

Security Trends Report

04/09

US Smart Grid Spending Opens American Homes and Businesses To Mass Blackouts

(March 21, 2009) The US's high technology, digitally based electricity distribution and transmission system known as the "Smart Grid" is slated to get \$4.8 billion from the recent stimulus bill. Tests have shown that a hacker can break into the system, and cybersecurity experts said a massive blackout could result. Garry Brown, Chairman of the Public Service Commission of New York, says the benefits outweigh the risks, but "before we go rushing headstrong into a Smart Grid concept, we have to make sure that we take care of business, in this case cybersecurity."

[Editor's Note (Paller) CNN's story hinted at a critical vulnerability.

Here is the article reporting the vulnerability has been exploited,

http://www.pcworld.com/businesscenter/article/161727/power_grid_is_found_susceptible_to_cyberattack.html

However, the article's author, Bob McMillan, tells NewsBites that "Travis retracted his comments about worm code being actually being written after I published the story, saying he was misinformed."

Despite this retraction, the bottom line is (1) that this vulnerability is real and its scope is huge, (2) that the meter manufacturers are trying to get billions in sales without fixing the flaws, and (3) that only fast leadership by people like Garry Brown of New York with strong help from the US government will stop the vendors from locking these vulnerabilities into millions of homes.]

Study: Most Organizations Hit by Cybercrime

By Joan Goodchild , CSO , 03/23/2009

A report released Monday by [Symantec](#) gauges the far reaching impact of cybercrime and finds most organizations have dealt with a cyber attack of some kind in the last two years.

Symantec surveyed 1,000 IT managers in the U.S. and Europe in January. In its 2009 Managed Security in the Enterprise Report, almost all respondents, 98 percent, said their organization has experienced tangible loss as a result of a cyber attack incident. Additionally, 46 percent experienced downtime and 31 percent experienced theft of customer or employee personally identifiable information. Another 25 percent were hit with theft of corporate data

"IT departments are dealing with a perfect storm of problems when it comes to protecting their organizations: the threats are getting worse, losses are mounting," said Grant Geyer, vice president of Managed Services at Symantec.

The report also found cyber threats are growing rapidly. Nearly half of U.S. enterprises, 46 percent, said cyber threats have somewhat/significantly increased in the past two years and are expected to somewhat/significantly increase in the next two years. Most respondents, 88 percent, experienced a cyber attack in the past two years with 31 percent seeing attacks on a regular basis and 10 percent seeing a large/extremely large number of attacks.

Visa pilots new payment card security initiatives

In addition to OfficeMax and Fifth Third Bank pilots, Visa plans new alerting for consumers
By Jaikumar Vijayan

March 19, 2009 (Computerworld) Acknowledging the need for controls that go beyond those [offered by the Payment Card Industry \(PCI\) Data Security Standard](#), a senior Visa Inc. executive today described two new initiatives to reduce payment card fraud being tested by the company.

One of the [pilots involves Fifth Third Bank](#), which is testing the use of magnetic stripe technology to create unique digital fingerprints for cards, said Ellen Richey, Visa's chief enterprise risk officer. Each stripe contains unique characteristics that can be captured and used to verify the digital identity of the card, Richey said at a security event being hosted by Visa today. The goal is to stop the creation and use of counterfeit cards based on stolen payment card data.

Another initiative, being piloted by retailer OfficeMax Inc., involves the use of a challenge-response technique [at the point of sale](#). The project is aimed at testing the efficacy of asking consumers to respond to specific questions -- such as their ZIP code, the last four digits of their phone numbers or the first three digits of their area codes -- as part of the transaction approval process.

Dan Roeber, vice president and manager of merchant PCI compliance at Fifth Third, said the bank had rolled out about 1,000 card readers to retailers who have not been informed about the pilot effort. The terminals are capable of reading the magnetic stripe information and creating a "DNA picture" of the card, which is then matched during the authorization process against baseline information for that card stored by the card issuer, he said during a panel discussion at the event today.

During the pilot process, baseline images or fingerprints for a card are created when it is first swiped through one of the new readers, Roeber said. But going forward, if the approach works, baseline images for each card could be created and stored during the card-issuing process itself, Roeber said. "Even if somebody gets into a database and makes fraudulent cards, the DNS fingerprints are not going to match," Roeber said. "The thing I really like about this technology is that there are no key-management issues," as is the case with the use of end-to-end encryption for protecting cardholder data.

"We are very excited about this technology," he said.

Fifth Third is one of several "acquiring banks," which are responsible for [authorizing retailers to accept payment card transactions](#).

William Van Orman, treasurer at OfficeMax, said the retailer had rolled out its challenge-response process to about 1,000 of its stores across Illinois, Indiana and Florida. The process, which has required changes to point-of-sale systems at these locations, involves asking customers ZIP codes or other personal information after swiping a card. The responses are then matched against responses to the questions that were previously selected by the consumer.

For the pilot, the emphasis was on simply trying to understand what kind of changes needed to be made to the point-of-sale systems, and the kind of impact the new authorization process would have on merchants and consumers, Van Orman said. Customers were informed that the data was being requested for a pilot project and had the chance to opt out if they chose to, Van Orman said. After an initial six-month period, the pilot project has been extended by another four months at the request of Visa. "Overall, we think it's a successful project," he said.

Richey said that while these projects are not quite ready for broad rollout yet, they are indicative of the kind of approaches that could be used to make stolen data useless at the point of sale.

Richey also highlighted Visa's efforts to give consumers more tools to fight fraud. One of them is a new service called the Transaction Alert system and is currently available to Chase cardholders with Android-based smartphones, she said. The service provides real-time alerts of purchase activity on their mobile devices, which consumers can tailor using information such as whether they were online transactions and locations where the transactions were made. The program will become available to all card issuers later this year, she said.

The other program, which is still in development, is called Targeted Acceptance and would allow consumers to set personal limits on how, where and what amounts their cards can be used for. The service is already available to commercial customers and will be rolled out to consumers as well, Richey said.

She said Visa is not opposed to the idea of using in the future [chip and PIN technologies](#) that are used widely in Europe. They require consumers to enter PIN numbers, instead of signing, when making credit card

transactions. The approach is widely considered to be safer than purely signature-based transactions, but it would require considerable investments on the part of card issuers to make the change. Richey said that Visa fully supports the technology and that it isn't a matter of whether the technology will be adopted in the U.S., but when and how.

Dave Weick, CIO at McDonald's Corp., discussed during a panel a new plan to minimize threats against payment card data. He described how the fast-food giant is exploring how to completely segregate all payment card data and transactions from the rest of its internal network. Weick said McDonald's had developed a way to accept payment card transactions without letting any of that data touch any of its own internal systems, including its point-of-sale devices.

No one in the company's internal system would have access to any cardholder data, and even the portion of the network that deals with card transactions would be handled by an outside vendor, Weick said. "We are very early on in this," he said, adding that the plan is to first roll out the approach to company-owned restaurants before deploying it across all franchises.

Post-breach criticism of PCI security standard misplaced, Visa exec says

Chief risk officer: No breached companies have been compliant with the data security rules
By Jaikumar Vijayan

March 19, 2009 (Computerworld) Visa Inc.'s top risk management executive today dismissed what she described as "recent rumblings" about the possible demise of the [PCI data security rules](#) as "premature" and "dangerous" to long-term efforts to ensure that credit and debit card data is secure.

Speaking at Visa's Global Security Summit in Washington, Ellen Richey, the credit card company's chief enterprise risk officer, insisted that despite recent [data breaches](#) at two payment processors, the [Payment Card Industry Data Security Standard](#) (PCI DSS) "remains an effective security tool when implemented properly."

Richey added that breaches such as the ones at [Heartland Payment Systems Inc.](#) and RBS WorldPay Inc. were shaping public opinion and obscuring what otherwise has been "substantial progress" on the security front over the past year.

