

# ESO - Security Trends Report

11/08

## Over half of U.K. firms have lost data

Two out of three survey respondents said negligence caused their data loss

By Leo King

October 10, 2008 (Computerworld UK) An astonishing 55% of British companies have lost data, according to a new report of 785 IT professionals in the U.K.

Conducted by the [Ponemon Institute LLC](#), the survey found that 49% of them have had over two breaches in the last two years.

Around two-thirds of respondents said negligence, including that of outsourcers, was responsible for data breaches, compared with only 10% who said hackers were a major cause. A third said insiders were a threat.

Many firms were unable to track data breaches and find the source of the problem. Some 44% said they were not confident they could even detect a breach in the first place, and over half take several weeks to notify any customers affected.

Only 3% were tracking changes made to data, such as when account details are updated, even though 91% said this was an important part of tackling the problem.

Six in 10 firms said networks were one place they saw as having a high risk of data breaches, and 51% said mobile devices were a threat. But it was not just technology that was at risk, as over half reported that paper files were a problem.

A worrying six in 10 have not assigned responsibility for detecting and responding to data breaches. But 25% said it was the job of the chief information officer.

Atul Bhovan, U.K. technology manager at [Compuware Corp.](#), which commissioned the survey, told Computerworld U.K.: "Businesses just don't have enough information for an effective root-cause analysis when there is a data breach."

"They need to identify who is doing what, and if there's a breach, how many customers are affected. It's not just a case of addressing who can access data, it's also about recording transactional screens to aid forensic investigation if any problems happen."

## Data loss reduced by training programs: KPMG

Posted On: Oct. 03, 2008

[Michael Bradford](#)

LONDON—The risk of losing data to human error or hackers is greatly reduced when workers are given regularly updated awareness and education training programs, a new report advises.

Internal controls are vital to stopping data loss, whether it is from a stolen laptop, a hacked system or other incidents, according to KPMG L.L.P. in its recently released report, "Data Loss Barometer."

KPMG researched publicly-disclosed incidents of data loss and found that educational organizations, governments and health care operations are victims of most of the incidents. There were 598 data loss incidents from January 2007 to June 2008, most occurring in the United Kingdom and United States, the report says. Twenty-five percent of those involved computer theft and another 13% were hacking incidents.

Half of the data loss incidents during the period were from internal sources, according to the report. Forty-four percent were from external sources and it was unclear where the remainder originated.

Educating staff can help mitigate the threat of data loss, KPMG says. "Risks of errors are greatly reduced by implementing appropriate and clearly defined procedures around the use and handling of data," the report states. "Staff need to understand what is expected of them with regularly implemented, tested and updated awareness, training and education programs."

## **Cybergang moles steal company data**

Dan Raywood  
October 02, 2008

Criminal gangs have been placing staff members in companies to operate as moles, an internet security expert said this week.

In a podcast interview, Peter Wood, member of the ISACA Conference Committee and founder of First Base Technologies, claimed that placing moles is common.

Wood said: "Some people in the banking community have quietly and anonymously said to me over the last year that they have found employees who have been placed in their company by criminal gangs and they have been operating as moles over that period."

Wood said companies often make the mistake of storing sensitive and confidential data in one place, which makes it very easy for criminals to act.

"I think there is a huge gulf between the technical controls that firms put in place and the human and (human relations) control and the physical premises control," he said. "There is little or no communication between the three areas and it's through those gaps that criminals can walk unchallenged."

Wood said a colleague walked unchallenged into an insurance company and was able to steal data as part of a security exercise. This could be overcome by training, he added.

"If people are given some baseline education as to how to look for criminal activity then they can be the greatest asset any organization could possibly deploy," he said.

## **Tough economic climate can heighten insider threat**

As companies downsize, they need to keep an eye out for disgruntled employees

**By Jaikumar Vijayan**

October 14, 2008 (Computerworld) With a faltering economy resulting in increased jobs cuts and corporate belt tightening, security analysts are warning companies to be especially vigilant about protecting their data and networks against disgruntled employees.

As it is, one of the [biggest threats](#) to corporate data and systems traditionally has come from insiders, who with their privileged access to data and systems, have the potential ability do more accidental or malicious damage than even the outside attacker.

That threat greatly increases at times when companies are laying off staff, cutting back on raises and bonuses, deferring promotions, consolidating operations and [outsourcing](#) work to save money.

"All of these increase risk for the company from an insider perspective," said Shelley Kirkpatrick, director of assessment services at Management Concepts, a Vienna, Va.-based management consultancy.

Tough economic times create uncertainty in the workplace, she said. Employees for instance, can be worried about losing jobs and promotions, concerned about financial liabilities, mortgages and rising energy costs.

"When there is uncertainty, it creates stress for employees. It makes the company more vulnerable" to threats, said Kirkpatrick, who was previously a behavioral threat assessment researcher at the Homeland Security Institute.

The threats can manifest themselves in a number of ways. Insiders with access to corporate information, such as customer data or corporate secrets, might want to steal or disclose it for financial gain or simply to get back at their companies. Those with technical-savvy might seek to sabotage corporate data and systems by planting malicious code and so-called logic bombs that are designed to delete data at a future date on critical systems.

The danger is not confined to such actions alone. Stressed, unhappy workers make easy targets for opportunistic rivals as well, Kirkpatrick said. "If I am a competitor looking for a good opportunity to get trade secrets out of my competition, I am going to go after the people who may be stressed emotionally," she said.

### **Examples of insider sabotage**

The damage that insiders with privileged access can do should not be underestimated as several incidents in the past show, analysts said. In July, for instance, a [disgruntled administrator](#) for the city of San Francisco locked access to a critical network by resetting administrative passwords to its switches and routers and then refusing to divulge them to officials [for days](#).

In a similar incident, a Unix systems administrator at [Medco Health Solutions Inc.](#) who was concerned about being laid off, planted a [logic bomb](#) on an internal system that, had it gone off, would have deleted data on 70 servers.

While both incidents involved technically savvy insiders, similar threats can come from non-IT staff as well. In November 2006, a scientist working at [DuPont](#) admitted to stealing corporate data valued at around \$400 million shortly before he left the company to work at a rival.

The key to being prepared for such threats is knowing what warning signs to look and how to [respond](#) to them, said Matt Doherty, a senior vice president at Hillard Heintze LLC, a Chicago-based security consultancy.

One example of a red flag might be an employee who suddenly starts working after hours, stays late for no obvious reason or keeps asking for overtime to make ends meet. Similarly, someone trying to get access to systems and information that they really have no need for could be another sign that something is amiss, he said. Or it could be an employee who prints out large volumes of data after hours, or e-mails it to himself.

As important as such markers are, it is equally important to know what's going on in terms of employee behavior and morale, Doherty said. Supervisors need to be trained to spot employees in distress or those who could pose a security problem in the future, he said. Companies also need to educate employees about the importance of paying attention to signs of frustration among their co-workers and to have a centralized structure in place for reporting such behavior, he said.

"It's critical for a supervisor to be aware of the employees, who they are and what's going on in their lives. It's really about keeping a finger on the pulse," he said.

It's also important to know that the stress can come from outside the work environment, Kirkpatrick said. An employee, for instance, could be experiencing financial problems or may have lost a home to foreclosure because of an inability to meet the mortgage payments.

Identifying and defusing a potential situation takes a coordinated effort, Kirkpatrick said. It's best for companies to set up a cross-functional team composed of members from the human resources, IT, corporate security, legal and operations departments to deal with potential risks from insiders, Kirkpatrick said. It's important to ensure that information received about a potential problem is quickly acted upon. But companies need to make sure that any action they take does not violate the employee's basic rights, she said.

Almost always "there are warning signs. But they are not always listened to," she said.

Technical controls are vital as well. One of the most important is user authorization and access control, said Raffael Marty, chief security strategist at [Splunk Inc.](#), a San Francisco-based company that provides software to help firms search for data in large enterprise applications. Companies that lay off large numbers of people or that

engage in a consolidation or merger need to first ensure that former employees no longer have access to internal systems and data, Marty said.

"If a person either leaves his company or is fired, you have to make sure that user account is disabled and that has to happen immediately," he said. In addition to terminating accounts, it's also important to monitor critical applications and activity logs to make sure those who previously had access to them can't access them through some other entry point, Marty said.

It's a good idea, in general, to monitor privileged user activity to ensure that those with elevated and administrative access rights are not using them to "rob you blind," added [Ted Julian](#), vice president of marketing at Application Security Inc., a New York vendor of database security tools. "Some sort of monitoring on your most sensitive systems is a must. You need that safety," in addition to whatever other controls might be in place, he said.

The increased use of portable devices, such as laptops and handhelds, and removable media, such as USB memory sticks and [iPods](#), has also made it easier for rogue insiders to walk away with large amounts of corporate data. Analysts for sometime have said that it's important for companies to have measures in place for centrally controlling and monitoring which devices can be attached to corporate networks and systems and what data can be downloaded, uploaded and stored on them.

