

Bank's antifraud tactics stun security expert

By Ellen Messmer

December 14, 2009 04:31 PM ET

Network World - Checking out of a Hilton hotel in London, security expert Roger Thompson was told his Visa card had been declined due to suspicions it was stolen, a situation that only got more disconcerting when he learned the bank that issued the card had more personal information on him and his family members than he ever imagined.

In a tale he relates in his [blog](#), Thompson, chief research officer at AVG, said he was compelled to answer questions on the phone from a Wachovia Bank representative in its fraud-prevention division to prove he was really Roger Thompson and not a credit-card thief checking out of the London hotel.

It turns out Thompson's Visa card was flagged and suspended because he hadn't told the bank he was travelling overseas, a requirement he didn't know the bank had. But the "scary bit" about it all, he says, is that the bank fraud-prevention representative didn't just ask him to give the correct answers to questions such as his mother's maiden name, which he had provided to the bank for fraud detection purposes, but also a host of other questions about his daughter-in-law that he had no idea it knew.

"I was in shock," Thompson says about what he found out that Wachovia Bank had stored "at their fingertips" related to his daughter-in-law -- information Thompson thinks the bank may have found out through Facebook.

"They used her maiden name, they knew she was my daughter in-law, they wanted me to best describe the age range for this person," Thompson says, adding that he was in "shock and indignation" about how they would know all this, including how long she was married.

The bank fraud-prevention representative indicated it was all "publically available information," he says. At the hotel on the phone, Thompson answered the questions about his daughter-in-law, the bank lifted the suspension on his credit card, and he paid his bill and left for the airport.

Thompson says he wracked his brain to figure out where the bank may have gotten this information about his daughter-in-law but he could only reason it was from Facebook, where she's a friend.

Thompson, a security expert with decades of experience in identifying malware, fraud and hacker exploits of social-networking sites, such as MySpace and Facebook, says he doesn't see this as an issue around Facebook per se. Rather, this is about what kind of data that corporations may be collecting from Facebook or other social-networking sites -- if they are. He adds this strikes him as a serious data-privacy issue, and he notes that if a bank has this kind of database information on him, "they probably have it on you, too."

Wachovia, now owned by Wells Fargo, wasn't immediately available for comment on whether they do harvest information from social-networking sites for purposes of fraud detection or where they are obtaining personal information of this type not voluntarily provided by a customer.

TSA LEAK ILLUSTRATES NEED FOR ADEQUATE SOFTWARE/SECURITY TRAINING

DECEMBER 10TH, 2009 - BILL DETWILER

IT HASN'T BEEN A GOOD WEEK FOR THE DEPARTMENT OF HOMELAND SECURITY (DHS) OR THE TRANSPORTATION SECURITY ADMINISTRATION (TSA). ON SUNDAY, NEWS OF AN IMPROPERLY REDACTED AIRPORT SCREENING MANUAL BEGAN TO CIRCULATE THE WEB. BY TUESDAY THE STORY HAD HIT MAINSTREAM MEDIA AND THE EVENING NEWS. AND BY WEDNESDAY, HOMELAND SECURITY SECRETARY JANET NAPOLITANO WAS TELLING MEMBERS OF THE US SENATE JUDICIARY COMMITTEE THAT DHS AND TSA WERE TAKING STEPS TO ENSURE SUCH A LEAK DOESN'T OCCUR AGAIN.

