

# Security Trends Report

06/09

## Most claims dismissed in Hannaford data breach suit

Without damages, there's no case, judge rules

**By Jaikumar Vijayan**

May 13, 2009 04:27 PM ET

Computerworld - All but one of the legal claims filed against Hannaford Bros. -- the Maine-based retailer that [suffered a security breach](#) exposing some four million credit and debit cards -- has been dismissed.

U.S. District Court Judge Brock Hornby threw out the [civil claims against the grocer](#) for its alleged failure to protect card holder data and to notify customers of the breach in a timely fashion. In dismissing the claims, Hornby ruled that without any actual and substantial loss of money or property, consumers could not seek damages.

The only complaint he allowed to stand was from a woman who said she had not been reimbursed by her bank for fraudulent charges on her bank account following the Hannaford breach.

In a 39-page opinion, Hornby wrote that consumers with no fraudulent charges posted to their accounts could not seek damages under Maine law; neither could those who might have had fraudulent charges on their accounts that were later reversed.

The breach at Scarborough, Maine-based Hannaford affected customers at the company's supermarkets in New England and New York, at its Sweetbay stores in Florida and at some independently owned retail stores in the Northeast that carry Hannaford products. The intrusion began in late 2007 but was not discovered until March 2008 when it was publicly disclosed.

The company was hit with class-action lawsuits from multiple states that were consolidated into one suit last summer. The complaints included breach of implied contract, breach of implied warranty, negligence and violation of Maine's Unfair Trade Practices Act.

Hornby said three of the claims against Hannaford were valid under current Maine law. When a person uses a debit or a credit card in a grocery transaction, Hannaford should use reasonable care in protecting the card data, he wrote in the decision. Similarly, Hannaford's apparent delay in disclosing the data breach constituted an unfair trade practice under Maine law, he said.

"A jury could find that, if Hannaford had disclosed the security breach immediately upon learning of it from Visa, customers would not have purchased groceries at its stores with plastic," till the problem was fixed, he said.

Peter Murray, lead counsel for the plaintiffs and a partner at Murray, Plumb & Murray, in Portland, Maine, said no decision has been made on how to proceed. One option would be to pursue the lawsuit on behalf of individuals whose fraudulent charges may not have been reversed he said. Another would be to appeal the decision.

From a legal standpoint, it shouldn't matter whether the fraudulent charges were reversed, or whether it cost money for someone to reinstate previously authorized credit or account numbers, Murray said. "We believe that they have all suffered actual damage," he said. "We don't believe there is any legal distinction between the ways fraudulent charges impacted the consumer."

The Hannaford opinion is similar to several others involving data breaches in recent years. In August 2007, the U.S. Court of Appeals for the Seventh Circuit threw out a proposed class-action lawsuit against Evansville, Ind.-based Old National Bancorp (ONB) involving a 2005 data-breach incident.

In June 2007, a U.S. District Court judge in Ohio dismissed class-action claims against Litton Loan Servicing LP over a breach involving personal data. In that case, the judge said that without actual identity theft occurring, the

plaintiffs suffered only anticipated injury and therefore did not need to be compensated. In 2005, a federal judge threw out a lawsuit against TriWest Healthcare Alliance in Phoenix saying it was unclear whether any of the 500,000 records that were stolen had actually been accessed or used by thieves.

## Heartland breach costs at \$12.6M - and counting

Biggest portion of expenses has been a MasterCard fine

By Jaikumar Vijayan

May 11, 2009 12:00 PM ET

Computerworld - In an indication of how expensive the [breach at Heartland Payment Systems Inc.](#) could turn out to be, the payment processor last week said it has already spent or set aside more than \$12.6 million to cover intrusion-related costs.

Of that amount, about \$6 million is a fine imposed on the company by MasterCard, which Heartland is disputing.

In addition to the direct costs, the intrusion also hurt Heartland's first quarter revenues and its ability to pursue new customers, CEO Robert Carr said in an earnings release.

"With the first quarter behind us, we believe we are effectively managing the disruption to operations from the processing system intrusion and increasingly freeing additional sales resources to focus on our growth initiatives," Carr said in the statement.

Heartland, based in Princeton, N.J., is one of the largest payment-processing companies in the country with about 250,000 customers. In January, the company announced that intruders had broken into its systems last year and potentially compromised card data belonging to an unknown number of people. The intrusion is first believed to have occurred last May, though it remained undiscovered until January, even though credit card companies had warned Heartland about suspicious activity relating to transactions it had processed. The breach is believed to be one of the [largest involving credit cards](#), with some saying as many as 100 million cards may have been compromised.

The intrusion resulted in [several lawsuits against Heartland](#) by consumers as well as by banks and credit unions seeking to recover breach notification and card reissuing costs. It also led to Visa USA's [temporarily delisting Heartland from its approved list of service providers](#) that are compliant with a credit card industry security standard known as the Payment Card Industry Data Security Standard (PCI DSS). Heartland [recently got back](#) on to the approved list after passing a fresh PCI security audit.

In last week's earnings statement, Carr said Heartland would fight the fine imposed by MasterCard, which claimed that Heartland failed to respond appropriately after it was notified last year that it might have suffered a breach.

"We believe we took immediate and extraordinary actions to address the intrusion" and in working with the credit card companies in investigating the breach, Carr said. "(S)o we will vigorously contest any effort to hold us liable for the MasterCard fine," he said.

The amount that Heartland says it has spent or set aside for the breach so far "seems reasonable based on what they have publicly talked about," said Avivah Litan, an analyst with Stamford, Conn.-based Gartner Inc. But "the case still remains shrouded in too much mystery to know for certain what other potential damages will add up to," she said.

Unlike the January 2007 data compromise involving Massachusetts retailer [TJX Companies Inc.](#) "for some reason, the banking and card industry has been much quieter about this case in public," Litan said. I suspect it's because this is a top 10 U.S. processor and damage to Heartland, especially in a soft economy, could boomerang on the banks," she added.

The TJX compromise, which at the time was believed to be the largest involving credit and debit cards, resulted in the company having to pay a staggering [\\$150 million in breach costs](#). The number, which one Forrester analyst predicted could reach \$1 billion in direct and indirect costs, included a [\\$41 million settlement](#) with various banks that had sued the retailer.

## 5 Steps for Achieving Effective Mobile Security Governance

***How do you keep mobile security intact as devices proliferate? Consultant Robert Zhang breaks down the keys to success.***

***By Robert Zhang, GlassHouse Technologies***

May 13, 2009 — CSO

Advanced mobile devices—iPhone, BlackBerry and other handhelds—have created a growing wireless mobility environment for business, personal communication and entertainment. However, their growing use has also led to a faster increase in the depth and breadth of mobile security threats. Using a mobile device to access corporate information systems can potentially create a hole to corporate security if not protected and used properly. In a recent report from CSI, the theft or loss of corporate proprietary and customer information by mobile devices is nearly half of all sources. [Data breaches](#) are real to nearly every organization of virtually any size, from the big multinational corporation to the small to medium business, including device loss, theft, misuse, and unauthorized access to corporate network and data disclosure.