Another category of tools used by companies as a measure against data theft is the so-called data leak prevention tools that keep an eye on network traffic to ensure that protected information doesn't go outside in an unauthorized manner.

## NRI Secure Technologies (Japan) Web Application Security Assessment Trend Analysis Report

A security assessment survey of 169 websites conducted by Japan's leading cyber security consulting organization, NRI Secure Technologies, Ltd., during the 2007 fiscal year found that 41 percent of the sites had critical security flaws that could allow access to sensitive information. An additional 30 percent of the sites were found to have vulnerabilities that could lead to information leaks. The majority of vulnerabilities in websites were found to be due to "incomplete measures," in which security measures have been applied to some extent, but not broadly enough to prevent access to sensitive data.

[http://www.nri-secure.co.jp/news/2008/1010\\_report.html](http://www.nri-secure.co.jp/news/2008/1010_report.html)

[Editor's Note (Skoudis): This report offers great insights into the problems we face with web security. In particular, it makes it clear that, from a defensive perspective, we aren't getting any better. And, as the bad guys ramp up their attack skills and techniques, we are in fact falling behind, relatively speaking (i.e., with a constant level of vulnerabilities and steadily increasing threat, our relative risk rises). The remaining prevalence of XSS attacks is particularly disheartening, as this vector offers attackers major opportunities for controlling victim's browsers to undermine applications.

(Pescatore): This is a fairly optimistic view, probably because the survey was skewed towards financial companies and overall security in Japan tends to be higher in general. Most similar studies show more like 75% of sites have critical security flaws. One factoid they did state, which mirrors what I see a lot, is that web sites that have never had a vulnerability assessment are four times more likely to have a critical flaw than those that had assessments. Seems simple but I'm always surprised to find how many businesses do not regularly check their web sites for vulnerabilities - even if you are sure you locked the doors, rattling the door knobs to be sure is a very good idea.]

## Researchers Expect Hackers to Prey on Cell Phones

Associated Press (10/15/08) ; Robertson, Jordan

Georgia Tech security researchers say that hackers will likely target cell phones for use in creating botnet armies. They say that as cell phones get more computing power and better Internet connections, hackers will be able to exploit vulnerabilities in mobile-phone operating systems and Web applications. Millions of PCs have already become part of botnets, and owners generally never know. The Georgia Tech researchers say that if cell phones become absorbed into botnets, new types of scams could be created. For example, infected phones could be programmed to call pay-per-minute 900 numbers, or to buy ringtones from companies established by criminals. The researchers say hackers are particularly drawn to cell phones because they are always on, they are always sending and receiving data, and they generally have poor security. "This is the perfect platform (for hackers)," says Georgia Tech professor Patrick Traynor. "There are some challenges for the adversaries, but we've seen them overcome the challenges in their way before." One challenge for hackers is learning how cellular networks work, which are tightly controlled by cell phone operators.

## State Data Encryption Laws Starting to Take Effect

(October 16, 2008) A law that took effect this month in Nevada requires that all businesses encrypt electronically transmitted customer data. While Nevada's encryption law is the first to take effect, other states are starting to enact similar laws. A Massachusetts law that will take effect in January 2009 will require businesses that collect information about Massachusetts residents to encrypt sensitive data stored on laptops and other portable electronic devices. Businesses are subject to the state laws if they have customers or otherwise conduct business operations within those states.

<http://online.wsj.com/article/SB122411532152538495.html>

[Editor's Note (Schultz): I predict that Nevada's law requiring encryption of transmitted customer information will (like California SB1386) serve as a huge impetus for passing similar legislation in other states.]

## Cybersecurity needs to move beyond IT

New study suggests CFOs, other departments tackle cyberrisks

By Grant Gross

October 20, 2008 (IDG News Service) Businesses need to expand in-house departments that focus on cybersecurity beyond IT, and the chief financial officer should be dedicated to assessing and reducing cyberrisk, suggests a new report released Monday.

While the IT department should remain a major player in [cybersecurity efforts](#), the CFO and the legal, risk management, human resources, public relations and other departments need to be involved in decisions about risk before cybersecurity breaches happen, the report said. It was released by the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI), a nonprofit group focused on setting standards for U.S. industries.

The two trade groups released the report, "The Financial Impact of Cyber Risk," through a series of workshops in which more than 30 organizations participated. Participants represented the perspectives of several corporate departments, and among the organizations involved were [IBM](#), [Lockheed Martin](#), Crimson Security, State Farm Insurance, [Carnegie Mellon University's Software Engineering Institute](#), and the U.S. Departments of Justice, Commerce and Homeland Security.

"The lesson that this workshop learned quickly was that cybersecurity, which has been traditionally viewed by some companies as an IT issue, is not just an IT issue," said Ty Sagalow, president of product development for general insurance at [American International Group](#) (AIG) and the workshop leader. "Just like it is not just a legal issue to be solved by the general counsel. Just like it is not just a reputation issue or a communications issue to be solved by the head of public relations."

The report, subtitled "50 Questions Every CFO Should Ask," recommends that business CFOs become heavily involved in focusing on cyberrisk if they aren't already. CFOs are in a position to see the big picture and budget for increased IT spending, if needed, or cybersecurity insurance or more resources in other departments, Sagalow said. In addition, CFOs need to understand the potential financial risks to breaches or leaks, he said.

Asked if some CIOs or IT department heads would see increased involvement from CFOs and other departments as encroaching on their turf, members of the task force that produced the report said they shouldn't. Many IT departments already recognize that they're only part of the solution to cybersecurity issues, said Edward Stull, a software architect for Direct Computer Resources and chairman of an IT security best practices group for the InterNational Committee on Information Technology Standards.

Many IT departments are underfunded, added Larry Clinton, ISA's president. Increased attention from the CFO could result in additional funding and an additional focus on IT needs, he said.

It may be obvious why the report recommends the legal and public relations departments be involved in cyberrisk decisions. But even human resources has a role to play, as an estimated 70 percent of breaches come from inside the organization, Stull said.

Among the questions CFOs should ask department heads, according to the report:

- Has the company analyzed our cyberliabilities?
- What's the potential for us to be named in class-action lawsuits after a breach?
- Are there valid reasons we're collecting personal information?
- What is our biggest cybervulnerability?
- Do we have a documented and proactive crisis communications plan?

The annual economic impact of cyberattacks in the U.S. is about \$226 billion, according to a 2004 estimate from the Congressional Research Service. It's time for businesses to look at cybersecurity in a new way, with multiple departments involved in the issue, said members of the report task force. "If companies view cybersecurity as solely an IT issue, then we're not going to be as secure as we can be," Sagalow said.

ISA and ANSI believe the report reflects a new way of looking at cybersecurity and cyberrisk, he added.

"Cybersecurity isn't an IT issue," Clinton added. "It's an enterprise-wide risk management issue that affects every aspect of the organization."

## Up next: Cellular botnets, cybermilitias

More troubles ahead to keep security pros up at night

By Jaikumar Vijayan

October 17, 2008 (Computerworld) The ability of malware writers to consistently [stay ahead](#) of those seeking to stop them has been a constant factor in the security industry over the past several years.

Looking to 2009, don't expect that situation to change, security analysts and vendors concede glumly. In fact, with cybercrime getting more organized and as more money is poured into malware development, it will be a challenge to stop cybercrooks from pulling even further ahead, according to the authors of a report on emerging cyberthreats for 2009 and beyond.

The report was released this week by the [Georgia Tech Information Security Center](#) (GTISC) and looks at the threats that security managers are likely to confront next year and how to deal with them.

For the most part, the threats are not unexpected or especially new. What's different is the increasing sophistication and refinement that malware writers are adding to their tools and attack techniques. Among the emerging threats identified in the report are the following:

#### **Bugs and [botnets](#) in the mobile world:**

The features built into smart phones, such as [Apple's iPhone](#), [Research In Motion's BlackBerry](#), [Google's Android](#) and Windows-enabled mobile devices, are making them increasingly computer-like in their functionality. And therein lies a security problem.

The more the systems emulate traditional PCs and notebooks, the more prone they are to the security risks that have bedeviled the computer industry for years, said Patrick Traynor, an assistant professor in the School of Computer Science at [Georgia Tech](#) and a GTISC member.

A user surfing the Web using an unprotected smart phone will, in the not-too-distant future, be just as likely to catch a nasty bug as a user doing so with a PC today, Traynor said. Malware writers will need to first re-architect and retool their products to get them to run in a mobile environment. As more people begin using smart phones to transact business and to store personal identity information and credit card numbers, the mobile device category as a whole becomes a lot more attractive for cyberthieves. This is especially so because mobile devices are relatively less protected than PC environments.

Expect to see attackers attempting to inject malware into cell phones to turn them into remote-controlled bots, Traynor said. Such bots can then be used to deliver spam, steal data or launch distributed denial-of-service attacks that can cripple cell phone networks, Traynor said.

Tools are already available for crafting exploits for the iPhone, said [Tom Cross](#), a security researcher with IBM's Internet Security Systems, X-Force security team and a contributor to the GTISC report. It's just a matter of time before the same kinds of tools become available for every major cell phone platform, he said. The only reason it hasn't happened already is because cell phones are not viewed as being especially attractive targets by malicious attackers, he said.