"I'm sure that everyone in this room has read the headlines questioning how an event of this magnitude could still happen today," Richey said, referring to the [Heartland breach](#). "The fact is, it never should have" — and indeed wouldn't have if Heartland had been vigilant about maintaining its PCI compliance, according to Richey. "As we've said before," she continued, "no compromised entity has yet been found to be in compliance with PCI DSS at the time of a breach."

Pointing to Visa's decision last week to [remove both of the breached payment processors](#) from its list of PCI-compliant service providers, Richey said that Heartland would face fines and probationary terms that were proportionate to the still-undisclosed magnitude of the breach. "While this situation is unfortunate, it does not make me question the tools we have at our disposal," she said of the PCI rules.

Richey's defense of PCI DSS and criticism of Heartland come as Visa, which has taken the lead among credit card companies in seeking to enforce the standard, is itself facing some criticism over its enforcement actions.

For instance, some analysts have been critical of the so-called probationary period that Visa has imposed on Heartland, saying that designation — which requires the payment processor to meet more stringent security requirements than usual — appears to have been created purely in response to the Heartland situation. Some also see Visa's insistence that Heartland and RBS WorldPay weren't compliant with PCI DSS when the breaches occurred as an attempt by the credit card company to protect itself legally and prevent the payment processors from using PCI as a shield against [breach-related lawsuits](#) filed by banks and credit unions.

In addition, questions are being raised about what exactly it takes to remain fully PCI-compliant at all times. "It's easy to find somebody to be in noncompliance if that is the primary goal" of an audit, said David Taylor, founder of [PCI Knowledge Base](#), a Web site that offers advice on PCI-related issues.

In an interview earlier this week about Visa's removal of Heartland and RBS WorldPay from its PCI-compliant list, Taylor said that auditors are bound to find problems if they really want to. "It's easy to go in and say, 'You don't have this patch, or you didn't centralize your logs,'" he said.

During a panel discussion after Richey's talk at the Visa summit today, Dan Roeber, vice president and manager of merchant PCI compliance at Cincinnati-based Fifth Third Bancorp, said there are "lots of moving parts" in the PCI standard. That sometimes can make complying with the rules a challenge, he added.

Roeber called on Visa and other credit card companies to give merchants more flexibility in implementing security controls based on the specific risks that they face in their own environments. He also said PCI Security Standards Council LLC, the organization responsible for administering PCI DSS, "needs to do a more thoughtful job" and "get as much risk-oriented language as possible" into the rules in order to make them more digestible for companies trying to figure out why they need to implement certain controls.

Princeton, N.J.-based Heartland has maintained that its compliance with the PCI standard was validated by an auditor last April, only about a month before the breach of the company's systems is thought to have begun. Similarly, Atlanta-based RBS WorldPay, which was certified as being compliant with the PCI rules last June, said this week that it has made "no material system changes that would have negatively altered the certification." In fact, the company added, it has "enhanced the security of our systems in the interim."

Expert: Hackers penetrating industrial control systems

Digging out from infrastructure attacks could take months, Joseph Weiss says

By Grant Gross

March 19, 2009 (IDG News Service) The networks powering industrial control systems have been breached more than 125 times in the past decade, with one resulting in U.S. deaths, a control systems expert said Thursday.

Joseph Weiss, managing partner of control systems security consultancy Applied Control Solutions, didn't detail the breach that caused deaths during his testimony before a U.S. Senate committee, but he said he's been able to find evidence of more than 125 control systems breaches involving systems in nuclear power plants, hydroelectric plants, water utilities, the oil industry and agribusiness.

"The impacts have ranged from trivial to significant environmental damage to significant equipment damage to deaths," he told the Senate Commerce, Science and Transportation Committee. "We've already had a cyber incident in the United States that has killed people."

At [other times](#), Weiss has talked about a June 1999 gasoline pipeline rupture near Bellingham, Wash. That rupture spilled more than 200,000 gallons of gasoline into two creeks, which ignited and killed three people. Investigators found several problems that contributed to the rupture, but Weiss has identified a computer failure in the pipeline's central control room as part of the problem.

It could take the U.S. a long time to dig out from coordinated attacks on infrastructure using control systems, Weiss told the senators. Damaged equipment could take several weeks to replace, he said. A coordinated attack "could be devastating to the U.S. economy and security," he said. "We're talking months to recover. We're not talking days."

The industrial control system industry is years behind the IT industry in protecting cybersecurity, and some of the techniques used in IT security would damage control systems, Weiss added. "If you penetration-test a legacy industrial control system, you will shut it down or kill it," he said. "You will be your own hacker."

Part of the problem is that there are only a handful of control systems suppliers, and their architectures and default passwords are common to each vendor, Weiss said. In addition, there are probably fewer than 100 experts in control system cybersecurity worldwide, and U.S. universities don't have curriculums focused on control system cybersecurity, he added.

Attacks are coming from outsiders, but also from employees or former employees, Weiss said. "I believe the threat is increasing not only because of nation states ... but because the economic downturn has created many disgruntled but knowledgeable antagonists," he said.

Weiss gave three examples of cases involving disgruntled employees, including a recent case in California, where an employee disabled the leak detection systems in three oil derricks off the coast.

Senators called for an increased focus on cybersecurity in the U.S. government and private industry. "It's very important for people to know that cybersecurity is not just about protecting our government networks from countries with terrorists or hackers who want our secrets," said Sen. Jay Rockefeller, a West Virginia Democrat and committee chairman. "It's about protecting our nation's critical infrastructure from cyberattacks that could severely impact commerce and the economy, that are absolutely devastating."

Too many U.S. residents don't think or know about the ongoing cyberattacks, Rockefeller added.

However, James Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies, also called on Congress to focus on traditional IT security in addition to control systems. Right now, intellectual property in the U.S. is being compromised, and those losses will hurt the long-term competitiveness of the nation, he said.

While control systems represent a potential for attack, "we're under attack right now," Lewis said. "I worry more about the loss of information. Right now, we are being robbed by foreign entities of our most valuable technology, and we have to stop that."

Companies Get Checklist on PCI Security Rules

The organization that administers the credit card industry's data security rules has released a new set of compliance guidelines

By Jaikumar Vijayan, Computerworld

March 16, 2009 — Computerworld —

The organization that administers the credit card industry's data security rules has released a new set of compliance guidelines, a move that reinforces the widespread perception that efforts to comply are going slowly at many companies.

[PCI Security Standards Council LLC](#), which was set up by [Visa, MasterCard, American Express and other credit card companies in 2006](#), this month issued a 15-page document that details a "prioritized approach" for complying with the rules.

The new framework maps the 12 security controls mandated by the [Payment Card Industry Data Security Standard \(PCI DSS\)](#) to a list of six milestones. Bob Russo, the council's general manager, said the goal is to help companies that have yet to start on their PCI DSS compliance efforts and are wondering where to begin.

The first version of the security standard, which applies to all entities that accept credit and debit card payments, went into effect nearly four years ago. But many businesses still aren't fully compliant, said Jim Huguelet, a PCI consultant in Bolingbrook, Ill.

"I think there are a lot of [merchants who feel overwhelmed](#) at the amount of remediation [work] they need to undertake," Huguelet said. That, he added, has led to a state of "paralysis" in which companies either are doing nothing or are only implementing the easier PCI requirements, which by themselves do little to reduce the overall

threat of data breaches. The milestone-based framework finally gives those companies a template for moving forward, Huguelet said. "The journey of a thousand miles begins with a single step," he noted. "And the PCI [council] has now officially announced what those first steps should be."

Russo said the milestones are meant to provide an organized compliance methodology that ensures that the highest-risk issues are addressed first. In addition, a spreadsheet-based tool released with the framework can be used to plot progress against the milestones and to give auditors a snapshot of a company's compliance status.

The first milestone focuses on purging sensitive card-authentication data from systems and limiting the amount of information that companies collect and retain. Others revolve around network and application security, user access control and the protection of stored data.