Enjoying many advantages in productivity, efficiency and flexibility, many current security efforts in organizations may lag behind exposures and risks. Organizations are either not fully aware of existing security issues facing the organization or simply treating these issues as a sole IT task. Very likely, such issues often remind IT managers to look into a number of technologies or software tools, such as firewall, [antivirus software](#), file encryption, etc. Not surprisingly, this often leads to an insufficient or failed effort. Merely focusing on technologies cannot conquer the organization's weaknesses in employees' behavior, and inherent gaps in policy and management processes.

Rapid development of mobile technologies and applications has increasingly changed the way organizations do business, as well as their risk management environment. To effectively minimize an organization's security risks requires a corporate wide effort in security strategy, policy development, employee training and revised IT infrastructure. Here are five steps of how to achieve effective mobile security governance:

### **Knowing Your Mobile Environment Risks**

Using mobile devices to get a job done anywhere as you move is a great benefit to many organizations. But the reality is that organizations at the same time also face a variety of unprecedented exposures and risks. These risks are a result of potential exploitations of weaknesses in technology, organization and its employees. Each year, millions of mobile devices are lost, stolen or discarded with personal information still in device memory. Loss of a mobile device that contains personal identity and network access credentials opens an organization for unauthorized network access and intrusion. Mobile data disclosure of business confidential information and personal records puts an organization at high risk of legal and regulatory compliance.

To develop an effective mobile security strategy, it is essential to understand an organization's mobile security risk profile. The fundamental questions include:

- What are the corporate mobile data assets that require protection?
- What, how and where the corporate data systems are accessed by mobile employees?
- How mobile devices are being used, protected and managed?
- Do employees know the procedures in responding to an incident?

To fully determine an organization's mobile security posture, a comprehensive security assessment against an organization's specific business environment is needed.

### **Developing an Effective Mobile Security Policy**

Lack of an effective mobile security policy is a fundamental root cause for many failed security efforts. The policy must be risk-based, covering all identified risks on mobile devices, both organization-issued and individually owned, and all user groups, including regular employees and temporary contractors.

The policy development process should determine which applications are to be made available to which mobile user group and on what types of devices. Typical mobile applications may include email, sales force automation, field service applications, dispatching, extended CRM, etc. These applications can drive productivity and revenue growth if deployed and managed securely.

An effective security policy needs to clearly translate regulatory compliance requirements into organization's risk management processes and procedures to protect data from loss or compromise. It also needs to speak clearly on user's responsibility for device configuration, its usage, data backup and protection. The information stored on a mobile device should be limited to what is required while on the move.

In addition, the policies must be enforceable via active IT monitoring and software tools. Organizations should regularly review the policies to take into account of any new security threats associated with business environment changes.

### **Ensuring Employees' Responsibility and Awareness**

The employee is a great factor for both good and bad in mobile security. In a recent CSO survey, 28% of all mobile users use their mobile devices to access the Internet, and 86% of them admitted to having no mobile security. A careless or security-unconscious user can easily put an organization's confidential information at risk.

Lack of mobile user training and awareness is a major factor that contributes to many user errors and incidents. A less-trained user may not even know a procedure to handle security. In some cases, a mobile user may simply bypass any required configuration procedures in order to get a job done.

Employee education and awareness should become a valuable corporate culture. A well trained employee can help an organization to greatly minimize mobile security risks. It is critical that all security policies should get buy-in from lines of business leadership, end users and support team across the organization.

Organizations should put employees in a driver seat for an effective security governance effort. They can become a most critical layer of security defense in any risk mitigation strategy.

## **Establishing a Baseline Security Configuration**

As the use of mobile technologies in business increases, more and more critical business and sensitive personal information is being collected, processed and transmitted over shared wireless networks. Mobile devices need to be configured adequately to protect the device itself and data on it from unauthorized use, data disclosure and malicious attacks.

During a planning phase of mobile device deployment, all devices should be considered to meet a baseline requirement in terms of corporate security policy. A baseline security configuration may include:

- Password protection at power-on
- File or directory encryption
- VPN for email and internal network access
- On-device firewall
- AV software
- Latest security patches

Enforcing the baseline security configuration for all devices can help an organization to establish a bottom-line of defense from each device. Similar to an Internet facing device hardening, on-device resources, wireless interfaces, e.g. WiFi, Bluetooth, RFID, wireless printer, and application functions should be minimized to reduce the likelihood of wireless attacks.

## **Building a Mobile Aware IT infrastructure**

Organizations may have well defined IT tools in place to manage enterprise systems (e.g., servers, networking and storage). As advanced mobile devices become increasingly used in business applications, their roles have been quickly shifting from email access to business-oriented transactions with back-end database systems (e.g. ERP, CRM and SFA). In the meantime, the growing business mobility is taking traditional IT boundary outside an organization's perimeter.

Organizations need to [implement strong authentication](#) and user role-based data access and distribution. Strong password enforcement, including two-factor authentication (e.g. software token) for a particular user group for additional security, should be performed. Existing network-based segregation or zoning should be revised to be data centric and extended to mobile users and devices.

To avoid increased integration cost, and later challenges in software support and upgrade, organizations should plan a centralized device management solution at the time of device deployment, ideally to be directly integrated with existing IT systems for network, application, server and device. A number of advanced solutions exist today that can support multi-platforms on a centralized enterprise console. IT managers can achieve proactive controls over device usage, configuration setting, software update and security patching. In particular, remote password reset, device lock and wipe are necessary features in many cases. Such solutions should be deployed with little or no user involvement, easy integration with existing directory structure and good scalability for a large number of users with diversified devices and on different wireless networks.

## **Conclusion**

Increased mobility has led to some incredible advances for organizations that can now conduct business

anywhere and at any time. However, as we have explored this increase in mobility is coupled with rising security threats that could transform these benefits into a catastrophic security issue. Taking the proper steps and putting into place a risk control process to prevent these occurrences can go a long way. But it is also important to remember that it doesn't end with the organization. The business AND the employees both need to do their part to ensure that best practices are followed and education is provided to increase security precautions. If everyone in the organization takes the responsibility to manage this task then an organization will achieve its goals in effective mobile security governance.

## **Agencies still fail to take steps to secure information systems**

(Govt. Exec, 5/5/09)

Computer systems and networks at nearly all major federal agencies are vulnerable to cyberattacks, a panel of government oversight officials and industry security professionals told a House subcommittee recently. Agencies need to implement comprehensive security programs to better protect sensitive information, they said. Despite growing concern about cyber threats and an increasing number of reported breaches, agencies fail to take the potential for widespread attacks on systems and networks seriously enough, James Lewis, director of the technology and public policy program at the Center for Strategic and International Studies, told the House Oversight and Government Reform Subcommittee on Government Management, Organization and Procurement.

According to the Government Accountability Office, weaknesses in security controls to detect, limit or prevent access to computer systems were detected at 23 of 24 major agencies in fiscal 2008. Agencies did not consistently identify and authenticate users; ensure that access was necessary and appropriate; apply encryption to protect sensitive data; or log, audit and monitor security-related events, said Gregory Wilshusen, director of information security issues at GAO.

## **Most Enterprises Expect To Get Hacked This Year**

(Dark Reading, 5/5/09)

Call it realism, or call it pessimism, but most organizations today are resigned to getting hacked. In fact, a full 94 percent expect to suffer a successful breach in the next 12 months, according to a new study on ethical hacking released by British Telecom (BT) The twist: Those who conduct network penetration tests think their chances of getting hacked are less likely than those who don't. Those who pen test estimated their chances of a breach at around 26 percent, while those who don't thought they had a 38 percent chance, according to BT's new 2009 Ethical Hacking study, which polled more than 200 IT professionals worldwide from mid-February through the end of March.