Cross said that one of the big questions that needs to be answered before the attacks start is who should be responsible for addressing the issue -- the users, with potentially battery-draining third-party fixes; device manufacturers; or the service providers. "We think that the impact that botnets of infected smart devices will have on the performance and reliability of telecommunications networks will affect the decision-making process," he said.

#### **Smarter 'headless' botnets**

Botnets, which are large clusters of compromised computers that can be controlled centrally from a remote location, have become the delivery mechanism of choice for cybercrooks that want to distribute spam and other sorts of malicious code. Though such networks have been very efficient at distributing malware, they have become relatively easy to neutralize by tracking and taking down the command and control servers that control them.

"Bot masters have been relatively stupid so far," said Mustaque Ahamad, director of the GTISC. "There are a variety of interesting ways to detect bot activities fairly quickly," he said. That's already changing, however, as cybercriminals put more effort into hiding bot activity by, among other things, disguising bot traffic as normal traffic, he said.

Another technique gaining favor in the botnet world is the use of so-called [fast-flux](#) networks, said Jon Ramsey, chief technology officer at Atlanta-based security vendor SecureWorks Inc. and also a report contributor. Such networks allow compromised systems in a botnet to be controlled by multiple command and control servers instead of just one system, as is the case today. These "headless" botnets are going to be a lot harder to shut down than today's typical hierarchical models, Ramsey predicted.

Botnet operators have also started using HTTP for communications between the compromised machines and the command and control servers. As a result, it will become a lot harder to distinguish botnet activity from normal traffic going forward, Ramsey said.

## Cybermilitias and cyberwarfare

Russia's military invasion of Georgia earlier this year was preceded by a [meticulously planned cyberattacks](#) against media and government communication infrastructure targets in the Georgian city of Gore.

A post-mortem by Secure Works shows that the [attacks were coordinated](#) among known hacking groups and military operators. The attacks included DDoS and cache-poisoning attempts targeting DNS servers for major Georgian networks. The attacks were launched from Russia's state-operated Rostelecom and Moscow-based Comstar networks, using the same tools and infrastructures that are being used by organized cybergangs to steal data and send spam.

At its peak, the amount of traffic directed at the targeted servers during the DoS attacks touched an astounding 80GB per second, Ramsey said. "That is the shock and awe version of cyberwarfare," he said. The huge success of the attacks is sure to serve as a model for similar attacks by nation states using cybermilitias, he said.

## U.S. government bolsters efforts to fight ID theft, report says

But public and private organizations must remain vigilant, flexible

By Grant Gross

- October 21, 2008 (IDG News Service) The U.S. government has taken several steps to combat identity theft during the past two years, including increased prosecutions of criminals and decreased use of Social Security numbers (SSNs) to identify constituents, according to a report released Tuesday ([download PDF](#)).  
Efforts to [reduce and fight ID theft](#) are happening across the U.S. government, said the report from the [U.S. Department of Justice](#) (DOJ) and the [U.S. Federal Trade Commission](#) (FTC). The report serves as an update on the efforts of the [U.S. Identity Theft Task Force](#), established by [President George Bush](#) in May 2006.  
Among the steps taken in the past two years, according to the report:
  - The DOJ increased the number of ID theft prosecutions by 27% between fiscal year 2006 and 2007. In 2006, the DOJ charged 1,946 defendants with violating one of the two main federal identity theft statutes and 1,534 defendants were convicted. In 2007, 2,470 defendants were charged and 1,943 were convicted.
  - The FTC and the [U.S. Securities and Exchange Commission](#) (SEC) have also investigated cases involving ID theft. In the past year, the FTC brought six new enforcement actions against companies that allegedly failed to take reasonable measures to protect sensitive consumer data, bringing the total of FTC data security cases to 20.
  - In March 2007, the SEC launched an effort to combat [spam-driven stock market schemes](#) and to protect investors from fraudulent e-mail campaigns hyping small-company stocks. Since then, the number of spam complaints reported to the SEC's online complaint center has dropped by 50%.
  - U.S. agencies have cut back on their use of SSNs to identify employees and constituents. The [U.S. Department of Defense](#) has launched an effort to reduce its internal use of SSNs, including eliminating them from military ID cards. The Internal Revenue Service has been redacting taxpayer SSNs to the last four digits on all federal tax lien documents filed in public records.
  - In 2007, the Office of Management and Budget and Department of Homeland Security sent a list of 10 common data security risks and the best ways to address them to all federal CIOs.

- In September, Bush signed the Identity Theft Enforcement and Restitution Act which allows victims to recover the value of their lost time when dealing with ID theft and creates new categories of crimes related to ID theft.
- In February, the U.S. Postal Service mailed ID theft protection information to 146 million people and businesses in the U.S.
- Several agencies, including the DOJ, FTC and U.S. Secret Service, have provided ID theft training seminars for more than 900 law enforcement officers.

The Identity Theft Task Force issued a strategic plan outlining 31 recommendations for the federal government, in April 2007.

"Due to the dynamic and rapidly changing nature of identity theft, the struggle to protect consumers' personal information will not end with the implementation of the recommendations from the Strategic Plan," the FTC and DOJ said in a statement. "Government and the private sector, working together with consumers, must remain vigilant and adaptable as new generations of identity thieves and techniques develop over the coming years."

## **Data Breaches at State, Local Agencies Expose Data About Millions** **Government Computer News (10/20/08) ; Jackson, William**

During the first three quarters of the year, there were 20 security breaches at state and local government agencies that resulted in the exposure of the personal information of almost 3.8 million Americans, according to the Privacy Rights Clearinghouse. The largest of these breaches was an incident in July at the Colorado Division of Motor Vehicles, which resulted in the exposure of the personal information of 3.4 million people. Meanwhile, federal agencies experienced five security breaches that resulted in the exposure of the personal information of 23,024 people. NCircle Network Security CEO Abe Kleinfeld attributed the lower federal numbers to the improvements in data security that have been brought about by the standardized processes and controls required by the Federal Information Security Management Act. He said that requirements like those laid out in FISMA could eventually be extended to state and local agencies that oversee federal programs or share information with federal agencies. Kleinfeld added that data security also could be improved by implementing a program to share best practices among federal, state, and local government agencies and create cyber security templates.

## **Survey Finds Majority of Organizations Lack Data Leakage Solutions** **Access Control & Security Systems (10/21/08)**

Although the overwhelming majority of IT professionals and security decision makers at North American firms with more than 500 employees are concerned about sensitive data being leaked through email, 72 percent of organizations do not have solutions in place to prevent such security breaches, according to a recent IDC survey. However, the survey also found that 56 percent of organizations are planning to implement a solution to prevent data leaks over email in the coming year. In addition, the study found that many organizations are failing to protect themselves from spam. The study found that 89 percent of organization do not have an anti-spam solution that blocks 99 percent or more of unsolicited messages. Many of the organizations surveyed said their anti-spam solution was not even 95 percent effective. As a result, the number of spam messages slipping through messaging security systems is growing, particularly at large organizations. The survey noted that 28 percent of organizations experienced a more than 10 percent increase in spam complaints compared with 2007.

## **Reports: Social Security Numbers Still Widely Accessible** **CNet (10/22/08) ; Condon, Stephanie**

The U.S. federal government has taken a number of steps to fight identity theft since the President's Identity Theft Task Force issued recommendations for combating the problem in its strategic plan last year. For instance, the Internal Revenue Service in January began redacting most of the digits of taxpayers' Social Security numbers on federal tax lien documents filed in public records and issued to taxpayers and their representatives.

The IRS also is considering redacting most of the digits of taxpayers' Social Security numbers on other documents. Meanwhile, the Office of Personnel Management and several other federal agencies participated in an initiative to eliminate the unnecessary use of Social Security numbers in human resource functions. However, many local government agencies across the country have not followed the federal government's lead in reducing the availability of Social Security numbers. A Government Accountability Office survey found that many counties make public records containing Social Security numbers available in bulk in order to comply with state open records law. The survey also found that only 12 percent of counties have completed their efforts to redact or truncate Social Security numbers. Another 26 percent are in the process of doing so, the survey found.

## Getting enterprises ready for smartphone security

October 24, 2008

The [Android phone from Google is now available](#) in stores near you. Actually calling Android or even Apple's iPhone a mobile phone is a misnomer - these are full fledged mobile computing platforms. Ask any user for a demo of their iPhone and I bet 99% of them will show you a cool app, fun game and playful display features. Maybe 1% will show off the telephone features. These devices have gigabytes of persistent data storage, can easily download applications, have browser-based user interfaces to corporate applications, and the phone just seems to be a special application. It is much closer to a personal handheld computer that will be within 10 feet of you 24/7.

