip Dunkelberger.

## **Use of tracking cookies on government sites sparks privacy concern**

### **Feds seek comments on use of Web tracking tools on agency sites**

**By Jaikumar Vijayan**

July 28, 2009 05:54 PM ET

Computerworld - Privacy advocates are raising questions about a proposal to revamp the use of tracking cookies on federal government Web sites.

Under the proposal, U.S. government agencies would be allowed to use single-session and multi-session cookies, including persistent cookies, to track users -- as long as security and privacy standards governing the collection and use of tracking information are met. The agencies would have to post clear notice of data collection and allow users to opt-out.

The idea is to make government Web sites more user-friendly and to enable better customer service and Web analytics, according to federal CIO Vivek Kundra and Michael Fitzpatrick, the associate administrator at the Office of Information and Regulatory Affairs. They wrote about the proposed changes in a [blog post](#) Friday.

Agencies and the public have until Aug. 10 to comment on the proposal, which came from the Office of Management and Budget.

If the plan is adopted, it would mark a departure from a policy first put in place in 2000 and [updated in 2003](#) that prohibits government sites from using persistent cookies "or any other means" such as Web beacons to track visitor activity, unless agency heads authorize their use. When tracking cookies are used, agencies must conspicuously post the reasons for collecting information, spell out the sort of data collected and detail privacy safeguards.

Privacy advocates have for some time maintained that such restrictions protect site visitors from being tracked and profiled. They have argued that users should reasonably expect privacy when visiting a government site and that any attempt to dilute the protections is ill-advised. Those concerns have grown in recent months, with many worried that the Obama Administration's espousal of Web 2.0 technologies and social networking tools will affect long-held privacy protections.

Soon after Obama took office, for instance, privacy advocates [were up in arms over a White House policy change](#) that permitted the use of tracking cookies in [YouTube videos](#) embedded on the WhiteHouse.gov Web site.

"The Obama Administration must tread very carefully here and think about our civil liberties in the digital era," said Jeffery Chester, executive director of the Center for Digital Democracy (CDD), a privacy rights advocacy group. "Given the unique data collection and targeting power of online media, the government should be limited in the information it can collect on us."

As administrations change, policies regarding the use of data collected by Web analytics tools could also change, he said. "[The] government could have an arsenal of profiling data that could be used to influence voters and the public." While there are benefits from using cookies, the blog post by Fitzpatrick and Kundra "glossed over" concerns that have been previously expressed by many including lawmakers.

Cindy Cohn, legal director of the Washington-based Electronic Frontier Foundation said that the government needs to clearly articulate what it wants to do with any data it gets. "The devil is going to be in the details," she said. While session cookies can yield information that is useful in delivering a better user experience, the use of persistent cookies on government Web sites should be studied carefully.

"We would want to see a pretty serious case effort ... showing us why the information would be useful," what officials would do with the data and what kind of checks would be there to ensure compliance, Cohn said.

Just because commercial enterprises have been using persistent cookies doesn't automatically mean that government agencies should be allowed to use them, she said. "The government doesn't need to do the same sort of analytics that commercial companies do. The government doesn't have the same interests and shouldn't have the same interests."

## Privacy group wants U.S. to detail computer monitoring program

**By Grant Gross**

July 28, 2009 04:25 PM ET

IDG News Service - President Obama's administration needs to answer several questions about the privacy implications of a new version of a computer intrusion detection system that can reportedly read e-mail, a privacy and civil rights advocacy group said.

The Center for Democracy and Technology (CDT), in [a report](#) released today, called on the Obama administration to release information about the legal authority for the so-called Einstein intrusion detection system, a version of which has been rolled out at the U.S. Department of Homeland Security.

The CDT report also asks the Obama administration to release information about the role of the National Security Agency (NSA) in the development and operation of Einstein 3, a new version of the software reportedly being developed.