SECRETARY NAPOLITANO DOWNPLAYED THE LEAK'S SEVERITY, BUT AS CBS NEWS CORRESPONDENT BOB ORR POINTS OUT IN THE VIDEO, THE DOCUMENT CONTAINS LOTS OF SENSITIVE INFORMATION, SUCH AS:

- HOW WALK-THROUGH METAL DETECTORS ARE CALIBRATED
- PICTURES OF THE BADGES AND ID CARDS USED BY THE ATF, CIA, FEDERAL AIR MARSHALS, AND MEMBERS OF CONGRESS
- ITEMS WHICH AREN'T REQUIRED TO BE SCREENED (WHEELCHAIRS, PROSTHETIC DEVICES, ETC.)
- SPECIAL TREATMENT FOR FOREIGN DIGNITARIES
- THOSE COUNTRIES WHOSE TRAVELERS ARE ALWAYS SUBJECT TO EXTRA SCREENING

TO MAKE MATTERS WORSE, THIS LEAK WASN'T THE WORK OF CYBER SPIES. NO. A REDACTED VERSION OF THE DOCUMENT WAS INTENTIONALLY POSTED ON A GOVERNMENT WEB SITE AS AN ADOBE PDF FILE. UNFORTUNATELY, THE INDIVIDUAL WHO CREATED THE FILE MERELY PLACED BLACK BOXES OVER THE SECTIONS TO BE REDACTED. THE HIDDEN TEXT WAS LEFT WITHIN THE DOCUMENT. TO VIEW THE TEXT, INDIVIDUALS NEEDED ONLY COPY THE TEXT AROUND AND UNDER THE BOXES AND PASTE IT INTO ANOTHER WORD PROCESSOR.

WHILE IT'S TOO LATE TO UNDO ANY DAMAGE CAUSED BY THE RELEASE OF THIS DOCUMENT, THE EVENT SHOULD SERVE AS A WARNING TO ALL ORGANIZATIONS AND IT DEPARTMENTS THAT HANDLE SENSITIVE INFORMATION. ELECTRONIC DOCUMENTS OFTEN STORE HIDDEN INFORMATION (METADATA) THAT ISN'T IMMEDIATELY VISIBLE WHEN VIEWING THE DOCUMENT ON A COMPUTER OR PRINTING IT. ALL EMPLOYEES RESPONSIBLE FOR RELEASING, PUBLISHING, OR TRANSMITTING DOCUMENTS WITH SENSITIVE INFORMATION SHOULD BE THOROUGHLY TRAINED ON THE EXISTENCE OF AND PROPER WAY TO REMOVE METADATA. IN FACT, WE WOULDN'T BE HAVING THIS DISCUSSION IF THE TSA EMPLOYEES INVOLVED HERE HAD FOLLOWED THE **NATIONAL SECURITY AGENCY GUIDELINES ON REDACTING INFORMATION FROM MICROSOFT WORD OF ADOBE PDF FILES.**

I ENCOURAGE ALL IT DEPARTMENTS TO REMIND THE INDIVIDUALS YOU SUPPORT ABOUT THE DANGERS OF HIDDEN METADATA AND THE PROPER WAY TO REMOVE IT.

RETHINK WEB-SITE SECURITY MANAGEMENT: CYBERCRIMINALS ALREADY HAVE

DECEMBER 23RD, 2009

MICHAEL KASSNER

WEB SITES ARE BECOMING CYBERCRIMINALS' PREFERRED WAY TO STEAL SENSITIVE INFORMATION. IT'S ALSO THEIR METHOD OF CHOICE FOR INSTALLING MALWARE ON VISITOR'S COMPUTERS.

THE BAD GUYS FIGURED IT OUT. WEB SITES ARE AN EASY MARK. ONCE COMPROMISED, A WEB SITE CAN BE AN ENTRY POINT TO BACK-END SERVERS. AT THE SAME TIME, IT CAN BE A PLATFORM TO DOWNLOAD MALWARE. JUST PLUG "COMPROMISED WEB SITES" INTO ANY SEARCH ENGINE AND YOU WILL SEE HOW SUCCESSFUL THIS VENTURE IS. TOP SLOT ON GOOGLE WAS AN SC MAGAZINE **ARTICLE** TALKING ABOUT A **WEBSense** STUDY: "OF THE TOP 100 MOST POPULAR SITES ON THE WEB, 70 PERCENT ARE EITHER HOSTING MALICIOUS CONTENT OR CONTAIN A HIDDEN REDIRECT."