The technology behind Google's Android and Apple's iPhone is spectacular (and Windows Mobile is none too shabby). The vendors will tout security features, but the reality is that these will need to be added in as the phones become commonplace within the enterprise. [Mocana](#) is one start-up with a security toolkit for developers of Android software. Their product set contains the crypto foundation - key management, VPNs, etc. They stress small footprint and tight code, but really I believe there is an opportunity to do so much more. The real security issues are protecting the data that sits on the device for those inevitable occasions when it is left in the backseat of a taxi, protecting business applications and interfaces from malicious activity, and reducing the cost of extending the infrastructure to include these phones.

There are a couple of opportunities to fundamentally change the way IT secures and supports application access via these devices. If we try to do everything the same old way (e.g. load up on antivirus, personal firewall, data leakage prevention, encryption, patch distribution, configuration fingerprinting, etc) IT will collapse.

- **A smart phone such as Android can always be reachable - IT does not have to wait for a network connection.** This changes the rules as now IT can access the phone (or the phone can initiate action) during off-hours to backup and remove confidential data, copy audit logs, and upgrade corporate-sourced software.
- **Look at delivering applications as a service.** Use the connectivity of the phone to connect to host-based applications with a browser, or custom interface app. I know a gazillion people that use their phones to check customer account data on salesforce.com before a meeting, and everybody checks email. Those are applications where the data and application software resides in the data center where IT can provide services and the data won't be lost. It's simple - keep data and sensitive software off the phone.
- **A smart phone is the ultimate device for shared personal and corporate use.** Virtualization technology can reduce the exposure of using smart phones for business, even when the phone is littered with games picked up on the Internet. All business will be virtualized, with verification of the integrity of the virtual interface, and frequent refresh of sensitive code. It is not perfect, but at least the data and the corporate apps will remain protected.

## IT security spending not darkened by economic gloom

By Ellen Messmer

October 28, 2008 (Network World) The [global financial crisis](#), so visible this past month, is beginning to take its toll on [IT spending](#), though IT security spending is expected to be spared in what many think will be a dismal [coming year](#).

The financial crisis was largely triggered by billions of dollars in bad mortgage loans made as America's housing boom went bust, spreading losses throughout global markets. With credit tight and a recession in sight, businesses are laying off employees and tightening budgets, including reducing IT spending. But even amid the kind of financial upheaval not seen since the Great Depression, spending on information security is expected to survive the next year largely unscathed, according to several analysts and end users forced to take stock of it all.

Even in the midst of this [turmoil](#), spending on IT security will largely escape the cost-cutting measures anticipated for other aspects of IT. That's an opinion shared by some network managers -- at least for now.

"There's no inkling whatsoever on cutting back on security spending. In fact, it's the opposite based on what I've heard," said Adam Ferrero, executive director of network services at Temple University, where the word just came down that IT spending in general would be reduced.

Temple University, which just swapped out an older stand-alone Check Point firewall and IBM ISS Proventia intrusion-prevention system for a single Crossbeam unified threat management device combining both technologies, is not expected to cut back on planned security projects.

In fact, despite the gloomy financial outlook, some analysts actually think IT security spending will increase.

In its annual Global State of Information Security Survey published this month, consultancy PricewaterhouseCoopers (PWC) said the more than 7,000 IT security professionals from 119 countries who responded indicated that 44% would increase their spending on security, while 31% said IT security spending would remain the same, 5% anticipated a decrease and 20% didn't know.

"The good news for security folks in general is we saw 44% of respondents say their security spending would increase year over year," said Mark Lobel, partner in the PWC information security advisory practice.

Lobel said the main reason that IT security spending will remain fairly strong is that "business models are changing, going online, Web-enabling everything they touch. That creates risk, and there has to be a protection component to it to mitigate that risk. Compliance is also one of the drivers, and it's just not an option to cut."

Boston-based Institute for Applied Network Security doesn't see the fiscal crisis upending IT security. The institute conducts research mainly through direct interaction with security managers, holding forums to discuss topics such as virtualization, Web 2.0 and security metrics, and surveying for opinions.

"We've been asking what's on the mind of the practitioners in this current fiscal crisis," said Jack Philips, managing partner at the research firm. In mid-October, the institute held a two-day gathering in Chicago where about 200 individuals representing 120 U.S.-based organizations were asked about the impact the fiscal crisis was having on their IT budgets and security spending.

Over three-quarters of those attending indicated they expected adjustments in their organization's IT security budgetary allotment and priorities, but about 15% did not, said Philips.

"For the most part, security spending will not be cut as aggressively as other IT priorities," said Philips. He said he got the sense from those at the conference that "in times like this, the bad guys are more dangerous and our organization is realizing to cut security is not a wise decision."

"The financial crisis is ugly and real, and it has now spread from the U.S. to Europe and Asia," said Forrester Research Inc. analyst Andrew Bartels in his report "What the Financial Crisis means to the Tech Market," published in mid-October.

Forrester predicts the last quarter of the year and the first half of next year will see a slowdown in the software and IT services sector, with vendors averaging 3% to 5% growth instead of the 9% to 12% they had earlier in 2008.

### 3 Reasons Why Employees Don't Follow Security Rules

***A recent survey finds employees continue to ignore security policies. (Surprise, surprise.) Here's a reminder about what often is missing in organizations that tempts workers to walk the wrong side of security law.***

By [Joan Goodchild](#)

October 29, 2008

According to a recent survey from security firm RSA, a majority of workers polled said they regularly feel the need to dodge corporate security policies in order to get their job done.

The survey points out that while many companies are concerned about malicious insider threats, the real danger lies in the huge amount of seemingly innocent rule-breaking that goes on daily by otherwise well-intentioned employees.

We asked Frank Kenney, a [Gartner analyst](#) focused on application development and integration, for some thoughts on the major reasons why people don't adhere to corporate security policies -- and what they need in order to get on board with the rules.

#### **They don't know the rules**

The RSA survey found most respondents said they are 'familiar' with their organization's security policies. But policies aren't always black and white, according to Kenney. Many companies may be sending out mixed messages to employees.

"If I work for a company where I can't use gmail, but I have access to gmail, the company isn't giving me better way to send out large files, and they haven't blocked gmail, I'm going to use gmail," said Kenney.

Kenny's point is that if a corporation is going to insist that workers not use certain applications or visit certain Web sites, they need to do more than just put it down in the company manual. CSOs need to [make sure workers are aware](#) by making the points clear upon hire, and also by sending out refresher materials. Also, put the tools in place so breaches don't happen, stresses Kenney. If you don't want employees on gmail, take the time to block the site.

#### **If they do know the rules, no one is enforcing them**

Even if you have the rules in place, and you know everyone is aware of them, what will stop employees from breaking them if they know there is no repercussion for their actions?

"If you run red light, you know there is a chance the police will stop you," said Kenney. "But with many security rules, employees know they will never be reprimanded for going against company policy."

RSA said respondents to their survey admitted to accessing work e-mail accounts through a public computer. A majority also said they had accessed work e-mail accounts over a public wireless network. Both these tactics [put sensitive corporate data at risk](#). But do your employees really know that? And why should they care if they never get caught? Kenney suggests educating staff about the implications of their actions. And take it a step further by backing up your policies with both incentives and punishments.

"Education can work when it is reinforced with the incentives to do the right things. And even punishment for the wrong things can be effective."

Ideas to get people motivated to follow the rules include offering everyone tickets to a group event -- or free lunch -- for a certain number of days without an infraction. Conversely, if someone on staff continues to ignore the rules, "it is time to sit that person down and say I'm going to have to reprimand you," said Kenney.

### **Rules get in the way of productivity**

People have been working around security since the dawn of IT in order to get their jobs done, said Kenney. Early examples include printing out sensitive documents that IT has blocked from download or distribution over email.

"You can lock laptops down and keep people from putting in flash drives to save things. But you know what they will do? They will print them out and do what they need to do to be productive."

Staff often view IT and security policy as a hindrance to productivity. And in many ways, it is, said Kenney. In his opinion, the riskiest behavior employees engage in lately is the aforementioned use of free Web-based services like [Yahoo](#), [Hotmail](#) or gmail to send company documents.

A recent report from Aberdeen found demand for secure/managed file transfer products is growing in several industries because of the need to share large files safely.

"When employees use Web e-mail as a work around, companies don't know what kind of intelligence property is ending up in the cloud. They need the tools in order to transfer files safely."

## **Cisco study: IT security policies unfair**

Most employees acknowledge they break rules to get their job done

By [Jim Duffy](#) , Network World , 10/28/2008

Unfair policies prompt most employees to break company IT security rules, and that could lead to lost customer data, a Cisco study found.

Cisco this week released a second set of findings from a global study on data leakage. The [first part](#) dealt with common employee data leakage risks and the potential impact on the collaborative workforce.

Part two deals with the 'whys' of behavior that raises the risk of corporate data leakage. More than half of the employees surveyed admitted that they do not always adhere to corporate security policies.

And when they don't, it can lead to leakage of sensitive data. Of the IT respondents who dealt with employee policy violations, one in five reported that incidents resulted in lost customer data, according to the Cisco study.

