

ESO - Security Trends Report

02/10

DDoS Attacks Are Back (and Bigger Than Before)

By Bill Brenner

January 13, 2010 08:48 PM ET

CSO - [Distributed denial-of-service \(DDoS\) attacks](#) are certainly nothing new. Companies have suffered the scourge since the beginning of the digital age. But DDoS seems to be finding its way back into headlines in the past six months, in thanks to some high-profile targets and, experts say, two important changes in the nature of the attacks.

The targets are basically the same -- private companies and government websites. The motive is typically something like [extortion](#) or to disrupt the operations of a competing company or an unpopular government. But the ferocity and depth of the attacks have snowballed, thanks in large part to the proliferation of botnets and a shift from targeting ISP connections to aiming legitimate-looking requests at servers themselves.

In fact, said Andy Ellis, CSO of Cambridge, Mass.-based Akamai Technologies, the botnets launching many of today's DDoS attacks are so vast that those controlling them probably lost track of how many hijacked machines they control a long time ago. (Listen to the full interview with Ellis in [The Long, Strange Evolution of DDoS Attacks](#).)

Ellis has been watching the trend from a pretty good vantage point. Many people use Akamai services without even realizing it. The company runs a global platform with thousands of servers customers rely on to do business online. The company currently handles tens of billions of daily Web interactions for such companies as Audi, NBC, and Fujitsu, and organizations like the U.S. Department of Defense and NASDAQ. There's rarely a moment -- if at all -- when an Akamai customer IS NOT under the DDoS gun.

"We see a lot less of the fire-and-forget malware-based attacks designed to bog down the machines that were infected," Ellis said, referring to old-school worm attacks like [Blaster](#), Mydoom and Code Red. "Now the malware is used to hijack machines for botnets and the botnets themselves are used as the weapon."

In the last year, Akamai has seen some of the largest DDoS attacks in recent memory, which Ellis described as "huge attacks of more than 120 gigabytes per second." If you are on the receiving end of that much punch, Ellis said, "It's not a pleasant place to be."

A [massive attack last July 4 weekend was a good example](#) of this. In that onslaught, a botnet of some 180,000 hijacked computers hammered U.S. government Web sites and caused headaches for businesses in the U.S. and South Korea. The attack started that Saturday, knocking out websites for the U.S. Federal Trade Commission (FTC) and U.S. Department of Transportation (DOT). [US Bancorp, the nation's sixth-largest commercial bank](#), also took a direct hit. Attackers have also targeted the likes of Google, Yahoo! and Amazon.com. Attacks against Google didn't last long, but when one considers that [Google content accounts for about 5 percent of all Internet traffic](#), the prospect of more sustained attacks affecting some of the Internet's biggest brands is sobering.

Paul Sop, CTO of Prolexic Technologies, has seen the botnet effect on DDoS attacks from his perch, where about 30 engineering staffers spend all their time studying the problem. "We've built an IP Reputation database that tracks non-spoofed IP addresses that attack our customers, and the list now tracks about 4 million infected computers," he said. "What is surprising is how many botnets there are, and how easy it is to build new ones."

Increasingly, he said, his company is seeing layer-7 attacks to HTTP, HTTPS, and DNS services. These attacks don't punish the user's ISP connections. Instead, they punish the servers and are far more difficult to identify and stop, especially as the individual bot behavior becomes less aggressive and tries to act like legitimate user traffic.

Most attacks his team observes can be best classified as competitive sabotage of corporate entities.

"In certain high-stakes markets like online gambling, which is very popular in Asia, there is fierce competition and quite a lot of DDoS," he said. "Politically-motivated attacks are becoming more popular and we've protected many news and media outlets both large and small. Usually it's just a news item that foreign hackers find offensive, but sometimes, as in the case of the Democratic Voice of Burma, the attacks could be said to be more state sponsored, or at least, state approved."

In a just-released report on botnet-generated DDoS attacks, Prolexic noted that attackers are quickly tweaking their botnets to make attack traffic look increasingly similar to legitimate, routine traffic.

"Instead of the huge burst of traffic that marks when an attack begins, traffic will begin to ramp up slowly as bots join the attack at random intervals with each bot varying its attack style, making it increasingly difficult to separate real users from bots," the report said.

Protect your company from social engineering

What you need to know about this most insidious of security attacks

By Joan Goodchild

January 11, 2010 03:45 PM ET

CSO - You've got all the bells and whistles when it comes to network firewalls and your building's security has a state-of-the-art access system. You've invested in the technology. But what about the staff?

Social engineers, or criminals who take advantage of human behavior to pull off a scam, aren't worried about a badge system. They will just walk right in and confidently ask someone to help them get inside. And that firewall? It won't mean much if your users are tricked into clicking on a malicious link they think came from a Facebook friend.

In this guide, we outline the common tactics social engineers often use, and give you tips on how to ensure your staff is on guard.

What is social engineering?

Social engineering is essentially the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password.

Famous hacker Kevin Mitnick helped popularize the [term 'social engineering'](#) in the '90s, although the idea and many of the techniques have been around as long as there have been scam artists of any sort.

How is my company at risk?

Social engineering has proven to be a very successful way for a criminal to "get inside" your organization. In the example given above, once a social engineer has a trusted employee's password, he can simply log in and snoop around for sensitive data. Another try might be to scam someone out of an access card or code in order to physically get inside a facility, whether to access data, steal assets, or even to harm people.

Chris Nickerson, founder of Lares, a Colorado-based security consultancy, conducts 'red team testing' for clients using social engineering techniques to see where a company is vulnerable. Nickerson detailed for CSO how easy it is to get inside a building without question.

In one penetration test, Nickerson used current events, public information available on social network sites, and a \$4 Cisco shirt he purchased at a thrift store to prepare for his illegal entry. The shirt helped him convince building reception and other employees that he was a Cisco employee on a technical support visit. Once inside, he was able to give his other team members illegal entry as well. He also managed to drop several malware-laden USBs and hack into the company's network, all within sight of other employees.

How do social engineers pull off their tricks?

Criminals will often take weeks and months getting to know a place before even coming in the door or making a phone call. Their preparation might include finding a company phone list or org chart and researching employees on social networking sites like LinkedIn or Facebook.

But once they are ready, knowing the right thing to say, knowing whom to ask for, and having confidence are often all it takes for an unauthorized person to gain access to a facility or sensitive data, according to Nickerson.

The goal is always to gain the trust of one or more of your employees. In *Mind Games: How Social Engineers Win Your Confidence* Brian Bushwood, host of the Internet video series *Scam School*, [describes](#) some of the tricks scam artists use to gain that trust, which can vary depending on the communication medium:

On the phone:

A social engineer might call and pretend to be a fellow employee or a trusted outside authority (such as law enforcement or an auditor). According to Sal Liferi, a 20-year veteran of the New York City Police Department who now educates companies on social engineering tactics through an organization called Protective Operations, the criminal tries to make the person feel comfortable with familiarity. They might learn the corporate lingo so the person on the other end thinks they are an insider. Another successful technique involves recording the "hold" music a company uses when callers are left waiting on the phone.

In the office:

"Can you hold the door for me? I don't have my key/access card on me." How often have you heard that in your building? While the person asking may not seem suspicious, this is a very common tactic used by social engineers.

In the same exercise where Nickerson used his thrift-shop shirt to get into a building, he had a team member wait outside near the smoking area where employees often went for breaks. Assuming this person was simply a fellow-office-smoking mate, real employees let him in the back door with out question. "A cigarette is a social engineer's best friend," said Nickerson. This kind of thing goes on all the time, according to Nickerson. The tactic is also known as tailgating. Many people just don't ask others to prove they have permission to be there. But even in places where badges or other proof is required to roam the halls, fakery is easy, he said.

"I usually use some high-end photography to print up badges to really look like I am supposed to be in that environment. But they often don't even get checked. I've even worn a badge that said right on it 'Kick me out' and I still was not questioned."

Online:

Social networking sites have opened a whole new door for social engineering scams, according to Graham Cluley, senior technology consultant with U.K.-based security firm Sophos. One of the latest involves the criminal posing as a Facebook "friend." But one can never be certain the person they are talking to on Facebook is actually the real person, he noted. Criminals are stealing passwords, hacking accounts and posing as friends for financial gain.

One popular tactic used recently involved scammers hacking into Facebook accounts and sending a message on Facebook claiming to be stuck in a foreign city and they say they need money.

"The claim is often that they were robbed while traveling and the person asks the Facebook friend to wire money so everything can be fixed," said Cluley.

"If a person has chosen a bad password, or had it stolen through malware, it is easy for a con to wear that cloak of trustability," he said. "Once you have access to a person's account, you can see who their spouse is, where they went on holiday the last time. It is easy to pretend to be someone you are not."

Why do people fall for social engineering techniques?

People are fooled every day by these cons because they haven't been adequately warned about social engineers. As CSO blogger Tom Olzak points out, [human behavior](#) is always the weakest link in any security

program. And who can blame them? Without the proper education, most people won't recognize a social engineer's tricks because they are often very sophisticated.