The second version of Einstein is deployed at the DHS and is being rolled out to other U.S. agencies. While Einstein 2 is able to detect malicious code during predefined code signatures, Einstein 3 will also be able to read e-mail and other Internet traffic, according to recent press reports.

"This raises serious privacy concerns," the CDT report says. "While its predecessor merely detected and reported malicious code, Einstein 3 is to have the capability of intercepting threatening Internet traffic before it reaches a government system, raising additional concerns. According to press accounts, Einstein 3 will operate inside the networks of the telecoms ..."

The Einstein 3 used capabilities created by the NSA, the CDT paper says. The NSA is the agency that partnered with U.S. telecom carriers in recent years to conduct surveillance on U.S. residents exchanging telephone calls or e-mail messages with foreigners with suspected ties to terrorism.

Spokespersons for the DHS and the NSA didn't immediately return messages seeking comment on the CDT report.

The kind of information the CDT is asking the Obama administration to disclose about Einstein is similar in some ways to information released in a privacy impact statement for Einstein 2, released in May 2008, said Gregory Nojeim, CDT's senior counsel. The information CDT is seeking "wouldn't help an adversary overcome the system," he said.

Among other things, CDT wants to know what law gives DHS the legal authority to conduct such surveillance, Nojeim said. "Some facts about the program might need to remain secret, but the law that supports it cannot be a secret," he added.

CDT also wants to know:

- If the private sector was involved in developing Einstein 2 and 3.
- What safeguards will be put in place to prevent the misuse of private information collected.
- What personally identifiable information will be collected by Einstein 3.
- How will DHS share data collected with Einstein 3?

## **P2P ban plan for government gets mixed response**

Poorly crafted law could would also block some cost-saving file-sharing tech, some say

**By Jaikumar Vijayan**

July 30, 2009 09:16 PM ET

Computerworld - A proposal to introduce a bill seeking to formally ban the use of peer-to-peer (P2P) file sharing applications on government and contractor networks is evoking a mixed response.

Rep. Edolphus Towns (D-NY) yesterday announced his intention to introduce such a bill, after he, and other members of the House Oversight and Government Reform Committee heard testimony about numerous highly sensitive government documents being found on P2P networks as a result of inadvertent leaks.

Examples of such leaks that were highlighted at the hearing included [details on the President's motorcade routes and the First Family's safe house location](#) -- to be used in a national emergency -- being found on P2P networks.

Towns, who is the chairman of the House oversight committee, said that the leaks pointed to a continuing failure by developers of P2P software to implement features for preventing inadvertent data disclosure on file-sharing networks.

He said that a ban on P2P use on government and contractor computers and networks had become necessary because the developers had so far shown themselves to be "unwilling or unable" to ensure P2P user safety. "It's time to put a referee on the field," he said at the hearing.

The idea is an "excellent" one, said Thomas Sydnor, a director at the Progress & Freedom Foundation, a Washington based think-tank. "The real questions are over how it gets implemented and by whom," Sydnor said.

Over the past few years there has been some debate in Washington over the need to regulate use of P2P software on government networks, because of data leak fears, he said.

A [2004 directive from the White House Office of Management and Budget](#) recommends measures federal agencies for governing the use of P2P software on federal agency and contractor networks, he said.

The question now is whether the time has come to transition the directive into a formal law with Congressional oversight or let it remain an executive directive, he said.

The difference right now is that if a federal agency is not complying with the OMB directive it remains an executive branch concern. "The debate is whether it should be done by law or by directive," he said.

Either way, the time has come for greater oversight over the use of file-sharing tools on government and contractor networks, especially because more government workers are logging into to work from home, these days Sydnor said. Care needs to be taken to ensure that any law that is crafted not "sweep in" useful file-sharing technologies as well, he added.

But Fred von Lohmann, a senior staff attorney with the Electronic Frontier Foundation said a government wide ban on P2P use would have dubious benefit. "I'm sure there are at least as many leaks that occur thanks to unwise uses of e-mail and Web browsers," compared with P2P use, he said.

