CCC News

Control Computer Crimes

Issue 0008 - 15 October 2009

Message from the Editor

Welcome to the eighth issue of CCCNews Magazine.

We have been constantly evolving based on readers' feedback. The recent and this issue carry only analysis, research, reports and surveys. All news are provided in CCCNews Newsletter. The CCCNews Magazine will be a digest to provide value addition to news.

In this edition, we provide an analytical report, giving details of password usage habits of various users. The real eye-opener in this analytical report is the creation and usage of insecure passwords by more than 65% of users. Only 6% created relatively secure passwords.

We also bring you report on – What Security Professionals preaches but do not practice. Seven undesirable habits of security professionals are described in this analysis.

We bring a next report on - What are the predictions about the future of information security. This will help us to find the right direction towards information security.

We also bring an article on 9 real life IT horror stories and another on real top 50 data breaches in 2009 till date.

Happy reading,

Rakesh Goyal
Editor

CONTENTS

CCC News
Issue 0008
15 October 2009

Rakesh Goyal
Editor
editor@cccnews.in

Published by
CCC Media
Mumbai, India

Research

Statistics from 10,000 leaked Hotmail passwords

An anonymous user posted usernames and passwords for over 10,000 Windows Live Hotmail accounts to web site PasteBin.

PasteBin is currently down for maintenance but I managed to get a copy of the list and quickly generated some statistics from these passwords.

First, my impression is that these passwords have been gathered using phishing kits.

Even more, I think it was a badly designed phishing kit, one that didn’t further authenticated the users to the Hotmail/Live website.

I think it just returned an error message after grabbing the credentials.

I’m saying that because some of the passwords are repeated once or twice (sometimes with different capitalization).

The users didn’t understand what happened and entered the same password again and again trying to login.

Below are the statistics:

The list initially contained 10028 entries.

After I’ve cleaned up the list, removing entries without a password, I’ve remained with 9843 entries (passwords).

There are 8931 (90%) unique passwords in the list.

- The longest password was 30 chars long: **lafaroleratropezoooooooooooooo**.
- The shortest password was 1 char long : **)**

Top 20 most common passwords:

1. **123456** - 64
2. **123456789** - 18
3. **alejandra** - 11
4. **111111** - 10
5. **alberto** - 9
6. **tequiero** - 9

7. **alejandro** - 9
8. **12345678** - 9
9. **1234567** - 8
10. **estrella** - 7
11. iloveyou - 7
12. daniel - 7
13. 000000 - 7
14. roberto - 7
15. 654321 - 6
16. bonita - 6
17. sebastian - 6
18. beatriz - 6
19. mariposa - 5
20. america - 5

Based on these passwords I think the phishing kit was targeted towards the Latino community.

Password length distribution:

- 1 chars – 2 – 0 %
- 2 chars – 4 – 0 %
- 3 chars – 4 – 0 %
- 4 chars – 31 – 0 %
- 5 chars – 49 – 1 %
- **6 chars – 1946 – 22 %**
- **7 chars – 1254 – 14 %**
- **8 chars – 1838 – 21 %**
- **9 chars – 1091 – 12 %**
- 10 chars – 772 – 9 %
- 11 chars – 527 – 6 %
- 12 chars – 431 – 5 %
- 13 chars – 290 – 3 %
- 14 chars – 219 – 2 %
- 15 chars – 157 – 2 %
- 16 chars – 190 – 2 %
- 17 chars – 56 – 1 %
- 18 chars – 17 – 0 %
- 19 chars – 7 – 0 %
- 20 chars – 14 – 0 %
- 21 chars – 10 – 0 %
- 22 chars – 8 – 0 %
- 23 chars – 3 – 0 %
- 24 chars – 3 – 0 %
- 25 chars – 3 – 0 %
- 26 chars – 0 – 0 %
- 27 chars – 3 – 0 %

- 28 chars – 0 – 0 %
- 29 chars – 1 – 0 %
- 30 chars – 1 – 0 %

As you can see from the list above, most of the passwords are between **6** and **9** characters long. Average password length is **8** characters.

What kind of passwords were in the list? :

- **3,713 = 42 %;** lower alpha passwords : passwords containing only characters from 'a' to 'z'.
- Example : *iloveyou*
- **291 = 3 %;** mixed case alpha passwords : passwords containing characters from 'a' to 'z' and from 'A' to 'Z'.
- Example: *ILoveYou*
- **1707 = 19 %;** numeric passwords: passwords containing only numbers ('0' to '9')
- Example: *123456*
- **2655 = 30 %;** mixed alpha and numeric passwords: passwords containing characters from 'a'-'z', 'A'-'Z' and '0'-'9'.
- Example: *Iloveyou12*
- **565 = 6 %;** mixed alpha + numeric + other characters.
- Example: *1Love You$%@*

As we can see and conclude from the list above, a big majority of users still use very poor passwords: **42** % (lower alpha only) and **19** % (numeric only), while only **6** % from all the passwords had passwords which use a selection of alpha numeric and other characters.

Courtesy : Bogdan Calin; http://www.acunetix.com
06 October 2009

Analysis

7 Ways Security Pros DON'T Practice What They Preach

IT security pros are often driven to drink -- literally -- over the daily battles of their job: bosses unwilling to accept the rationale for some new security investment, employees who regularly infect their computers by doing things that have nothing to do with their jobs, and vendors who don't understand the company's needs.

But in a recent, unscientific and informal poll CSOonline conducted over such social networks as Twitter and LinkedIn, many IT security pros admitted they've often looked the enemy in the eye only to find themselves staring back in the mirror. Or, they've seen carelessness in well-meaning professionals who should know better.

Paul V de Souza, a former chief security engineer at AT&T and owner of the CYBER WARFARE Forum Initiative (CWFI), has seen many an example where IT security pros fail to practice what they preach. "I have noticed that many security professionals do not encrypt their hard drive," he said. "I also see a lack of two-factor authentication deployment. Many of us security professionals rely only on passwords."

Based on the poll and a list provided by Andy Willingham, former network security engineer at EBFC, information security engineer at MARTA and founder/owner of AndyITGuy Consulting, here are seven examples of how security pros cut corners:

Using URL shortening services

URL shortening services have become immensely popular in recent years, especially among security pros who use such forums as Twitter to share content. The problem is that URL-shortening services are sometimes insecure and unstable. For examples, see New Spam Trick: Shortened URLs and 5 More Facebook, Twitter Scams to Avoid.

In the latter example, Graham Cluley, senior technology consultant with U.K.-based security firm Sophos, noted in a recent interview that some URL-shortening services have begun to try filtering out bad sites by checking URLs against known black lists, but that the issue is far from resolved, particularly because despite increased efforts to block malicious links, Twitter and Facebook do not have a filtering mechanism for bad shortened URLs.

Granting themselves exemptions in the firewall/Web proxy/content filter

Willingham noted that it's not uncommon for security pros to bypass the very security mechanisms they enforce on other employees, often because those mechanisms get in the way or because they are in a hurry to get a particular task done.

One, senior system engineer, who isn't named due to the sensitive nature of the topic, admitted he has run several development and test systems without an active firewall or antivirus out of necessity.