Social engineers use a number of psychological tactics on unsuspecting victims. As Bushwood outlines in *Mind Games*, successful social engineers are confident and in control of the conversation. They simply act like they belong in a facility, even if they should not be, and their confidence and body posture puts others at ease.

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

Social engineers will also use humor and compliments in a conversation. They may even give a small gift to a gate-keeping employee, like a receptionist, to curry favor for the future. These are often successful ways to gain a person's trust, said Bushwood, because 'liking' and 'feeling the need to reciprocate' are both fixed-action patterns that humans naturally employ under the right circumstances.

Online, many social engineering scams are taking advantage of both human fear and curiosity. Links that ask "Have you seen this video of you?" are impossible to resist if you aren't aware it is simply a social engineer looking to trap you into clicking on a bad link.

Successful phishing attacks often warn that "Your bank account has been breached! Click here to log in and verify your account." Or "You have not paid for the item you recently won on eBay. Please click here to pay." This play plays to a person's concerns about negative impact on their eBay score.

"Since people spend years building eBay feedback score or 'reputation,' people react quickly to this type of email. But, of course, it leads to a phishing site," said Shira Rubinoff, founder of Green Armor Solutions, a security software firm in Hackensack, New Jersey. "Many people use eBay, and users often bid days before a purchase is complete. So, it's not unreasonable for a person to think that he or she has forgotten about a bid they made a week prior."

Recent phishing lures even take advantage of the economic downturn, said Rubinoff. It has not been uncommon for fake emails to turn up that claim to be from human resources which say: 'You have been let go due to a layoff. If you wish to register for severance please register here,' and includes a malicious link.

No one wants to be the person that causes problems in this economy, so any email that appears to be from an employer will likely elicit a response, noted Rubinoff. Lares' Nickerson has also seen cons that use fake employer emails.

"It might say, 'In an effort to cut costs, we are sending W-2 forms electronically this year,'" said Nickerson.

How can I educate my employees to prevent social engineering?

Awareness is the number one defensive measure. Employees should be aware that social engineering exists and also aware of the tactics most commonly used.

Fortunately, social engineering awareness lends itself to storytelling. And stories are much easier to understand and much more interesting than explanations of technical flaws. Chris Nickerson's success posing as a technician is an example of a story that gets the message across in an interesting way. Quizzes and attention-grabbing or humorous posters are also effective reminders about not assuming everyone is always who they say they are.

"In my educational sessions, I tell people you always need to be slightly paranoid and anal because you never really know what a person wants out of you," said Lifrieri. The targeting of employees "starts with the receptionist, the guard at the gate who is watching a parking lot. That's why training has to get to the staff."

Social engineering tricks are always evolving, and awareness training has to be kept fresh and up to date.

Security Manager's Journal: Conficker worm just keeps on coming

By J.F. Rice

January 11, 2010 11:20 AM ET

Computerworld - Many people are worried about H1N1 this flu season, but I'm more concerned about a different kind of virus right now. My company is dealing with an outbreak of the Conficker worm, which uses some fairly sophisticated techniques to evade detection and removal. Meanwhile, some cleverly designed spam is getting past our filters as well. Both of these problems are examples of evolving network threats that present some challenges to the security team.

How did we get infected by Conficker? [Computerworld has reported that this worm is infecting 50,000 computers every day](#) and [as of October had passed the 7 million-victim milestone](#). Some observers say that number will double by the end of this month. The worm takes advantage of a [Microsoft](#) security hole that, if not patched, leaves computers open to infection.

In my company, the use of USB thumb drives is prevalent, and the worm is infecting these portable storage devices and taking advantage of the autorun feature of Windows to spread. It then proceeds to take over the processor, shut down services and generally make the infected computer unusable. Of course, there's a patch for that (the worm has been around for over a year, and so has the patch), and Microsoft's removal tool for malicious software can clean it -- but as always, patching needs more attention in my company. I still maintain that a good patching program would save us a lot of time and trouble, since we would have to expend only a little bit of effort upfront while avoiding a lot of work later in cleaning up problems. What's more, regular patching creates a generally more stable environment. But it will take time to get there. In the meantime, we have to deal with this outbreak.

The Conficker worm has gotten a lot of press, having infected some high-profile organizations such as military organizations and government agencies around the world. It uses some fairly sophisticated techniques to contact its controllers, avoid detection and spread itself, as well as random-seeming Web sites to update itself. It propagates via USB drives, networks and peer-to-peer software. It's easy to get, and hard to kill.

So, we've been chasing this annoying beastie, and cleaning it when we find it, but it keeps coming back. It's a persistent bug. Of course, when something like this happens, it helps my case by focusing attention on the importance of patching and proactive security measures, but that makes me feel slightly guilty, as if there should have been more I could have done to avoid the situation in the first place. I think it's unfortunate that it sometimes takes a security incident to get people to realize the risks the business is taking.

At the same time, a couple of spam messages are regularly getting through our filters. One claims to be from the Internal Revenue Service, trying to trick people into clicking a link to either deal with an IRS fine or get a refund, and the other uses the tried-and-true technique of telling users they must execute a program to get the latest emergency security update.

We have a third-party spam-filtering service, which until now has had almost 100% effectiveness. When these messages started getting through, I called our provider and found out that these particular messages are hard to block. They are sent by botnets, collections of computers infected with malware not unlike Conficker. And yes, a few of our users have actually fallen for these scams. Given our spam-filtering service's inability to block all of these messages, I'm left with few options other than educating our users about spam, so that's what I'm doing. I'm running an educational campaign to help people understand what phishing scams look like and how to avoid them - and as an experienced security manager, I find myself surprised to find people still falling for these old tricks in this day and age. I think people know enough to be generally suspicious, but when they are promised a tax refund, the instinct to take advantage of easy money outweighs common sense. Live and learn, I guess.

EMPLOYEE BACKGROUND SCREENINGS UP DRAMATICALLY

TONI BOWERS - JANUARY 13TH, 2010

ACCORDING TO THE **WORKFORCE MANAGEMENT** SITE, BECAUSE OF THE EXPLOSIVE GROWTH IN THE BACKGROUND SCREENING INDUSTRY DURING THE PAST DECADE, CRIMINAL CREDIT CHECKS OF JOB CANDIDATES ARE BECOMING NEARLY UNIVERSAL. THEY ESTIMATE THAT 16 PERCENT OF EMPLOYERS NOW SCREEN THEIR EXISTING EMPLOYEES ON AN ONGOING BASIS (THAT'S UP FROM 12 PERCENT A YEAR AGO).

HIRERIGHT, A BACKGROUND SCREENING PROVIDER BASED IN IRVINE, CALIFORNIA, CONDUCTED A STUDY IN WHICH THEY SURVEYED 1,411 EMPLOYERS OF ALL SIZES FROM MORE THAN 15 INDUSTRIES. THEY FOUND THAT:

- 93 PERCENT OF EMPLOYERS REPORT THAT THEY RUN CRIMINALITY CHECKS, UP FROM 85 PERCENT IN 2008.
- 84 PERCENT OF EMPLOYERS CONDUCT COMPREHENSIVE SCREENING BEFORE THE FIRST DAY OF WORK; 8 PERCENT SCREEN IMMEDIATELY AFTER THE START.
- 10 PERCENT OF EMPLOYERS REPORT THAT SCREENING ADVERSELY AFFECTS THE HIRING DECISION IN A STAGGERING 50 PERCENT OR MORE OF THE CASES.
- 71 PERCENT OF EMPLOYERS REPORT THAT THEIR ORGANIZATION CONDUCTS SCREENING TO "REDUCE RISK TO THE ORGANIZATION"; 68 PERCENT SAY THE PURPOSE IS TO "ENSURE A SAFER WORKPLACE."
- EMPLOYEE SCREENING USED TO HAPPEN MORE COMMONLY IN CERTAIN INDUSTRIES, BUT THE PRACTICE IS BECOMING MORE WIDESPREAD ACROSS INDUSTRIES.

IS IT LEGAL?

THOUGH MANY EMPLOYERS SAY THEIR ORGANIZATIONS CONDUCT SCREENING TO REDUCE THE RISK TO THE ORGANIZATION OR TO ENSURE A SAFER WORKPLACE, MANY ARE USING THE SCREENINGS TO WHITTLE DOWN LONG LISTS OF JOB APPLICANTS. IN ESSENCE, THEY ARE USING CRIMINAL RECORDS OR POOR CREDIT HISTORIES TO MAKE CHARACTER JUDGMENTS AGAINST JOB CANDIDATES WHEN THERE IS NO JOB-RELATED OR BUSINESS NECESSITY.

WHETHER YOU BELIEVE THE RESULT OF A SCREENING IS A CORRECT PREDICTOR OF BEHAVIOR AND PERFORMANCE OR NOT, THE ACT OF SCREENING FOR THAT PURPOSE IS COMING UP AGAINST NEW LEGISLATIVE RESTRICTIONS AND LEGAL CHALLENGES.