Audit Report Issued on IRS

Posted by [Ralph DeFrancesco](#) Mar 18, 2009 9:47:58 AM

I love the fact that someone is auditing the Internal Revenue Service. I guess I have to be careful not to pick on the agency too much before my taxes are due, but I just can't help myself. Last week, Deputy Inspector General for Audit Michael Phillips issued four [recommendations](#) to the chief information officer of the IRS. The recommendations are so basic that if these people worked in industry, they would be fired for letting them happen. According to the report, the IRS is doing virus scans on 89 percent of its servers. Why wouldn't they scan 100 percent? Do they really need someone to tell them to scan 100 percent of their servers? The report went on to say that the auditors found that the reason was because the administrators failed to carry out this responsibility. My reaction is what "The Donald" Trump says, "You are fired!"

The second recommendation was that the administrators should not use their privileged accounts to access the Internet. During the week that the auditors monitored account use, 63 administrator accounts accessed the Internet a total of 820 times. I say: "Fired!"

The third recommendation I really had to laugh at. I'm sorry, but do you really need someone to tell you that when an employee blatantly violates IRS Internet access policies that you have to tell him or her? Isn't that a manager's job? To pour more salt into the wound, the IRS does not have a policy on how to deal with such rule-breaking. I know you are saying that I am enjoying this.

The last recommendation I have to agree with. Training users on proper computer, Internet, and e-mail use is very important. However, the IRS claims to have a training program in place that every employee and contractor must certify that they have taken on a yearly basis. This training, The IRS Information Protection Mandatory Briefing, includes a security-awareness refresher and covers common ways users can infect their system. I'm not sure what the problem is here.

I chose this topic for multiple reasons: first, to show readers that even large organizations that have money are no better off than any other organization. In other words, money won't fix all problems. Second, to show you that organizations suffer with similar problems. Granted, you would expect to see the problems outlined in smaller organizations. Finally, if this were to happen in industry, the people responsible would probably be fired or have to go before the audit committee and explain why it happened. I guess that's probably why no one was fired. There is no one holding these people responsible.

I guarantee that next year, or the year after, there will be more findings like this, or worse. We can only hope that now that [Vivek Kundra](#), the new federal CIO, is [back on the job](#) that he has the authority to fire people who do not follow some basic IT principles. However, I know that he will be too busy working on way more important projects rather than working on mundane problems like developing IT policies. If they are struggling with these

basic issues, it makes you wonder what other problems there are; and I just mean at the IRS. Don't be surprised if you see more break-ins on government servers, an increase in internal threats and more identity theft. I believe that this will happen because it's a year in transition. We have a new administration, a new federal CIO and soon a new federal CTO. Hackers know the best time to attack is in an atmosphere of change.

Perhaps the issue is that there is an assumption that IT is responsible for all of these points, rather than just the first one, and their information security/risk team (which needs to be independent of IT so it is NOT an IT Security team purely focussed on IT) being responsible for the rest, and that technology can fix the above issues.

IT do technology: they make it work and fix it when broken. They look after the businesses information on the IT systems and connect it all together. If they had a standard for scanning desktops and servers for viruses and other malicious code, with some input from their security team, and been audited against it, these issues would then have been identified and addressed a lot earlier - having audit points against you is a great way to focus minds on what needs looking at, and either accepting the actions, or explaining why action cannot/will not be taken and the resulting risk to the organisation.

Information security focusses on people and process, supported by technology, and looks at how the information needs to be secured, regardless of the medium. The last three issues you mention are primarily people issues.

An Information Security team would have a security policy, and supporting standards that would prohibit the use of administrative IDs for Internet access, and also an acceptable use standard that warns of disciplinary action when users breach it. (This would require the support of HR, but above all, senior management.)

Then it all needs wrapping up with an awareness and education programme that encourages/teaches the right behaviours so users follow good practice. It sounds as though the content of their current programme is either not up to scratch or that as there is no enforcement of any policy there is no reason for users to behave any differently.

A major cultural change is required there, and an increase in the political will to make these necessary changes happen.

NASCIO Says States Deal with Complex Array of IT Security Standards

Mar 25, 2009, News Report

"This brief should make clear that the standards environment for IT security is complex and dynamic." -- Michigan CIO Ken Theis, co-chair of the NASCIO Security and Privacy Committee (pictured)

The National Association of State Chief Information Officers (NASCIO) released a new issue brief: [Desperately Seeking Security Frameworks -- A Roadmap for State CIOs](#). The brief, a product of NASCIO's Security and Privacy Committee, maintains that CIOs, chief security officers and the IT security professionals who work with them face a challenging and sometimes confusing array of security frameworks that may be pushed down by federal agencies, issued by national or international standards bodies, promoted by industry as best practice, or in some instances, be written into law or federal regulation. *Desperately Seeking Security Frameworks* provides an overview of the primary security standards, regulations, and laws that impact state IT security programs, highlights how states have used the frameworks to shape their security architectures, policies, standards, and controls, and identifies the key issues for CIOs as they establish and maintain IT security programs.

"This brief should make clear that the standards environment for IT security is complex and dynamic," said Michigan CIO Ken Theis, Co-Chair of the NASCIO Security and Privacy Committee, "but I would underline the criticality of state CIOs selecting a security framework to drive their programs forward. The security of the digital infrastructure maintained by state IT programs makes this imperative."

Colorado CIO Mike Locatis, Co-Chair for the NASCIO Security and Privacy Committee added, "The infusion of federal dollars coming as a consequence of the American Recovery and Reinvestment Act puts significant new pressures on state IT programs to support recovery programs and services. It also increases the likelihood that the federal government will impose stricter security controls as part of broader concerns about transparency and accountability in the use of recovery monies. This heightens the need for states to understand existing and new IT security standards to ensure that their programs employ and integrate these as necessary."

4 Telecommuting Security Mistakes

A look at some common security no-nos committed frequently by mobile workers, and tips on how to stop them

By [Joan Goodchild](#), Senior Editor

March 25, 2009 — [CSO](#) —

According to figures released recently by the Nemertes Research Group, an Illinois-based research advisory firm, as many as 71 percent of U.S. companies offer full-time or part-time telecommuting to employees. Despite the large number of employees who work out of office, another recent study from The Center for Democracy and Technology found many continue to sideline the issue of telecommuting security in favor of more urgent needs.

Whether it is employees who travel frequently for their job or staff that work out of a home office full or part-time, their mobility poses serious security risks to your organization. CSO spoke with two security strategists about common mistakes employees often make while telecommuting, and asked for advice on how to put a damper on them.

Careless use of Wi-Fi and accessing unsecured networks

In research released late last year, Cisco polled more than 1,000 end users in 10 countries and found 12 percent of people who work out of the office regularly connect to a neighbor's wireless network when working at home. Another study from Accenture found one in seven Americans admit to "borrowing" Wi-Fi from an unsecured connection

"Today, this is very easy to do," said Ralph DeFrancesco, a computer science professor at Drexel University and consultant who helps companies assess and develop security programs. "You are sitting in a Starbucks or a Borders with your laptop and you need access to the Internet. You open your laptop and connect to the first unsecured network you find."

Firewalls will provide some protection against some malicious wireless intruders, but risks certainly still exist, said DeFrancesco, who recommends companies tell employees to limit their time on an unsecured network and use encryption, like PGP, whenever possible.

"What people don't realize is that hackers sit on these networks, or set up their own, and put password sniffers on them to capture passwords," he said. "I have had many friends that have noticed funny things with their personal e-mail and work accounts after connecting to an unsecured network."

Another thing to consider: In addition to the obvious risks this poses to an organization's sensitive data, it is also potentially illegal.

"The law is very vague here, but you could be committing fraud depending on the network," said DeFrancesco.