"I preach security every day, and I know I'm guilty of many of the worst offenses I warn people to avoid," he said. "As a field employee, I am very much my own system administrator. I know in an office environment I could, and probably would, have many more restrictions in place, but working from home and customer locations, as well as the occasional coffee shop, I just can't take the time to follow all the rules I tell others to follow."

Snooping into files/folders that they don't own

Nobody admitted outright that they have done this themselves, but Willingham and others polled said they know of cases where fellow security practitioners have gone into someone else's files. Sometimes it was because of an investigation into a security incident. Other times, it was simply a matter of having the access and being nosy.

Using default or easy passwords

Willingham noted that IT security practitioners are often guilty of giving themselves easy-to-remember passwords such as the name of their city or town, a pet's name or a favorite beverage. This, of course, flies in the face of everything we've heard about using complex passwords or nixing passwords altogether in favor of a more secure method of authentication.

Failure to patch

The second Tuesday of each month, e-mail inboxes are crushed beneath the weight of advisories from vendors, analysts and others regarding the security patches Microsoft almost always releases on that day. But security practitioners say they don't always keep their systems fully patched or that they have seen others make do without some critical fixes. [See Example 5 in 7 Deadly Sins of Networking Security] The reasons range from underdeveloped patch management systems to the simple belief that fast patching isn't the imperative some make it out to be. "I don't always keep my own systems patched/updated," said the anonymous security practitioner first mentioned in Example 2.

"While professing a defense-in-depth strategy, many security pros leave their own systems unpatched and with the default settings untouched because 'I know what I am doing,'" said Tomas Palmer, a partner at SkyCipher, former senior security program manager at Microsoft and former director at Spacelabs Healthcare.

Using open wireless access points

IT security practitioners know it's not always safe to latch onto the wireless network at an airport, coffee shop or conference (including Black Hat and Defcon, where wi-fi hacks have become legendary), but when one needs to get online to get some crucial e-mail, check on problems with a Web page or simply stave off boredom, the nearest wi-fi is often good enough.

Misuse of USB sticks and other removable storage devices

Security practitioners often complain that employees lose removable storage devices containing sensitive data on airplanes, buses and curbsides. But Willingham said security pros are often just as guilty.

Admitted the anonymous security practitioner first mentioned in Example 2: "I use USB sticks often, frequently not cleaned of other customer data, or confidential proprietary data."

Courtesy : Bill Brenner; http://www.computerworld.com
September 22, 2009

Development

What Star Trek Predicts About The Future of Information Security

I had a funny thought while talking with some folks from Intel about what the future state of information security would look like and how that relates to what our favorite nerdy show, Star Trek, has to say on the topic. This is meant to be a funny post, but there may be some truth buried in here somewhere too. Without further ado:

Physical security will always be a problem:

How many times have we seen people open up random access panels on the Enterprise and start pulling out chips when something goes awry or just start swapping them out right and left? Crawling through tubes to get past obstacles and the like… all point to the fact that even the most sophisticated military war machine of the future won't stop some teen aged acting ensign in engineering from taking over control of the whole ship in about 35 seconds.

Organizations will focus on secure transport and network security and will still ignore drive encryption and the insider threat:

I don't really recall any times where enemies were able to intercept any meaningful communications between the Enterprise and other federation ships. That must mean they are using TLS16/SSL34.0 in the future, which is good, but for some reason any schmuck diplomat from some third world (pun intended) alien race can get any information out of the computer he wants without ever even supplying a password!

PCI doesn't stop hackers, now or ever:

They don't use money in the future. Probably because consumers are so sick of having their credit cards stolen is my guess. I'm also guessing based on how many holes still exist; SQL injection still exists even hundreds of years in the future. So currency, and therefore the payment industry had to go. Even Quark trades in gold-pressed latinum - you don't see the Ferengi taking plastic.

Biba and Bell La-Padula security models will always be a good idea, but will still never be properly implemented:

Seriously, the federation is pretty lax in their whole openness. I mean, should you really let people on your ship, carrying weapons, with no or minimal escort and allow them to use your computers, write to them, copy information off of them and so on? Balancing the prime directive and giving some industrial revolution era alien species access to a computer with the engine schematics to the warp core of the most advanced war ship in the fleet sorta seems a little out of whack. Maybe that's what they get for not having money in the future - no one's worried about losing their job.

The singularity is a non-event and will end up being a wash for security:

I mean, Data is pretty cool, but he is really more than a oddity in the show. Sure, he's saved the Enterprise a number of times, but he's also pretty darned hackable in the future too. He's been compromised more than most of the other people on the show combined. This is not a good outlook. Why they didn't bother to root-kit him, I'll never know. But if Data is the tipping point of a potential Skynet, I'm not too worried - he plays violin and he owns a cat.

Individuals will almost completely give up on the idea of protecting their privacy:

Everyone on the Enterprise is pretty happy with the idea of carrying around RFID chips on their badges all the time, even when they're off duty and getting some R&R and T&A on Risa.

Organizations will always ignore single points of failure, even after it bites them in the ass:

I can't even tell you how many times the Enterprise has managed to damage the one and only di-lithium crystal that they have on the whole ship. They know they can't whip up a new one with the replicators but they still don't carry even one spare. Then they end up being stranded or having to use the sensor array to catch radiation from some exploding sun or some other retarded plan that always manages to work out exactly perfectly, but always necessitates near death experiences in the process. Why, for all that's holy, wouldn't you just bite the bullet and pay to have two on board? Yes, I'm talking to you, Jean Luke and you too Mr. CISO.

The iterative development model will be proven bad for security and quality exactly 1,000,000 times but will still be used in production anyway:

How many times have we seen engineering making changes to the warp core while they are 200 light years from any star base or any other craft for that matter? And how many times has that gone smoothly again? No, it's a bad idea now, and it will always be a bad idea. But then again, maybe you shouldn't worry so much about keeping your data and integrity intact… it always manages to get fixed in an hour or so anyway, right?

Biometrics will always be used as a backup to password authentication - but both still suck:

Sure, voice print recognition has been used a few times, as has hand scanners and even an iris check a few times. But the vast majority of times someone has entered in a password on the show (which incidentally is almost never - giving you an idea about how lax security will be in the future) it has been by saying it out loud. Hackers must be pretty un-inventive in the future because I'm guessing digital voice recorders are pretty easy to get your hands on.

Virtualization security is an oxymoron - even in the distant future:

I mean, really, how many times has the whole damned ship been taken over by some overzealous holodeck character? Whoever wrote the holodeck hypervisor really needs to be put in a room with Warf for a few hours so he can explain with his batleth what the need for true physical and logical isolation is. Why some Sherlock Holmes character should have access to main memory, I'll never know. Too bad we aren't smart enough in the distant future to think about hardware isolation instead of relying exclusively on dangerously faulty software.

And with that, I'll let you go back to your regular scheduled programming.

Courtesy : http://ha.ckers.org
September 18th, 2009

Research

A psychological experiment

I've been thinking a bit about human psychology in the wake of the Fan Check virus scare. There were a lot of rumors flying – depending on who you listened to, the Fan Check Facebook app was malicious, not malicious, a hoax...And while I was thinking, a controversial psychology experiment kept coming back to me.