Around 60 percent of organizations have budgeted for pen testing, while around 38 percent have not, the study found. Nearly 70 percent allocate 1 to 5 percent of their security budgets for penetration testing, 17 percent allocated 6 to 10 percent, and 2 percent set aside 20 percent. In BT's previous ethical hacking survey, in 2007, nearly half of all IT pros said their organizations had only a 1 to 10 percent chance of getting hacked. But that number dropped to about 40 percent in this year's study.

## Can Social Networking Be Secure at Work?

*A new report revealed that hackers are increasingly targeting social networking services like Twitter and Facebook. Many employees who log on during the day at work might be causing information security risks at their companies. But banning the technologies would be short-sighted.*

---

By C.G. Lynch

That's the contention of a **recent report measuring Web 2.0-targeted hacks** that occurred in the first quarter of this year and was conducted by the **Secure Enterprise 2.0 Forum**, an industry group aimed at enabling the safe use of social media in the workplace.

Increasingly, hackers have turned their attentions away from e-mail, in part due to the fact people spend more of their time communicating with friends, family and colleagues over mediums like Facebook and Twitter. In addition, the e-mail environment has reached a level of maturity that makes the new frontier of social networks more attractive to hackers and spammers, says David Lavenda, a vice president at **WorkLightt**, a vendor that sponsored the study.

"E-mail is in a steady state," Lavenda says. "It's an electronic warfare game with spammers, filters and security tools, and it's reached some sort of status quo. With the new [social] tools, as people come online and get more involved with them, there is an opportunity to cause harm."

The list of security hacks on Web 2.0 and social networking sites were impressive, the report found. Nearly one-fifth were caused by authentication hacking (where someone is able to gather user names and passwords). Others included database hacking (21 percent), content spoofing (11 percent) and cross site scripting (XSS), an incident where malicious code runs on a webpage and eventually can enable phishing attacks.

The consequences of these types of hacks can be incredibly harmful. According to the report, nearly 30 percent lead to the leakage of sensitive information. Around 13 percent resulted in actual monetary loss, while more than 10 percent installed malware on computers or their corresponding networks.

The report will likely fuel the resolve of **CIOs and heads of technology who have banned social networks in the workplace**. By most measures, **nearly half of employers have gone that route** out of concerns about security and productivity.

Lavenda's company, WorkLight, has a vested interest in the study: It **provides enterprises with a server that allows them to move company information over consumer portals like Facebook and iGoogle** without it living on the servers of those sites.

The company takes a different approach to social networking than other Enterprise 2.0 vendors. ("**Enterprise 2.0**" is a marketing term used to describe how Web 2.0 technologies are mimicked for enterprise use.) While most focus on creating new enterprise software based on blog, wiki or social networking technology, WorkLight claims that it allows your employees to stay (safely) on their favorite consumer sites to connect with each other and customers and partners.

In the market, Lavenda says **CIOs have been more willing to let employees use the tools**, but have been at times reluctant, due to anecdotal stories about security breaches. The report, he says, will allow them to know what those threats are and make informed decisions about letting users access the sites.

"Forbid it or not, most **CIOs know users will find a way to use these tools anyway**," he says. "Even if they don't buy our product, this report moves the market forward because they know what the threats are and can see about addressing them. Once you know what the threats are, then you can go about mitigating them."

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

They worry about retaining workers, cybersecurity issues

**By Grant Gross**

April 30, 2009 12:00 PM ET

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."

# Web Attacks Routinely Hosted by Real Web Sites

## *Recent surge shows web's underbelly*

**By John E. Dunn, Techworld.com**

May 18, 2009 — IDG News Service —

The number of legitimate websites being hacked to host malware has hit startling highs in recent days, new figures from MessageLabs have revealed.

Data taken from the days between the 4th to 8th of May showed that 84.6 percent of websites blocked by the company for hosting malicious content were 'well-established' domains that have been around for a year or more.

During the same period, 10.2 percent of blocked domains were less than a year old and only 3.1 percent were less than a week old.

At first glance this, this runs counter to the assumption that malicious websites more commonly exist for only days or hours in some cases, the better to avoid detection and filtering. This is termed 'fast-fluxing', cycling websites through a maze of bogus sub-domains.

However, according to MessageLabs, the likely explanation is that a move to genuine domains means that the fast-fluxing has now migrated to use a different part of the domain tree.

"The bad guys will compromise the DNS and add sub-domains," said MessageLabs' Paul Wood. The recent figure represented a high mark, admitted Wood, but still represented a gathering storm.

"People need to be extra vigilant and understand that even sites they know and trust can be compromised through attacks such as SQL injection attacks, while businesses need to ensure they take the necessary precautions to block all the latest malicious sites," said Wood.

"With the ever advancing world of cyber crime, nothing can be taken at face value."

One consequence was that the days of reputation filtering services could be numbered as a primary defence. If the domains were fraudulent sub-domains exploiting legitimate domains, this would be difficult to defend against on such a scale.

## **7 Key Elements for Fed Cybersecurity**

### **No Cyber Czar; Harmonize Federal, Commercial Standards**

May 22, 2009 - Eric Chabrow, Managing Editor

The federal government doesn't need another czar to secure its information systems, but could use a federal chief information security officer. That's one of seven recommendations offered by IT advisor Gartner in a new report entitled [Toward a National Cybersecurity Strategy](#).

"Government policy that attempts to force top-down solutions onto an inherently peer-to-peer problem will always fail, as has been demonstrated by U.S. government cybersecurity initiatives during the last 15 years," the report's author and Gartner Vice President John Pescatore said in a statement accompanying the release of the report.

In the report, Gartner says the federal government has a major role to play in stimulating progress toward higher level of cybersecurity. Gartner analysts find that reducing vulnerabilities is the high-leverage area for strengthening information security; an operations-centric approach is needed, not another czar; and many agencies can be used as best-practice examples of enforcing current regulations.

Here are the advisory firm's seven recommendations on how best the federal government should shape its cybersecurity strategy:

1. **Stop Studying and Start Acting** - There have been plenty of existing efforts to define and measure the shortcomings of cybersecurity, so there is no need to reinvent the wheel.
2. **Harmonize Federal Security Standards with Commercial Equivalents** - Although there will always be a need for higher levels of security than commercial standards allow, harmonizing the base level will eliminate duplication and waste and enable the government to drive suppliers to higher levels of security more easily. Similar harmonization at the federal level of data privacy and disclosure rules is needed, as well.
3. **Use Purchasing Power to Drive Security to be Built-In** - Because the key to increasing cybersecurity lies in reducing vulnerabilities, all government software procurements should require application vulnerability testing as part of the acceptance criteria.
4. **Evaluate Existing Regulations and Rejuvenate Enforcement** - There are areas where federal legislation is needed to harmonize conflicting state laws, but the biggest bang for the federal buck will be in the actual enforcement of existing rules and regulations.
5. **Keep Offense and Defense Separate** - The primary goal of a cybersecurity strategy must be to make attacks ineffective through prevention rather than detect successful attacks by enabling surveillance. Combining the two functions will inevitably result in lower levels of security and possibly increased privacy violations.
6. **Reward Best Practices** - Most of the publicity tends to go toward the government agencies with low [Federal Information Security Management Act](#) scores in annual audits, and currently there seems to be little or no effort to spread best practices across agencies.
7. **Establish a Federal Chief Information Security Office, Not a Cybersecurity Czar** - The bottom line is that increasing the national cybersecurity is an operations issue. The problems are well-understood, solutions are known, and gaps have been identified. Organizations with high security in private industry and government almost invariably have a strong security office and a chief information security officer, and that should be the model that the U.S. government follows.