FOR EXAMPLE, ON OCTOBER 1, 2009, THE EQUAL EMPLOYMENT OPPORTUNITY COMMISSION (EEOC) FILED A DISCRIMINATION LAWSUIT AGAINST FREEMAN COS., A CORPORATE EVENTS MARKETING COMPANY THAT IT CLAIMS HAS REJECTED JOB APPLICANTS BASED ON THEIR CREDIT HISTORY AND

IF THEY HAD CRIMINAL CHARGES IN THEIR BACKGROUND. THE EEOC SAYS THESE EXCLUSIONARY PRACTICES ARE NOT JOB-RELATED OR JUSTIFIED BY BUSINESS NECESSITY.

ARE THE RESULTS INDICATIVE OF EMPLOYEE PERFORMANCE?

ACCORDING TO WORKFORCE MANAGEMENT, EEOC HEARINGS ON SCREENING PRACTICES IN NOVEMBER 2008 INCLUDED EXPERT TESTIMONY THAT THE RESULTS ARE *NOT* GOOD PREDICTORS OF EMPLOYEE BEHAVIOR OR PERFORMANCE. IN ADDITION TO GREATER EEOC SCRUTINY OF CRIMINAL RECORD SCREENING PRACTICES, A GROWING NUMBER OF STATES NOW PROHIBIT OR LIMIT PRE-EMPLOYMENT ARREST INQUIRIES.

NEW TECHNOLOGIES

ONE OF THE REASONS EMPLOYEE SCREENING IS BECOMING SO WIDESPREAD IS THAT THERE ARE A SLEW OF TECHNOLOGIES, INITIALLY USED BY ANTI-TERRORISM AND POLICE INTERROGATION, NOW AVAILABLE TO PRIVATE-SECTOR EMPLOYERS. FOR EXAMPLE, SUSPECT DETECTION SYSTEMS LTD., AN ISRAELI SECURITY COMPANY, IS NOW MARKETING ITS COGITO "HOSTILE INTENT" DETECTION TECHNOLOGY TO EMPLOYERS.

THERE'S EVEN A FREE **IPHONE APPLICATION** THAT LETS USERS CONDUCT BACKGROUND SCREENING ON ANY PERSON IF THE USER INPUTS BASIC PERSONAL INFORMATION. SO EVEN IF YOU'RE NOT BLABBING ABOUT YOUR EVERY PERSONAL EVENT ON FACEBOOK OR TWITTER, YOUR LIFE COULD BE AN OPEN BOOK.

Hacking takes lead as top cause of data breaches

Business sector was the most likely to suffer a breach

[PC World Staff](#)

09 January, 2010

Hacking has topped human error as the top cause of reported data breaches for the first time since such tracking began in 2007, according to the Identity Theft Resource Center's 2009 Breach Report.

In its [report](#), titled "Data Breaches: The Insanity Continues," the non-profit ITRC found that 19.5 percent of reported breaches were due to hacking, with insider theft as the second most common cause at 16.9 percent. For the past two years, "data on the move," a typically human-error loss of a portable devices such as laptops or even briefcases, was the most common reported cause.

The ITRC is careful to note that its statistics are based on incomplete data, as differing laws and practices among different states mean that some breaches are not reported publicly, and the cause of the breach is not listed for about one third of those that are reported.

But according to the data available, the number of reported data breaches dropped since 2008, but was still more than in 2007. Last year, there were 498 breaches recorded by the ITRC, with [657 in 2008](#) and 446 in 2007.

With 41.2 percent of reported breaches, the business sector was the most likely to suffer a breach. But "the

financial and medical industries, perhaps due to stringent regulations, maintain the lowest percentage of breaches," according to the report.

The ascendance of hacking as the prime data breach cause underscores a troubling point. As the ITRC report states, a data breach does not equal identity theft. A state might require a company to report a lost laptop with sensitive data as a data breach, particularly if the data was foolishly stored unencrypted. But that data might never be used for nefarious purposes, and might simply be ignored or even deleted by the laptop's finder or thief.

On the other hand, a hacker specifically wants the data, likely for identify theft and [financial fraud](#). The insider theft category also represents someone intentionally going after valuable data, according to ITRC founder Linda Foley. Taken together, these two categories account for 36.4 percent of those breaches with known causes, while those with human error causes comprise 27.5 percent.

That doesn't bode well for the safety of our data.

Smartphones need smart security practices

Yes, it's 'blue and plays music,' but that cute smartphone is also a serious computer that must be secured

By Mary Brandel

January 18, 2010 06:00 AM ET

Computerworld - As vice president of IT at Windsor Foods in Houston, Stephan Henze has to stay one step ahead of the latest IT trends. That's why he's spending a lot of time thinking about securing and deploying smartphones enterprisewide. The company had only a few-dozen smartphones just a short time ago, but IT now manages about 100 of them, and Henze foresees substantial growth in the near future.

The task of securing smartphones keeps getting hairier, Henze says, while the company's need for mobile communications grows stronger, even on the shop floor, where maintenance engineers will soon receive automatic SMS alerts on their phones.

He's not sure he can continue to enforce the company policy of supporting only Windows Mobile-based phones, yet nonstandard devices will complicate his [security efforts](#). He is well aware that for some people, a smartphone is a fashion statement. "With PCs, I was able to tell them we're not a Mac environment, but I'm not sure I can do that with phones down the road," he says.

Henze is among a growing number of IT and security leaders grappling with the challenge of securing these increasingly popular devices. The primary concern, of course, is the risk of exposing sensitive data if a phone or removable memory card is lost or stolen. Data can also be exposed if a phone is sold or sent in for repairs without its memory first being erased.

There's also the risk that VPN-connected devices could expose corporate networks to hacker and malware intrusions. And there's a growing potential for viruses to attack the phones themselves through SMS hacks and other exploits. "If I take your device and muck around with it, what if the VPN is set up on it?" asks Philippe Winthrop, an analyst at consultancy Strategy Analytics Inc. "It's a huge risk not being dealt with enough today."

10 smartphone security risks

Here's a look at 10 common smartphone security risks, with tips for dealing with them from Gartner analyst John Girard:

1. No configuration management plan.

Tip: Responsibility for managing smartphones should be given to the same staffers who provision and manage PCs.

2. No power-on password, or a weak password policy.

Tip: Several vendors' device management consoles allow you to configure password complexity rules and password reset questions and answers.

3. No inactivity timeout/auto-lock.

Tip: Timeout policies should be enforced over the air through your device management console, so that the enterprise can maintain near-real-time control.

4. No auto-destruct/data-wiping plans.

Tip: Two methods should be used: over-the-air commands and locally initiated wipes. The latter should occur after a password has been entered incorrectly a certain number of times or when a device has been off the network for a predefined amount of time.

5. No memory encryption rules.

Tip: Major enterprise smartphone operating systems provide settings for enforcing encryption.

(continues on next page)

Complicating matters, users are apt to view smartphones as their own personal gadgets, not something IT should control. "There's a deep underlying current of 'This is my mobile device,' " says John Girard, an analyst at Gartner Inc. A user will often see his smartphone as something that's "blue and plays music," not as an asset that needs to be secured, he says.

Smartphones' multimedia capabilities raise other concerns, Girard says. For instance, company policy might prohibit moving corporate documents to external media, but is there a policy that governs using a smartphone to take photographs in the office or record meetings?

Many companies try to take control by purchasing standard phones for employees -- a move that at least enables them to support just a single operating system. But even then, users may adhere to the standard only loosely, says Paul DeBeasi, an analyst at Burton Group. "I see employees who have the company phone in their left pocket and their personal phone in their right," he says.

Indeed, in a recent study of 300 companies in the U.S. and Europe by Good Technology Inc., a vendor of mobile security and management tools, nearly 80% of the respondents reported an increase in the number of employees who wanted to bring their own devices into the workplace in the past six to 12 months, and 28% reported a data breach because of an unauthorized device.

Despite all of the security risks, "two out of three organizations are struggling in terms of not only defining but enforcing IT and business policies around mobility," Winthrop says.

Girard concurs that companies have been slow to realize the implications of a phone-related data breach. "If clients do call and ask about phones, they're asking me to render an opinion that reduces their liability for employees using smartphones, [rather than] trying to do something to improve security," he says. "I'm waiting for the level of concern to grow up and match what exists for PCs."

And it should. Whether companies buy smartphones for employees or just allow their use, it's the company that's liable if data gets exposed, Winthrop says.

Technology to centrally secure and manage smartphones, whether via a third-party platform or from smartphone vendors themselves, does exist. Most analysts agree that, among smartphone vendors, [BlackBerry](#) maker Research In Motion Ltd. (RIM) and Microsoft Corp., with its latest version of Windows Mobile, provide the best management platforms.

For other devices -- or for companies that support phones from multiple vendors -- there are a variety of options, including management software from vendors such as Credant Technologies, Good Technology, Sybase, Trust

Digital, Trend Micro and MobileIron, among others. Key capabilities offered by such platforms include centralized control of the following:

- Password management.
- Authentication authorization.
- Strong encryption.
- Inactivity timeout, in which users are logged out of an application session after a specified period of inactivity and are prompted for a password to restart.
- Remote wiping of memory if a device is lost or stolen or if the user enters his authentication credentials incorrectly a given number of times.