Back in 1963, Yale psychologist Stanley Milgram published an article in the Journal of Abnormal and Social Psychology detailing his research findings on how people respond to authority figures. In Milgram's experiment, a test subject was told to give electric shocks (which escalated in intensity) to an individual in a separate room if the individual failed to respond correctly to questions. The test subject was also told that the individual had a heart condition. No electric shocks were actually administered, but when the button was pressed to "deliver" a shock, a pre-recorded response was played – ranging from screaming to pleading for the shocks to stop to silence. Many of the test subjects continued to administer shocks up to "maximum voltage", even though they admitted they felt uneasy about doing so.

Milgram's experiment showed clearly that when a person is told to do something, they'll usually do it, even if it goes against their own perceived values. Our adversaries, the malware authors, have a great understanding of basic psychology, and they know that this principle holds true in the digital world as well. Their latest "experiment", where they sent Facebook users messages asking them to warn their friends about the "Fan Check" virus was pretty successful. People complied simply because they'd been told to.

Of course, this case isn't exactly analogous to the study described above; those who "warned" their friends didn't see any harm in doing so, and probably thought they were being helpful. But the behavior is very similar to the "blind obedience" mentality highlighted by Milgram.

The behavior demonstrated in the Milgram study has been replicated in the real, non-research world. And the boundaries between the physical world and the digital world are getting increasingly blurred. At the moment malware scares are mostly created unwittingly. But we've also seen the emergence and rise of cyberbullying and other nasty behavior. How long will it be before we see cybercitizens knowingly acting against their own values, simply because they've been told to do so?

Courtesy : Josh; http://www.viruslist.com
September 22, 2009

Analysis

Nine Real-Life IT Horror Stories

IT horror never ends: more real-world disasters, courtesy of your network's weakest link.

Nothing can screw up a well-managed network faster than the people for whom you built it. Whether it's user error, optimistic expectations, or simply that bastard Murphy, IT's job is rarely predictable.

Lucky for you, there are lessons to be learned from others' misfortunes. So rather than wait to make your own forehead-shaped dent in the office wall, familiarize yourself with the screwups detailed below. It will make you that much more prepared to safeguard your IT environment from the ever-evolving boneheaded tendencies of those you serve.

Stupid user trick No. 1: Home is where the malware is

It happens at least once a year, and this year it happened twice, writes one IT admin: "And though we make the point with memos and lectures, there always seems to be someone who gives their work PC to the kids at night."

The situation is familiar: To save on expenses, folks buy fewer home PCs, but their kids want to use them more than ever. Enter the corporate laptop into the home Web surfing environment -- a recipe for disaster for IT.

And it's not just kids playing games and doing homework. It's spouses using social networking -- and that uncle nobody talks about surfing porn on your corporate machines.

"Our security tends to be better than the average home box, but that won't protect you forever if you actually run out and *look* for attack sites," our admin warns. Sooner or later, one of your user's laptops will get compromised, leaving your network exposed to infection the next time he or she logs on at the office.

"We've gotten better at catching these compromised machines early, so instead of it being the big problem it used to be, last year it mainly just confirmed our investment in end-client security," the admin says.

The worst offender? A procurement manager who was found to have a keyboard logger installed on his company-issued laptop. "And this was a guy who spent several $100K a year online for the company," the admin informs us.

Solution: End-point security goes a long way toward preventing infected machines from gaining access to the corporate net, but they'll never be 100 percent effective. Web browsers are the gateway to hell when it comes to attack entry points. Let your users surf helter skelter and your attack potential goes way up. The only preventative measure: a strong fair-use policy and a management staff that'll enforce it.

Moral: Users will continue to break your official-use policy as long as money is tight and they believe the consequences are minor. Include disciplinary action in your policy, and make sure users know you're tracking Web site visits and system access. Otherwise, you are simply setting yourself up for disaster. Another solution: Sponsor employee discounts on netbooks. That way, your users will be less tempted to transform company property into their home PCs.

Stupid user trick No. 2: Message to self: E-mail isn't for everything

Sometimes all it takes is a well-meaning IT management decision to set stupid users in motion, writes P. Lindo, an IT admin at a New York-based organization with more than 1,000 e-mail inboxes, which the firm first maxed out at 100MB per mailbox, then at 500MB.

"In 2007, we hired a new IT manager who got placed in charge of e-mail management," says Lindo. "He saw the load of user requests for larger mailbox space and decided this was where he was going to make a big difference."

And so he set about purchasing enough hardware to increase individual mailbox sizes to 1GB -- barely.

"He also used all the user requests to get backing to upgrade everyone to Office 2007 -- the one with the new Outlook mailbox search," Lindo says.

Throw in a new policy for teaching users proper inbox maintenance, and watch inbox utilization hover at a manageable 75 percent -- until you put policy into practice.

"Turns out users don't read documents titled 'Proper Inbox Space Management,'" Lindo says. What they see instead is the fine print that tells them they now have 1GB of mailbox space. And then they start using Outlook's handy new search feature to turn their e-mail clients into personal information managers.

"Nobody deletes attachments anymore. Instead they leave them in their inboxes so that they can run quick searches against them, where all they need to remember is a rough description of the attachment and the name of the person who might have sent it to them," Lindo explains.

Worse, they send attachments to themselves just so the doc will be in the inbox somewhere.

"Our mail servers got maxed out inside of three months."

The small saving grace?

"We actually saw a 35 percent decrease in the amount these users used their network home directories," Lindo reports. "Outlook became the main network gateway for personal storage. So we were able to repurpose some storage from the file server machines on the e-mail infrastructure, but we still had to make several large and unscheduled server purchases to keep up with new demand."

Solution: A big inbox may sound like a good idea, but proper capacity planning is an even better one. Moreover, planning for 75 percent utilization is a recipe for trouble. Instead, target 50 percent or less, or run a pilot project before committing. A low-cost SAN can help here as well; adding capacity to one of those is significantly easier than installing new servers.

Moral: If it seems like everyone's working harder these days it's because they are. Users will utilize any tool you put in front of them to get the job done. And if they're more familiar with their e-mail client than other network resources, they'll use it as a substitute -- as long as you let them. Expand your definition of "desktop management" to include reaching out to users to train them on the tools your company is spending money on.

Stupid user trick No. 3: Outsourcing Web development to the corner office

Here's a thought: Don't let the CEO design your company's customer-facing Web site just so he can save a few bucks, advises an IT consultant.

"We tried to sell a medium-sized company client on both a network install and a Web site design project," the consultant says. "We got the install contract, but the CEO figured he could design his site himself.

"When his general manager -- who was also his wife -- called us back in, she pulled the site up and it was hard not to wince. He'd used an open source editor with what looked like every freely downloadable template, fonts, and flashy widgets he could find. It looked like a teenage MySpace page."

Sure, the company's product information was now available on the Web, but the lack of customer-facing tools and analysis features did not bode well for the company's Web future.

"Even the Webmaster e-mail link didn't work," the consultant says. "Needless to say, the site was not attractive to customers, so Web revenue was low, and all those new and expanding Web marketing possibilities were crippled. The same CEO who built the site started spouting about how the rumors of e-commerce revenue were false."