The surveys were conducted of more than 2,000 employees and IT professionals in 10 countries: the United States, the United Kingdom, France, Germany, Italy, Japan, China, India, Australia and Brazil. They were executed by InsightExpress, a U.S.-based market research firm, and commissioned by Cisco.

The study found that the majority of employees believe their companies' IT security policies are unfair. Indeed, surveyed employees said the top reason for non-compliance is the belief that policies do not align with the reality of what they need to do their jobs, according to Cisco.

The study found that the majority of employees in eight of 10 countries felt their company's policies were unfair. Only employees in Germany and the United States did not agree.

In Germany, even though the majority of employees felt their companies' policies were fair, more than half of them said they would break rules to complete their jobs, the study found. Of all the countries, France (84%) has the most employees who admitted defying policies, whether rarely or routinely.

In India, one in 10 employees admitted never or hardly ever abiding by corporate security policies. Overall, the study found that 77% of companies had security policies in place.

But defiance may not be intentional. IT and employees have a disconnect when it comes to policy and adherence awareness, the study found.

IT believes employees defy policies for a variety of reasons, from failing to grasp the magnitude of security risks to apathy; employees say they break them because they do not align with the ability to do their jobs.

But IT could do a better job communicating those policies. The study found that, depending on the country, the number of IT professionals who knew a policy existed was 20% to 30% higher than the number of employees.

The largest gaps – 31% -- were in the United States, Brazil and Italy.

## Report: Malicious Spam Spikes in the Enterprise

***New survey results from Sophos find the number of spam emails with dangerous attachments have soared. The report reveals the malicious messages rose eight-fold in just three months***

By [Joan Goodchild](#), Senior Editor

October 27, 2008

Cyber criminals are increasingly turning to [spam](#) as a means of infecting computers, according to a new report from IT security and control firm [Sophos](#).

The Boston-based firm found an eight-fold increase in the number of spam emails containing dangerous attachments that were sent to business organizations between July and September 2008. The Q3 Dirty Dozen spam report not only documents an alarming rise in the proportion of spam emails, but an increase in spam attacks using social engineering techniques to snare unsuspecting computer users, according to Sophos senior technology consultant [Graham Cluley](#).

The survey found that one in every 416 emails contained a dangerous attachment designed to infect the recipient's computer. That number is up from only one in every 3,333 the previous quarter, said Cluley.

Much of the increase is due to several large-scale [malware](#) attacks made by spammers during the period, he said. The worst single attack was the Agent-HNY Trojan horse, which was sent disguised as the Penguin Panic arcade game for [Apple iPhones](#). Other major incidents included the EncPk-CZ Trojan, which pretended to be a [Microsoft](#) security patch, and the Invo-Zip malware, which masqueraded as a notice of a failed parcel delivery from firms such as UPS.

"While many people may know better than to click on an attachment that says 'sexy pictures', these new tactics are more alluring," said Cluley "Too many people are clicking without thinking -- exposing themselves to hackers who are hell-bent on gaining access to confidential information and raiding bank accounts."

Spammers continue to embed malicious links and spam out [creative and timely attacks](#) designed to prey on users' curiosity, said Cluley. In August, a wave of spam messages claimed to be breaking news alerts from [MSNBC](#) and CNN. Each email encouraged users to click on a link to read the news story, but instead took unsuspecting users to a malicious webpage which infected Windows PCs with the Mal/EncPk-DA Trojan horse.

"When a spam email appears to come from a trusted source, too many users are fooled and end up clicking through to a malicious webpage," said Cluley.

Education continues to be [key to preventing infection](#), said Cluley, who encouraged business organizations to [give users initial and also refresher instruction](#) on avoiding suspicious emails.

"The advice is simple: you should never open unsolicited attachments, however tempting they may appear," he said.

The United States remained in the number one spot for relaying spam across the globe, generating 18.9 percent of the malicious emails. Russia has increased its contribution to the world spam problem, soaring from 4.4 percent last year, to 8.3 percent during this time period, according to the report. Turkey, China and Brazil were the other countries on the top-five spam relaying list.

## **RSA: Wireless Security Getting Better, Still Needs Improvement**

***New research from RSA finds wireless security is gaining sophistication. But more companies need to wake up to better protection before it's too late***

By [Joan Goodchild](#), Senior Editor

October 28, 2008

A new survey published this week by RSA concludes [wireless security](#) is improving, but too many organizations are still relying on primitive security protections when it comes to wireless networks.

The seventh annual Wireless Security Survey from security firm RSA finds wireless networks continue to grow at a rapid pace in the major cities around the world. The survey looked at New York, London, and Paris and examined the security of corporate wireless access points, public hotspots and in-home networks, according to a statement from the company.

The survey revealed London is the 'most wireless city' with a total of 12,276 access points, which exceeded the number in New York City by more than 3,000. Public hotspots - designed to allow anyone with a wireless device to access the Internet on a pay-as-you-go or pre-paid basis - continue to grow in prevalence across all three cities, said RSA officials. New York City is the leader in concentration of hotspots.

The survey also examined how many of the [wireless](#) access points detected were secured with some form of encryption, excluding hotspots. RSA officials said the 2008 results show some dramatic improvements in security practice. In New York City, 97 percent of corporate access points had encryption in place - up from 76 percent last year. The results are the best in the survey's history, said RSA. In Paris, 94 percent of corporate access points were encrypted. London still has 20 percent of all business access points unprotected by any form of wireless encryption.

Now that [Wired Equivalent Privacy \(WEP\)](#), the original wireless encryption standard, is discredited, "the 2008 survey paid close attention to the types of encryption in-play, and the relative adoption of more advanced forms of wireless encryption, including Wi-Fi Protected Access (WPA) or WPA2," RSA said in the statement. "Overall, the adoption of non-WEP advanced encryption is encouraging."

Paris lead the way in non-WEP security, with 72 percent of access points (excluding public hotspots) found to be using advanced security. New York City and London were more modest at 49 percent and 48 percent respectively. A majority of wireless access points relied on either on WEP or used no encryption at all, according to the survey.

[Sam Curry](#), vice president of Identity and Access Assurance at RSA, criticized WEP and said it "barely constitutes paper-thin protection in the face of today's sophisticated hackers."

"We would strongly urge [wireless network administrators](#) to discount WEP as a viable security mechanism and upgrade to WPA - or stronger - without delay," said Curry. "It is also critical that business access points are protected by encryption - even if the corporate network itself can only be accessed via an encrypted VPN. Not using WPA1 or WPA2 can leave the organizations involved vulnerable to whole classes of attacks against both access points and wireless client computers."

## **Some Good News on Government IT Security**

**Federal Computer Week (10/28/08) ; Robinson, Brian**

Government agencies are increasingly using security technologies to protect data stored on its networks, concludes a new PricewaterhouseCoopers report. The report found that public-sector organizations have made "wholesale, double-digit advances" in using technologies such as data encryption, reduced or single sign-ons, and centralized user data stores. The report also found that 75 percent of government agencies have employees that are directly responsible for security, up from roughly 50 percent in 2006. However, the report noted that public-sector organizations still need to make progress in a number of areas. For instance, less than two-thirds of government officials said that their organizations have an overall information security strategy or centralized security information management process, while half said that they do not understand things such as the risks to sensitive data. In addition, less than half of public-sector organizations said they have identity management strategies or tiered authentication levels that restrict users' access to data. The report called on government agencies to address these issues by adopting a number of security practices, such as implementing a risk-based approach to security, protecting employee data, and auditing and monitoring users' compliance with security policies.

## **Most Enterprises Unprotected Against E-Mail Security Risks, Study Finds**

**Enterprise Systems (10/28/08) ; Swoyer, Stephen**

Nearly three-quarters--72 percent--of companies do not have security measures in place to mitigate data leakage over email, concludes a new Secure Computing survey. The survey included responses from 100 IT professionals from organizations with a workforce of 500 or more. Almost 90 percent of the professionals surveyed said their companies do not have an effective anti-spam protection system for their corporate email networks. IDC's Brian Burke says firms have a responsibility to enhance their data protection techniques. "While organizations have expressed concern about inbound and outbound email security, their current solutions are not getting the job done," Burke says. The reverberations of this issue could be more widespread than many IT professionals believe. Figures from IDC show that as many as 90 percent of data loss occurrences are unintentional. Twenty-eight percent of the respondents said their organizations have seen a higher intake of spam within the past year, mostly due to dated technologies that are ineffective at blocking increasingly complex spam attacks.

## **IT Security: The Least Understood Management Function in Government?**

**Government Technology (10/16/08) ; Rutledge, Mark**

Government security initiatives often do not receive enough attention during the budget process because IT security continues to be one of the least understood management functions within government organizations. In order to ensure that these initiatives get the funding they deserve, government CIOs need to focus on improving three areas of security management, beginning with their agency's appreciation of the need for IT security. Many government executives do not have such an appreciation because they believe that stories of security breaches exaggerate the scope and seriousness of the problem, and that the security industry falsely portrays the state of cybersecurity in order to increase sales of its products. As a result, they are hesitant to take steps to prevent data breaches, despite the fact that research has shown that basic security controls could have prevented nearly 87 percent of all security breaches. This lack of appreciation results in poor security awareness, particularly among rank-and-file employees. CIOs can address this lack by taking several steps, including requiring IT security training for all new employees. Finally, CIOs need to ensure that employees are educated on the best practices for adopting technology.