## IT Managers Feel Pressured to Relax Security Policies

(May 20, 2009) According to a recent survey of 1,300 IT managers, 86 percent said they were being pressured by company executives, marketing departments, and sales departments to relax web security policies to allow access to web-based platforms such as Google Apps. Nearly half of respondents said some employees bypass security policies to access services like Twitter and Facebook. More than half of the respondents noted that they lacked the means to detect embedded malicious code and prevent URL redirect attacks.

[http://searchsecurity.techtarget.com/news/article/0,289142,sid14\\_gcil356896,00.html#](http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gcil356896,00.html#)

[Editor's Note (Pescatore): The risks of allowing employees to access Facebook and Twitter and the like are not all that different from allowing web access in general. Providing web security services that do inbound filtering in addition to outbound blocking is absolutely required these day - and the ability to extend that protection via proxied services to protect laptop users is needed, as well. Using Google Apps for business data storage and collaboration is a whole 'nuther' issue - a lot of missing business-strength security and reliability capabilities still need to be added.

(Ranum): It's easy to make such decisions in a short-term context since "nothing bad has happened yet." Risk-taking is rewarded in the short-term and paid for in the long run in the form of massive expenses to "fix" the

problem later. Unfortunately, it's sometimes impossible to fix the problems later and we just grit our teeth and pay through the nose. That's computer security in a nutshell.  
(Paller) People do a lot of risky things, such as driving cars, because the convenience and value are worth the risk. The convenience and value of cloud computing are worth the risk - but the equation becomes MUCH better if we take John Pescatore's approach and bake much stronger controls in, to lower that risk to more acceptable levels.]

## Are Your "Secret Questions" Too Easily Answered?

Research finds that the answers to secret questions used to retrieve forgotten passwords are easily guessed.

By Robert Lemos

Brian Green's experience with not-so-secret questions began when he logged on to his World of Warcraft account in March of this year and found all of his characters in their underwear. Someone had stolen the account and sold off all of his virtual equipment.

"My first thought was that I might have a keylogger on my computer," Green wrote in a description of the event. Yet his own research into the incident--and the attacker's ability to change his account passwords multiple times--led Green, who is himself a game designer, to a different conclusion: "My 'secret question' has an all-too-common answer . . . This wasn't something I considered when I filled it out way back when."

The incident bares similarities to the high-profile case involving Alaska governor and former vice-presidential candidate Sarah Palin. In September 2008, hackers used the name of the location where Palin and her husband met to gain access to her Yahoo e-mail account via the "secret question" password-recovery mechanism.

Palin and Green are not alone. In research to be presented at the [IEEE Symposium on Security and Privacy](#) this week, researchers from Microsoft and Carnegie Mellon University plan to show that the secret questions used to secure the password-reset functions of a variety of websites are woefully insecure. In a study involving 130 people, the researchers found that 28 percent of the people who knew and were trusted by the study's participants could guess the correct answers to the participant's secret questions. Even people not trusted by the participant still had a 17 percent chance of guessing the correct answer to a secret question.

"Secret questions alone are not as secure as we would like our backup authentication to be," says Stuart Schechter, a researcher with software giant Microsoft and one of the authors of the paper. "Nor are they reliable enough that their use alone is sufficient to ensure users can recover their accounts when they forget their passwords."

The least-secure questions are simple ones whose answers can be guessed with no existing knowledge of the subject, the researchers say. For example, the answers to the questions "What is your favorite town?" and "What is your favorite sports team?" were relatively easy for participants to guess. All told, 30 percent and 57 percent of the correct answers, respectively, appeared in the top-five list of guesses.

But answers that require only a little personal knowledge to guess should also be considered unsafe, the researchers warn. Of people that participants would not trust with their password, 45 percent could still answer a question about where they were born, and 40 percent could correctly give their pet's name, the researchers found.

Backup-authentication schemes should have two important characteristics, Schechter says. They should be reliable, allowing a legitimate user to regain access to his or her account, and they should be secure, preventing unauthorized users from gaining access.

The study found that secret questions fall short on both accounts. Even for the most memorable questions--Yahoo's, as it turned out--the participants forgot 16 percent of the answers within three to six months. Overall, one out of every five people forgot all of the answers to their secret questions, the researchers found.

"People tend to underestimate the likelihood of their forgetting some clever technique or glib answer," Schechter says.

For most of a decade, security expert Bruce Schneier has criticized secret questions for their vulnerability to attack. In 2005, Schneier wrote, "I like to think that if I forget my password, it should be really hard to gain access to my account. I want it to be so hard that an attacker can't possibly do it."

Yet companies focused on reducing customer-service costs have introduced a back door into people's accounts that is easier to circumvent than attempting to guess the password, he says. "The weird security thing that is being done is that there is a backup system to reset your password that is less secure than the system that it's intended to support," Schneier says.

Schechter agrees that researchers will have to find a completely different mechanism for backup authentication--secret questions just don't cut it. "We would eventually like to see these questions go away," he says. "Unfortunately, since we didn't find many questions that were conclusively good, it's hard to recommend simply changing questions."

Schechter recommends not choosing questions that may have common answers. Schneier goes farther and says that he frequently just types in a random answer; if he needs to retrieve a password, he says, he will call the company.

Green, whose secret question asked the name of his high school, plans to use more secure e-mail in the future. And that may mean forgoing password retrieval. "Being able to reset my password on the site is nifty if I forget my password, but it sucks if someone else manages to figure out how to do it without my permission," he says.

## **Report: Spammers Work by US Clocks and Target Facebook, Twitter**

### ***Research from Symantec finds spammers, like many Americans, work from 9 to 5 and now favor sites like Twitter and Facebook for dirty tricks***

By [Joan Goodchild](#), Senior Editor

May 27, 2009 — [CSO](#) —

While many working Americans are heading into the office and starting their day, spammers are busy, too, readying for their next onslaught of junk messages. According to a new report from Symantec, spammers favor the same work schedule as the typical American office worker.

The research, conducted by Symantec's MessageLabs, indicates that spammers are most active during the US working day for a variety of reasons, but could be because most are either based in the US, or find the workday a good time for potential success, said Paul Wood, MessageLabs Intelligence senior analyst.

"Like any direct-marketing agency, they have direct times when they will want to send their mail shots," said Wood. "It's usually in the mornings, when people are more receptive and have not yet gotten into their work cycle, before the inbox fills up."

If you are located in the US, spam activity peaks at between 9 □ 10 a.m. local time, and trails off to much lower levels overnight, according to the research. The report also said Europeans are likely to receive a steady stream of spam throughout their day, while users in the Asia-Pacific region are likely to start their day with an inbox already full of spam, with only small amounts trickling in after this point until the evening.