Solution: Today, Web site design is cheap. From local outfits to eBay or Craigslist, the cost of a decently designed Web page has dropped from thousands of dollars per page to hundreds -- or less. Stop being penny-wise and pound-foolish.

Moral: Company Web sites can't be an afterthought investment, especially for small businesses. Not just an important face to your customer, your Web site is possibly the best way to analyze exactly who your customers are and how to sell to them. Treat it professionally, and you can leverage it for additional opportunities, including market research, customer analysis, and more.

Stupid user trick No. 4: Keep your enemies close, but your Linux talent closer

Going open source can save big bucks -- unless you leave your entire open source infrastructure in the hands of a single college intern, warns an admin at a small IT services firm.

"I finally find a small-business client who made the jump to Linux -- well, Linux and HP-UX due to a silo app they had to run for two big clients," the admin says. "Our new client had used his college intern to setup the basic network, but the kid had left for summer vacation a day earlier and suddenly the network was down. We were the first outfit in the phone book that didn't shy away from the phrase 'Debian on the desktop.'"

When the admin and his cohorts arrived, all the client's server lights were green, but nobody was connecting to anything and no one could log in to the system.

"We had to restore the servers from the ground up, which took about an hour. Everything was humming after that, so we took the time to sit down with the CEO and discuss plans for the network," the admin says. Stoked to locate someone unafraid to talk about open source software, the admin and his team got a little carried away shooting the bull with the CEO and stayed for more than an hour.

"As we were on the way out, the servers dumped again," the admin says. "Same story as before. Not wanting to lose our new penguin client, we rolled up our sleeves, restored the servers, and started digging for root cause."

What they found was a cron job set up off root.

"The cron 'cd'ed to a backup directory that tried to remove the files from a lengthy list of source directories, including several that didn't exist," the admin says. "Seems the kid had been changing these on the fly for some reason -- and he apparently liked doing sys admin as root. Academics."

Solution: Protect root access. Test your cron jobs. And maintain those server backup images.

Moral: Linux has definite benefits, but there's no denying that managing it requires a certain skill set. It's not something to trust entirely to an intern.

Stupid user trick No. 5: Facebook

Face it, even the most stringent social networking policies can't diffuse the ticking time bomb that is Facebook. Throw in a little Jäger, some IT naivete, and you're set for devastating corporate embarrassment.

"About a year ago, I get a call from a junior VP who's yelling at me that he's desperate and needs me to do a 'recall on Facebook,'" says one admin who wishes to remain anonymous. "I try and get a word in edgewise, but he's ranting about what crap Web technology is and why computer people can't just leave well enough alone and how everything was fine when we just used the telephone. Then he ends with, 'Is it done yet?'"

"'Is what done?'"

"'The Facebook recall, for @#$%'s sake.'"

Which gave our admin the obvious pleasure of asking, "What the @#$% is a 'Facebook recall'?"

As it turns out, the junior VP had updated his Facebook page from his phone while having a few drinks with some senior VPs and potential new clients.

"He stated that he'd dated one of the clients' wives and made some nasty comment about what she looked like naked," the admin says. "All his college buddies were on Facebook in their college group, and he knew her when they were both at school. Turns out that's where she met her husband, too, and he was on the college Facebook group as well, which the genius junior VP figured out when he got back to the table and started a conversation about Facebook with the potential clients."

As for the "Facebook recall," it appears that the junior VP thought updating his Facebook page was like sending an e-mail in Outlook.

"I told him how to lock down his page, but apparently that was a little late," the admin says. "We didn't get that account."

Solution: There really isn't one, other than trying to make sure your users have some idea of where the power of IT ends and the big, bad world begins.

Moral: The beauty of social networking is that it connects you with millions of other people. The danger of social networking is that it connects you with millions of other people.

Stupid user trick No. 6: Offshoring while under the influence of MBA

Whoever said offshoring was idiot-proof? After all, it often involves upper management -- potentially the worst IT offenders of all.

"We got a new CIO just before the bubble burst back in 2000," says D. Aubrey, who at that time worked at a Web services firm with a solid market position that it now had to defend against upstarts. "She was one of those MIS MBAs -- emphasis on MBA. All you press types started writing stories about the benefits of outsourcing around then, so she jumped on the trend, canned our Web dev team, and outsourced the whole shebang to an outfit in Mumbai that worked for $25 an hour."

The plan looked good on paper -- until you looked at the paper.

"We got a hold of the plan spreadsheet she presented to the CEO, and all she'd done was compare the cost of software tools and staff from in-house to out-of-house, so obviously the savings looked huge," Aubrey says.

"Then came the phone bill, which I think had quadrupled for that project," he adds. "And the security audit bill, since the data our Web dev guys were working with was quite a king-size waffle of personal customer data. And the hardware/services bill for moving our data out of the outsource outfit's internal datacenter -- which as far as we could tell was four servers in a closet somewhere -- and into a professional data hosting facility in Europe."

If that weren't enough, the final product -- a redesigned site -- "looked so average it might as well have been beige."

"Just a vanilla template with shoddy JavaScript and Perl behind it," Aubrey says.

As it turned out, the new CIO had outsourced not just development, but project management and QA as well.

"There was literally nobody on our side proofing the work. They just kept showing her screenshots and she kept approving them until the day the redesign flipped," recalls Aubrey.

The volume of customer complaints about the site's new look and lack of functionality was put to a stop by the site itself, which crashed twice on the first day.

"The CEO ordered her to pull the plug and go back to the previous design," Aubrey says. "When they added it all up, she'd spent about 75 percent of the original project budget and had nothing to show for it."

"Normally, we'd have just snickered as they walked her out the door, but this was a down economy and this crap just cost us about five months of competitive advantage," he says.

The company never recovered. And though our intrepid offshorer was the first out the door, the rest of the crew followed by year's end.

"I'm not saying outsourcing doesn't work," Aubrey says. "But it takes a hell of a lot more planning than just comparing staff costs."

Solution: Go back and reread No. 3, and then realize that this submitter didn't go far enough. Web site development doesn't have to be isolated to be cheap.

Moral: If the Web site is a key revenue stream, do not entrust site development to a single exec.

Stupid user trick No. 7: Duct tape doesn't fix everything

"This one still makes us laugh over beers," says H. Foreman, an admin at a Midwest-based organization.

"We were growing pretty well in 2004 and 2005, so we opened an office across the street," Foreman says. To connect the two offices, they decided to buy two microwave bridges.

"The setup is easy enough that we were able to do the job ourselves, though we had professional carpenters install the bridges to the walls of each building, just under the roof, pointing through double-paned office glass, so we would have no weather worries."

Success carried over into 2006, when the company decided to extend its leases.

"As part of the deal, they get permission to put up a fancy sign near the top of both buildings -- indoors but facing outward through the windows," Foreman says. "The day the sign goes up, our network goes down for about 15 minutes. We're still doing the basic set of troubleshooting diagnostics when it suddenly comes back up. Our guy shrugs, verifies everything again, and lets it go."