IF THAT ISN'T BAD ENOUGH:

"THE NUMBER OF LEGITIMATE WEBSITES COMPROMISED WITH MALICIOUS CONTENT EXCEEDS THE AMOUNT OF SITES SPECIFICALLY CREATED BY CYBERCRIMINALS TO CARRY OUT THEIR EXPLOITS."

WHY?

WHAT I DID NOT UNDERSTAND WAS, WHY? THEN I CAME ACROSS THE REPORT, "**VULNERABILITIES HIGHLIGHT THE NEED FOR MORE EFFECTIVE WEB SECURITY MANAGEMENT**" (PDF). THE TITLE SAYS IT ALL. IT'S WHAT DEPARTMENT OF HOMELAND SECURITY (DHS) INSPECTOR GENERAL RICHARD SKINNER AND HIS TEAM FOUND AFTER ASSESSING THE NINE MOST-POPULAR WEB SITES RUN BY THE DHS:

- CUSTOMS AND BORDER PROTECTION (**CBP.GOV**)
- DHS HEADQUARTERS (**INTERACTIVE.DHS.GOV**)
- FEDERAL EMERGENCY MANAGEMENT AGENCY (**FEMA.GOV**)
- FEDERAL LAW ENFORCEMENT TRAINING CENTER (**FLETC.GOV**)
- IMMIGRATION AND CUSTOMS ENFORCEMENT (**ICE.GOV**)
- NATIONAL PROTECTION AND PROGRAMS DIRECTORATE (**US-CERT.GOV**)
- TRANSPORTATION SECURITY ADMINISTRATION (**TWICPROGRAM.TSA.DHS.GOV**)
- UNITED STATES COAST GUARD (**USCG.MIL**)
- UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES (**USCIS.GOV**)

THOSE ARE DEFINITELY IMPORTANT WEB SITES AND NEED TO BE SECURE AS POSSIBLE. I WAS ESPECIALLY INTERESTED IN THE NATIONAL PROTECTION AND PROGRAMS DIRECTORATE'S (NPPD) WEB SITE. YOU MAY RECOGNIZE NPPD AS US-CERT OR THE UNITED STATES COMPUTER EMERGENCY READINESS TEAM. FORTUNATELY, US-CERT'S WEB SITE ALONG WITH THOSE CONTROLLED BY USCG AND FEMA CONTAINED NO CRITICAL VULNERABILITIES AND ALL SECURITY PATCHES WERE APPLIED. MR. SKINNER MENTIONED THAT:

“THESE COMPONENTS’ (WEB SITES) SECURITY PRACTICES, THROUGH PERIODIC ASSESSMENTS, PATCH AND UPDATE POLICIES, AND DOCUMENTED PROCEDURES, SET THE EXAMPLE OF AN EFFECTIVE DEFENSE-IN-DEPTH APPROACH TO GOOD IT SYSTEMS SECURITY.”

WHAT WAS TESTED

PART OF THE ASSESSMENT WAS TO CHECK THE WEB SERVERS. THE INSPECTORS FOUND THE EQUIPMENT AND OPERATING SYSTEM SOFTWARE TO BE MORE THAN ADEQUATE SECURITY-WISE. THAT’S NOT WHAT I EXPECTED. THEN MR. SKINNER MADE THE FOLLOWING COMMENT:

“COMPONENT IT SECURITY PERSONNEL REGULARLY PERFORMED THESE TESTS ON OPERATING SYSTEMS, BUT ONLY A FEW HAD THE TOOLS OR EXPERIENCE TESTING WEB APPLICATIONS FOR SECURITY VULNERABILITIES. AS WEBSITE CONTENT IS UPDATED OR CHANGED, EXISTING VULNERABILITIES MAY REMAIN OR NEW VULNERABILITIES CAN BE INTRODUCED, PUTTING THE SYSTEM AND DATA AT RISK.”