Central control

At Robinson Lerer & Montgomery LLC, CIO Jeff Saper has approached the security challenge by standardizing on the BlackBerry, which is issued to all employees at the New York-based strategic communications firm. Saper uses several of the 450 wireless IT policies and commands provided by BlackBerry Enterprise Server. The firm has also used Good Technology's platform to handle Palm and Treo devices, but Saper turned exclusively to BlackBerries when he decided to keep things consistent on a single platform.

10 smartphone security risks

(continued from previous page)

6. No master plan for backup and synchronization.

Tip: Use a secure, over-the-air backup-and-restore tool that performs periodic background synchronization.

7. No e-mail-forwarding barriers.

Tip: Forwarding of e-mail and attachments can be regulated with server-side settings of a corporate e-mail system, and additional filtering is available through commercial data loss prevention filters.

8. No application certification rules.

Tip: Private keys can be used to restrict which applications are allowed to install or execute.

9. No default browser permission rules.

Tip: Choose browser default settings that comply with company policy when phones are provisioned, to avoid providing an entry point for malicious code.

10. No plan for dealing with smartphone diversity.

Tip: Set a policy that defines what levels of support different devices will receive. Assign smartphone support to a single IT group.

Security measures include inactivity timeouts after 10 minutes of nonuse, and remote wiping of the devices if there is any fear of data compromise following a loss or theft, or if the password is entered incorrectly more than 10 times. "Even if someone could hack the password, it's safe," Saper says.

Most important, he says, users can't disable any of the security functions.

With remote wiping, it's important that data is backed up to the BlackBerry server so that it can be restored, Saper says. He can restore message history too, because the server ties into Microsoft Exchange. Such backups can make clear what data is on a device and hence what would be vulnerable if the phone were stolen, Girard points out.

While other platforms can perform remote wipes, the BlackBerry server also provides confirmation that the wipe was accomplished, which would give a company a stronger position if a case involving a smartphone data breach ended up in court, he says. "If you can't prove you did the wipe, it doesn't sound good," he adds.

Girard also believes it's important to set devices to time out after periods of inactivity. He recommends setting inactivity timeouts at one to five minutes for devices with high-value information, no more than 10 minutes for those with medium-value data and no longer than 15 minutes for those with low-value information. To resume using the device, employees should have to re-authenticate by entering a strong password.

That's easier said than done. "Because it's mobile, people think it's supposed to be easy, and they resist having to type in a seven- or 12-digit code," Girard says. "But you can't just have a four-digit code, because there's a very real chance of someone observing you typing it in."

Girard has also had clients who allow more than 10 password retries before deactivating a device. That's a highly questionable policy. "Even if you're drunk, you should be able to get in after that many tries," he says.

Christopher Barber, CIO at San Dimas, Calif.-based Western Corporate Federal Credit Union (Wescorp), supports two devices, the BlackBerry and Apple Inc.'s [iPhone](#) 3G. The iPhone runs e-mail and a relationship management application used by salespeople. To secure the iPhones, Barber set up a standard security profile that includes all the safeguards he wanted, with Microsoft Exchange Server pushing it out to the devices.

He uses RIM's Enterprise Server for the BlackBerries. Security features include strong password protection, encryption and remote kill capabilities.

Data out the door

"Our biggest concern with any smartphone is [that] it acts as a storage device," Barber says. "Users can plug it into the USB, download company files and walk out the door with them." With the global profile, however, he can enforce password strength and encryption, so even if users do put sensitive data on a portable device, there is a reduced chance of someone else accessing it if the phone is misplaced or stolen.

Lax smartphone security

Only 23% of smartphone owners use the security software installed on the devices. (*Source: Trend Micro Inc. survey of 1,016 U.S. smartphone users, June 2009*)

Taking a centralized approach to encryption is key, Girard says. All the well-known vendors have an encryption feature for their phones, "but unless the company takes enterprise control, it's strictly optional," he says.

But Barber says that securing smartphones is a matter of managing risks, not covering every base. He says he recently saw a YouTube video of someone who used a hacking program to break into an iPhone that was password-protected and encrypted. He also says the iPhone's removable SIM card is a vulnerability, because if a thief removes the card, the phone won't be able to receive a remote kill command because it won't be able to connect to the corporate network.

To offset this risk, Barber relies on a combination of policy and education.

"We train everyone not to put sensitive data on the iPhone," he says. In the future, he hopes to back that up with data loss prevention technology, which would monitor data being moved into an e-mail attachment or USB drive. "We're as comfortable as we can be, but there's always risk."

At Windsor Foods, Henze has also gone the centralized management route, using MobileIron's Virtual Smartphone Platform. The decision was based on his desire to manage not just security from one platform, but also carrier contracts and deployment. In addition, while he has standardized on Windows Mobile devices, he wanted to be sure he wasn't locked into that decision. MobileIron supports BlackBerries and iPhones and plans to support Symbian and [Android](#) devices.

Henze started with the basics, such as password management, auto-disable and remote wipe, but is adding centralized encryption. The platform also backs up applications and data on the phones and reports on configuration and memory utilization, which speeds troubleshooting. It also takes inventory of applications stored on the phones and disables any that aren't approved.

Henze also notes that the help desk manages the smartphones rather than a senior network engineer. In fact, a portal enables users to check on their phone usage and even perform tasks such as remote wipes and configuration themselves. "The [MobileIron] appliance makes it easier from an IT perspective," he says.

For Henze, the work of smartphone security has just begun. For instance, he's considering integrating digital rights management with the smartphone management platform.

"Let's say a person working with us has a laptop full of confidential information, and he gets terminated," Henze says. "With digital rights management, the device would check in with the authentication server to see if he's still a legitimate user, and if he isn't, he wouldn't be able to read those files anymore." This works better than remote wipe, he says, because if files are stored on a removable card, there is no way to delete them.

There have been concerns from some users about the Big Brother aspect of having IT monitor their phones. However, this concern is outweighed by the fact that IT can provide better service when it comes to new phone deployments, replacements and remote troubleshooting, Henze says. For instance, IT will be able to configure a new phone right after it's purchased, rather than taking three or four days. "They'll be up and running in no time, and when that happens, they'll appreciate it," Henze says.

In the end, there's no single means of maintaining security as more and more smart phones enter the enterprise, whether they're issued by the company or brought in by employees. But what's certain, says Winthrop, is that you can't just give employees free rein. It's not uncommon for IT to allow individuals to be responsible for their own devices, or even encourage the idea. But in the end, he says, it's the employer that's liable if data gets leaked.

"There's a fascinating issue here, in that employees don't think too long or hard about which laptop they're going to get," Winthrop says. "But they're absolutely going to ask 'Why did or didn't they give me a BlackBerry?' or 'Why can't I bring in my iPhone?' or 'I wonder if I can get a [Palm] Pre?' " But even if organizations want to cater to every user's desire, he says, they need to take into account the need to manage the devices and the information that passes through or is stored on them.

In fact, smartphones should be viewed not as phones, but as PCs that happen to make phone calls, Winthrop says.

According to Henze, that notion has turned the world inside out. "In the old days, there was the Internet, the intranet and the internal corporate network," and each was distinct from the other. But today, with miniature yet powerful mobile devices carrying data wherever a person can go, "the egg is scrambled," Henze says. "Data sits wherever, and it's much more difficult to get ahead of it."

Lincoln National Warns Customers of Potential Data Security Breach

(January 14 & 15, 2010)

Lincoln National Corp. has begun notifying about 1.2 million customers of an incident that may have compromised the security of their personally identifiable information. The Financial Industry Regulatory Authority (FINRA) learned of the breach last August when an unidentified source provided the organization with a username and password that allowed access to Lincoln's portfolio management system. An investigation conducted by Lincoln found other instances of shared usernames and passwords at one of its subsidiaries. The shared passwords were established a decade ago to perform administrative activities. All shared access information has been changed. The management system in question is not used to conduct transactions, but does contain Social Security numbers (SSNs), account numbers and balances and other personal information valuable to identity thieves.

[Editor's Note (Pescatore): While the high profile targeted attacks got all the press coverage, *this incident is indicative of the types of problems (shared passwords, weak internal practices) that cause way more material damage to businesses in the long run.* Lincoln National did the right thing in taking the very expensive step to notify customers even though there is no evidence that any compromise actually occurred. The cost of avoiding

this incident (detecting and stopping the use of shared administrative passwords) would have been a small fraction of the cost of going through this disclosure event.]

UK ICO Will Have Authority to Levy Fines Up to GBP 500,000 (US \$817,000)

(January 14, 2010)

As of April 6, 2010, the UK Information Commissioner's Office (ICO) will have the authority to fine organizations up to GBP 500,000 (US \$817,000) for violations of the Data Protection Act. The level of the fine in each case will be determined by the seriousness of the breach as assessed by the ICO. Factors that will be taken into account will include whether the breach was deliberate or accidental, how much distress the exposure of information caused, and what measures the organization had in place to prevent the breach.

Minimize Risk by Maximizing Accountability

Risk management only works when it factors into everyone's thinking. Kerri Grosslight of Wells Fargo lays out steps for getting there.