The next morning wasn't as forgiving. The network went down and stayed down.

"The basic software diagnostics aren't working, so we go to physical link monitoring," Foreman says. "Pretty quick, we see that one of the bridges isn't responding anymore. Upstairs we go."

Apparently the bridges had been in the way of the signs.

"The outfit that put up the signs just detached the bridges and moved them -- outside," Foreman says. "There was a balcony on the upper floor and they just moved both bridges out there and then *duct-taped* both of them to the railings.

"What kills us is that the network somehow recovered the first time," he says. "The duct tape across the street held, but the one on our side slipped off during the night and the bridge fell eight stories, bounced off the dumpster, and landed behind it. The sign installers apparently left a note explaining what they'd done with the receptionist across the street and she hadn't passed it on."

Naturally, Foreman and company had fun pointing the finger at the sign company in front of the CEO, who then ran out to chew out the install rep.

"But as soon as he left the room, the CIO, who is a really good ex-tech, pointed out that if we knew someone was going to be doing construction around a critical piece of network infrastructure, why the hell hadn't we gone up there to check it? Especially after the network went down during the construction process," Foreman says. "He had a point."

Solution: The basic network monitoring software this company was evidently using is as good a technology solution as you need in this instance. Without such software, however, this would have been a much nastier adventure.

Moral: What the CIO said. Construction around network infrastructure requires personal attention from your IT staff. Remote monitoring is no substitute for "eyes-on" during critical times.

Stupid user trick No. 8: Executive privilege

This one hits close to home, as some tech magazine editors epitomize the worst kind of user an IT admin can encounter: those who have read so much about IT that they simply assume hands-on expertise. What results are "special requests" of IT not unlike those we find dealing with higher-up execs.

Let me set the stage: I was working as a technical editor for an IT magazine some years back and happened to be in the executive editor's office three days in a row when this little drama went down. I can't remember whether Windows 95 or Windows 98 had just come out, but it was one of those two. The executive editor had requested the new OS on his honking Toshiba notebook -- a $6,000 box, the price of which I still can't fathom. IT had obliged and installed it. He'd happily used it for a day, taken the box home, and when he returned the next morning it was dead. Windows wouldn't boot. The conversation went something like:

IT tech: "So what did you do?"

Executive editor: "Nothing, it just didn't reboot."

IT tech: "It couldn't have just stopped for no reason. Did you install something?"

Executive editor: "No. Really. It just wouldn't reboot."

IT tech: [sigh] "OK. Fine. I'll fix it."

The next day, the tech returned the notebook, Win 95/98 fully reinstalled and working fine. The day goes well; no crashes. The next morning, the executive editor returns yet again with a $6,000 paperweight. I'm in his office for this part and had to work hard not to shoot coffee out my nose.

IT tech: "Come on, you had to have done something. Everything was working yesterday!"

Executive editor: "No, really. I didn't install a thing. I was just working and organizing."

IT tech [suspicious]: "What do you mean 'organizing'?"

Executive editor: "You know, just arranging folders so that I can find things more easily."

IT tech [still suspicious]: And which folders were you 'organizing'?"

Executive editor [annoyed]: "What does that matter?"

IT tech [equally annoyed]: "Trust me. Which ones?"

Executive editor: "My personal folder, the issue folders, the system folder --"

IT tech [squeezing his eyes shut]: "What did you do in the system folder?"

Executive editor [slowly dawning]: "Uh, well it was so messy. They had one folder for 16-bit DLLs and another for 32-bit DLLs, so I thought it'd be more efficient if they were all, you know, in a single folder."

I'm not sure who the tech wanted to kill more: the executive editor for what he did or me for sitting there, shoulders shaking, beet red, with my mouth clenched shut and tears coming out of my eyes.

Solution: Don't let your users become case studies for denying administrative access to local machines. Deny them administrative access to begin with. With senior execs, however, it still takes a social engineering degree to keep that rule enforced. That's a line of patter every IT guy needs to develop.

Moral: Even Microsoft computers don't suddenly quit for no reason. There's always a guilty user somewhere on the chain of causality. Find him early and you can avoid a large load of trouble down the line.

Stupid user trick No. 9: User populations are like bacterial ecosystems from distant planets

This particular stupid user trick hails from my days as an IT consultant, when our clients' CIO types, who had read about Shadow Copy, immediately wanted to engage on it. After all, in many cases they'd paid for it already, so they wanted it up and running right away.

Rolling out Shadow Copy was easy -- once we had Windows 2000 on every desktop and a working Active Directory domain controller. Then I used my vaunted writing skills to pen a short and sweet "Shadow Copy Advisory" memo and e-mailed it to every user. We followed that up with personal visits to all the managers in the company, explaining how the feature worked and what they needed to tell their employees about it.

The upshot was that My Docs was now being shadow-copied for every user, so all those folders they had on their desktops should be moved to My Docs to make sure everything got backed up to the network automatically.

In retrospect, I might as well have been asking them to bite off their own fingers for my amusement.

Everyone nodded excitedly, but nobody had any intention of using it.

To be fair, this was our fault as much as theirs. Assuming that users will put data exactly where they say they will is a newb mistake. But like true consulting newbs, we set up a backup policy to perform daily backups of "data" folders -- the shadow-copied stuff and the file shares users said they were going to be using -- and weekly snaps of the full server. Desktop backups relied entirely on users making My Docs their sole data dump.

Naturally, when a nasty virus hit and took out a large percentage of the desktops and simultaneously dumped two out of three servers, we found only 8 percent of users had been taking advantage of Shadow Copy. The rest were simply screwed. Worse, we found out that they had decided to build new "informal" network shares right off the server's hard disk (exactly where we hadn't expected them to), so those files were lost, too.

Solution: First, realize that you will never get away from users using their desktops as data storage. Ever. That's why it's called the "desktop." Whatever desktop backup strategy you employ, it needs to cover the desktop -- My Docs and any personal folders they've built themselves -- automatically. On the server side, you need a daily snap, so just thank God for block-level change technology.

Moral: Great ideas are fine, but you have to weigh them against every user's inherent resistance to change. User populations are like bacterial ecosystems from distant planets. You can't predict with very much precision how they'll evolve, so things like backup need to use the word "holistic" rather than "targeted."

Courtesy : http://www.pcworld.com
September 21, 2009

Analysis

2009 Data Breaches: An Interactive Timeline

A Look at the Top Breaches Involving U.S. Financial Institutions

Total number of targeted financial institutions as of September 23, 2009: 50

Note: The following is a list of data breaches that have affected U.S. financial institutions in 2009. The information was compiled from the 2009 Data Breach Report by the Identity Theft Resource Center (ITRC), based in San Diego, CA.

JANUARY:

Heartland Payment Systems,
Princeton, NJ
Date: January 20
Records Taken: 130 million credit and debit card account numbers
Type of Breach: Outside network intrusion

Heartland Payment Systems announced on Jan. 20 that its network had been breached. The payment processor handles transactions for 250,000 merchants. Subsequently, it was revealed through indictments that 130 million credit/debit cards were compromised by the breach.