Letting family and friends use work-issued devices

It is a fairly common scene: An employee brings a laptop home and later that evening, that person's son or

daughter wants to use the device to surf the Web. But can you trust that what they are viewing and downloading is safe?

"I have entered environments where children's games were installed on machines, instant messaging and more," said Jason Hall, president of Stuart Hall Technologies, an Ambler, Pennsylvania-based consultancy. "Something like this can be addressed with local security settings. A user should not be an "administrator" of their machine."

Employees should be clear that the work-issued device is for their use only. And, keep in mind, computers and mobile devices aren't the only place where friends and family can cause problems. DeFrangesco shared a story of a friend with a son in middle school.

"The son was working on a project on his home computer and needed to bring it to school the next day to finish it in class. The father told his son he could have the USB drive in his brief case."

Unfortunately, the son took the wrong USB drive and lost several important documents his father needed for work.

"I know many companies where using USB drives is acceptable and encouraged to the point where they even buy the drives for their employees to use," said DeFrangesco. "I do not recommend or encourage the use of these drives."

If a company does allow employees to use USB drives, make sure the drive has security built in. If the drive does not have security, encrypt the data yourself, said DeFrangesco.

Altering security settings to view Web sites that have been blocked by the company

Cisco in its survey of end users also found more than half have changed the security settings on their company-issued laptop to view restricted Web sites. Those polled said they did so because they wanted to visit it regardless of their company's policy. Another find: 35 percent said it is none of their company's business if they have changed the security settings on their computer.

"I have to admit I have been guilty of this many times," admits DeFrangesco. "I do a lot of presentations and frequently need information or graphics for my slides, after gaining the proper permissions of course. However, when I find myself being blocked from a site, I often use a proxy to get around it. A proxy will act as a go between your computer and the site you want to connect to, fooling the filtering software from blocking you."

Both Hall and DeFrangesco point out that organizations can stop some of this activity by adjusting content filtering to block particular sites that allow the bypassing of a firewall or content filter. But, although IT is responsible for locking down these settings, the end-user still needs to be educated, said Hall.

"The end-user has to recognize the risk they pose on the organization and themselves," he said.

Both Hall and DeFrangesco recommend companies train users on proper computer usage and consider having them sign an acceptable use policy every year.

Leaving a work-issued device in an unsecured place

Several high-profile laptop theft cases have many organizations now looking at data loss prevention as a security priority. For example, in 2006, a laptop was stolen from the home of a Veterans Affairs employee. The employee had taken it to a private residence despite agency regulations which forbid this kind of activity. The theft resulted in the possible identity theft of 2.2 million active-duty military personnel. Last year, FEMA was in the news because of a lost laptop that contained the names, social security numbers, dates of birth, and phone numbers of flood victims that applied for federal assistance.

"I like using a laptop and I think they make sense for businesses to issue them to road warriors," said DeFrangesco.

His advice? "Encrypt. I know that I sound like a broken record, but it works and it's cost effective. A lot of encryption software is free today. Even though it is free, there still is a cost to deploy and support it. If you can't afford that cost, then don't issue laptops."

DeFrancesco also recommends tracking devices that can recover lost laptops and issuing cable locks.

Hall believes this is an area where the end user needs to be held most accountable.

"Leaving a laptop in an unlocked car is a user problem, not an IT issue."

China becoming the world's malware factory

By Robert McMillan

March 24, 2009 (IDG News Service) With China's economy cooling down, some of the country's IT professionals are turning to cybercrime, according to a Beijing-based security expert.

Speaking at the [CanSecWest security conference last week](#), Wei Zhao, CEO of Knownsec, a Beijing security company, said that while many Chinese workers may be feeling hard times, business is still booming in the country's cybercrime industry. "As the stock market dropped like a stone, a lot of IT professionals lost lots of money on the stock market," he said. "So sometimes they sell zero days," he said, referring to previously unknown software bugs.

"China is not only the world's factory, but also the world's malware factory," Zhao said.

China's red-hot economy has been hit by the global recession, and while the economy is still growing, technology companies such as Intel, Motorola and Lenovo have all laid off employees in China in recent months.

Last December, Chinese hackers found a previously undisclosed zero-day vulnerability in Internet Explorer. When employees of Zhao's company inadvertently published details of the bug on a public forum, Microsoft was sent scrambling to patch the issue.

Chinese hackers tend to focus on hacking software that runs on the desktop, rather than the server, because the underground market pays big money for client-side bugs, which are then often used to install malicious software on millions of desktops.

While recently investigating a single, but widespread attack, Zhao's researchers counted more than 4 million infected computers over a one-day period.

China has an estimated 250 million computer users, so attackers can do pretty well targeting only Chinese systems. "We have a huge amount of users and a very big local market," he said.

Hackers have had a lot of success launching widespread zero-day attacks against programs like RealPlayer and Adobe Flash, but they have also hit local Chinese programs, including Xunlei, QQ and UUSee.

Security is often little more than an afterthought for local software developers, Zhao said.

"In China, you have all this third-party software that's very popular, but which is much less secure than Microsoft software," said Wayne Huang, CEO of Web security consultancy Armorize, which has research labs in Taiwan. Not only are exploits for Chinese programs like QQ much easier to find -- software companies tend to take much longer to patch the exploits. "QQ is not going to be able to react as quickly as Microsoft," he said.

Cyberattacks in the region can be ingenious. Earlier this month, criminals redirected Taiwanese traffic to the tw.msn.com and taiwan.cnet.com Web sites using what's known as a [nonblind TCP spoofing attack](#).

In this attack, the hackers managed to compromise a switch in Singapore, the country where the Web sites were hosted, Huang said. They then monitored the switch for traffic and when they saw packets looking for the MSN and CNET Web sites, they sent back spoofed packets that redirected the victims to a malicious Web site, which launched attack code.

The attack lasted about 10 days, in part because security experts had such a hard time figuring out how it was working. "No attack that I have known has persisted for such a long time," Huang said.

He agreed that the economic downturn has had an effect on computer security. "People are more reluctant to disclose vulnerabilities because now they sell them," he said, and Chinese newsgroups are now awash with postings about hackers receiving large payouts for their exploit codes.

"I think the downturn has definitely made the crime scene a lot more active," he said.

Cyber Crime Profits Running Into Trillions of Dollars

VNUNet (03/27/09) ; Neal, David

The annual revenue from cybercrime now exceeds \$1 trillion, concludes Finjan's first quarter 2009 report. Finjan found that cybercrime is so profitable that a single rogue-ware network can bring \$10,800 a day, or \$39.42 million a year. AT&T chief security officer Edward Amoroso says the techniques cybercriminals are using are changing. "In the mid 1990s, attacks on the infrastructure were clumsy, or so sophisticated as to be admired, but they did not cause lasting damage," Amoroso wrote in a recent report. "But just as computing has advanced and evolved, so too has the frequency and form of attacks." Meanwhile, Finjan chief technology officer Yuval Ben-Itzhak says that cybersecurity threats have increased significantly over the past five years, and are now a threat to all types of organizations. Ben-Itzhak says the sour economy is forcing unemployed IT professionals to purchase and use crime-ware toolkits sold by hackers, and that some are choosing to use these toolkits against their former employers.

Companies Neglect Wi-Fi Network Security

Computer Weekly (03/27/09) ; Saran, Cliff

Nearly two in three large companies are relying on their wired security measures to protect their wireless local area networks (LANs), concludes a recent Motorola study. The study found that only 47 percent of companies are using Wi-Fi Protected Access (WPA) or Wired Equivalent Privacy (WEP) to deal with the risks and threats that are specific to LANs. More than half of the companies surveyed acknowledged that employees probably send sensitive company data over unsecured wireless networks, such as those found in coffee shops, but still only 30 percent require workers to use a wireless intrusion prevention platform. As employees become more mobile, they are likely to use their machines on vulnerable networks where a security "back door" is present, says Motorola's Amit Sinha. "Education is vital to improving wireless network security," he says. "Wireless introduced vulnerabilities in the corporate network that traditional security architectures cannot mitigate."