A ban specifically on P2P use would not go far enough in tackling leaks stemming from e-mail, browsers and other sources, von Lohmann said. At the same time, it could also have the effect of banning the use of potentially useful P2P tools within government enterprises, he said.

He pointed to the increasing use of BitTorrent and other P2P architectures by video game companies and licensed music services such as Spotify as examples where the technology can play a very useful role. "So it could be very difficult to ban only the "bad" software without also banning the "good" software," von Lohmann said.

"It would be an unfortunate outcome if, 10 years from now, the US government were unable to take advantage of new, cost-saving software products because of an antiquated P2P software ban enacted today."

This is the second time in the last two years -- and the third time overall -- that House oversight committee has held a hearing on the data leak risks associated with the use of P2P file-sharing software. If Towns does introduce a bill seeking to ban P2P, it would become the second piece of legislation introduced recently to deal with concerns stemming from inadvertent data leaks on file-sharing networks.

In March, Rep. Mary Bono Mack (R-CA) introduced [The Informed P2P User Act \(H.R. 1319\)](#), which is designed to get file-sharing software developers to provide clear disclosure to users on whether and how their files will be made available for sharing with others on a P2P network.

## Researcher reveals massive 'professional thieving' botnet

Ultra-stealthy Clampi Trojan snags 'tremendous' amount of financial info, money

By Gregg Keizer

July 29, 2009 03:39 PM ET

Computerworld - A ferocious piece of malware that's infected up to a million PCs is stealing a "tremendous" amount of financial information from consumers and businesses that log on to their bank, stock broker, credit card, insurance, job hunting and favorite e-shopping sites, a noted botnet researcher said today.

"Clampi is the most professional thieving pieces of malware I've ever seen," said Joe Stewart, director of malware research for SecureWorks' counter-threat unit. "We know of few others that are this sophisticated and wide-ranging. It's having a real impact on users."

The Clampi Trojan horse has infected anywhere between 100,000 and 1 million Windows PCs, said Stewart -- "We don't have a good way of counting at this point," he acknowledged -- and targets the user credentials of 4,500 Web sites.

That's an astounding number, said Stewart, who has identified 1,400 of the 4,500 total. "There are plenty of other banking Trojans out there, but they usually target just 20 or 30 sites."

Hackers sneak Clampi onto PCs by duping a user into opening an e-mailed file attachment or by using a multi-exploit toolkit that tries attack code for several different Windows vulnerabilities, Stewart said. Once on a machine, the Trojan monitors Web sessions, and if the PC owner browses to one of the 4,500 sites, it captures usernames, passwords, PINs and other personal information used to log on to those sites, or to fill out forms.

Periodically, Clampi "phones home" the hijacked information to a command-and-control server run by the hackers, who then empty bank or broker accounts, purchase goods using stolen credit card information or simply compile it for future use, said Stewart.

Although that describes most key-logging or spying malware, Stewart said Clampi is different, both because of the obvious scale of its operation and because of the multiple layers of encryption and deception used by its makers to cloak the attack code and make it nearly impossible for researchers to investigate its workings.

Stewart started tracking Clampi in 2007, but began an intensive examination earlier this year. "The packing that Clampi uses is very sophisticated, and makes it really, really difficult to reverse engineer, said Stewart. "I'd say this is the most difficult piece of malware I've ever seen to reverse engineer." Security researchers often will reverse engineer malware -- pulling it apart to try to decipher how it works -- during their investigations.

"They're using virtual machine-based packers that lets them take code from a virtual CPU instruction set, so that the next time it's packed, it's completely different," said Stewart. "You can't look at Clampi with a conventional tool, like a debugger. It's a real mess to follow, frankly."