Gregory Navone,
Las Vegas, NV
Date: January 21
Records Taken: 230 credit reports
Type of breach: Missing paper documents

The Federal Trade Commission charged a Nevada mortgage broker with discarding consumers' tax returns, credit reports and other sensitive personal and financial information in an unsecured dumpster. The records included tax returns, mortgage applications, bank statements, photocopies of credit cards and drivers' licenses and at least 230 credit reports.

Developers Diversified Realty Corporation,
Beechwood, OH

Date: January 29, 2009
Records Taken: Unknown
Type of breach: Accidental breach

The New Hampshire Attorney General's office was notified by DDR that National City Bank, one of DDR's dividend disbursing agents, mailed some 1099-DIV tax forms on January 29 to the wrong shareholders. In some cases, tax forms were included in the mailings to the other shareholders. The tax forms contained names, addresses, Social Security numbers and other dividend-related information.

American Education Services - Student Loan,
Harrisburg, PA.
Date: January 29, 2009
Records Taken: 49 Social Security numbers, birthdates
Type of breach: Accidental breach

AES, the service provider for Student Loan Xpress, inadvertently transmitted names, addresses, SSNs and birthdates to another student loan lender with which AES contracted. The other lender said it destroyed all information mistakenly received. Forty-nine people in NH may be at risk of compromise.

Rhode Island Hospital,
Cranston, RI
Date: January 30, 2009
Records Taken: Unknown number of personal information on patients
Type of breach: Insider theft

A security guard at a Cranston hospital stole the identities of hospital patients and was sentenced to three years and three months in prison. He used the information to open accounts at RadioShack and bought cell phones. Three former clerks at the RadioShack store admitted their part in the scheme.

FEBRUARY

Commerce Bank - TD Bank,
Philadelphia, PA
Date: February 10, 2009
Records Taken: 240 personal information on bank customers Type of breach: Insider theft

A Philadelphia man pleaded guilty in February to charges stemming from a scheme in which he admitted using personal information of customers at a Mount Laurel bank to open fraudulent credit card accounts. Between March 1 and Oct. 30, 2007, the man used his bank job to access at least 240 bank documents with customer information, including loan information and account numbers.

Bank of the West,
Benton County, WA
Date: February 11, 2009
Records Taken: Unknown
Type of breach: Insider theft

A mother/daughter team used customer personal and financial information to open new credit cards. The daughter worked at Bank of the West in Benton County.

Bank of America,
Metro Atlanta area, GA
Date: February 17, 2009-08-23
Records Taken: Possibly hundreds of bank card numbers and passwords
Type of breach: Skimming

Federal indictments against Nikolay Nikolov, 23, and Yordan Kavaklov, 29, both of Bulgaria, allege multiple felony charges of conspiring to steal the bank card numbers and passwords of perhaps hundreds of individuals through the use of a skimming device the defendants are said to have connected to ATMs in the Metro Atlanta area in September 2008.

Unknown payment processing gateway
Date: February 19, 2009
Records Taken: 19,000 credit card numbers
Type of breach: Unknown

A defunct payment gateway exposed as many as 19,000 credit card numbers. It was discovered by an IT worker via a Google search engine where information is cached and available to anyone. The cached data included 22,000 credit card numbers, complete with CVVs, expiry dates, names and addresses. Up to 19,000 of these numbers could be active. Most are customers in the US and UK, although some are Australian.

Cornerstone Fitness Center,
Edinburg, TX
Date: February 20, 2009

Records Taken: Unknown
Type of breach: Missing paper documents

The Texas Attorney General's office charged Cornerstone Fitness Center with identity theft prevention act violations after discovering that sometime after the Edinburg fitness center closed in 2007, a filing cabinet was found behind the company's closed location, containing personal identifying information.

North Star Realty,
Draper, UT
Date: February 26, 2009
Records Taken: Unknown
Type of breach: Missing paper documents

Personal information on mortgage papers from the spring of 2004, including bank account and Social Security numbers, was found near the dumpster of North Star Realty. The realty office blamed a new employee for improper disposal of records.

MARCH

Borrego Springs Bank,
Borrego Springs, CA
Date: March 4, 2009
Records Taken: Unknown
Type of breach: Stolen or missing hardware

The theft of six laptop computers from a Laguna Hills auditing firm prompted the Borrego Springs Bank to send warning letters to all of its customers, saying their personal financial information may be in the hands of criminals. The auditing firm says the information included personal information from multiple banks, not just Borrego Springs Bank.

Branch Banking & Trust,
Winston-Salem, NC
Date: March 5, 2009
Records Taken: Unknown
Type of breach: Insider theft

While investigating another matter, BB&T conducted an internal investigation and discovered that a former employee who had legitimate access to client accounts abused the access and sold client signature card information to others for fraudulent purposes. The client information sold included names, addresses, Social Security numbers, birthdates, bank account numbers, driver's license numbers and signatures.

Taco Bell,
Southern Colorado
Date: March 12, 2009
Records Taken: 48 credit card account numbers
Type of breach: Insider theft

Three alleged crooks were charged with stealing personal information from unsuspecting customers by skimming credit cards. A restaurant employee sold the customers' card information to three suspected crooks, who went shopping around town. The suspects were charged with racketeering for allegedly ringing up more than $14,000 on other people's credit cards.

Metro City Bank,
Doraville, GA
Date: March 16, 2009
Records Taken: Unknown
Type of breach: Outside network intrusion

Researchers from Prevx, a UK-based online security firm, discovered a data trove used to store stolen information from 160,000 infected computers. According to sources at Metro City Bank, their computer was one of the infected computers.

Breakwater Mortgage Corporation,
Williamsburg, VA
Date: March 16, 2009
Records Taken: Unknown
Type of breach: Missing paper documents

A Virginia man who bid on seven file cabinets at a storage auction discovered dozens of files inside with personal and financial information that belonged to Breakwater Mortgage Corporation. The firm went out of business in 2008.

Clear Star Financial Credit Union,
Reno, NV
Date: March 25, 2009
Records Taken: 28 personal identities
Type of breach: Unknown

The Reno Police Department is working with a local credit union after nearly 30 reports of credit card fraud. There have been 28 reports of fraud at Clear Star Financial Credit Union. All victims reported unauthorized charges at Chicago-area stores.

Bank of America,
Bethlehem PA
Date: March 26, 2009
Records Taken: 286 bank accounts
Type of breach: Skimming

Bethlehem police confirmed a skimmer had been attached to the Bank of America ATM on East Third Street. Video surveillance was also used to film ATM users' personal information as it was entered into the machine. A total of 286 accounts have already been compromised and over $43,000 lost, says investigator Rob Toronzi.

LPL Financial,
Alpharetta, GA
Date: March 27, 2009
Records Taken: Unknown
Type of breach: Stolen or missing hardware

Two desktop computers were stolen from the office of Sullivan and Schlieman Wealth Management, LLC, a financial advisor in Alpharetta, GA. Personal information of LPL clients, including names, addresses, financial account information and Social Security numbers "may have been breached," according to a June 1 letter sent to the New Hampshire Attorney General's office by LPL. Although the theft occurred on March 27 and was reported to the local police, LPL was not notified of the incident until April 29. Affected individuals were notified in May.