Survey Gauges Web Application Security Spending

IDG News Service (03/26/09) ; Kirk, Jeremy

More than one in four companies plan to increase Web application security spending in 2009 despite financial hardships, reveals a recent survey of IT security officers by Wireless Generation's Boaz Gelbord and White Hat chief technology officer Jeremiah Grossman. Gelbord and Grossman plan to carry out the benchmarking survey on a quarterly basis to compensate for the lack of data on corporate IT security spending. They say that firms save money by performing transactions online but run huge risks of costly data breaches that can lead to a loss of consumer confidence. Thirty-six percent of the 51 companies surveyed said they planned to maintain current levels of security spending. However, more than one in three companies said they do not use a firewall for their Web applications.

Smart Grid Will Only Be as Good as Security Behind It

Government Computer News (03/24/09) ; Jackson, William

Smart grid technology, which uses intelligent networking and automation to better control the transmission of electricity to consumers and create a more reliable and environmentally-friendly energy system, is vulnerable to cyberattacks, warns IOActive. The company says that smart grid technologies are prone to a number of security vulnerabilities, including protocol tampering, buffer overflows, rootkits, and code propagation. This is problematic

because some smart grid technologies make it possible to shut off a customer's power from a remote location or allow someone to access the rest of the electric grid. Despite these vulnerabilities, government and industry programs are only now beginning to develop security standards for smart grid technology. Nevertheless, the electric power industry is not holding up its effort to implement smart grid technology, says GridWise Alliance president Katherine Hamilton. IOActive CEO Joshua Pennell says progress in introducing smart grid technology does not need to be delayed as long as security issues are addressed quickly. However, he says that it will be difficult to address security problems after smart grid devices have already been deployed, and points out that smart grid technology is likely to be in place 40 to 50 years after it is implemented.

FBI: Internet Fraud Complaints Up 33 Percent

With attackers becoming more sophisticated, Internet crime complaints have jumped

By [Robert McMillan](#)

March 31, 2009 — IDG News Service —

2008 was the busiest year yet for online fraudsters according to an annual Internet Crime Report released Monday by the [U.S. Federal Bureau of Investigation](#).

The FBI's [Internet Crime Complaint Center](#) (IC3) logged more than 275,000 complaints last year -- a jump of 33 percent from the year before -- accounting for about US\$265 million dollars worth of losses, according to the center's 2008 Internet Crime Report.

Complaints to the IC3 had been dropping since 2005, but last year broke the previous record of 231,000. The median dollar loss per complaint was \$931. In 2007 it was \$680.

The jump in complaints isn't surprising. Computer security experts say that 2008 was a watershed year for cybercriminals as they perfected their techniques, building automated "SQL Injection" programs that could quickly place malicious attack code on thousands of Web sites, and running massive networks of botnet computers that could be used to steal sensitive information and infect other computers.

As in previous years, online auction fraud and nondelivery of merchandise accounted for more than half of the complaints, although auction-fraud complaints dropped more than 10 percentage points from 2007 levels.

Credit and debit card complaints were up in a year when two major payment card processors -- [Heartland Payment Systems](#) and [RBS WorldPay](#) were hacked. In 2007, credit and payment card fraud made up 6.3 percent of complaints. Last year, with even more complaints on the books, this kind of crime accounted for 9 percent of the total.

Most fraudsters use e-mail to reach their marks, and spam designed to steal sensitive financial information was "one of the more significant scams" the IC3 saw last year. In one new scam, the criminals sent messages doctored to look as though it had come from the FBI, asking for bank account information in order to help with a financial investigation. "Many of these e-mails also contain an element of extortion," the IC3 report states. "Recipients are told that if they do not comply with the FBI's request for information they will be prosecuted."

In another widespread scam, the criminals would hack into a victim's e-mail account and then send out messages to friends, claiming that they were stranded in Nigeria or some other foreign country and needed some quick cash to get out of a jam.

The IC3 data comes from the cybercrime victims themselves. It is then shared with law enforcement and regulatory agencies that use it to get a track on crime trends and to prosecute criminals.

Data Security: Whose Job Is It Really?

Forrester believes CISOs must revisit the need to centrally control data security

By Andrew Jaquith, Forrester Research

March 30, 2009 — [CSO](#) —

Forrester has a recommendation for CISOs struggling with how to secure corporate data:

Stop trying so hard.

Despite years of investments in technology and processes, protecting enterprise-wide data remains a maddeningly elusive goal for chief information security officers (CISOs). Software-as-a-service (SaaS), Web 2.0 technologies, and consumerized hardware increase the number of escape routes for sensitive information. Regulations, statutes, and contractual expectations drown CISOs in audit requests and ratchet up the pressure to do something about the problem. Hordes of vendors confuse CISOs with innumerable sales pitches.

Instead of beating your head against the wall, devolve responsibility to the business, keeping controls closest to the people who use the data. IT security should be primarily responsible only for deploying data protection technologies that require minimal or no customization.

Data-Centric Security Is More Important Than Ever—But Harder To Achieve

Today's regulatory climate forces IT security to comply with statutes such as Sarbanes-Oxley and HIPAA, industry-imposed security standards such as the PCI Data Security Standard (DSS), and an unending barrage of audit requests from key customers, banks, and auditors. From Boeing to Petrobras to The TJX Companies, daily newspaper headlines grimly announce the latest toxic data spills, causing increased customer scrutiny.

The pressure on IT security to secure enterprise data in all its forms has reached its breaking point. According to Forrester's Enterprise And SMB Security Survey, North America And Europe, Q3 2008, a huge majority of IT professionals—85 percent—worry about the loss of intellectual property. But IT security staffs are stretched thin and are increasingly challenged to solve an essentially unbounded problem. Organizations today face:

-- **Massively increased conduits for information flow.** Fifteen years ago, the most common Internet connection was the T1. Today, it is the OC-12—two orders of magnitude more bandwidth. Increasingly, mainstream technologies like virtualization are redrawing the lines between operating systems and the hardware they run on. And the adoption of non-owned IT assets continues apace. The confluence of outsourcing, SaaS, and unmanaged consumer gadgets ensures that IT security's grip on information has never been more tenuous.

-- **Consumerization of IT moves data beyond the reach of the CISO.** The increased use of Web 2.0 technologies such as blogs, social networking, and consumer-grade instant messaging increases the speed with which information moves outside of the enterprise. Worse, the pace of change of consumer gear tempts employees to ditch stodgy corporate hardware and bring their own gear to work—creating even more data worries.

-- **Too many vendor point products.** In considering solutions for securing data, enterprise CISOs are confronted with the tyranny of choice. Lost a laptop lately? Full-disk encryption will fix that. Employees promiscuously passing around payment card records? A dab of data loss prevention (DLP) will surely do the trick. The surfeit of solutions to narrowly defined technical problems ensures that the wish list only gets longer.

Confronted with these three challenges, some nervous CIOs and CSOs choose to throw the proverbial kitchen sink at the problem: [DLP](#), encryption-everywhere, enterprise key management, [network access control \(NAC\)](#), and employee education. However, this approach will fail because at its roots, the problem of data security stems from four sources: digital information was meant to move; information classification isn't ingrained into work processes; technical solutions aren't standardized; and accountable parties are too far from the controls.

Succeeding at data security means CISOs must define data security down: reset the commonly accepted definitions of what the problem is, who owns it, and what the solutions should be. That means:

1. Name the exact business content that requires tough security measures. Enterprises don't have "data security" problems or "intellectual property" problems, but they do have legitimate, spontaneous, sweat-inducing worries about the circulation of specific, named data assets such as earnings forecasts, product road maps, system passwords, financial models, and personally identifiable information about customers. Asking each part of the enterprise to name its most important digital assets is the first step. CISOs must push for business unit ownership, rather than taking the easy way out and making decisions on their behalf.
2. Put accountability where it belongs—with functional areas and business units. Responsibility for classifying information and restricting its flow is ultimately a business challenge, not a technical challenge. How documents, spreadsheets, and emails are used depends on workgroup and business unit preferences. So it is with data security.