THE ACTUAL VULNERABILITIES ARE IN THE REPORT, BUT WERE REDACTED ALONG WITH OTHER SENSITIVE INFORMATION. EVEN SO, THINGS WERE STARTING TO MAKE SENSE. COULD THIS BE THE CASE WITH OTHER WEB SITES?

RECOMMENDATIONS

THE INSPECTOR GENERAL MADE THE FOLLOWING RECOMMENDATIONS:

- REQUIRE PERIODIC SECURITY VULNERABILITY ASSESSMENTS OF ALL PUBLIC-FACING WEB SITES.
- REQUIRE PROMPT APPLICATION OF SECURITY PATCHES TO SERVERS SUPPORTING PUBLIC-FACING WEB SITES.
- CLARIFY THE DEPARTMENT’S VULNERABILITY-ASSESSMENT POLICY, MAKING SURE TO ADDRESS THREATS SPECIFICALLY ASSOCIATED WITH ITS WEB SITE.
- CREATE AN INVENTORY OF ALL MAJOR APPLICATIONS AND SUPPORT SYSTEMS USED BY PUBLIC-FACING WEB SITES.

I ASKED A FRIEND OF MINE, WHO IS A WEB-SITE DESIGNER, ABOUT THE RECOMMENDATIONS. SHE FELT THEY WERE GOOD, MENTIONING THAT MORE OF HER CLIENTS NEED TO IMPLEMENT THEM.

FINAL THOUGHTS

THE REPORT ANSWERED MY QUESTION. WE NEED TO FOCUS AS MUCH ATTENTION ON THE WEB-SITE APPLICATION AS THE WEB SERVER HOSTING IT. REPORTS LIKE THE DHS INSPECTOR GENERALS SHOULD GET US MOVING IN THE RIGHT DIRECTION. AS, THERE IS A LOT OF MONEY RIDING ON CONSUMERS BEING ABLE TO TRUST WEB SITES.

FIVE TECHNOLOGY TRENDS TO WATCH IN 2010

DECEMBER 23RD, 2009

JASON HINER

TECHNOLOGY INNOVATION CONTINUED ITS RUTHLESS PACE IN 2009, DESPITE THE ECONOMIC HEADWINDS. NOW IT’S TIME TO TURN OUR SIGHTS ON 2010, WHERE THERE ARE GOING TO BE SOME REALLY INTERESTING

THINGS TO KEEP AN EYE ON. LET'S COUNT DOWN THE FIVE TECH TRENDS THAT SHOULD BE ON YOUR RADAR FOR 2010.

5: THE CONSUMERIZATION OF IT

THIS IS SOMETHING WE'VE BEEN TALKING ABOUT FOR A COUPLE YEARS BUT THE TREND IS ACCELERATING. WE SEE IT IN EMPLOYEES USING THEIR OWN PERSONAL LAPTOPS AND DEVICES FOR WORK TASKS AND USING FREELY AVAILABLE WEB TOOLS TO HELP THEM GET THEIR JOBS DONE. THIS CAN CREATE A WHOLE HOST OF PROBLEMS FOR IT, BUT IN MOST CASES YOU DON'T WANT TO SQUASH IT ALTOGETHER. WHAT YOU'LL NEED IS A POLICY THAT GIVES EMPLOYEES GUIDANCE ON HOW AND WHEN THESE TYPES OF TOOLS CAN AND CAN'T BE USED, AND WHY.

4: DESKTOP VIRTUALIZATION

TECHREPUBLIC RECENTLY ASKED ITS CIO JURY ABOUT DESKTOP VIRTUALIZATION AND 75% SAID THEY WEREN'T INTERESTED. HOWEVER, THE 25% THAT ARE INTERESTED ARE VERY ENTHUSIASTIC ABOUT USING IT TO CUT COSTS AND SIMPLIFY IT SUPPORT. IN 2010, IT'S GOING TO BE INTERESTING TO SEE IF THIS TREND GAINS MOMENTUM AND BECOMES MORE MAINSTREAM, OR IF IT'S SIMPLY RELEGATED TO A FEW NICHE SCENARIOS AND INDUSTRIES.