By Kerri Grosslight, risk management and compliance, Wells Fargo

January 14, 2010 — [CSO](#) —

Faced with challenging economic times and heightened legislative and regulatory scrutiny, companies across all industries are increasingly compelled to keep risk management top of mind. Success depends upon customer and shareholder confidence in a company's [ethical standards](#) and its ability to make prudent decisions about handling risks. Whether a company's risk management framework is centralized, decentralized, or somewhere in the middle, what's most important are the *people* in that framework—those who identify and manage risks every day.

Only through a culture of accountability, in which it's clearly understood that risk identification and management is everyone's responsibility, can a company truly meet its risk management and compliance commitments and deliver for its customers and shareholders.

As a first step toward building a culture of accountability, an assessment of the company's risk management model and framework is essential. Ensure that everyone knows who's responsible for understanding and addressing risks in each part of the organization. From a divisional or business line perspective, who is responsible for executing against corporate policies and understanding what the business needs to do to adhere to the policies, including training and awareness? Who aggregates and looks at risk holistically? It's critical to know these things, because the accountability model starts with every employee understanding the potential risks that cross his or her desk.

All leaders must understand the risks in the businesses for which they're accountable and risk professionals must support employees and managers in risk mitigation. Beyond that, enterprise oversight is crucial so that risk is aggregated across the organization—this is particularly important if business groups are siloed.

As a next step, CSOs and other personnel in charge of risk activity need to acknowledge and address potential blind spots—the areas of concern or potential threat that can be missed if one is not careful. Even the strongest cultures have them. Blind spots include:

- The familiar sense that "It can't happen to us." To counteract it, continuously be aware of the fact that bad things can and do happen, and be on the lookout for potential risks.

- When a leader must communicate his or her own mistakes or those made externally, there's often a reluctance to deliver this news; it may be equated to a sense of failure or punishment. Instead, open communication should be viewed as an opportunity to share risk awareness and help others avoid similar pitfalls.
- If business groups are siloed, there's often a lack of transparency across the organization when risks arise. As mentioned above, an aggregated, enterprise view of risk trends and patterns is necessary, allowing business decision makers to connect the dots across the company, share risk awareness, and avoid one-off solutions.
- When employees aren't clear about an organization's risk tolerance, they may get mixed messages around risk, which can be a real danger to a culture of accountability. A lack of clarity and insight around risk leads to assumptions that could negatively impact business or a tendency to take on more risk than is prudent.

As a next step toward building a culture of accountability, companies need to emphasize to managers at all levels of the organization the importance of role-modeling behavior. This includes ensuring that those responsible are helping employees identify and take responsibility for the risks that cross their desks. At the same time, leaders must remind employees that there are no penalties for bringing forward risks—it's when issues are not brought forward that can lead to damaging consequences. When employees do bring forward risks, it is important to make certain managers demonstrate how to address the risk, learn from it, put into place the appropriate action plans, and shore up gaps so that the same, or similar, issues do not arise again.

Finally, it is critical to communicate broadly and often to create awareness of blind spots and to help employees understand that risk management is everyone's responsibility - just talking about it makes a difference. Encourage leaders to cascade information through their teams, have critical conversations about risk on an ongoing basis and instill a mindset where people feel that their roles matter. For example, leaders can use communication channels that employees recognize and trust, whether it's e-mail, newsletters, video clips, or town hall meetings.

Also remember that keeping teams and business partners informed and building trust with them by sharing what you can, as soon as you can, minimizes potential roadblocks to success. It is also critical to offer forums in which employees can identify and share "bright ideas" —simple, everyday actions that will help everyone better identify and manage risk. This type of proactive activity also reminds employees that leadership doesn't profess to have all the answers and that employees really are the first line of defense. Perhaps most important, leaders need to ensure that they communicate success stories, which helps make risk management real for employees.

Whatever an organization's risk management model looks like, remember that instilling and reinforcing the right culture is foundational to effective risk management and helps protect customers and shareholders. Everyone has a responsibility for risk management, and with the right culture, everything else falls into place.

Hackers are defeating tough authentication, Gartner warns

(Computerworld, 1/18/10)

Security measures such as the use of one-time passwords and phone-based user authentication -- considered among the most robust forms of IT defenses -- are no longer enough to protect online banking systems against fraud, a Gartner Inc. report warns. Cybercriminals are using increasingly sophisticated tactics to outmaneuver security systems so they can steal customers' log-in credentials and pillage their bank accounts, according to Gartner analyst Avivah Litan, who wrote the report.

Trojan horse programs lurking inside a customer's Web browser can steal one-time passwords and immediately transfer funds, or intercept a transaction between a bank and a customer and make changes unbeknownst to the user or the bank, Litan said. In cases where a bank uses a phone-based, "out of band" authentication system, criminals use call forwarding so that the fraudster, not the legitimate customer, gets the call from the financial institution, Litan said.

Social Engineering is seen as the primary attack vector

(TMCnet.com, 1/17/10)

With the rise of polymorphic threats and the explosion of unique malware variants in 2009, the industry is quickly realising that traditional approaches to antivirus, both file signatures and heuristic/behavioural capabilities, are not enough to protect against today's threats. The IT industry has reached an inflection point where new malicious programs are actually being created at a higher rate than good programs. As such, the industry has also reached a point where it no longer makes sense to focus solely on analysing malware.

Social Engineering is now seen as the primary attack vector as more attackers are going directly after the end-user and attempting to trick them into downloading malware or divulging sensitive information. Social engineering's popularity is at least in part spurred by the fact that what operating system and Web browser resides on a user's computer is largely irrelevant, as it is the actual user being targeted, not necessarily vulnerabilities on the machine. Social engineering is already one of the primary attack vectors being used today, and Symantec estimates that the number of attempted attacks using social engineering techniques is sure to increase in 2010.

Report: ISPs Fear Many More DDoS Attacks in 2010

Internet service providers are worried about increasingly sophisticated attacks on cloud-based services, according to new survey from Arbor Networks

By [Joan Goodchild](#)

January 19, 2010 — [CSO](#) —

Heading into 2010, Internet Service Providers (ISPs) are most worried about botnet-driven distributed denial-of-service (DDoS) attacks, according to a report released Tuesday.

Attacks are shifting to cloud-based services and nearly 35 percent of service providers believe that more sophisticated service and application attacks pose the largest operational threat in the next 12 months. Large scale botnet-enabled attacks came in second at 21 percent. The surveyed was conducted by Arbor Networks, a Massachusetts-based network security firm. The firm surveyed 132 IP network operators around the world for their fifth annual security report. All survey participants are directly involved in network security operations at their respective organizations, according to Arbor Networks.

The poll also found more than half of the surveyed providers reported growth in service-level attacks at one gigabit or less bandwidth levels.

"Such attacks are also driven by botnets and are specifically designed to exploit service weaknesses, like vulnerable and expensive back-end queries and computational resource limitations," the report states.

Several ISPs reported prolonged, multi-hour outages of prominent Internet services during the last year due to application-level attacks. These service-level attack targets included distributed domain name system (DNS) infrastructure, load balancers and large-scale SQL server back-end infrastructure, the report said.

Over the last six years, service providers reported a near doubling in peak DDoS attack rates year-to-year. Peak attack rates grew from 400 Mbps in 2001 to more than 40 Gbps in 2007. However, officials noted providers reported a peak rate of only 49 Gbps in the most recent report, which is lower than the 22 percent growth over the previous year.

The report also points to a convergence of issues, or a "perfect storm," that are facing the Internet architecture and operations community, including looming IPv4 address exhaustion and the preparedness for migration to IPv6, DNSSEC and to 4-byte ASNs.

"Any one of these changes alone would constitute a significant architectural and operational challenge for network operators; considered together, they represent the greatest and potentially most disruptive set of circumstances in the history of the Internet, given its growth in importance to worldwide communications and commerce."

Users Still Make Hacking Easy with Weak Passwords

In a report likely to make IT administrators tear out their hair, most users still rely on easy passwords, some as

By Jaikumar Vijayan

January 21, 2010 — Computerworld

In a report likely to make IT administrators tear out their hair, most users still rely on easy passwords, some as simple as "123456," to access their accounts.

A report released today by database security vendor Imperva Inc. serves as another reminder of why IT administrators need to enforce strong password policies on [enterprise](#) applications and systems.

Imperva's report is based on an analysis of 32 million passwords that were exposed in a recent database intrusion at [RockYou Inc.](#) a developer of several popular Facebook applications. The passwords belonged to users who had registered with RockYou and had been stored by the company in clear text on the compromised database. The hacker responsible for the intrusion later posted the entire list of 32 million passwords on the Internet.

An analysis of that list provides the latest confirmation that a majority of users still don't care about the strength of their passwords if they are left to choose on their own.

According to Imperva, about 30% of the passwords in the hacked list were six characters or smaller, while 60% were passwords created from a limited set of alpha-numeric characters. Nearly 50% of the users had used easily guessable names, common slang words, adjacent keyboard keys and consecutive digits as their passwords.

In fact the most common password among RockYou users was "123456" followed by "12345" and "123456789." The other passwords rounding out the top five were "password" and "iloveyou."

Many of the top 5,000 passwords in the list were identical to those found in password dictionaries, which are used by hackers to brute force their way into accounts, said Amichai Shulman, chief technology officer at Imperva. On average, a malicious attacker using such a password dictionary would have been able to break into a RockYou account at the rate of roughly one every second using an automated password guessing tool, he said.