The incidence of spam on corporate networks has increased around 5 percent compared to last month's MessageLabs analysis. Spam accounts for more than 90 percent of all email messages, according to the report. One in 317.8 emails in May contained malware and one in 404.7 emails comprised a phishing attack. More time spent on web mail and social networks is aiding in the increase, according to the report

"Active profiles on social networks are goldmines for spammers to lure unsuspecting users," the report states. "All spammers use is a subject line and a valid hyperlink to active profiles on one of a number of major social

networking sites. These emails originate from legitimate addresses on some of the main webmail providers making them harder to catch by regular anti-spam filters."

Earlier this month many Facebook users were targeted in a phishing attack and Twitter has also been hacked by spammers recently.

The report also finds legitimate, well-known sites such as Facebook, are just as dangerous, perhaps even riskier, when it comes to malware. Wood said a common assumption is that most web-based malware resides on less reputable websites, such as adult content sites. But MessageLabs analysis debunks this and finds cybercriminals appear to be more likely to hide malicious content on older domains that have been well-established. The report states 84.6 percent of website domains blocked for hosting malicious content are well-established domains that are over a year old.

"When you look at a lot of the domains that are being used to host the bad stuff, it's interesting to find they are well-known domains, not necessarily ones that have been compromised through an injection attack," said Wood. "They are domains that enable you to generate your own content, the Web 2.0 environment."

## Committee Calls for National Cyber Security Coordination Center

(May 22, 2009) The National Security Telecommunications Advisory Committee has approved a proposal calling for a national cyber security coordination center.

Both the public and the private sectors would be represented at the center, which would provide 24-hour monitoring to allow for real-time warnings about cyber attack that threaten government and critical infrastructure networks.

[http://www.nextgov.com/nextgov/ng\\_20090522\\_5667.php](http://www.nextgov.com/nextgov/ng_20090522_5667.php)

<http://www.ncs.gov/nstac/nstac.html>

## One In Five Teenagers Claim to Have Used Hacking Tools

(15th May 2009) A recent survey of 4,000 teenagers between the ages of 15 to 18 years of age states that 17% of those surveyed know how to find hacking tools online with one third of that group admitting that they have used the tools. The survey also reveals that 67% of the teenagers surveyed admitted to trying on at least one occasion to hacking into a friend's email or social networking account.

<http://www.scmagazineuk.com/One-in-five-teenagers-can-find-hacking-tools-online/article/136977/>

<http://www.techworld.com/security/news/index.cfm?newsID=115913>

## CIS issues free benchmark on iPhone security

Set of recommendations is designed to reduce attacks, help in erasing data

**By Matt Hamblen**

May 27, 2009 02:04 PM ET

Computerworld - The nonprofit Center for Internet Security today released what it termed the industry's only consensus security benchmark for the iPhone, which is aimed at helping IT managers and users reduce the risk of data stored on the device from being compromised.

The [benchmark is free](#) with a required registration at the CIS Web site.

The document takes users through more than 20 simple recommendations for system settings, Safari settings and iPhone Configuration Utility settings, a spokeswoman said. Using the recommendations is designed to help reduce the the chance of a remote attack, with instructions on securely erasing data and setting up strong passwords.

A separate benchmark for multi-function device security provides configuration and deployment guidance for business printers, copiers, scanners and fax machines.

The iPhone benchmark applies to iPhone OS version 2.2.1 and the iPhone Configuration Utility version 1.1.043, CIS said.

Blake Frantz, chief technology officer at CIS, said the iPhone presents "security challenges" for enterprises. Some large businesses, such as Kraft Foods and Oracle Corp., have adopted the iPhone for workers on a large scale, although there have been some holdouts in the financial sector, including Bank of America, [over security concerns](#).

Over the past year, CIS has had more than 1 million downloads of its benchmarks, which it develops according to a wide range of standards and with input from 150 members in corporations, government, universities and security organizations, the CIS Web site said.

## **The President's 10-Point Cybersecurity Action Plan**

### **Obama to Name IT Security Adviser**

May 29, 2009 - Eric Chabrow, Managing Editor

President Barack Obama on Friday presented a 10-point near-term action plan aimed at securing the federal government's and the nation's critical IT infrastructure.

"This new approach starts at the top, with this commitment from me: From now on, our digital infrastructure - the networks and computers we depend on every day - will be treated as they should be: as a strategic national asset," Obama said. "Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage."

Though he said he would personally pick a cybersecurity adviser, no choice has been made. That person, though, will not report directly to the president, which could disappoint those on Capitol Hill seeking a higher ranking adviser.

Still, initial reaction from Congress was positive, even among those who had hoped for a more senior-level cybersecurity adviser.

"This White House report is a good starting point for the work that lies ahead and incorporates many of the CSIS (Center for Strategic and International Studies) recommendations, including increased coordination between the private and public sectors and within various government agencies," Rep. Jim Langevin, the Rhode Island Democrat who co-chairs the House Cyber Security Caucus as well as the CSIS's Commission of Cybersecurity for the 44th Presidency said in a statement. "I am especially pleased to hear President Obama refer to our cyber infrastructure as a strategic national asset a top national security priority."

Karen Evans, who served as the de facto federal chief information officer for more than five years until this past January, said she was excited by Obama's remarks, which recognize the importance of cybersecurity to the entire nation. What impressed her, she wrote in an e-mail message, was the coordination of IT security policy between the new cybersecurity director and the federal CIO and chief technology officer. Plus, she said, there's accountability. "The difference I see now is there is one person the president will hold accountable to address this issue to ensure all aspects are being addressed throughout the country while also addressing the economic impact of any future policy direction," she said.

The president assured Americans that the government will not monitor private-sector networks or Internet traffic. "We will preserve and protect the personal privacy and civil liberties that we cherish as Americans," he said. "Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be - open and free."

In his White House speech, Obama said he plans to:

- 1.** Appoint a cybersecurity policy official responsible for coordinating the nation's cybersecurity policies and activities; establish a strong National Security Council directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the National Economic Council, to coordinate interagency development of cybersecurity-related strategy and policy.
- 2.** Sign off on an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of Comprehensive National Cybersecurity Initiative activities and, where appropriate, build on its successes.
- 3.** Designate cybersecurity as one of his key management priorities and establish performance metrics.
- 4.** Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
- 5.** Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the federal government.
- 6.** Initiate a national public awareness and education campaign to promote cybersecurity.
- 7.** Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
- 8.** Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement.
- 9.** In collaboration with other Executive Office of the President entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
- 10.** Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the nation.

"The task I have described will not be easy," Obama said. "Some 1.5 billion people around the world are already online, and more are logging on every day. Groups and governments are sharpening their cyber capabilities. Protecting our prosperity and security in this globalized world is going to be a long, difficult struggle demanding patience and persistence over many years.

"But we need to remember: We're only at the beginning. The epochs of history are long - the Agricultural Revolution; the Industrial Revolution. By comparison, our Information Age is still in its infancy. We're only at Web 2.0. Now our virtual world is going viral. And we've only just begun to explore the next generation of technologies that will transform our lives in ways we can't even begin to imagine."