## Crooks can make \$5M a year shilling fake security software

Scareware affiliate operation may also be a money-laundering front, says researcher

By Gregg Keizer

October 31, 2008 (Computerworld) Criminals can make as much as \$5 million a year by planting nearly worthless security software on PCs, then badgering users with so many bogus malware warnings that they fork over their credit card, a noted crimeware researcher said today.

That's the estimate of the annual income a dedicated crook could earn by pumping fake antivirus software, dubbed "scareware" by some, said [Joe Stewart](#), director of malware research at [SecureWorks Inc.](#)

Stewart led an investigation into a Russian-based operation in which affiliate members seed PCs with Antivirus XP 2008, recently renamed Antivirus XP 2009, then reap commissions of up to 90% on the software's \$40 to \$50 price tag. The program is virtually worthless and is able to spot only a handful actual threats.

After convincing a real cybercrook to provide a recommendation to an affiliate program dubbed "Bakasoftware," Stewart accessed records that showed some members pulled in as much as \$146,000 in just 10 days.

"We were able to convince another affiliate [of our bona fides], and got an invitation that let us see the back end of the affiliate site and see how the promotion works," Stewart explained. Although the Bakasoftware program had been known to researchers, its operations had received little, if any, analysis, since the program's site is in Russian and the invitation-only requirement for new memberships made it easy for the criminals to keep outsiders at arm's length.

During SecureWorks' investigation, Stewart also stumbled across messages posted on Russian forums by a hacker calling himself "NeoN" who claimed to have broken into the Bakasoftware administrative server. NeoN posted evidence that Bakasoftware affiliate members had raked in between \$75,000 and \$158,000 in one week.

NeoN tried to steal from the crooks but was blocked, said Stewart. Soon after that, however, Bakasoftware's administrator, a user pegged only as "kreb," changed members' access passwords.

Bogus antivirus programs are not a new criminal tactic, but using them to collect money from naive users has been on a major upswing. The increase, in turn, has prompted reactions from some technology companies. [Just last month](#), for instance, [Microsoft](#) joined the attorney general of Washington state to file several lawsuits against suspected scareware distributors.

"This is a huge moneymaker in the underground," Stewart said. "It carries little risk, because they're not out and out stealing credit cards or bank-account details. So even if law enforcement finds out about them, they're not going to be first on the list."

The crooks also have a tenuous excuse, said Stewart, because his analysis of Antivirus XP showed that it did, in fact, detect a very small number of threats. "They have some plausible deniability," he argued. "They could just say they didn't know that the program sucked so badly."

Useless security programs like Antivirus XP rely on their near-constant blizzard of pop-up warnings -- all faked -- to irritate or worry users enough to pay for the software. Only after paying for the program, then registering it, do the pop-ups stop.

The brazenness of the criminals' claims are astounding: On a PC running a pristine, just-installed copy of Windows, Stewart said that Antivirus XP "found" and "disinfected" more than 300 nonexistent threats.

But while affiliates can make serious amounts of money, Stewart speculated that Bakasoftware's operator might be making even more. And not by just taking his cut of the money coming in.

"We think that Bakasoftware might just serve as a way to launder money," Stewart said, adding that there's some evidence that stolen credit cards are used by at least one affiliate member to pay for downloaded and installed copies of Antivirus XP. Even though the bulk of those payments are denied by the credit card

companies, enough get through to launder significant sums. "From what we can tell, it looks like [Bakasoftware] may be doing this themselves," said Stewart, "and hiding a smaller volume of fraudulent money in the larger volume of legitimate credit card payments users are making for the software."

The Bakasoftware operation continues, Stewart said. "I don't think they've noticed our investigation," he said. But stopping even one affiliate program, much less the scores that are active, is nearly impossible.

"The best way to make money as a criminal is to set up an affiliate program of some kind, then get someone else to do the dirty work," said Stewart. "They don't even need to work hard at it [to make plenty of money]."

## Revision of IT security rules could cost feds \$600M over four years

Bill to strengthen FISMA would increase annual compliance costs by 2.5%, estimate says

By Jaikumar Vijayan

October 31, 2008 (Computerworld) A proposed bill aimed at [strengthening the provisions](#) of the Federal Information Security Management Act would require the U.S. government to spend an additional \$610 million on FISMA implementation costs over the next four years if it is passed, according to an estimate by the Congressional Budget Office.

The CBO said in a cost estimate released on Tuesday that the bill could also affect spending on security by agencies, such as the [U.S. Postal Service](#), that don't receive annual funding for compliance with the act. But any increase in costs at those agencies is likely to be relatively small and could be offset by increasing the fees they charge for their services, the CBO added.

FISMA was approved by Congress and signed into law in 2002, in the aftermath of the 9/11 terrorist attacks, with a goal of improving data security within the federal government. The law mandates a [series of security measures](#) that agencies have to comply with and be evaluated against on an annual basis. For instance, FISMA requires agencies to adopt standard system configurations, create security training programs and develop processes for testing their security controls and contingency plans.

Over the past few years, the annual FISMA reports issued by each agency's inspector general have been widely used as an indicator of the security preparedness at individual agencies and within the government as a whole. [Rep. Tom Davis \(R-Va.\)](#), who authored FISMA, uses the reports to prepare an [IT security report card](#) each year. Many agencies, including the departments of Defense, State and Homeland Security, have typically [fared poorly](#) on the report cards, getting "D" or even "F" grades.

FISMA's mandates have focused much-needed attention on the security of federal systems and IT infrastructures. Even so, over the past few years, there has been a growing concern that many agencies have begun treating the FISMA process as little more than a [paperwork exercise](#), resulting in little in the way of actual security improvements.

The big problem, according to [critics of the process](#), is that FISMA merely requires agencies to attest to the measures they have implemented for protecting their data and systems without actually requiring them to prove anything. The requirements have also been criticized for not being holistic enough and for being too focused on process issues, while not covering technology issues.

The so-called FISMA Act of 2008, which was introduced in the Senate on Sept. 11 and is officially known as S. 3474 is designed to address some of those concerns. For instance, the bill would require all agencies to create a chief information security officer's position with specific duties and authority. It also calls for the creation of a CISO council that would set security guidelines and best practices.

In addition, the bill would require formal and standardized security audits at agencies, instead of mere "evaluations," and impose new reporting requirements. And IT vendors that sell products to government agencies would need to comply with certain FISMA mandates.

According to the CBO, federal agencies spent about \$6 billion meeting the FISMA requirements last year. Its projected cost increase of about \$150 million per year if the proposed bill is approved represents a 2.5% hike in the current spending level.

But some security analysts think that the added-cost figure might be overblown. "I think the CBO estimate was just a wild stab," said Gartner Inc. analyst [John Pescatore](#), adding that the size of the projected increase is "really hard" to envision, considering the relatively small extent of the changes being proposed to FISMA.

For instance, while agencies would have to designate CISOs, those positions wouldn't necessarily have to be full-time positions, according to Pescatore. Instead, the CISO role could be handled by someone whose existing job primarily involves security responsibilities. "So this doesn't really even mean any new hires for most agencies," Pescatore said. Similarly, he added that while the creation of a CISO council will add some spending at the executive level, it is unlikely to be a big cost factor.

[Alan Paller](#), director of research at the [SANS Institute](#), a Bethesda, Md.-based security training and certification organization, said he thinks the FISMA revision would actually end up saving money. Paller said the new requirements would force agencies to "focus their spending" on measures that they could prove had improved security protections.

## Three ways Internet crime has changed

By Joan Goodchild

- November 3, 2008 (CSO) Gone are the days when most hackers were looking for fame with a splashy, large-scale attack on a network that made headlines. Today's cybercriminals are quietly taking over vulnerable web sites as part of an elaborate process in the underground economy.

Cupertino, Calif.-based security products provider [Symantec](#) publishes a biannual internet threat report. Data collected through their managed security services are reviewed and analyzed for the report, which was recently published in its 13th edition.

One trend highlighted in the report change is the motivation of hackers, according to the data. "The trend has moved from hacking attempts being done for notoriety to hacking for criminal intent and fraud," said Grant Geyer, vice president of Symantec Managed Security Services.

How are cyber criminals working today? And what do you need to know to stay on top with your security strategy? Read on for the latest news on malicious web activity.

Botnets spearhead for-profit hacker activities

The latest data from Symantec confirms that the web is now an integral tool for criminals looking to make money (not merely mischief). Malware-infected systems are used as network of bots for a wide variety of inappropriate activities.

"Bots can do denial of service attacks, they can be used to send out spam, to send out phishing data, they can be the Swiss Army knife of malware distribution," said Geyer. "We're seeing more and more of both consumers, as well as corporations, being targeted by bots for malicious purposes."