3: E-READERS

WHILE MOST OF THE BUZZ AROUND E-READERS IS CENTERED AROUND CONSUMERS READING BOOKS AND NEWSPAPERS, THERE ARE ALSO A NEW SET OF E-READERS THAT WILL HIT THE MARKET IN 2010 THAT ARE AIMED AT HELPING BUSINESSES STREAMLINE THE MEETINGS THAT REQUIRE HUGE STACKS OF PAPER AND BRING MORE MULTIMEDIA CAPABILITIES TO BUSINESS DOCUMENTS. FOR MORE AMMUNITION ON WHY YOU SHOULD FOLLOW THIS TREND, SEE JACK WALLEN'S ARTICLE "**10 REASONS WHY E-READERS MAKE SENSE IN THE ENTERPRISE.**"

2: WAN ACCELERATION

I CONSIDER WAN ACCELERATION TO BE ONE OF THE BEST KEPT SECRETS IN THE IT AND BUSINESS WORLDS. BY CACHING BIG FILES AND OFTEN-USED DOCUMENTS, WAN ACCELERATION APPLIANCES AND SOFTWARE CAN SAVE BIG MONEY ON BANDWIDTH COSTS AND GIVE YOUR BRANCH OFFICES AND REMOTE WORKERS FAR BETTER PERFORMANCE ON THEIR BUSINESS APPLICATIONS. COMPANIES LIKE RIVERBED ARE EVEN TAKING WAN ACCELERATION A STEP FURTHER AND USING IT TO HELP SPEED UP HOSTED CLOUD APPLICATIONS BY PARTNERING WITH MAJOR SAAS PROVIDERS. ALL OF THIS MAKES WAN ACCELERATION ONE OF THE HOTTEST PROJECTS IN IT RIGHT NOW, BECAUSE IT CAN OFFER FAST ROI AND IMMEDIATE PRODUCTIVITY BENEFITS.

1: BERRIES, APPLES, AND ROBOTS

WHAT DO THESE THREE THINGS HAVE IN COMMON? WELL, OF COURSE, WE'RE TALKING ABOUT SMARTPHONES WITH BLACKBERRY, APPLE IPHONE, AND GOOGLE ANDROID. THESE ARE THE THREE SMARTPHONE PLATFORMS THAT HAVE THE MOST MOMENTUM HEADING INTO 2010. WITH SMARTPHONES BECOMING STANDARD TOOLS FOR MORE AND MORE BUSINESS WORKERS, IT'S GOING TO BE IMPORTANT TO WATCH WHICH DEVICES USERS GRAVITATE TOWARD, WHICH PLATFORMS OFFER IT MORE SECURITY AND MANAGEABILITY FEATURES, AND WHICH ONES DEVELOPERS LATCH ON TO AS THE BEST PLACE TO BUILD NEW APPLICATIONS FOR BUSINESS USERS.

Cloud Computing Continues to Put Jobs at Stake

by [Michael Overly](#)

Mon, 2009-12-28

What jobs are we talking about? Yours. That is, the trend in cloud computing continues, in general, to be service offerings provided under some of the most minimal service level protections ever seen. When those meager service levels are further diluted by numerous exceptions to and qualifications on performance and, in many cases, unlimited downtime for "scheduled maintenance" (i.e., as long as the vendor gives you a heads up, it can take the service down for as long as it wants without fear of a service level failure), you have a service that is being provided on more or less an as-is basis. While this approach may actually be considered in non-critical, low-risk engagements, it can be a "job-coster" for the business person who accepts these risks in the context of critical, high value engagements.