## Bank Sues Company That Certified CardSystems Solutions Before Breach

(May 26 & 27, 2009) Merrick Bank has filed a lawsuit against Savvis, alleging negligence because the company certified CardSystems Solutions as compliant with Visa and MasterCard security requirements less than a year before the payment processor suffered a massive data security breach. Merrick claims that fraudulent transactions resulting from the breach cost it US \$16 million in payments to the credit card companies for using a non-compliant processor, payments to banks affected by the breach and legal fees. Attackers were able to steal information on 40 million credit card accounts because CardSystems stored unencrypted card data on its servers.

<http://www.finextra.com/fullstory.asp?id=20067>

<http://www.digitaltransactions.net/newsstory.cfm?newsid=2221>

[Editor's Note (Pescatore): Making this charge stick will require proving that the non-compliant condition existed at the time of the audit and should have been discovered with reasonable diligence. But it will be good to see some external attention focused on the PCI audit process.

(Schultz): The issue concerning whether an organization is (but probably more importantly, \*was\* at the time of a data security breach) PCI-DSS compliant is becoming increasingly complex. If a bank, merchant, or other organization has passed a PCI-DSS audit, but then a security breach involving credit card information occurs sometime later, the PCI Consortium has increasingly suddenly declared the organization to be non-compliant. As good as they are, PCI-DSS standards do not require anything near perfect data security, and no audit is 100 percent comprehensive. Residual risk will always be present as long as systems are connected to any network. If PCI-DSS auditors are going to become legally liable for future data security breaches, the cost to perform these audits will, unfortunately, most likely skyrocket out of control.

(Hoelzer): While the legal system is an important tool when it comes to forcing organizations to be responsible, this may mark a dangerous time for PCI. PCI/DSS isn't perfect but it's a pretty good start. If lawsuits continue to pile on, however, we could see energy start to build for the elimination of standards of this kind since they may appear to be leading toward greater liability rather than reduced liability.]

## Eighteen Percent of Computers at Interior Missing or Lost

(May 28, 2009) According to a report from the US Department of the Interior's inspector general (IG), the Department cannot account for the whereabouts of 18 percent of its computers. The vast majority of the missing computers, 450 out of a sample of 2,500, belonged to the Fish and Wildlife Service.

Just two of the department's eight bureaus have kept good records of their computer inventories, according to the report, and disposal procedures for machines from bureau to bureau. In addition, the majority of department's PCs are not encrypted.

<http://www.eweek.com/c/a/Security/Department-of-Interior-Computers-Missing-Report-Finds-443176/>

[Editor's Note (Skoudis): If you don't know where a computing asset is or whose control it is under, you cannot secure it. Building and maintaining an asset inventory is difficult work, to be sure, but it is vital. An effective inventory maps each system to an employee, a manager, and an asset owner. Let's learn a lesson from this story, and double check our own asset inventories to make sure they are being maintained.

(Northcutt): It's 8 P.M. do you know where your computers are? Critical security control 1, quick win 1: "QW: Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to the enterprise network. Both active tools that scan through network address ranges, and passive tools that identify hosts based on analyzing their traffic should be employed."

<http://www.sans.org/cag/control/1.php>]

## Group Calls for Overhaul of Privacy Regulations

**CongressDaily (05/27/09) ; Noyes, Andrew**

The National Institute of Standards and Technology's Information Security and Privacy Advisory Board has sent a report to Office of Management and Budget (OMB) director Peter Orszag that calls on Congress to update the 1974 Privacy Act and several provisions of the 2002 E-Government Act. According to the board, which is made up of technology experts from private industry and the academic world, both of these laws should be updated in order to bring privacy law and policy in line with the technological changes that have taken place during the last several years. Among the revisions the board called for were amendments that would improve federal privacy notices, clearly cover sources of commercial data, and update the definition of the term "system of records" so

that it includes relational and distributed systems based on government use of records instead of its possession of them. The board also called on the government to take on more of a leadership role on privacy issues and to hire a full-time chief privacy officer at OMB who would provide regular updates on Privacy Act guidance. Major agencies should also hire chief privacy officers, and a chief privacy officers council similar to the Chief Information Officers' Council should be created, the report said. Finally, the report called on OMB to issue privacy guidance for federal agencies' non-law enforcement use of location data and to work with the U.S. Computer Emergency Readiness Team to create interagency information on data loss across government agencies.

## **FISMA Efficacy Questioned**

**GovInfoSecurity.com (05/20/09) ; Chabrow, Eric**

Several government IT officials appeared before the House Committee on Oversight and Government Reform's Subcommittee on Government Management, Organization, and Procurement on May 19 to tell lawmakers that the Federal Information Security Management Act (FISMA) is not doing its job of protecting federal IT systems. Among those who testified at the hearing was federal CIO Vivek Kundra, who noted that the performance information collected under FISMA does not fully reflect the security posture of federal agencies. He added that the processes used to collect that information take time away from substantive analysis, and that the law has made the federal government more focused on compliance than outcomes. Kundra called for the adoption of metrics that would provide a glimpse into agencies' security postures and potential security vulnerabilities on an ongoing basis. Also testifying at the hearing was Gregory Wilshusen of the Government Accountability Office. He said that 23 of the 24 major federal agencies had weaknesses in the agency-wide information security programs FISMA requires them to adopt, which could be one of the underlying causes for information security weaknesses at federal agencies. Finally, Margaret Graves, the acting chief information officer of the Department of Homeland Security, said that while FISMA has helped strengthen her agency's IT security posture, the law is not enough to advance cybersecurity. Some lawmakers appear to be in agreement that more needs to be done to protect federal IT systems. The Senate is currently considering legislation that would replace FISMA by requiring continuing security monitoring of government IT systems.

## **Security Manager's Journal: At this point, the cloud remains too leaky**

For a security manager, even a test environment could be too vulnerable when it's located in the Web-accessible cloud.

**By Mathias Thurman**

June 1, 2009 12:01 AM ET

Computerworld - What great timing! I had no sooner returned from [the RSA Conference](#), where my focus was on [cloud computing](#), than I was invited to a meeting to discuss our [first venture into "the cloud."](#)

The IT department has decided to contract with an infrastructure-as-a-service provider to host a portion of our development environment. If this trial is successful, some of our production environment could be next. Having read up on the subject in white papers and attended seminars at RSA, I felt informed enough to ask the questions that needed to be answered before I could feel comfortable about an initiative that was going to open new portals to our network and our data.

And there's no question that this could expose us to new dangers.

Our plan is to move our SAP development environment to the cloud. Our developers typically test apps with our actual production data. It's not a problem when they put our financial data on a test server in our own data center. It's another matter entirely when the server is far away and out of our control. In this case, in fact, our hosted servers will actually be located at a hosting provider's data center, so there are two degrees of separation.

The plan is to configure several virtual Linux and Windows servers on a shared VMware ESX Server. The cloud vendor wants us to set up a VPN tunnel. I'm not thrilled that we won't control the VPN termination point, and it doesn't help that the termination point is a Linux server running open-source VPN software.

Compounding my concerns, the vendor wants us to use a shared key for VPN authentication between the devices. I have countered that plan by mandating the use of certificates to handle authentication. I have also established firewall rules that restrict the servers at the server farm from accessing our network.

## Making Things Easy

Next in my sights was the Web-based management application that our technicians must use. When you put this application side-by-side with our current data center access controls, the vulnerabilities of the Web app are enough to make a grown security manager cry.