That means that inside counsel owns email eDiscovery and retention, product engineering owns CAD drawings, and finance owns accounts and earnings projections. These groups know who should and should not have access and what should happen if their assets are misused. IT security's primary role should be to help source, design, and install the technical controls in place that will enable them to express and enforce their compartmentalization needs—not to be the gatekeeper.

3. Re-engineer the workplace so thinking isn't required. The most obvious and visible data threats to enterprises are employee-related: the loss of a laptop, disgruntled workers, theft of documents by thumb drive, or abuse of email. IT security's natural instinct is to be the wet blanket; instead, IT should seek to engineer environments that foster efficiency, impose no productivity burdens, and offer security as a side effect. Not all approaches will work everywhere, but honest discussions about the realities of how information is created and consumed will unearth solutions that centralized, tools-reliant approaches won't.

The net effect of these three priorities is to reshape the CISO's data security priorities. Instead of trying fruitlessly to be the enterprise's all-knowing content guardian, censor authority, and compliance guru, the CISO devolves responsibility of these activities to the business. IT security becomes a clearinghouse for data security tools that business groups can use as they see fit.

Data-Centric Security Means Devolution

Devolution means avoiding the trap of shelfware and stalled pilots and putting accountability where it belongs—with the business units. Forrester recommends three key steps CISOs should take to succeed:

Step one: Take ownership for basic data security tools. IT security should take the lead with tools that require no customization, such as laptop whole-disk encryption and terminal services. Both are relatively simple to implement and offer effective protection while not impeding productivity. In addition, IT security should offer data flow monitoring services to all business units.

Step two: Allow business units, not IT security, to drive business data protection initiatives. For tools like database encryption, port/URL blocking, and data loss prevention, IT security's role should be limited to providing expert advice, ensuring consistency by setting standards, and consulting with business units as they deploy solutions.

Step three: Rethink how users work. Accepted best practices for security programs rely heavily on end user education—perhaps too much. IT security should perceive gaps in information handling practices as opportunities to re-engineer the workplace. Rather than stress inordinately the necessity to "educate" employees on the need to think about security, IT security should focus on making controls no-load/no-think and inescapable. In particular, the enterprise should promote strategies that reduce the need for sensitive data on endpoint devices.

Succeeding at data security requires CISOs to abandon plans to control data access in a centralized manner. Devolution of data security responsibilities to business units is the key.

10 security threats to watch out for in 2009

Date: March 25th, 2009

Along with the explosion of new technologies, user habits, and social practices comes the inevitable wave of new security threats. Deb Shinder examines emerging vulnerabilities, from social networking to cloud computing to IP convergence.

We're well into the new year now, and we're beginning to see trends emerging on the security front. Some of the threats we'll see this year will be similar to those in years past (after all, many of the basic con games now being perpetuated online were around long before the advent of computers and the Internet). However, attackers are becoming much more sophisticated in their methods to circumvent the increased levels of security built into operating systems and applications. Here are 10 security threats that are likely to become more prominent in 2009.

1: Social networking as an avenue of attack

Social networking has experienced a boom in popularity over the last few years. It's now finding its way from the home into the workplace and up the generational ladder from the young folks into the mainstream. It's a great way to stay in touch in a mobile society, and it can be a good tool for making business contacts and disseminating information to groups. However, popular social networking sites have been the target of attacks and scammers. Many people let their hair down when posting on these sites and share much more personal data (and even company data) than they should.

Think you'll solve the problem just by blocking social networking sites on your company network? Not so fast. As Steve Riley pointed out in his recent talk on attack progressions at the 2009 MVP Summit, today's young professionals are growing up with social networking, and they expect to have it available to them at work just as older employees expect to be able to use their office telephones for reasonable, limited personal calls. In addition, you lose the business benefits of social networking if you shut it down completely. After all, companies didn't shut down e-mail because it could present a security threat. A better approach is to educate your workers about social networking practices and develop policies governing social media use.

2: More attacks on the integrity of the data

Another point Steve made in his presentation is that "First they came for bandwidth; now they want to make a difference." In the past, many attackers were looking for a free ride on your Internet connection (for example, by connecting to your wireless network and using it to access the Web, send e-mail, etc.). Then the nature of attacks progressed. Instead of the network being the target, it was the data. The next step was stealing data,

but step after that is even more insidious: the malicious modification of data (making a difference).

This can result in catastrophic consequences: personal, financial, or even physical. If a hacker changed the information in a message to your spouse, it could harm your marriage. If the change were to a message to your boss, you might lose your job. Changing information on a reputable Web site regarding a company's financial state could cause its stock prices to drop. A change to electronic medication orders on a hospital network could result in a patient's death.

3: Attacks on mobile devices

Laptop computers have presented a known security risk for many years. Today, we are more mobile than ever, carrying important data around with us not just when we go on business trips but every day, everywhere we go, on smart phones that are really just small handheld computers. These devices have important business and personal e-mail, text messages, documents, contact information and personal information stored on them. Many of them have 8 or 16 GB of internal storage and you can add another 32 GB on a micro SD card. That's much more storage space than the typical desktop computer had in the 1990s.

People lose their phones all the time, but many of these devices aren't configured to require a password to start the system, the data on them isn't encrypted, and very few protective measures have been taken. They are security disasters waiting to happen. Businesses should develop policies regarding the storage of company information on smartphones and require encryption of data on internal storage and on flash cards, strong passwords, use of phones that can be remotely wiped when lost, etc. Of course, you don't have to lose the phone to have its data stolen. Attention should also be paid to the potential for attacks using Bluetooth and Wi-fi.

4: Virtualization

Virtualized environments are becoming commonplace in the business world. Server consolidation is a popular use of virtualization technologies. Desktop virtualization, application virtualization, presentation virtualization — all of these provide ways to save money, save space, and increase convenience for users and IT administrators alike. If it's properly deployed, virtualization can even increase security — but that's a big "if." Virtualization makes security more complicated because it introduces another layer that must be secured. In essence, you now have to worry about two attack surfaces: the virtual machine and the physical machine on which it runs. And when you have multiple VMs running on a hypervisor, a compromise of the hypervisor could compromise all of those machines.

Another virtualization-related threat was demonstrated by the infamous Blue Pill VM rootkit. Hyperjacking is a form of attack by which the attacker installs a rogue hypervisor to take complete control of a server, and VM jumping/Guest hopping exploits hypervisor vulnerabilities to gain access to one host from another.

The easy portability of virtual images also presents a security issue. With modern virtualization technology,

VMs can be easily cloned and installed to a different physical machine. The ability to go back to “snapshots” of past images can inadvertently wreak havoc with patch management.

5: Cloud computing

If virtualization was last year’s buzzword, this year it’s all about “the Cloud.” The uncertain economy and tight budgets have companies looking for ways to lower operating costs, and outsourcing e-mail, data storage, application delivery, and more to cloud providers can present some attractive potential savings. Microsoft, IBM, Google, Amazon, and other major companies are investing millions in cloud services.

Cloud advocates envision a day when we’ll all use inexpensive terminals to access our resources that are located someplace “out there.” But when your data is “out there,” how can you be sure that it’s protected from everyone else “out there?” In fact, the biggest obstacle to moving to the cloud, for many companies and individuals, is the security question. [IDC recently surveyed 244 IT executives and CIOs](#) about their attitudes toward cloud services, and 74.6% said security is the biggest challenge for the cloud computing model.

Google, a prominent player in the cloud space, is the subject of a recent complaint to the Federal Trade Commission (FTC) by the Electronic Privacy Information Center (EPIC), which seeks [a suspension of Google’s cloud computing services](#) until verifiable safeguards are established.