Imperva's report is by far not the first to highlight the tendency by many to use easily hackable passwords for online accounts. What sets it apart, however, is the sheer size of the sample that was analyzed for the report. Though the passwords in this case only controlled access to a relatively low-value user account, previous studies have shown that users tend to use the same password for multiple accounts, including corporate and financial accounts.

The Imperva report comes at a time when malicious attackers are [increasingly going after user credentials](#) to break into enterprise networks.

Last November, for instance, the FBI's Internet Crime Complaint Center noted that cybercrooks had attempted to steal approximately \$100 million from U.S. banks using stolen log-in credentials. On average, the FBI is seeing several new cases opened each week, the complaint center said. In most instances, the crooks used sophisticated keystroke-logging Trojan horse programs to steal login credentials from company employees authorized to initiate funds transfers on behalf of the business, the FBI noted.

Such attacks are highlighting the need for stronger access control and user authentication measures. For IT administrators, the main takeaway is the need for them to enforce a strong password policy over applications that they own, Shulman said. "If you let the user choose at their convenience, they will choose weak passwords," he said.

Companies should also consider implementing controls for slowing down brute-force attacks, in which attackers try breaking into an account by trying to guess the password using an automated tool. Putting obstacles such as CAPTCHAs (Completely Automated Public Turing Test to Tell Computers and Humans Apart) in the way of a brute-force attacker are a good way to slow them down, the Imperva report noted.

Administrators also need to enforce a periodic password change policy and encourage users to create harder-to-crack passphrases instead of passwords, the report said.

Incomplete Data Breach Reporting Makes Tracking Hacks Tough, Organization Says

Jan 20, 2010, By [Hilton Collins](#)

Cyber-security's always a hot topic because people always worry about keeping data safe, but concerned parties may be missing out on the whole story when it comes to how many, or how few, data breaches happen at any given time.

The Identity Theft Resource Center (ITRC), an organization that collects information about data breaches from media sources and government notification lists, publishes data breach reports and researches IT security in public- and private-sector entities. But according to Linda Foley, who founded the center with her husband Jay Foley, it's difficult to provide a clear picture of how secure the cyber-world is because breached organizations aren't upfront enough when they've been breached and how badly.

"Breached entities, No. 1, are afraid of the consequences. They're afraid that their reputation will be damaged, of fines they might incur, of the repercussions of a trust issue," she said.

The ITRC issued a press release on Jan. 8, 2010, titled, [Data Breaches: The Insanity Continues](#), citing the lack of a single data breach list requiring mandatory public reporting. Foley feels that this might change if the law intervened and forced organizations to step up.

"It takes law enforcement response. It takes the response of someone sitting there and saying, 'What are you going to do about it?'" she said.

The ITRC's 2009 Data Breach Report recorded more than 222 million potentially compromised records last year in 498 breaches, but in more than 52 percent of the breaches, the victimized organizations didn't disclose how many records were affected. So that 222 million? That only accounts for the breaches people wanted to talk about in public.

The insanity in this case is how difficult it is to count breaches in these circumstances. But of the data the ITRC has, breaches in the business sector number at 205 of 498 reported breaches in 2009, 41.2 percent. That's a larger concentration than in 2008, when business breaches numbered at 241 of 657 breaches, 36.7 percent. Government and military breaches constituted 90 of 498 breaches in 2009, for 18.1 percent. That's a smaller concentration than the 2008 figure, when that sector had 110 out of 657 for 16.7 percent.

Foley said many of the breaches can be reduced with better encryption and redaction, and she's hopeful that upcoming legislation can make better breach reporting required by law. [S. 139](#), which was introduced by Sen. Dianne Feinstein, D-Calif., would required federal agencies and people involved in interstate commerce to disclose breaches of data containing personally identifiable information. The bill has passed through committee and is on the legislative calendar.

Creating Secure Passwords You Can Remember

January 22, 2010 ([ITNEWS](#)) -

A study of passwords hacked from RockYou.com illustrates just how insecure most passwords are.

Microsoft Chairman Bill Gates declared the password dead. He told his audience that the password can't meet the challenge of keeping sensitive information protected, saying "People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure."

That was six years ago at the 2004 RSA Security Conference. Paraphrasing some wisdom from Samuel Clemens, the rumors of the password's demise have been greatly exaggerated. It is still the primary security control used to protect data, accounts, and pretty much everything else on a computer.

Gates may have been premature in calling the time of death on the password, but his assessment of why the password is inadequate as a security control were accurate. A study of more than 30 million passwords exposed when Rockyou.com was hacked found that almost half use names, common dictionary words, or sequential characters like "qwerty".

Fingerprint scanners and other biometric controls are becoming more mainstream, but the password will still be the main barrier between hackers and your data for the foreseeable future. With that in mind, here is how to create a secure password that you can actually remember in "12345" easy steps.

- 1.No Personal Information. Any novice hacker can easily find out your full name, the names of your spouse or children, your pets, or your favorite sports teams. Never choose a password that has anything to do with you personally.
- 2.No real words. Let's take that a step farther. Not only should you not use your name or your pet's name, you shouldn't use any actual word that can be found in a dictionary. Passwords like that can be easily cracked by password software.
- 3.Mix Character Types. Passwords are almost always case-sensitive, so use both upper and lower case letters to make it more difficult. To really make it complex, be more creative than just capitalizing the first letter. For example, do "paSsw0Rd" instead of just "Password". Better yet, throw in some numbers and special characters to substitute for letters, and do "p@Ssw0Rd".
- 4.Use a Passphrase. Scratch that. Some password cracking utilities are also smart enough to use common character substitutions for common words. Cracking "p@ssw0rd" may take longer than cracking "password", but it will still be relatively trivial to crack because, special characters or not, the password is still "password".

Instead, take your favorite line from a movie, song, or book and convert it to a passphrase. If you like the scene from A Few Good Men when Jack Nicholson is on the stand, take the line "You want the truth? You can't handle the truth!" and convert it to "Ywtt?Ychtt!". It has upper case and lower case letters, as well as special characters. It is not a word appearing in any dictionary, yet it is simple for you to remember.

- 5.Use a Tool. The main reason that users choose passwords that are easy to crack is that they want to choose passwords that are easy to remember. It is obviously much easier to remember your dog's name, or type characters in the order they appear on the keyboard, like "123456", than it is to recall "a5\$jgFD118@Kle45@".

But, guess which one is more secure?

You can use a password management tool to store complex passwords. It has some impact on security since cracking the password to access the password management tool grants access to all the rest of the passwords, but it does enable you to use stronger passwords for various Web sites, accounts, and applications without having to remember them all.

Windows has included a Credential Manager utility since Windows XP that lets users save passwords and provides a single sign-on solution. Logging in to Windows unlocks the vault and automatically applies the credentials from the vault as needed to access sites and applications.

Researcher: Flaws In Facebook App Authorization Could Lead To Clickjacking

January 20, 2010 ([darkREADING](#)) -

Vulnerabilities could enable attackers to collect data on Facebook users and friends, Dhanjani says...

Vulnerabilities in the way members authorize the use of third-party applications in Facebook could potentially lead to loss of personal information or even targeted attacks on specific individuals, a security researcher said today.

Nitesh Dhanjani, a well-known security researcher and author of *Hacking: The Next Generation*, says he has discovered design flaws in Facebook that could allow attackers to collect the personal information of users on the social networking site, and even build profiles of "friends" that might facilitate direct attacks on specific individuals within a company.

The flaws were presented to Facebook in November; Dhanjani has agreed not to release specific code or other details for two weeks while technical staffers at the social networking site continue their efforts to patch the vulnerabilities. Dhanjani says he has begun to speak generally about the problem, without specifics.

The vulnerabilities center around the way Facebook enables users to place third-party applications on their social networking pages, Dhanjani says. In a nutshell, Facebook allows the use of third-party apps within the confines of the site, but only if the user authorizes them. "If you click on a link that requires a third-party application, you see a dialog box, and you have to click 'yes' to authorize it," Dhanjani explains. "Once you authorize its use, all of your information -- your user ID, your friends list, everything -- is shipped to the third party. I'm not sure people really understand what's happening to their data."

Worse, Facebook also has enabled some applications to provide "automatic" authorization, Dhanjani observes. "When the user visits the application from within the Facebook environment, Facebook inserts "a parameter," he states in a report about the vulnerability. "If this parameter is present when the application is rendered, the application is allowed to scour information from the user's profile. The intention in this situation is that if the user clicked on the application [rather than a third-party site that redirects the user], the user has implicitly granted some level of authorization."

Dhanjani calls this automated authorization a "design flaw" in Facebook, but the social networking site has chosen not to comment on this particular concern. "They want users to be able to use the applications more easily, so it's basically a business decision to leave it the way it is," he states.

However, Facebook is responding to Dhanjani's assertion that flaws in these authorization procedures could potentially be exploited to create clickjacking attacks.

"The goal is to write a rogue Facebook application that is rendered when a user visits a malicious third party Website," Dhanjani explains in his report. "If the user already has an established session in Facebook [on another browser tab or window], the third-party site can load the malicious Facebook application in an iFrame to identify the user and steal the user's Facebook information."