Bots, Geyer confirms, are being used as business model; part of the underground economy that is run and organized like any major corporation.

"If you want access, if you want one of these bot networks to send out your specific spam message, you can purchase time on bot network, there are rates being established," noted Geyer. "Bots are also being used to steal confidential data. Credit card numbers are sold online. Market prices are established for that, too."

Cyber criminals are quieter, and sneakier.

While early hackers wanted to make a big splash by attacking as many computers as possible in a show of genius and savvy for taking down network, now criminals don't want to be detected. Takeovers are done in a slow, methodical fashion.

"If you can go as slow and stealthily as possible and take over systems in a selective manner, you don't get caught. By not getting caught, you can use the systems you've taken over for a variety of purposes."

Geyer said sites in the United States are consistently the top target worldwide. China is usually second and many countries in Western Europe also in the top ten.

In the first few years the report was published, the number of vulnerabilities in operating systems and software increased annually. The good news is that has begun to change in the last 18 months, said Geyer. Vendors have become more proactive about patching. The bad news is hackers have taken on other techniques to exploit a system and are focusing more on site-specific vulnerabilities.

"Site-specific vulnerabilities are lot harder problem to solve," said Geyer. "You can't just send out a patch and protect everyone if the problem is site-specific."

Large organizations were the main target of attacks less than a decade ago; now the end user is the primary target, said Geyer. Phishing web site hosts are dramatically increasing and so are new variants of malware.

"In past 18 months, the increase is just staggering. So much is being introduced, organizations are having tough time. A lot of it is the same piece of malware that is tweaked to be slight variant of other pieces already written. It just shows how easy it is to write it and also that there is true financial gain. This is proving to be a good business model for people in the underground economy."

## ***Recycled Tapes Yield Data On Former Owners***

### **Study of 100 "recertified" tapes turns up sensitive data from major bank, hospital**

Oct 30, 2008

**By Tim Wilson**  
***DarkReading***

The widespread process of erasing data storage tapes and "recertifying" them for sale isn't safe and could cause enterprises to expose sensitive business data, a major tape vendor said yesterday.

[Imation](#), which makes tape cartridges and other storage media, says [there's no way to completely erase the data that has been recorded on computer tape](#).

"Today's tape cartridges have storage capacities of 500 gigabytes or more. Even if 99.9 percent of data is erased from a tape, hundreds of megabytes of potentially sensitive data could remain on the tape," says Subodh Kulkarni, vice president of global commercial business, R&D, and manufacturing at Imation. "This could include thousands of customer names and Social Security numbers."

To prove its point, Imation purchased 100 recertified tapes from mainstream channels and scoped each one to see what data it could find. According to its report, the company found sensitive data from a major U.S. bank -- including employee credit card records, computer user names, and server inventories. It also found detailed patient information from a major U.S. hospital, field research data from a scientific research center, and details on the Human Genome Project from a large university.

"In our lengthy testing and analysis, which has spanned many months, we have confirmed industry guidance that the only way to properly dispose of data is to destroy the media itself," Kulkarni says. "The technical truth is there is no practical and secure way to completely erase and 'recertify' most used tape products."

Imation's conclusions could certainly be seen as self-serving, since the company loses dollars to the recertified tape market every day. But other studies, including one published several years ago by [Computer Technology](#)

[Review](#), have arrived at similar conclusions. Several other tape storage vendors, including Maxell and FujiFilm, have published similar studies.

Graham Media, one of many vendors that sells recertified tapes, asserts that the risk of buying recycled media is negligible. "Any data that remains on the tape is not usable/readable, much in the same way that old unreadable data resides in every overwritten tape cartridge in every data center in the world," the company said in a [written response to tape vendors' warnings about recertified media](#).

## California tightens policy on shielding personal information

By Andrew McIntosh

Nov. 08, 2008

The state has adopted a sweeping new policy that aims to protect confidential personal information and better manage security breaches like the one this summer at the Department of Consumer Affairs.

The policy was spelled out last week in a statewide management memo issued by Michael Saragoza, an undersecretary at the State and Consumer Services Agency.

"Safeguarding against and preventing security breaches involving personal information is essential to maintaining the public's trust in government," Saragoza wrote.

"Failure to protect personal information can place people in jeopardy in a variety of ways, including identity theft, damage to reputation and physical injury," he added.

The new policy comes five months after Consumer Affairs personnel specialist Rachael Dumbrique sent to her home e-mail a personnel roster with 5,000 names and Social Security numbers of department staff members.

That triggered concerns about identity theft because Dumbrique was married to a convicted murderer and member of the Mexican mafia serving a life sentence in Corcoran State Prison, documents show.

Dumbrique pleaded no contest to one felony count and is scheduled for sentencing Nov. 18.

While Joanne McNabb, chief of the state Office of Information Security and Privacy Protection, said the memo had been in the works for months before the Dumbrique case, Saragoza said it gives officials an added tool to reduce the risks of similar incidents.

McNabb and Saragoza praised Consumer Affairs' handling of the Dumbrique case, saying its e-mail filtering security system detected the breach immediately and the case was dealt with quickly.

The new policy urges agencies to reduce their stores of personal information and explore alternatives to using Social Security numbers to identify people.

From now on, every agency must consult with the Office of Information Security and Privacy Protection before issuing written notifications of security breaches.

## On Security, Microsoft Reports Progress and Alarm

**New York Times (11/03/08) P. B9 ; Markoff, John**

The security of the Windows operating system has significantly improved, but the threat of computer viruses, fraud, and other online threats has become far more serious, concludes Microsoft's biannual "Security Intelligence Report." Microsoft blames organized crime, naive users, and its competitors for the deteriorating situation. Microsoft reports that the amount of malicious or potentially harmful software removed from Windows computers increased by 43 percent during the first half of 2008. The report also says that improved Windows security caused attackers to shift their attention to security holes in individual programs. For example, the report notes that 90 percent of newly reported vulnerabilities involved applications in the first half of 2008, while only 10 percent of new vulnerabilities involved operating systems. Microsoft says that software practices must change industry wide otherwise the improvements in Windows will be meaningless. Security researchers agree. "The

only thing that Microsoft can patch is their own software," says F-Secure chief security advisor Patrik Runald. "That's not what the bad guys are using to get into computers these days. It's certainly a challenge." The computer security industry has been fighting a losing battle as computer criminals are increasingly able to profit from identity theft and a variety of other scams. Microsoft has tried to combat the problem by building a variety of safeguards into its operating systems and its Internet Explorer browser, with mixed success. The Microsoft report notes that the infected rate of U.S. computers rose 25.5 percent in the last six months.

## **Internet Apps & Social Networking Office Boom Linked to Breaches**

**Dark Reading (10/27/08) ; Higgins, Kelly Jackson**

There is a correlation between the increased use of social networking services among employees and an increased frequency of security breaches at organizations, concludes a new FaceTime Communications survey. The survey found that of the nearly 60 percent of organizations who reported that their employees use social networking services at the office, the ones that experienced an increase in social networking use compared with six months ago had an average of 39 security incidents a month requiring 24 hours worth of remediation. Meanwhile, organizations that reported about the same or fewer users of social networking versus six months ago experienced 22 or 23 security incidents a month requiring roughly 12 hours worth of remediation. FaceTime's Frank Cabri says IT departments can mitigate the security risks posed by employees' use of social networking services by trying to find common ground with their user community. Cabri notes that IT can do this by allowing employees to use some applications with restrictions. He also says that IT should measure and report on what employees are doing with those applications.

## **Security Issues Abound as Social Networking Goes to Work**

**IT Business Edge (10/23/08) ; Weinschenk, Carl**

The escalating use of social networking sites by employees has the potential to become a very large problem for IT departments. According to some estimates, the corporate Web 2.0 wave will expand into a \$4.6 billion sector by 2013, and \$2 billion of that could come from social networks. Ideally, companies will be working to deal with the mounting security threats on the front end. Web filters used to block malware on sites such as Facebook and MySpace work as little as half the time, experts say. An attack reported in the Washington Post describes a spear phishing scam against approximately 10,000 LinkedIn members who mistakenly opened a legitimate-sounding email that led users to download a malicious phishing program, exposing sensitive customer content on thousands of corporate machines. Like cell phones and PDAs, social networking sites are becoming more entrenched in corporate culture because employees are using them at home and then bringing them to work. Maximizing on security and interactivity with these sites remains a major obstacle for IT leaders.

## **Security, virtualization lead 2009 tech plans**

**By Denise Dubie**

November 11, 2008 (Network World) IT organizations consider [security](#), [server virtualization](#) and [business-related technologies](#) to be their top priorities for 2009, according to research released by the [Society for Information Management](#).

SIM surveyed 300 of its member organizations in June and learned that the top five application and technology developments for the coming year include [antivirus protection](#), [business intelligence](#), [business process management](#) (BPM), continuity planning and [disaster recovery](#), and server virtualization.

[Jerry Luftman](#), SIM's vice president for academic affairs and distinguished professor and associate dean at the [Stevens Institute of Technology](#) said the highest-ranking technologies reflect a few key issues on IT leaders' minds.