6: More targeted attacks on non-Windows operating systems

Although Windows still has 91% of the desktop OS market, there has been a big push in some quarters to deploy Linux or Macintosh as a supposedly more secure alternative. But are they really? One reason the non-Windows operating systems have enjoyed fewer attacks is the simple fact that the Windows installed base presents a much bigger target for attackers. Just as terrorists prefer to attack large gatherings of people where they can do the most damage, so do hackers prefer to write malware that will spread to the greatest number of computers — and that means Windows.

However, as other systems get more publicity and become more popular, they also become more attractive to the bad guys. Malware has been becoming less Windows-centric for the last few years; the 2007 Open Office worm, for example, infected Linux and Mac OS X systems as well as Windows. And [Charlie Miller](#), a security researcher who won a recent hacking contest by breaking into a fully patched MacBook in a few seconds, said, “Hacking into Macs is so much easier. You don’t have to jump through hoops and deal with all the anti-exploit mitigations you’d find in Windows.”

Whatever the reality, the perception is that non-Windows operating systems are becoming more popular as Apple steps up its advertising campaign and vendors offer more netbooks preinstalled with Linux. As they become more high profile, look for hackers to spend more time and energy creating attacks that target non-Windows systems.

7: Third-party applications

Microsoft has put tremendous effort into securing the Windows operating system and its popular productivity applications, such as Microsoft Office. Linux and Mac receive regular security updates. As operating systems become more and more secure, attackers will focus less on OS exploits and more on application exploits. The major Web browsers are routinely updated to patch security vulnerabilities. But the vendors of many third-party applications are less security-aware. This is especially true of freeware applications written by independent developers. These programs, which may not have been written with security in mind to begin with and which do not automatically check for and download security updates, present an opportunity that we can expect attackers to take advantage of.

8: Side effects of green computing

Green computing is all the rage today, and saving energy is certainly a good thing — but as with beneficial medications, there can be unexpected and unwanted side effects. Recycling computer components, for instance, can expose sensitive data to strangers if you don't ensure that hard drives have really been wiped cleaning. (Hint: Deleting files or even formatting disks doesn't guarantee that the data is gone.)

On the other hand, such green initiatives as powering down systems that aren't in use can actually enhance security, since a computer that's turned off isn't exposed to the network and isn't accessible 24/7.

9: IP convergence

Convergence is the name of the game today, and we are seeing a melding of different technologies on the IP network. With our phones, cable TV boxes, Blu-ray players, game consoles, and even our washing machines connected to the network, we're able to do things we never even imagined a decade ago. But all of those devices on an Internet-connected network present myriad "ways in" for an attacker that didn't exist when only our computers used IP.

We can only hope that the manufacturers of all these devices put security at the forefront; otherwise, we may see a rash of new malware targeting vulnerabilities in our entertainment devices and household appliances.

10: Overconfidence

Perhaps the greatest threat to the security of our networks, whether at work or at home, is overconfidence in our security solutions. Many home users believe that as long as they have a firewall and antivirus installed, they don't have to worry about security. Businesses tend to put too much faith in the latest and greatest security solutions. For example, there is an assumption that biometric authentication is infallible and undefeatable — but it can be compromised in various ways, and when it is, the legitimate user it was meant to protect becomes the victim. If the system shows that *your* fingerprint was used to log on, you may be presumed guilty, and an investigation might not even be deemed necessary.

Another type of overconfidence is common among home users and in the business environment, especially with small companies. That's the idea that "We don't have anything worth hacking into so we don't need to

worry about security.” In today’s interconnected world, neglecting security doesn’t just put you at risk; it also puts others at risk. Your systems could be used as zombies to attack a whole different network.

End users on a business network often think of security as somebody else’s problem and operate on the assumption that the IT department is taking care of them, so they don’t have to do anything about security.

Overconfidence of any type is a dangerous security threat — but it’s one that you can most easily do something about because it doesn’t require expensive technology or sophisticated technical skills — just a change in attitude. We all have a responsibility to keep our own systems as secure as possible.

Security policies need simplifying, expert says

By Robert Westervelt, News Editor
26 Mar 2009 | SearchSecurity.com

BOSTON -- Company security policies are often unfocused and get in the way of overall business objectives. The result is a hodgepodge of security rules frequently ignored by end users and ultimately an increased risk of data leakage, said Charles Cresson Wood, a consultant at InfoSecurity Infrastructure Inc., a Mendocino, Calif., consultancy.

Wood urged attendees at SecureWorld Boston Expo, Wednesday, to conduct a thorough review of company security policies, simplifying and focusing them to be more consistent with business needs.

"Policies are supposed to be the glue that holds everything together in a cohesive fashion," Wood said. "Management needs to support it ... and psychologically the whole environment needs to be fostered around valuing security."

Companies are increasingly neglecting security policies and failing to enforce them resulting in apathetic employees, Wood said, pointing out a study of 890 IT professionals conducted by the Ponemon Institute in 2007. The study found that 87% of those surveyed used USB sticks to carry company information even though company policy prohibited them from doing so. Another 46% said they routinely share passwords with colleagues, despite two-thirds of them knowing that security policies prohibit password sharing.

Ignored security policies destroy businesses, Wood said pointing to Chicago-based Arthur Anderson LLC which never recovered from its shoddy accounting practices uncovered during an investigation of the Enron scandal. Employees there ignored Arthur Anderson's document retention and destruction policy.

"This was a fraction of their problems in the area of implementing information security policies," Wood said.

Having and maintaining a document is not enough. Sound policy needs to be refined over time to adjust for regulatory requirements, business strategy changes and risk assessments, Wood said.

"We haven't done the basics well," Wood said. "It's time and money well spent for you to go back and review your policies. The payoff for doing this is high."

Among the best practices cited by Wood is to conduct an annual risk assessment and tie it into the company security policies; uniquely tailor policies to the organization's risk profile; and create a culture of quality control whereby being in compliance with security policies is highly valued.

In the future, violations of policy could become much more visible, Wood said. Security systems are already becoming more proactive rather than defensive and business processes will continue to become more automated, he said.

"The average time of a violation of policy and the discovery of that violation will come down rapidly," he said.

Wood also envisions a new series of regulations much like Sarbanes-

Oxley. The regulations would be tailored toward data protection and privacy. The rules would require CEOs and other top business executives to sign off that security controls are in place. Wood also said security controls could be monitored by an appliance, much like that of a black box on an airplane, to allow investigators to track down missteps that led to a data breach. "Security policy used to be a one-size-fits-all approach, but now you need your policy to support your business in the years ahead," Wood said.

Stimulus Bill Includes First (and Maybe Only) Federal Data Breach Notification Law

Posted by [Lora Bentley](#) Mar 26, 2009 12:00:13 PM

Among tax cuts and credits, more bailout funds and restrictions on executive pay packages, the American Recovery and Reinvestment Act ([ARRA](#)) also includes a section that introduces the first federally-mandated data breach notification law.

As I've written [before](#), Title XIII of ARRA, also known as the Health Information Technology for Economic and Clinical Health Act (HITECH Act) reserves \$22 billion to "advance the use of health information technology" so that we will be able to meet President Obama's goal of moving to e-health records by 2014.

The HITECH Act also expands the reach of HIPAA data privacy and security requirements to include the "business associates" of those entities (health care providers, pharmacies and the like) that are subject to HIPAA, and [strengthens HIPAA enforcement](#) measures. All are significant changes to HIPAA compliance.

Of particular interest to industry observers, however, is the fact that the HITECH Act includes data breach notification requirements for protected health information. Though several states have data breach notification laws covering information used in identity theft (Social Security Numbers, credit card numbers, banking information, etc.), only a few have extended such notification laws to health information. And the federal government has never addressed the issue. Until now.