Since only part of the actual Facebook site is being displayed in the iFrame, the attacker is essentially executing a "clickjacking" attack, Dhanjani says. The attacker is essentially creating a malicious application that looks like a legitimate app -- and then when the user clicks on the right link, the malware uses Facebook's flawed authorization process to collect all of the user's Facebook data, including information about the user's "friends."

"We've already seen clickjacking work on Facebook, but those attacks were mostly used to spread spam to users and their friends," Dhanjani says. "What's happening in this case is that the attacker is using clickjacking to collect the data of the user, as well as the data on their friends. You could map that data to specific domains, such as users who are in a company and their friends."

Cybercriminals could potentially use such a flaw to collect data on specific individuals, Dhanjani warns. "If you want to install malware on the computer of a user in a particular business unit of [a corporation], for example, that's pretty hard to do with a traditional browser attack. But with this, you can actually target an individual or build a group of individuals that you want to target with a specific piece of malware."

It's hard to tell how dangerous these attacks might be because the severity of targeted attacks can't be measured in numbers of infections or numbers of instances detected, Dhanjani says. "But I would be very surprised if there aren't already [hackers] looking at this vulnerability," he says.

Dhanjani plans to provide more details on the vulnerability, including specifics on code, in about two weeks -- "Hopefully, after Facebook has fixed the problem," he says.

Cybersecurity: Make It Work This Year

By Keith Rhodes - 11 January 2010

2009 had all the makings to be a banner year for cybersecurity: The need had been identified, guidance was promised, appointments were planned and mandates were discussed. Unfortunately, 2009 will be remembered as the year that wasn't, and the challenge facing us now is to make sure 2010 doesn't follow suit.

Many people mistakenly believe that cybersecurity protects only consumers and other civilian uses for the Internet, but today's military is more dependent than ever on the civilian-based infrastructure for connectivity and information. Cyberspace has become a new dimension of the battlespace, so cybersecurity is much more than just firewalls and anti-virus protection on home or business computers.

From a defense standpoint, ineffective cybersecurity can compromise missions and cost lives. Piecemeal protection measures leave vulnerabilities for our troops and national security and are already inadequate in the face of new cyber threats.

Necessary advances in cybersecurity, even during a time when budgets are pressured, will be made only through cooperation and a common purpose among all stakeholders: civilian government, military and commercial industry.

The conditions during an economic downturn decidedly favor the attacker. Government agencies keep legacy systems longer and cut back on acquiring patches and other defenses, while attackers have the advantage of being able to work against familiar systems with familiar vulnerabilities. Successful cyber defense will depend on effective intelligence collection and analysis, mission assurance, and education on the evolving nature of the threat. Consider four ways in which cyber defense can move forward:

■ **Education.** The first step to realizing comprehensive cybersecurity is understanding the true connectivity in our nation's data. The responsibility to protect data, whether personal consumer information or troop movements, cannot fall solely on the desks of information technology officers. All users must understand that if they have access to information, they may also inadvertently allow unauthorized access to that information. We cannot simply believe that someone else is protecting our data.

Security problems are ultimately human problems, and there are no simple, bolt-on technological fixes. The military understands this for the rest of the battlespace; its task now is extending that understanding to cyberspace.

■ **Communication.** Conversations must occur between government and industry that clearly communicate the cybersecurity requirements of civilian government and military missions. The Department of Defense has done a good job in conducting risk analysis and focused protection, primarily because it understands its mission. But mission understanding cannot provide mission assurance until it is communicated to all stakeholders.

Cybersecurity is a continuous process of monitoring, testing and adapting - a process that hinges on communication. "Need to know" is quickly being replaced by "responsibility to share" because it is a paradigm that can keep up with the emerging cyber threats.

■ **Partnerships.** Private industry owns most of the government's infrastructure, and it needs to be incentivized to protect data and operating environments. Likewise, there should be repercussions when the infrastructure fails. For government and military operations, out of sight cannot be out of mind; without proper partnerships, data storage and transmission are only as safe as the weakest link among the instituted cybersecurity procedures.

Government aligns, harmonizes and synchronizes; it enables the establishment of standards within which people and organizations can operate. It can serve as a vital early adopter, or even as an angel investor. The other side of the coin is industry, which provides the rapid innovation needed in a dynamic, distributed marketplace. Without either side of the coin, cybersecurity is left inadequate.

■ **Mission understanding.** This is the most important piece of the puzzle. Without knowing what needs to be done, we cannot know what needs to be protected. Mission understanding needs to be the fabric that cybersecurity is made out of. Information isn't protected just because it exists, it is protected because it is necessary to a mission.

With mission understanding, all the other pieces fall into place: Education helps illuminate the sphere of operation, and communication and partnerships can bring into place effective, comprehensive protection of information. Such protection is quickly becoming the most important asset in our defense missions.

Report: CISOs Keep Breach Costs Lower

The latest "Cost of a Data Breach" survey from the Ponemon Institute finds companies with a CISO are better able to handle loss of sensitive information

By [Joan Goodchild](#), Senior Editor

January 25, 2010 — [CSO](#) —

Companies continue to pay a high price to clean up the mess created by a data breach, but having a Chief Information Security Officer (CISO) may offer some protection. That is the conclusion of a study released Monday by the Ponemon Institute, a Michigan-based consultancy that conducts independent research on privacy, data protection and information security policy.

This is the fifth year Ponemon has conducted its "Cost of a Data Breach" survey, which examined actual data breach experiences of 45 U.S. companies from 15 different industry sectors. This year, the cost of a data breach has increased to \$204 from [last year's \\$202 per customer record](#). However, companies that had a CISO (or equivalent title) who managed the data breach incident experienced an average per capita cost of \$157 versus \$236 for companies without such CISO leadership.

Approximately 40 percent of participating companies had a CISO in charge of managing the data breach incident, according to the survey.

"While other functional areas are typically involved in crisis management activities surrounding the data breach, our results suggest CISO leadership substantially reduces the overall cost of data breach," the report states.

"The one big take away on positive takeaway is that in (companies) that have CISO involvement, breaches tend to cost less because they have a more strategic view of protecting data than the old idea of whack-a mole, fix-it a hundred different times," explained Phillip Dunkelberger, president and CEO of PGP Corp., which co-sponsored the study. "CISO involvement at a higher level means less cost of a data breach and less chance of repeating it because of the strategic view of protecting it that these professional take."

While the cost of a breach only rose two dollars per record this year, Dr. Larry Ponemon, founder and chair of the Ponemon Institute, pointed out the massive increase in cost over the five years since the study's inception, when breaches cost \$138 per compromised customer record. In figuring out the costs, the study takes into account a wide range of business costs, including expense outlays for detection, escalation, notification, and after the fact (ex-post) response. The economic impact of lost or diminished customer trust and confidence, measured by customer churn or turnover rates, is also analyzed.

Other highlights from this year's research include:

- Forty two percent of all cases in this year's study involved third-party mistakes or flubs. Data breaches involving outsourced data to third parties, especially when the third party is offshore, are most costly. The per capita cost for data breaches involving third parties is \$217 versus \$194, more than a \$21 difference, according to Ponemon.

Twenty four percent of all cases in this year's study involved a malicious or criminal attack that resulted in the loss or theft of personal information. Research shows data breaches involving malicious or criminal acts are much more expensive than incidents resulting from negligence. The per capita cost of a data breach involving a malicious or criminal act averages \$215. The per capita cost of a data breach involving a negligent insider or a systems glitch averages \$154 and \$166, respectively.

-Thirty six percent of all cases in this year's study involved lost or stolen laptop computers or other mobile data-bearing devices. Data breaches concerning lost, missing or stolen laptop computers are more expensive than other incidents. Specifically, in this year's study the per victim cost for a data breach involving a lost or stolen laptop is \$225.

"Its not just about bad guys, but also good guys who make mistakes," noted Ponemon.

Agencies identify biggest threats to cybersecurity

Jan 25, 2010

More than half of all federal agencies experience a cybersecurity incident on a weekly or daily basis. That's according to a survey of 150 civilian and 150 Defense Department information technology professionals conducted by CDW Government. Malware and access control issues were the top challenges.

How often does your agency or network experience a cybersecurity incident?

Daily: 31%
Weekly: 23%
Monthly: 13%
Bimonthly: 4%
Quarterly: 6%
Yearly: 5%
Unsure: 17%

What are the top three cybersecurity issues you deal with every day?

1. Malware: 33%
2. Inappropriate employee activity or network use: 25%
3. Remote user access: 25%

Where does your agency's or network's biggest threat come from?