The Trojan also encrypts the traffic between hijacked systems and the botnet command-and-control server using multiple methods, said Stewart. Not only is the network communications traffic encrypted in 448-bit blowfish encryption, but the strings inside the attack code binaries are also encrypted. Clampi also uses another unusual tactic to hide from antivirus scanners; its modules -- there are anywhere from four to seven different pieces of the malware -- are stored as encrypted "blobs" in the Windows registry.

The sheer scope of the Clampi operation also separates it from run-of-the-mill financial malware, Stewart argued. "They're targeting not just banking sites, but a wide variety of sites where people put in credentials that help them steal money somehow," said Stewart. Among the 1,400 site he has identified are military information portals, mortgage, insurance, online casino, utility advertising networks and news sites. The sites are hosted in 70 different countries.

"That, in itself, speaks to a vast operation on the back end," Stewart said.

It's impossible to say for certain, but all clues point to Russia or Eastern Europe as the base for the criminal gang riding herd on the Clampi botnet. "It looks like it's just one group behind it," said Stewart. "We don't see [chatter about it] on the usual underground forums, which is one reason why there's little or no coverage about Clampi up till now. It's very closely held, and the group is very secretive."

In fact, Stewart held out little hope of nailing the criminals behind Clampi. The command-and-control servers they use to direct the hijacked PCs -- and to receive the stolen usernames and passwords -- are not hosted by a commercial hosting service, but instead are hidden within individual compromised PCs. "I don't think we'll ever get the command-and-control servers," Stewart admitted.

One victim of a Clampi infection, and resulting theft, that has come forward is Slack Auto Parts, in Gainesville, Ga., which was robbed of nearly \$75,000, according to a story last week in the [Washington Post](#). The co-owner of the company, Henry Slack, told the newspaper that the malware ripped off log-on information for the firm's bank accounts, then managed to move the money to multiple money "mules" across the U.S.

Clampi had been on a Slack PC for more than a year before the bot's controllers used the information gathered to pillage the company's bank account.

One way for businesses -- and users -- to stymie this ultra-stealthy Trojan, said Stewart, is to do any financial tasks on an isolated, dumbed-down PC that is used only to connect to banks, brokers and the like. That advice works because Clampi spreads most efficiently on company networks. If it manages to infect one PC inside an organization, it uses a Windows SysInternals tool dubbed "PsExec" made by Microsoft to copy the Trojan to all the machines on the domain.

"Clampi can spread across Microsoft networks in a worm-like fashion," said Stewart. "Forget things like Conficker. You'd better rank this [botnet] up there right at the top."

## **New Technology to Make Digital Data Self-Destruct**

(NY Times, 7/21/09)

A group of computer scientists at the University of Washington has developed a way to make electronic messages "self destruct" after a certain period of time, like messages in sand lost to the surf. The researchers said they think the new software, called Vanish, which requires encrypting messages, will be needed more and more as personal and business information is stored not on personal computers, but on centralized machines, or servers. In the term of the moment this is called cloud computing, and the cloud consists of the data - including e-mail and Web-based documents and calendars - stored on numerous servers.

The idea of developing technology to make digital data disappear after a specified period of time is not new. A number of services that perform this function exist on the World Wide Web, and some electronic devices like FLASH memory chips have added this capability for protecting stored data by automatically erasing it after a specified period of time. But the researchers said they had struck upon a unique approach that relies on "shattering" an encryption key that is held by neither party in an e-mail exchange but is widely scattered across a peer-to-peer file sharing system.

## **Fake Security Software Steals \$34 Million Monthly**

By [Thomas Claburn](#) - July 29, 2009 (04:50 PM EDT)

Ignorance may be bliss, but it can also be expensive. Insufficiently knowledgeable [computer](#) users are downloading and paying for fake security [software](#) in increasing numbers, creating massive revenue for cybercriminals.

"More and more people are acclimating to the Internet and they feel they can make these important security decisions," said Sean-Paul Correll, security evangelist and threat researcher for [Panda Security](#). "They don't feel the need to call their tech-savvy grandson."