APRIL

LPL Financial,
Westlake, OH
Date: April 8, 2009
Records Taken: Unknown
Type of breach: Stolen or missing hardware
Two computers and a server were stolen from the office of Sandru Financial, which included LPL Financial client names, financial account information and SSN. LPL has had multiple breaches over the past several years. The company notified Maryland's AG about the breach.

Staten Island Bank & Trust,
Oakwood, NY
Date: April 15, 2009
Records Taken: Information on 50 bank accounts
Type of breach: Skimming

An ATM security breach at SI Bank & Trust's Oakwood branch went undetected for more than a month, but now is under investigation by the FBI. An ATM device captured customer info and at least 50 of the bank's customers were affected.

DFS Capital Funding
Franklin, IN
Date: April 19, 2009
Records Taken: Unknown
Type of breach: Missing paper documents

A man found a pile of personal documents along the side of the road in rural Johnson County in April. Among the documents was a folder containing a loan application of an Ohio couple, including their Social Security numbers, bank information, places of employment and phone numbers. Franklin-based DFS Capital Funding is the company listed on the paperwork. It looks to have given a loan approval to the Ohio couple in 2005.

Centaurus Financial Inc.,
Orange County, CA
Date: April 28, 2009
Records Taken: Unknown
Type of breach: Outside network intrusion

The Financial Industry Regulatory Authority (FINRA) fined Centaurus Financial, Inc. (CFI), of Orange County, CA, $175,000 for its failure to protect certain confidential customer information. FINRA says from April 2006 to July 2007, CFI failed to ensure that it safeguarded confidential customer information. Its improperly configured computer firewall - along with an ineffective username and password on its computer facsimile server - permitted unauthorized persons to access stored images of faxes that included confidential customer information, such as social security numbers, account numbers, birthdates and other sensitive, personal and confidential data.

WaMu Investments, Inc.,
Irvine, CA
Date: April 30, 2009
Records Taken: Unknown
Type of breach: Missing paper documents

WaMu Investments notified the New Hampshire AG that during a review it discovered that personal documents containing names, account numbers, addresses, estimated annual income and estimated net worth are missing. They have searched "extensively through files ...both in our offices and at our offsite storage location." The documents were from 2001 and 2006. This affects people in various states.

MAY

Southern Florida ATMs,
Broward, Palm Beach, Miami-Dade Counties, FL
Date: May 1, 2009
Records Taken: Unknown
Type of breach: Skimming

According to a Department of Justice indictment, the defendants and their co-conspirators used a "skimming device" to capture the information stored on the magnetic stripe of bank debit cards when the cards were placed into ATMs throughout Broward, Palm Beach and Miami-Dade Counties. The skimming devices and hidden micro-video cameras were placed on the ATMs to record customers' PINs as they conducted their transactions. The money was sent to individuals in the US, Romania and other locations.

First Bank,
Westminister, CO
Date: May 2, 2009
Records Taken: Unknown
Type of breach: Skimming

Local police report that a "skimming device" used to steal information from credit and debit cards was found near an ATM at a First Bank branch in Westminister.

First Republic Bank,
San Francisco, CA
Date: May 4, 2009
Records Taken: 560 bank customer PII
Type of breach: Insider theft

A former San Francisco bank mailroom supervisor accused in an identity theft scam faces up to seven years in prison if convicted. San Francisco prosecutors say that over a six-month period beginning in April 2007, he allegedly opened customer mail at a First Republic Bank branch containing both commercial and personal identifying information. He then allegedly made copies of checks, and sold those copies as part of a larger identity theft scheme. The checks were later used by someone else to replicate the bank account. The Secret Service says as many as 560 pieces of mail may have been opened.

Countrywide Financial,
Fort Worth, TX
Date: May 4, 2009
Records Taken: 4,000 account numbers
Type of breach: Insider theft

A man posing as an Air Force reservist seems to have gotten thousands of account numbers from Countrywide Financial in Forth Worth. The investigators tracked the case to his accomplice, a customer service rep. The Air Force impostor stole $500,000.

CompuCredit, Aspire,
Indianapolis, IN
Date: May 11, 2009
Records Taken: 120 credit card statements
Type of breach: Exposure of data on Internet

A major credit card company is investigating how more than 100 statements were made available online. Account information including SSNs was involved. Further information reveals that it was a computer processing error that created a single image file of 120 account statements.

Sovereign Bank,
Staten Island. NY
Date: May 11, 2009
Records Taken: 250 bank customer account numbers and PINs
Type of breach: Skimming

A band of thieves installed Sovereign Bank ATMs with skimmers so that they could steal account and password information from bank customers. They placed cameras to film victims typing in PIN codes. The bank is reimbursing customers for the fraudulent withdrawals. The thieves stole $500,000 from 250 customer accounts.

Colonial Penn,
Philadelphia, PA
Date: May 15, 2009

Records Taken: Information on 120 bank accounts
Type of breach: Insider theft

A former Colonial Penn Life Insurance Co. employee was indicted by a federal grand jury in May on charges of using company computers to steal personal and bank-account information of customers who also had accounts with Citizens Bank, M&T Bank and Wachovia Bank. More than 120 customers had their details stolen. Law enforcement says between Aug. 1, 2007 and Aug. 8, 2008, Lisa Bryant Nelson, 37, of North Philadelphia, PA passed on the customers' information to individuals who made fake IDs and counterfeit checks in the names of the bank customers.

Members Plus Credit Union,
Somerville, MA
Date: May 18, 2009
Records Taken: Unknown
Type of breach: Missing paper documents

MPCU says it lost a box in Sept 2008 that included account and SSN information of members from Dec 2000 to Nov 2001. The credit union became aware of the loss in April 2009. The credit union notified Maryland's AG about the breach.

Chase Bank
New York, NY
Date: May 18, 2009
Records Taken: Unknown
Type of breach: Skimming

Four Romanian men were arrested in Florida after being accused of skimming a Central New York Chase Bank ATMs. Police say several customers who used the ATM at a Chase Bank in Cicero later found cash had been withdrawn from their accounts from ATMs in New York City, totaling about $40,000. A skimmer was found in the card slot of the machine.

Four Peaks Financial Services
Scottsdale, AZ
Date: May 30, 2009
Records Taken: Unknown
Type of breach: Exposure of data on Internet

Four Peaks is accused of exposing its customers' sensitive personal information, including name and credit card numbers, on its website. The state's enforcement action charges Four Peaks with violating the Texas Identity Theft Enforcement and Protection Act, which carries penalties that range between $2,000 and $50,000 per violation of the act. Four Peaks is a debt reduction/settlement company.

JUNE

Charles Schwab Corp.,
San Francisco, CA
Date: June 12, 2009
Records Taken: Unknown
Type of breach: Stolen or missing hardware

Investment firm Charles Schwab notified the New Hampshire Attorney General's Office that in early May a computer hard drive containing client personal information, including Social Security number, name or account number, was stolen. The hard drive had been taken off of company premises, in violation of company policy, and was subsequently stolen.