1. External sources: 47%
2. Agency employees: 23%
3. Contractors: 10%

5 Tips for Cybersecurity-Training Your Employees

Federal Computer Week (01/21/10) ; Moore, John

Although providing employees with cybersecurity training can help protect against cybersecurity threats, it cannot prevent all types of security breaches. According to a recent survey conducted by CDW Government, nearly half of federal information technology (IT) managers had seen their employees post their passwords in public places, despite the fact that 80 percent of IT managers provide workers with ongoing classes on security policies and procedures. But federal IT managers can take a number of steps to ensure that their employees do not make similar mistakes after undergoing cybersecurity training. For example, federal agencies should conduct simple and routine tests to ensure that their employees are retaining what they learn in cybersecurity training. The Millennium Challenge Corp. (MCC), for example, uses a Tip of the Day awareness training application that asks employees a question about IT security when they log on to the government corporation's network. Federal agencies also should be sure that there are consequences for employees that fail to demonstrate knowledge of IT security. At MCC, employees who fail the Tip of the Day tests for a month are contacted about their performance, while those who fail for more than two months lose access to the network until they complete remedial training. Finally, federal agencies should be sure to invest money in tools that monitor users and detect security lapses, says NetWitness chief security officer Eddie Schwartz.

Consumer Awareness Of Online Threats Is Up, Study Says

Users more worried about phishing, social networking threats, according to RSA

Jan 25, 2010 | 08:54 AM

By Tim Wilson
DarkReading

Consumers are becoming increasingly concerned about the safety of their data online, according to a study published last week.

In a study of more than 4,500 consumers conducted by InfoSurv and sponsored by RSA, researchers found that consumer awareness of phishing attacks has doubled between 2007 and 2009. The number of consumers who reported falling prey to this attack increased six times during that same time period.

In addition, while hundreds of thousands of people join social networking sites each day, nearly two in three (65 percent) people who belong to these online communities are less likely to interact or share information due to their growing security concerns, the survey found.

Four out of five (81 percent) people using social networking Websites expressed concern about the safety of their personal information online.

Consumers might be more aware of phishing threats, but new attack methods duped six times as many of them in 2009 than in 2007, the study says.

The sheer volume of phishing attacks launched in recent months is also contributing to these trends, RSA said. The RSA Anti-Fraud Command Center recently reported the highest-yet detected rates of phishing attacks between August and October 2009, as well as a 17 percent increase in the total number of attacks between 2008 and 2009.

An increase in consumer knowledge of online threats is further evident from the growth in the number of respondents that expressed awareness of Trojans. In 2007, 63 percent of consumers stated they were aware of Trojans and in 2009 that figure climbed to 81 percent.

The RSA survey revealed that consumers using online banking (86 percent) Websites shared more concern with the theft of their personal information than those using healthcare portals (64 percent) and government Websites (68 percent). As a result of these concerns, more than half of all consumers reported they are less likely to share information and interact on these Websites.

Consumers agreed that their identities should be better protected than a simple username and password on social networking (59 percent), healthcare (64 percent), government (70 percent), and online banking (80 percent) Websites. Nine in 10 consumers are willing to use a stronger form of security if offered.

Preparing for future security threats, evolving malware

Nick Lewis, Contributor
01.21.2010

In the past year, malware has evolved in five major areas: bots, rogue security software, generic spyware, targeted malware and attacks on mobile phones and smartphones. These threats have, in turn, allowed criminals to find new ways to monetize the unauthorized access they have been able to gain. In the last year, malware has incorporated better techniques for hiding and staying resident on new hosts, improving their communications and increasing users' concerns about identity theft and related fraud.

Most security attacks get incrementally more dangerous over time, and some attacks will make major advancements in 2010. Malware, for example, will only get worse over the next year, even from its current state of sophisticated botnets. Malicious code will get easier to use, and criminals will have the ability to configure full-management applications, improved toolkits and update mechanisms to incorporate zero-day attacks and customizations. It may seem bleak, and enterprise security pros should certainly find it daunting. However, tools and techniques will also evolve over the next year to better protect corporate networks and data.

Predictions: Future security threats, defenses for 2010

There are few constants in information security, but the continued evolution of (and danger from) malware is one of them. Organizations can combat evolving malware and botnets through a combination of best practices like security awareness training, policies and procedures, and two emerging technologies: whitelisting and cloud-based antimalware. Let's discuss both of those technologies briefly:

1. Whitelisting will evolve in enterprises as organizations evaluate new products, their functionality and how they can be used to more effectively protect their environment. Whitelisting defines the executables that can run on a system and then stops all others when software isn't on a defined list of acceptable behavior.

Whitelisting has evolved in the last couple years. Initially, the technology was a complex system where enterprises needed to define every single executable. Now whitelisting products come with preconfigured templates, improved capabilities to approve new executables, and full management systems. Enterprises will realize that relying on antivirus software alone will not be tenable, and a new defense must be used. More enterprises in 2010 will use and set up their own whitelists and blacklists to supplement or replace their existing antimalware protections and then configure policy to determine what action to take for software that's not on either list.

2. Cloud-based antimalware will also evolve in enterprises to supplement the unknown software issues in whitelisting. Cloud-based antimalware allows checks to be made against centralized databases, identifying if the unknown software is malware. Because the signatures are based on research from software providers and other customers, this centralized database will have more signatures and can be updated faster than traditional antivirus signatures. Real-time checks, however, will require network access to the database and will need to be optimized to perform reasonably. This central location could also be used to track the spread of malicious files, but would need to protect the privacy of the users. Similar protections for PCs will continue to mature on mobile phones and smartphones.

Another rapidly evolving attack vector worth mentioning is threats against mobile and wireless devices. Smartphone attacks and malware have exploited Bluetooth and IP connections on mobile devices, but so far, they have rarely been malicious. Attacks on mobile phones and smartphones will continue to make headlines, but because of the complexities and heterogeneous nature of these devices, widespread attacks on multiple platforms will be unlikely. There will be advancements in attacks, like the recent iPhone SSH default password worm, or the recent malicious Android application that stole bank login details. These threats will evolve to be more than just low-level risks.

As more commerce is conducted on smartphones, the devices will be attacked more frequently, especially as development is opened to anyone developing and installing applications. Antimalware applications, like those on personal computers, will protect smartphones, but it is also important to use stronger controls on application distribution methods, such as only allowing signed applications to run and placing strong controls on the ability to sign them.

Common weaknesses in malware detection and protection will continue in 2010. Users and enterprises will start to accelerate their replacement of older, more vulnerable operating systems, which will help reduce their risks. Threats will continue to take advantage of these older systems while criminals find new ways to attack new systems that close the holes they had been exploiting. Security trends in malware and other information security threats will only continue to get worse as there is significant money to be made by criminals.

Enterprise infosec pros should not only seek to mitigate all of these potential threats with their current resources and the technologies and strategies mentioned above, but also continue to monitor these threat areas closely as the year progresses. Even small advances by attackers in any one of these areas could give those with

malicious intentions a significant advantage in exploiting enterprise defenses.

Facebook, Twitter, Social Network Attacks Tripled in 2009

New report from Sophos finds most Facebook and Twitter users have received spam or malware on the popular social networking sites

By [Joan Goodchild](#), Senior Editor

February 01, 2010 — [CSO](#) —

As more organizations allow employees to use social media like Facebook and Twitter at work, cybercrime attacks on these networks have exploded, according to a report released Monday by IT security firm Sophos. Reports of malware and spam rose 70 percent on social networks in the last 12 months, the security survey reveals

Sophos' investigation, titled "Social Security," finds 57 percent of users report they have been spammed via social networking sites, and 36 percent reveal they have been sent malware via social networking sites. The "Social Security" survey is part of Sophos' 2010 Security Threat Report, which looks at current and emerging computer security trends.

"Computer users are spending more time on social networks, sharing sensitive and valuable personal information, and hackers have sniffed out where the money is to be made," said Graham Cluley, senior technology consultant for Sophos. "The dramatic rise in attacks in the last year tells us that social networks and their millions of users have to do more to protect themselves from organized cybercrime, or risk falling prey to identity theft schemes, scams, and malware attacks."

While most of the 500 firms Sophos polled, 72 percent, were worried workers behavior on social networks is putting their business at risk, almost half of them, 49 percent, allow all of their staff unfettered access to Facebook and other social networking sites. "The grim irony is that just as companies are loosening their attitude to staff activity on social networks, the threat of malware, spam, phishing and identity theft on Facebook is increasing," said Cluley.

Survey respondents were also asked which social network they believed posed the biggest security risk and 60 percent said Facebook.

"We shouldn't forget that Facebook is by far the largest social network - and you'll find more bad apples in the biggest orchard," explained Cluley. "The truth is that the security team at Facebook works hard to counter threats on their site - it's just that policing 350 million users can't be an easy job for anyone. But there is no doubt that simple changes could make Facebook users safer. For instance, when Facebook rolled-out its new recommended privacy settings late last year, it was a backwards step, encouraging many users to share their information with everybody on the internet."

The report also points out the inherent security problems presented by LinkedIn, which is a social network targeted to working people that allows them to network and job seek, among other things. Although LinkedIn is considered to be by far the least threatening of the networks, Sophos advises that it can still provide a sizeable pool of information for hackers.

"Targeted attacks against companies are in the news at the moment, and the more information a criminal can get about your organization's structure, the easier for them to send a poisoned attachment to precisely the person whose computer they want to break into," explained Cluley. "Sites like LinkedIn provide hackers with what is effectively a corporate directory, listing your staff's names and positions. This makes it child's play to reverse-engineer the email addresses of potential victims."