Fake security software, also known as "rogueware," is a form of [malware](#) that attempts to convince people that their computers are infected with malware.

Following the exploitation of a [vulnerability](#) or a visit to a malicious Web site, rogueware will weasel its way onto a computer and then purport to find malware on the system in question. It will offer to remediate the problem once the victim enters a credit card number to pay for the "security software." But payment typically does not cure the infection.

"Cyber-criminals no longer need to steal users' information in order to make their money; instead, they simply need to find ways to get users to part with their cash voluntarily," says a report released by Panda Security on Wednesday.

According to Panda, the rogueware business took off in 2008 and has continued to surge. At the end of 2008, the company said that it had detected almost 55,000 rogueware samples. By the end of Q3 this year, Panda expects to identify more than 637,000 new rogueware samples, an increase of more than tenfold in less than a year.

Rogueware cybercriminals spread their fake software through social media by manipulating search engines to get their links to the top of [search](#) results lists, by inserting links into comments on Digg.com, by tweeting their links on Twitter, and by exploiting vulnerabilities in [blog](#) software and on Facebook.

Panda estimates that 35 million computers are infected by rogueware every month, affecting perhaps half that number of actual users.

Such large numbers, Panda claims, lead to substantial revenue. The company estimates that cybercriminals are earning about \$34 million per month from rogueware, which typically sells for between \$49.95 and \$79.95.

"They're making an insane amount of money," insists Correll.

This claim isn't merely speculation. According to Correll, a [hacker](#) known by the name "NeoN" infiltrated rogueware manufacturer Bakasoftware in September 2008 by exploiting an [SQL](#) vulnerability on the group's Web site. NeoN copied a spreadsheet of payments to Baka's affiliates. The numbers show that the malware group's top affiliate earned \$81,388.61 in a period of only six days.

"That's almost \$5,000,000 per year and it's an astronomical number considering that this projection is just for one of many affiliates in Baka's roster, not to mention that the rogueware business has grown about four times the size it was in 2008 (in terms of sample volume)," Panda's report states.

# Future proof your IT systems by keeping these security threats in mind.

By Nicole Kobie, 29 Jul 2009 at 15:56

In the future, online security threats will be much the same as they are now – but with a few new twists.

So claims the [Information Security Forum](#), which gazed into its crystal ball to come up with a threat list for 2011 – see below for the full list.

“Many of the threats in 2011 will be familiar ones that are evolving and will present new and sophisticated attacks to compliment tried and tested techniques,” said Jason Creasey, head of research at the ISF.

Cyber crime topped the list, with Crimeware as a Service – such as [ready-made malware or botnets](#) – becoming more prevalent, along with [insider threats](#).

“It is also clear that the financial crisis is accelerating these changes, fuelled by increasing staff turnover and dissatisfaction along with the increased involvement of organised criminal groups that see online crime as a lucrative and low risk alternative to other nefarious activities,” he added in a statement.

Other top security issues will be [IT infrastructure](#) weaknesses, tougher regulations, outsourcing, and network boundaries being worn down. Rounding out the top ten will be [mobile malware](#), Web 2.0 flaws, corporate espionage, the difficulties securing user driven systems, and the blurring line between work and personal life.

Indeed, some of those security trends will combine, with criminals recruiting unhappy employees for inside information. “This more sophisticated and planned approach by criminal gangs comes at time when IT budgets are under pressure and companies are also looking to outsourcing and offshoring to save money,” said Creasey.

“These potential weaknesses in the IT infrastructure and third-party relationships – particularly with the advent of cloud computing – pose further threats and it is important to have the right controls in place to mitigate the risks.”

The ISF called on companies to continue to invest in security in order to keep data safe. Chief executive Prof. Howard A. Schmidt said that “even in today’s financial climate and increased threat environment, we are better placed than ever before to meet these challenges – as long as we have the resolve to strengthen and invest in security rather than reduce it.”