Currently, a bad guy would have to know the physical location of our data center, obtain a badge to enter the building, procure yet another badge and somehow beat the biometric hand scan in order to enter the data center -- and then he'd have know exactly which racks contain the servers he's targeting. In contrast, the Web app asks only for a username and password, it's available via the Internet, and all customers use the same URL. The only thing a bad guy needs is something like a keystroke logger. And here's a clue to how much the vendor values security: It gives clients temporary passwords with no requirement to change them upon initial log-in, and it doesn't enforce the use of [complex passwords](#).

I had other questions as well, and the answers did not inspire confidence. How would we know if an unauthorized, rogue or disgruntled employee manipulated our environment? "Umm, well, uh, we haven't really thought about that, but our offering is strictly for development environments."

OK, then, how about encryption? "Since we cater to development environments, we advise customers not to use sensitive production data in the development environment." And do any customers really create data out of thin air, or do they just take what already exists from production?

The bottom line is that we have a long way to go before we establish a trust relationship between the cloud network and our company's network, and there is still quite a bit of room for improvement in cloud security.

## 5 Free Ways to Track Online Leaks of Information

By Brandon Gregg

June 1, 2009 01:38 PM ET

CSO - As you know, there is a wide range of threats online -- malware, [bots](#), phishing scams and more. While your security and IT department implement firewalls and virus protection programs to combat these threats, many companies are missing the most damaging threat to their business online: [Intellectual Property](#) posted online by their own employees, whether with or without malicious intent.

Unfortunately a lot of companies are stumbling across their own IP online by accident and well after it is too late. A best-case scenario for undoing the damage is that the data is quickly removed by the website and is never seen again. In the worst-case scenario, the information becomes a viral video on YouTube.

Although new brand protection companies like IPsec and Brand Protect have popped up and grown to fill a much-needed market, the following tools offer free and easy-to-customize Internet monitoring features that allow you to be seconds behind information leaks.

Monitter.com

Combine the word Monitor with the social networking tool Twitter and you have Monitter.com. This simple-to-use website allows you to customize Twitter searches by keyword and location and save your searches as RSS feeds to have the data emailed or texted to you instantly. Start off slow with searches for your company name or

a new product and monitor twitter for threats, disgruntle employees and internal leaks. You will be amazed to see how many employees actually post on Twitter about their own company or their boss. Limewire

As many of you know, Limewire is one of the most popular peer-2-peer file sharing programs on the internet. However, its poor design (which Congress is actually demanding they change) opens the world up to any documents, photos or files on your computer. During a quick install of the program, most users overlook the details and approve the program to share the entire contents of their My Documents folder. Most recently President Obama's [new military helicopter designs for Marine One were tracked to Iranian computers](#) after a defense contractor installed Limewire on his personal computer and shared his top-secret company documents to the world.

Simply download and install this program on your computer (make sure to disable all file sharing) and routinely search for your company's name. Documents with "Acme" in the metadata or title will flag and you can actually see the user's IP address and download the file.

Addictomatic.com

While some search tools overlap with data and can lead to information overload, addictomatic.com provides a quick and easy way to search for your company or keywords across a wide selection of sites including news, blogs, YouTube, and even popular photosharing site flickr. Countless unapproved videos and photos by employees can quickly be discovered.

Google

No search for data would be complete without Google. The company's proprietary collection of websites and vast arsenal of tools give it the fourth and fifth place on the list. The power behind Google's server farms full of processors, crawling the web for information, makes Google.com one of the first places to look for leaked information. However, unlike addictomatic, the information can easily be overwhelming without the right combination of search tricks.

Using a recipe of basic and advanced search features can greatly narrow the number of results returned and give you better data. Instead of searching for Acme Company, use "Acme Company" in quotations or narrow your results with more details like "Acme Company" "Confidential Handling" to find any leaked company documents with "confidential handling" in the metadata or headers. Check out Google advanced search or search for "Google Hack Lists" for more tricks like finding your company's [IP CCTV cameras](#) and password lists.

Google Alerts

Once you have narrowed your search and tested it out, use Google Alerts ([www.google.com/alerts](http://www.google.com/alerts)) to make Google work for you. In this example I have setup two searches in Google Alerts, the first is a simple search to specifically search Myspace users postings about ACME : "Acme Company" site:profile.myspace.com and a second more complex search looking for any Acme file on free file sharing websites: Acme (rapidshare. | megaupload. | sharebee. | mediafire. | slil. | sendspace. | turboupload. | speedshare. | depositfiles. | massmirror.com | ftp2share.com| zshare.net). To setup, make sure to search narrow or specific topics, Acme alone might provide too much invaluable data. After you have picked a good search, simply paste in your term(s), select Comprehensive, select how often Google should search (I use As-It-Happens), enter your email and soon you will be getting information sent directly to you.

## Thousands of Web sites stung by mass hacking attack

Hackers redirect unwitting victims to a Web site that tries to infect PCs with malicious software

**By Jeremy Kirk**

June 2, 2009 10:08 AM ET

IDG News Service - As many as 40,000 Web sites have been hacked to redirect unwitting victims to another Web site that tries to infect PCs with malicious software, according to security vendor Websense.

The affected sites have been hacked to host JavaScript code that directs people to a fake Google Analytics Web site, which provides data for Web site owners on a site's usage, then to another bad site, said Carl Leonard, threat research manager for Websense.

Those Web sites have likely been hacked via a SQL injection attack, in which improperly configured Web applications accept malicious data and get hacked, Leonard said.

Another possibility is that the FTP credentials for the sites have somehow been obtained by hackers, giving them access to the inner workings of the site. It appears the hackers are using automated tools to seek out vulnerable Web sites, Leonard said.

The latest campaign underscores the success hackers have at hosting dangerous code on poorly secured Web sites.

Once a user has been directed to the bogus Google analytics site, it redirects again to another malicious domain. That site tests to see if the PC has software vulnerabilities in either Microsoft Corp.'s Internet Explorer browser or Firefox that can be exploited in order to deliver malware, Leonard said.

If it doesn't find a problem there, it will launch a fake warning saying the computer is infected with malware and then try to get the user to willingly download a program that purports to be security software but is actually a Trojan downloader, Leonard said. The fake security programs are often called "scareware" and don't work as advertised.

As of last Friday, only four of 39 security software programs could detect that Trojan, although that's now likely changed as vendors such as Websense swap malware samples with other companies in order to improve overall Internet security.

It's not clear what the hackers are doing with the newly compromised PCs, although it's possible they can be configured to send spam, become part of a botnet or have data stolen from them.

The malicious domain serving up the malware is hosted in the Ukraine, the same region where notorious Russian Business Network (RBN) operated. RBN is a gang of cybercriminals involved in phishing campaigns and other malicious activity, Leonard said. That Web site appeared to be down as of Tuesday. The RBN is thought to be inactive now.

"Whether this is a part of that group or whether it's a copycat using some of the techniques that are similar to those used by the malware group in the past we are not quite certain yet," Leonard said. "It is very difficult to pinpoint the exact people behind this."

Since so many Web sites have been hacked to deliver the attack, it's nearly impossible to contact them all, Leonard said.

Websense said the latest attacks don't appear to be related to Gumblar, a malware campaign under way last month. Gumblar resulted in at least 3,000 Web sites getting infected with malicious code that scanned users' computers for vulnerabilities in Adobe Systems software.