And the fact that Congress chose to address it in the HITECH Act, specifically where health care information is concerned, makes some wonder if this may be the only federal legislation we see on data breach notifications. In other words, the fact that Congress had the opportunity to craft a broader data breach notification law and didn't could mean that its members are content to let various state laws control.

Goodwin Procter counsel Jacqueline Klosek told me recently:

"People thought that eventually there would be a federal law that would supersede and kind of help out because there is such a tremendous number of state laws that companies have to consider every time there's a breach, but that didn't happen... I think it kind of came out of nowhere. Boom -- we all of a sudden have a federal breach notification law, but it's not really what we had expected in that it only applies to health information. I'm more skeptical now [that there will be a broader federal law]."

The fact that Congress chose to limit the requirements to health information also complicates matters for companies that operate in several states. They are already subject to the various state data breach notification requirements, which can be different and at times inconsistent. And those will still apply to information other than in the health arena. So those companies can't simply come up with a form letter that will work for every breach.

New Senate Bill Proposes Mandatory Security Standards and Certifications

(1st April 2009) A new bill, sponsored by Senators John D. Rockefeller IV and Olympia J Snowe, would see the introduction of a new cyber security czar, the National Cybersecurity Advisor, who would report directly to the White House. Included in the bill is the granting of authority to the National Cybersecurity Advisor to isolate computer networks that are part of the critical network infrastructure, including those in the private sector, should there be a cyber attack. The bill would also see the introduction of mandatory security standards, developed by the National Institute of Standards and Technology, applied to both private and public sector organizations that control parts of the critical network infrastructure. Included in the bill is the proposal that a licensing and certification program be introduced for cyber security professionals.

[Editor's Note (Schultz): Like it or not, mandatory security standards are inevitable in the US at some point in time. Without them, the US will continue to have too many weak links in its critical computing infrastructure.

(Northcutt): This is a fairly ambitious bill. We need to be aware of it and decide what parts we want to support, which parts might need more discussion. This seems to be a first step at professionalization for security workers as well.]

EU Calls For Development of Strategy to Protect European Cyber Space

(31st March 2009) The European Commission has called for the development of a strategy to protect Europe from disruption to critical networks resulting from cyber attacks or natural disasters. The EC highlights that the region is becoming more and more dependent on the continuous availability of IT and communications systems for supporting electronic commerce and for playing a crucial role in the management of other critical services such as transportation and the supply of food, energy and water. The strategy highlights the cyber attacks against Estonia and calls for a minimum standard of preparedness that organizations in the public and private sector in all member states should reach in order to ensure the overall security of the region.

Report: Cybercriminals have penetrated U.S. electrical grid

Hackers look to map power grid and install malware for possible attacks, *Journal* says

By Grant Gross

April 8, 2009 (IDG News Service) Cyperspies from China, Russia and elsewhere have gained access to the U.S. electrical grid and installed malware tools that could be used to shut down service, according to a story published today by *The Wall Street Journal*.

Thus far, the attackers haven't used their access to damage the electrical grid, but the [cyberespionage](#) appears to be "pervasive," the [Journal reported](#), citing anonymous national security officials. Federal officials are worried that the cyperspies could use their access to try to shut down the grid or take control of power plants during a time of crisis or war, the story said.

Many of the intrusions, which for now appear to be aimed mostly at mapping the domestic power grid, were discovered not by electric utilities but by U.S. intelligence agencies, the story added.

The cyperspies have left behind software tools that could be used to destroy components of the grid, one intelligence official told the *Journal*. "If we go to war with them, they will try to turn them on," that official was quoted as saying.

U.S. lawmakers and some security analysts have raised concerns for several years about the [security of the power grid](#) and other industrial control systems.

In 2007, for example, a [simulated attack](#) done by the Idaho National Laboratory for the U.S. Department of Homeland Security showed that a known software vulnerability in a Supervisory Control and Data Acquisition, or SCADA, system could be used to destroy power grid equipment.

There also have been previous disclosures of actual hacking incidents involving electrical grids, both in the U.S. and abroad. Early last year, the CIA said that cybercriminals had been able to [launch online attacks](#) that disrupted power equipment in several regions outside of the U.S.

And at a congressional hearing in March, Joseph Weiss, managing partner of Applied Control Solutions, claimed that networks controlling industrial control systems in the U.S. have been breached more than 125 times in the past decade, with one incident resulting in deaths.

A coordinated attack on critical infrastructure systems "could be devastating to the U.S. economy and security," Weiss said at the hearing. "We're talking months to recover. We're not talking days."

Other security experts have raised concerns that the electrical grid could become more vulnerable as it is transitioned into a two-way smart grid, potentially using the Internet for transmission. The federal government included \$4.5 billion for smart-grid deployment as part of the [economic stimulus package](#) approved earlier this year.

IOActive Inc., a Seattle-based security consultancy, has spent the past year [testing smart-grid devices for security vulnerabilities](#). The company said last month that it had discovered a number of flaws that could enable hackers to access networks and cut power.

Brian Ahern, president and CEO of Industrial Defender Inc., a vendor of security tools for control systems, also voiced concerns about the power grid in an interview before the *Journal* story was published.

"One of the challenges that we have today in this country is that you've got all this critical infrastructure that has been deployed over the last 20 years, and no one was even thinking about security," Ahern said. "When you think about our existing infrastructure today — power plants, transmission distribution systems — they all have their own security problems. That's what we're all working diligently on right now: making sure that our existing infrastructure is secure."

Growing Threat From Cyber Attacks: US General **Agence France Presse (04/07/09)**

General John Davis, the deputy commander of the joint task force for global operations, told Agence France-Presse in a recent interview that U.S. government and commercial networks are facing a growing threat from cyber attacks. Davis noted that such attacks can be anything from simple hacking attempts by teenagers to extremely sophisticated assaults on networks. He added that although the U.S. military has taken steps to protect its networks from such attacks, it is still somewhat vulnerable because many of its systems use the commercial infrastructure. Davis also discussed a number of other issues related to cyber security, including the worm that made its way onto military networks several months ago. According to the general, the Defense Department spent more than \$100 million over the past six months repairing the damage done from that and other cyber attacks. Davis also praised Defense Secretary Robert Gates' plans to provide funding to train an additional 170 cyber experts each year.

Internal Report Contradicts Interior's Claims That Systems Were Secure **NextGov.com (04/02/09) ; Nagesh, Gautham**

A year-old report from the Interior Department's inspector general is being used by lawyers representing American Indians in a case against the government for allegedly leaving U.S. citizens vulnerable by not adequately protecting department networks. The May 2008 report by former Interior inspector general Earl Devaney said the department's IT governance "is ineffective, costly, wasteful and lacks accountability." The department responded to the multi-billion dollar lawsuit filed April 1 in a U.S. District Court by saying it has drastically improved its information security since the report was released. The internal report described Interior's IT management issues as "urgent." The Interior's CIO said in 2008 that unless the department took swift action, it would fall further behind and become completely ineffective. An Interior employee who wished to remain anonymous because of the sensitivity of the issue said Interior Secretary Dirk Kempthorne formed an action

committee to address IT problems after receiving the report from Devaney, but never followed up on its progress.

Training Needed to Quell Breaches

Network World (03/31/09) ; Schurr, Amy

The greatest corporate security threats often happen at the hands of employees who lose machines or unintentionally compromise corporate data, concludes CompTIA's annual survey of IT security trends. These errors hinder worker productivity and ultimately threaten a company's bottom line. CompTIA says that more employee training is needed to increase awareness about proper usage of laptops, cell phones, and removable drives. "End users are exposed to new IT security threats every day," says CompTIA's Tim Herbert. "Security threats grow along with the expanding reach of IT so non-IT employees need to be continually trained on the latest IT security threats." The study's results showed an unexpected drop in the number of businesses providing IT security training to employees. Of the 553 information security professionals surveyed, only 45 percent said their firms provided security training to non-IT staff, down from 53 percent in 2007.