## **The ISF's top 10 threats in 2011:**

1. Criminal attacks
2. Weaknesses in infrastructure
3. Tougher statutory environment
4. Pressures on offshoring / outsourcing
5. Eroding network boundaries
6. Mobile malware
7. Vulnerabilities of Web 2.0
8. Incidents of espionage
9. Insecure user-driven development
10. Changing cultures

# Two in three Australian companies leak data

By [Brett Winterford](#)

Aug 11, 2009 2:52 PM |

## **Renews calls for mandatory data disclosure laws.**

Two in three Australian organisations experienced a serious data breach in the last twelve months, according to a survey by the Ponemon Institute.

The Institute, commissioned by data encryption company PGP, paid 482 IT security professionals in Australia to answer questions around the protection of their data.

Some 69 percent of respondents said they experienced at least one data breach in the last 12 months, up from 56 percent in 2008.

One in four of those companies that experienced a data breach suffered five or more breaches in the 12 months, up 22 percent on 2008.

Of those organisations that did admit to losing data, 65 percent chose not to inform the public - a figure the report's authors said was "sure to add to the demand for Australia to adopt data breach notification laws similar to those in the United States."

The Federal Government has spent the last few months reviewing privacy laws, the first draft of which was [due to be released to the public within a week](#).

But no timeline has been set for the introduction of mandatory data disclosure laws, as [recommended by the Australian Law Reform Commission](#) and the Office of the Privacy Commissioner.

In the interim, the Office of the Privacy Commissioner has produced a [voluntary guide to managing data breaches](#).

The survey also revealed some interesting data on what motivates organisations to protect their data.

Of those organisations that use data encryption technology to protect against the leak of confidential data, only 15 percent said they did so for regulatory reasons (citing the Federal Privacy Act, National Privacy Principles and PCI DSS requirements) whereas 70 per cent used encryption to protect their brand and reputation.

## 8 Dirty Secrets of the IT Security Industry

***IBM ISS Security Strategist Joshua Corman speaks out on what he believes are eight cancerous blights affecting the security industry. His goal: motivate people to wake up and battle the affliction.***

By [Bill Brenner](#), Senior Editor

August 17, 2009 — [CSO](#) —

Joshua Corman would seem an unlikely critic of IT security vendors. After all, he works for one. Yet Corman, principal security strategist for IBM's Internet Security Systems division, is speaking out about what he sees as eight trends undermining the ability of IT security practitioners to mount an effective defense against online outlaws.

Having worked for the vendor side, Corman says he is uniquely positioned to grasp its weaknesses up close. And so, with a PowerPoint presentation on the "8 Dirty Secrets" of the market in hand, he has traveled to seminars and worked the phones, hoping to motivate a change for the better. Here is the breakdown of those 8 dirty secrets and what Corman sees as practical ways to keep the vendors honest.

### **Dirty Secret 1: Vendors don't need to be ahead of the threat, just the buyer**

This is the problem that leads to the seven "dirty secrets" that follow. In essence, Corman said, the goal of the security market is to make money, not to ensure the customer's security.

Tom Vredenburg, regional IM manager for Houston-based Wartsila Corp., said Corman's take is consistent with what he has experienced in the trenches. "Not only has security become a phantom deliverable, but the vendors themselves have become equally tough to pin down and evaluate. Are they software sellers or risk managers? Are they service providers or network designers? Am I buying partnerships or licenses? Most of them don't know themselves what they are -- only that they need to sell something that most people don't really want to buy in the first place -- insurance."

Several security vendors defended themselves against that notion, including Cloakware product management director Terry Brown.

"Ultimately, there's still a quest for dollars across the security market, but now, because of the economic downturn, both vendors and customers are developing more reasonable expectations, right-sizing the market and IT spending."