"Security was the top priority last year as well, but people are struggling with other areas such as business intelligence," he said.

To start, security via antivirus protection reflects IT's ongoing balancing act of enabling services while also protecting environments. IT organizations are also tasked with combating more varied threats than they were in the past. Kenneth Washington, chief privacy officer and a vice president at [Lockheed Martin](#), explained to SIMposium 08 attendees how people are hyperconnected via multiple devices today, which poses a challenge to security and privacy leaders tasked with securing networks.

"Attackers today are motivated by theft, profit and data. And they are very patient," he said during a presentation at the SIM conference in Orlando.

Business intelligence and BPM landed in the second and third spots on SIM's survey. BI will continue to challenge IT organizations, according to Luftman, who said that business intelligence is "more complicated than previously envisioned and requires strong skills" that aren't readily available in the existing IT talent pool. BPM, on the other hand, is a top priority, because of the cost-efficiencies and streamlined operations it could offer an IT organization, he explained.

"BPM is about IT being able to reduce costs, and obviously that is top of mind," he added.

Fourth on the list, the area of business continuity and disaster recovery, continues to be a priority for IT leaders, but the fifth entry -- server virtualization -- is new to SIM's top five application and technology developments list. "It's another area seen as having the potential reduce costs and improve services," Luftman said.

SIM researchers were also intrigued by what technologies did not make the top five. For instance, [networking](#) and communications technologies, which were previously in the top five, slipped down to the tenth priority. And [wireless networking](#) was in the 25th position, while mobile/wireless applications, VoIP and shared services finished in a three-way tie for the 29th spot on SIM's list.

"Network technologies were in the top five last year, but for 2009, they lost priority," Luftman said. "There are relevant technologies there, and they are still being put in place, but it is not as hot as it was last year."

## Storage, security raises issues for telepresence

By Stephen Lawson

- November 13, 2008 (IDG News Service) [Telepresence](#), the high-end form of videoconferencing now coming from several vendors, is the first technology that might let enterprises easily record high-quality versions of all their meetings, essentially with the press of a button.

Though recording and playback features for these systems are still emerging, some issues are already being raised, including storage capacity, liability and playback quality. Those problems may grow as more enterprises seek to cut back on travel and bring dispersed teams together through telepresence.

The technology is designed to make videoconferences more like in-person meetings, with high-definition streaming video, multiple screens and "spatial" audio systems that associate sounds with a speaker's location. [Cisco Systems Inc.](#) made a splash about two years ago with a product it calls [TelePresence Meeting](#), which carried a price tag of \$598,000 for two six-person room setups with special lighting and furniture.

But numerous other vendors have been stepping up their games as well. [Polycom](#), [Hewlett-Packard](#), Tandberg and smaller players such as LifeSize Communications all have high-definition systems now, and [Mitel Networks Corp.](#) announced one on Monday. Mitel's TeleCollaboration Solution is a large-screen meeting setup with 1080p displays and spatial audio, available with as many as three screens for six participants. Set to ship in January, it will also work with the company's existing desktop videoconferencing client, which is being upgraded and renamed. Pricing has not been set, but the TeleCollaboration Solution will be significantly less expensive than Cisco's TelePresence, said Asif Rehman, director of propositions marketing at Mitel.

Meetings that take place via IP networks are just packets of data, so it seems natural that they could be recorded and played back later. Yet, even Cisco doesn't have that capability; it's coming soon, according to Marthin De Beer, senior vice president and general manager of Cisco's Emerging Technologies Group.

Other vendors are farther along. As [Mitel announced the TeleCollaboration Solution](#) this week, it also unveiled recording capability for its desktop videoconferencing system as well as for the new product. LifeSize Communications Inc. earlier this year offered an ad hoc recording feature. Polycom Inc., which has been selling video recording and streaming servers for about two years, already has a second generation of the boxes with greater capacity. Early next year, it plans a new release with the capability to link up to mass storage arrays for additional space, according to Joan Vandermate, vice president of marketing for video solutions.

But one vendor isn't even going near telepresence recording: Hewlett-Packard Co.'s approach reveals one of the issues surrounding the ability to save any virtual meeting. The company doesn't just sell the [Halo line of conferencing units](#) but also is the sole provider of a network linking them together. It won't sell its customers any recording equipment.

"That's not something that we offer as an option, just because of the privacy and security issues," said Darren Podrabsky, global marketing manager for Halo. Supplying recording capability would mean storing the data on HP's network, he said.

"The idea that somebody accessed the content without the customer's permission ... that's just not a position we want to be in," Podrabsky said. "We don't want the liability." If customers want to save recordings of their own telepresence sessions, HP refers them to third parties for products that will let them store the data on their own LANs.

Yankee Group Research Inc. analyst [Zeus Kerravala](#) said he thinks regulatory compliance will sometimes be an issue as companies start recording videoconferences. The systems will have to have ways to opt in or out of recording, he said. And after meetings are stored, IT departments will have to make them easy to search for and retrieve if requested.

In fact, despite HP's reticence about storing customers' recordings, Kerravala predicted that concerns about capacity and compliance will make managed services an attractive way to get telepresence.

Another issue is recreating the high-quality experience for which an enterprise bought an expensive telepresence system. In one sense, playback is simple: Most vendors allow a meeting leader to send out an e-mail with a link that those who missed the meeting can click on to access.

Sessions can be recorded at lower resolutions suitable for PC viewing or even transcoded into different formats, sometimes with third-party tools. Polycom offers two options for displaying multiple participants on a single screen: switch from person to person by detecting voices or show all simultaneously in small windows.

"As long as your expectations are in line, it's going to be fine," said Wainhouse Research LLC analyst Ira Weinstein. "But the expectations surrounding telepresence are off the charts."

Most LifeSize customers that want to record telepresence sessions are doing so with one-to-many presentations such as training or executive messages to employees, according to Michael Helmbrecht, director of product management. The company hasn't noticed demand for recording the kind of immersive virtual meetings with multiple participants that are the hallmark of telepresence, he said, partly because of confidentiality concerns.

"Boardroom conversations tend not to be something to record," Helmbrecht said.

The University of Colorado, Denver, along with its medical school and partner hospitals, holds thousands of videoconferences every year, including lectures, medical demonstrations and administrative meetings, and it records many of them for playback later. For most, the school uses Polycom standard or high-definition systems, said Betty Charles, associate director, educational support services.

Given its needs, the university has run into capacity issues with Polycom's RSS (Recording and Streaming Server) 2000 product because the system can't stream enough sessions out to the network while recording those currently going on. So the content is sent to a separate video server for distribution. The university doesn't have enough videoconferencing content that it needs to use a SAN or network-attached storage yet, but Charles said she could see that becoming an issue in the future.

Privacy and security are concerns, as well as compliance with Health Insurance Portability and Accountability Act rules for patient data. The university uses password protection to control access to both live streaming content and stored sessions, Charles said.

Participating in virtual meetings that can later be played back may present some peril for employees, warned Yankee's Kerravala.

"It's easy to tell when someone's not paying attention," he said. "Facial expressions mean a lot."

## **Human error becomes biggest security fear**

(Vnunet, 11/14/08)

Human error has become the biggest security concern for IT directors, according to new research from gateway security firm Secure Computing. The vendor surveyed IT managers in April and again in October and found that, although 35 per cent said that employee fraud was their biggest fear six months ago, this had been replaced by employee error, notching up 39 per cent of respondents.

"There have been quite a few public breaches and issues of best practice and data control in the news since April, and the government and FBI reports show a similar trend towards a focus on insider threats," said Secure Computing product manager Mike Smart.

## **Study: Critical infrastructure often under cyberattack**

(Computerworld, 11/11/08)

Computer systems that run the world's critical infrastructure are not as secure as they should be, according to a new survey. The survey asked 199 management, network engineers and administrators in nine infrastructure industries about the state of cybersecurity in the U.S., Canada and Europe. Insiders said that all of these industries, except for financial services, were unprepared for cyberattacks. These industries included water, utilities, oil and gas, telecommunications, transportation, emergency services, chemical and the shipping industry.

And that's bad news because more than half of them said that their companies had already been hit with some sort of cyberincident, data leak or insider attack. Another 14% said they were expecting something like this to happen in the next year.

## **Why veins could replace fingerprints and retinas as most secure form of ID**

(Financial Times, 11/11/08)

Forget fingerprinting. Companies in Europe have begun to roll out an advanced biometric system from Japan that identifies people from the unique patterns of veins inside their fingers. Finger vein authentication, introduced widely by Japanese banks in the last two years, is claimed to be the fastest and most secure biometric method. Developed by Hitachi, it verifies a person's identity based on the lattice work of minute blood vessels under the skin.

Hitachi claims that because the veins are inside the body, invisible to the eye, it is extremely difficult to forge and impossible to manipulate. While fingerprints can be "lifted" and retinas scanned without an individual realizing it, it is extremely unlikely that people's finger vein profiles can be taken without them being aware of it, the company says.