Beneficial,
South Bend, IN
Date: June 20, 2009
Records Taken: 80 loan application files
Type of breach: Missing paper documents

The Indiana attorney general's office investigated how at least 80 files of personal loan-application information ended up in a dumpster behind a shopping center in South Bend. In the files were loan applications, complete with names, Social Security numbers and bank account numbers. Also included in the records were tax returns, copies of checks, credit reports, good-faith estimates, signed disclosure notices, and certificates of survey.

JULY

American Express,
Phoenix, AZ
Date: July 7, 2009
Records Taken: Thousands of card numbers
Type of breach: Insider theft

Two Phoenix men are accused of stealing thousands of American Express card numbers and swindling more than $1 million dollars from customers. Police discovered during their investigation that a former employee had not only worked as a computer database analyst for American Express, he was one of the few who could have possibly downloaded all of their account holders information, including the PIN numbers used to access money from ATM machines at the different banks, according to court records.

Wachovia Bank,
Williamsburg, VA
Date: July 15, 2009
Records Taken: Unknown
Type of breach: Insider theft

A Hampton, VA woman was charged of using her Wachovia bank teller position to access customer information and open fraudulent credit card accounts in their names for a commission.

American Express,
Canfield, OH
Date: July 23, 2009
Records Taken: 300 American Express account numbers
Type of breach: Insider theft

A former American Express employee and four other alleged accomplices were arraigned for theft of 300 American Express account numbers. The alleged ring leader of the group is Melissa Zingarelli, 36, a former employee of American Express.

AUGUST
Morrison Financial Corp,
Wichita, KS
Date: August 4, 2009
Records Taken: Unknown
Type of breach: Missing paper documents

Client records from a defunct Wichita mortgage-brokerage firm were found in the dumpster outside the Holiday Inn in Wichita. Some of the information contained in the boxes of documents found at the Holiday Inn included Social Security numbers, bank account numbers and photocopies of drivers' licenses and checks.

Wachovia Bank,
Atlanta, GA

Date: August 7, 2009
Records Taken: Unknown
Type of breach: Insider theft

Three metro Atlanta residents were indicted on bank fraud conspiracy and identity theft charges for allegedly stealing Wachovia Bank account numbers and taking thousands of dollars from the accounts. One of the defendants worked in a department and had access to customer account information, including account numbers, signature cards, related accounts, and personal identifying information of the account holders.

Citigroup,
Boston, MA
Date: August 10, 2009
Records Taken: Unknown
Type of breach: Unknown

Bank of America Corp. and Citigroup Inc. have issued new credit and debit cards to Massachusetts customers after running into data-safety concerns. Charlotte-based BofA and Citigroup each recently issued replacement cards to consumers, telling them in letters that their account numbers may have been compromised by an undisclosed third-party.

Bank of America,
Boston, MA
Date: August 10, 2009
Records Taken: Unknown
Type of breach: Unknown

Bank of America Corp. and Citigroup Inc. have issued new credit and debit cards to Massachusetts customers after running into data-safety concerns. Charlotte-based BofA and Citigroup each recently issued replacement cards to consumers, telling them in letters that their account numbers may have been compromised by an undisclosed third-party.

Wells Fargo Bank,
Sacramento, CA
Date: August 14, 2009
Records Taken: Unknown
Type of breach: Insider theft

A Wells Fargo Bank employee working inside a bank call center was arrested on August 14, using customer account access to pay her own debts, says the U.S. Attorney's office. Ronita Prasad, of Antelope, CA, opened credit card accounts and

ATM cards between December 2008 and July 2009. She gained access to customer accounts through a protected system without authorization.

Unknown Denver Realtor,
Denver, CO
Date August 14, 2009
Records Taken: Hundreds of loan documents
Type of breach: Missing paper documents

The Colorado Division of real estate removed hundreds of loan documents that included house appraisals, social security numbers, addresses, phone numbers, even copies of checks from a dumpster at a Denver shopping center. The state regulator says an investigation is underway and may lead to censure or suspension of the realtor or appraiser's state license.

Sun Valley Mortgage
Weber County, UT
Date: August 18, 2009
Records Taken: 600 account numbers and SSNs
Type of breach: Stolen or missing hardware

The Weber County Sheriff's office is investigating a missing laptop from a Sun Valley Mortgage loan officer. Officers say the loan officer accidentally left his computer on a sidewalk instead of putting it in his car. On the laptop were the names, social security numbers and account numbers of 600 clients of the mortgage company.

SEPTEMBER

Jonathan Boxman
Staten Island, NY
Date: September 6, 2009
Records taken: Hundreds of credit reports
Type of breach: Missing paper documents

A former title-insurance agent who was arrested in July on charges he allegedly stole money from clients is also accused of dumping boxes of client files. Hundreds of Jonathan Boxman's clients' files were found behind the office building. Some files contained personal identifiable information, including Social Security numbers, copies of driver's licenses, original deeds and mortgage papers.

Capitol One Bank
Minneapolis, MN
Date: September 6, 2009
Records taken: Unknown number of bank customer accounts
Type of breach: Exposure of data on Web

Prosecutors in Minneapolis say between July 2008 and April 2009 a crime ring purchased the personal information of Capitol One Bank customers from an online source in the Ukraine, who illegally profited from the sale. It says the group then used the information to create counterfeit credit card accounts, withdrawing more than $652,205.49 from more than 170 ATMs throughout the Twin Cities. Eleven people have been charged in the counterfeit credit card scheme, eight of them are in custody.

7 Mortgage companies
San Francisco. CA
Date: August 1, 2009
Records taken: Hundreds of personal records
Type of breach: Missing paper documents

The San Mateo County Sheriff's department reports that it found hundreds of papers in a dumpster on August 1, including mortgage, titles and other personal information generated between Jan. 1 and July 1, 2006. Among the mortgage, lending and title companies listed on the paper work are Alliance Title; American Prime Funding; Funding Suite; Financial Title Company; Ticor Title Company; Orange Coast Title Company; and Bella Homes and estates.

Courtesy : Linda McGlasson; http://www.cuinfosecurity.com
September 23, 2009
Source: Identity Theft Research Center
Research : Dinesh Bareja

EVENTS

Gitex Technology Week

Date : October 18, 2009
Location : Dubai International Conventional Exhibition Centre, Dubai
Website : http://www.gitex.com/

---

fourth annual eCrime Researchers Summit (eCRS)

Date : October 20, 2009
Location : Tacoma, WA, USA
Website : APWG <http://www.antiphishing.org/>
http://www.ecrimeresearch.org/2009/cfp.html

The 3rd International conference on IPRs
Personal Data Protection and National Security

Date : October 20-22, 2009
Location : Beirut, Lebanon
Website : http://www.cybercrime-fr.org/index.pl/cyberlaw2009

OWASP AppSec Brasil 2009

Date : October 27, 2009
Location : Câmara dos Deputados in Brasília, DF
Website : https://www.owasp.org/index.php/AppSec_Brasil_2009

T2'09

Date : 29 October, 2009
Location : Câmara dos Deputados in Brasília, DF
Website : http://www.t2.fi/

New age cyber crime – by Marcusevans

Date: 29 & 30 October 2009
Location: Le Royal Meridian, Mumbai, India
Email: leec@macrusevanskl.com