Once on a PC, Gumblar steals FTP log-in credentials, using that information to help spread to other computers. It also commandeers a person's Web browser and replaces Google search results with other dangerous links.

## Hackers tweet, infect Twitter users with scareware

'Security nightmare' arrives; hackers use exploit kit to spread fake security software

**By Gregg Keizer**

June 1, 2009 02:07 PM ET

Computerworld - The latest attack to hit Twitter is a "security nightmare" and marks the first time hackers have taken to using the micro-blogging site for profit, a researcher said today.

Unlike earlier [cross-site scripting attacks](#) on Twitter, the latest wasn't a worm, said Roel Schouwenberg, a senior antivirus researcher with Moscow-based Kaspersky Labs. Instead, it's something even scarier: The first instance of hackers serving up "scareware," fake security software that, once installed, nags users with so many alerts that some fork over \$50 or more just to "register" the program and get rid of the warnings.

"This is just another scareware installer," Schouwenberg said, referring to the malware that's downloaded onto victimized PCs. "There's no worm component. But it's quite significant as it's the first time that Twitter's been used for a traditional type of attack."

Over the weekend, Twitter users began receiving tweets with the phrase "Best Video" and a link to a Russian domain. Although those who clicked on the link were directed to a site with a video, they were also served a malicious PDF document via an IFRAME on that site. The PDF, said Schouwenberg, contains a number of exploits, and tries each in turn. If it's able to compromise the computer using one of those exploits, the malware then installs phony security software.

The PDF appears to contain attack code from "LuckySploit," a relatively-new multi-strike hacker toolkit that uses malicious JavaScript, said Schouwenberg.

On Saturday, [Twitter warned users](#) of the tweets with the "Best Video" link, then later noted that it had [suspended compromised accounts](#), but would restore them shortly after they'd been scrubbed.

Twitter's not able to remove any malware installed by the attacks, of course, leaving that chore up to users.

Schouwenberg's sure that Twitter's talk of cleaning accounts was a smokescreen, as unlike attacks in April, this one wasn't a worm. "There was no self-replicating code in the binary," he said. Instead, Schouwenberg believes that the malicious tweets were sent from Twitter accounts whose log-on credentials had been hijacked previously by basic phishing-style scams.

"When I first saw this Saturday night, I thought of the Twitter phishing attack, which was quite high profile," said Schouwenberg. "Phishing always has a greater purpose ... so when all of a sudden you see a new 'worm' but there's no worm component [in the attack code], it's clear that this was based on compromised accounts, rather than self-replicating."

Schouwenberg also found the links in the malicious tweets on multiple Web forums, giving credence to his theory that hijacked accounts were used to launch the scareware attack.

Twitter users should expect to see more such attacks, Schouwenberg said. "The whole idea of Twitter is to click on links," he said. "It's a security nightmare."

## Spammers find new ways to flood corporate networks

By Robert McMillan

June 1, 2009 12:01 AM ET

Computerworld - Unsolicited e-mail accounted for 90.4% of all messages received on corporate networks during April, an increase of 5.1% from a month earlier, according to a report released May 26 by Symantec Corp.'s MessageLabs Intelligence unit.

The monthly MessageLabs report on threat trends also found that nearly 58% of all spam can be traced to [botnets](#).

Adam O'Donnell, a researcher at Cloudmark Inc., a provider of antispam tools, noted that in addition to using botnets, spammers in recent months have been experimenting with a new way to sneak unwanted e-mail past corporate filters.

Often, he said, a spammer will rent legitimate network services, often in an Eastern European country, and then blast a large amount of spam at the network of a specific ISP. The idea is to push as many messages as possible onto the network before any kind of filtering software detects the incident. O'Donnell estimates that hundreds of thousands of such messages are sent each day without detection.

Social networks are also becoming an increasingly important tool for spammers.

Security experts note that social-networking spam can't be filtered at the corporate firewall and appears to come from friends of the recipients.

## Web 2.0 Security: Things to Know about the Social Web

By Dan Hubbard

June 5, 2009 12:28 PM ET

CIO - Websense CTO Dan Hubbard outlines four ways companies can protect their information from threats and compromise on the social Web.

1) Most Web Posts on Blogs and Forums are Actually Unwanted Content (Spam and Malware) As more and more people interact with each other on sites allowing user-generated content, such as blogs, forums and chat rooms, spammers and cybercriminals have taken note and abuse this ability to spread spam, post links back to their wares and direct users to malicious sites. Websense research shows that 85 percent of all Web posts on blogs and forums are unwanted content - spam and malware - and five percent are actually malware, fraud and phishing attacks. An average active blog gets between 8,000 and 10,000 links posted per month; so users must be wary of clicking on links in these sites.

Additionally, just because a site is reputable, doesn't mean its safe. Blogs and message boards belonging to Sony Pictures, Digg, Google, YouTube and Washington State University have all hosted malicious comment spam recently, and [My.BarackObama.com](#) was infected with malicious comment spam.

2) The Top Search Results from Google are Safe, Right? [Search engine poisoning](#) is growing in popularity and used by cybercriminals to boost links to Web sites with malicious code or spam, up in the search rankings. Many users assume that the top results are "safe" but really they are directed to infected Web sites. For example in March, basketball fans who typed "March Madness" into their Google search bar and clicked on many of the top ranking links were actually led to Web sites infected with "rogue antivirus" software (see number 3).

3) You're Really NOT Infected; Be Careful Before You Download That In the past year Cybercriminals have increasingly used what's known as "rogue antivirus" to get information like credit card numbers and other private information from Web users. Typically, rogue antivirus authors use search engine poisoning to drive traffic to

sites they own or have infected (as noted above). Often they post links on blogs and forums that link back to a malicious site under their control. When a user visits these Web sites, a window pops up warning them that their computer has been infected with malware. The user is prompted to pay money and download an "antivirus" software program to clean their system. In reality, the attackers have tricked the user into disclosing their credit card information to pay for the fake software as well as successfully installed malware on the user's machine. One example is the well-publicized [Conficker worm](#) that infected millions of computers around the world. Some users with the Conficker worm observed a file downloaded onto their machine. Upon running the file, the user was asked to pay \$49.95 to remove the "detected threat."

The [Anti-Phishing Working Group](#) recently published some interesting statistics showing that the numbers of rogue antivirus programs rose 225 percent from July 2008 to December 2008, more than tripling the number of detected rogue programs from its July level.

Rogue antivirus attacks play on the fears of Web users and are a ploy for money, when in fact the computer user has not been infected, nor do they need to install an antivirus program.

4) Sadly, You Really Can't Trust Your Friends or Your Social Network As a tweet from the Websense Security Labs recently stated, "Web threats delivered via your personal Web 2.0 social network is the new black - do not automatically trust suspicious messages from friends." The social networking explosion has created [new ways of delivering threats](#). Web users are so accustomed to receiving tweets with shortened URLs, video links posted to their Facebook pages and email messages purportedly from the social networking sites themselves that most people don't even hesitate to click on a link because they trust the sender.

The unfortunate reality is that criminals are taking advantage of that trust to disseminate malware and links to infected Web sites. Websense Security Labs recently found examples of e-mails sent from what appeared to be Facebook, but were really from criminals that encouraged users to click on a link to a "video" that was actually a page infected with malware.