### **Dirty Secret 2: AV certification omissions**

While AV tools detect replicating malware like worms, they fail to identify such as non-replicating malware as Trojans. Though Trojans have been around since the beginning of malicious code, Corman said there's no accountability in AV certification tests. Companies are therefore lulled into a false sense of security, wrongly believing the AV they purchased is protecting them from all malware.

"Today Trojans and other forms of non-replicating malcode constitute 80 percent or more of the threats businesses are likely to face," Corman said. "AV accountability metrics are simply no longer reflective of the true state of threat."

### **Dirty Secret 3: There is no perimeter**

Corman said those who truly believe there's still a network "Perimeter" may as well believe in Santa Claus. That's not to say there is no perimeter. It's just that companies are foggy on what the perimeter truly is, and security vendors are doing little to fix that. For the sake of Dirty Secret 1, the reality of Dirty Secret 3 is swept under the rug, leading companies to buy products that are not always effective in addressing their particular risks.

"We need to define what the perimeter is," he said. "The endpoint is the perimeter, the user is the perimeter. It's more likely that the business process is the perimeter, or the information itself is the perimeter, too. If you design your security controls with no base assumption of a perimeter, when you have one you are more secure. The mistake we tend to make is, if we put the controls at the perimeter, then we will be fine. For many threats, we couldn't be more wrong."

#### **Dirty Secret 4: Risk management threatens vendors**

Risk management really helps an organization understand its business and its highest level of risk, Corman said. But a company's priorities don't always map to what the vendors are selling.

"Vendors focus on individual issues so you will continue to buy their individual products," he said. "If you don't have a clear picture of your risk priorities, vendors are more than happy to set them for you. Security needs to conform to and support your business priorities. Too often, vendors want your business to conform to their portfolio."

#### **Dirty Secret 5: There is more to risk than weak software**

Corman said the lion's share of the security market is focused on software vulnerabilities. But software represents only one of the three ways to be compromised, the other two being weak configurations and people. Unfortunately, he said, the latter two are far more dangerous risks than the big bad software security flaw of the week.

"While we need to find and patch vulnerabilities, we also must understand an organization is only as strong as its weakest link. More attention needs to be paid in mitigating the other two ways beyond software," Corman said.

#### **Dirty Secret 6: Compliance threatens security**

Compliance with such laws and industry standards as [Sarbanes-Oxley](#) and [PCI DSS](#) drives companies to spend far more on security than they might otherwise. Security vendors have obviously seized upon this fact, offering products that do everything from offer PCI compliance out of the box to ultimate cure-alls for healthcare entities coping with the demands of [HIPAA](#). Of course, this too leads to companies buying security tools that fail to properly address the particular risks they face.

#### **Dirty Secret 7: Vendor blind spots allowed for Storm**

The Storm botnet, as an archetype, is being copied and improved. The Storm [era of botnets is alive and well](#), nearly two years from when it first appeared, Corman said. How is this possible? He answered:

- 1.) Botnets thrive in the consumer world where there is little money for innovation, a fact Storm and its controllers know. They are making money off of everything from spam to pump-and-dump stock scams.
- 2.) They eat AV for breakfast. A lot of the techniques and innovations used by Storm are not new; they are just being leveraged artfully against the blind spots of AV certifications and AV vendors.
- 3.) Malcode does not need vulnerabilities. Most of the Storm recruitment drives have leveraged social engineering and play off of a holiday or sporting event.

#### **Dirty Secret 8: Security has grown well past "do it yourself"**

Technology without strategy is chaos, Corman said. The sheer volume of security products and the rate of change has super-saturated most organizations and exceeded their ability to keep up.

"Organizations realize only a fraction of the capabilities of their existing investments. Furthermore, the cost of the product is often a fraction of the cost of ownership," he said. "There was a time when you could do it yourself."

The vendor community must therefore stop trying to convince companies that they can buy a product, set it and forget it.