In a recent engagement, a vendor of an expensive, critical solution offered an SLA that provided little in the way of credits for failure to achieve required performance standards. When pressed on this issue, the vendor offered no movement on the relatively useless credits, but offered to provide the customer with the right to terminate in the event of ongoing poor performance. How did the vendor define "ongoing poor performance"? They offered termination if the service was down for four consecutive months or any five months in a seven month period. This type of offer is the reason for the title to this blog entry: it affords the business person who accepts this type of useless protection to place their job at risk when the vendor fails to perform. That is, more and more vendors simply cast their refusal to provide meaningful service levels and remedies as business risks that must be assumed by their customers.

In the current economic environment approving an agreement that would require the company to pay essentially full price for months and months in which service is not provided or performance is so spotty that it is all but useless, could be a career ending decision. That is why at least some business people are taking a long, hard second look at these types of arrangements and refusing to sign without appropriate protections. Those that don't had better update their resumes.

Social Networking Use Increases, But Has Yet to Transform Government

Dec 29, 2009, By Tod Newcombe,

For years, one of the ways the California Department of Motor Vehicles (DMV) connected with the public was by investing in old-fashioned audio-visual production, usually a series of films teaching safe driving. Despite their best efforts, DMV officials struggled to show these films to their most important audience: young drivers.

Two years ago, the country's largest state motor vehicles agency decided to post the videos online by creating a channel on YouTube. Suddenly the videos that no teenager wanted to watch became a huge hit, according to the department's CIO, Bernard Soriano. Today the DMV's YouTube channel has more than 3,500 subscribers and its videos have been watched nearly 500,000 times; ["Kyle's Drive Test"](#) leads the way with more than 250,000 views.

"We think the viral effect of the Internet made them so popular," Soriano said. "It really speaks to the power of social media."

What seemed like a radical idea two years ago is becoming increasingly commonplace. Not only is the California DMV posting videos on YouTube, but "friends" also follow the agency on Facebook, MySpace and Twitter. Numerous government agencies at the federal, state and local levels are doing the same. Mayors are posting their own videos online (check out some of the humorous YouTube postings by Denver Mayor [John Hickenlooper](#)) state legislators are using Twitter, and government executives like Federal CIO Vivek Kundra are blogging. The White House has approximately 1.5 million Twitter followers and 400,000 fans on its Facebook page.

The pace of adoption has been dizzyingly fast. An August 2009 survey by the Public Technology Institute (PTI) found that 72 percent of cities and counties use Facebook to communicate with citizens. Last year, a Public CIO reader survey found that social media didn't make the list of the 10 technology priorities for 2009. Today it's become the No. 1 topic among public CIOs.

So what's going on?

In the broadest sense, social networking and the social media tools that go with it -- often defined as Web 2.0 -- have generated the same sweeping buzz that the Internet's World Wide Web did in the 1990s. Inexpensive or free software allows people to communicate and interact in an entirely new way. Arguably these tools are changing business models: turning information into a commodity that can be used for new purposes and heightening the value of collaboration.

Some believe the same transformation will happen in government as it adopts social networking tools. This new platform for the public sector is sometimes called Government 2.0. Analysts believe the new era of social media represents the first significant development in the digital public sector since the dawn of e-government nearly 10 years ago.

Author and innovation expert Anthony Williams, pointed out in a 2008 interview with CIOInsight.com that e-government was essentially a one-way conversation between government and citizen that provided transactions and services that were online, but still stovepiped. As a result, the value was limited.

"In today's social media environment, these one-way conversations fail to build credibility and trust in government," he said. "With the new, function-rich infrastructure of Web 2.0, government no longer needs to work on its own to provide public value."

The expectation is that Web 2.0 will provide platforms for collaboration between citizens and government, resulting in communities of interest that tackle complex problems. Public programs will no longer be the exclusive domain of a single government agency.

Reaching New Constituents

At this point, government's use of Web 2.0 tools and strategies appears to be a mile wide and an inch deep. Interest and use is pervasive, but social media hasn't transformed the public sector yet.

Here is what's happening: If a government agency isn't using blogs, Twitter, Facebook or wikis, it's looking seriously into the matter. In particular, local governments seem to be experimenting with Web 2.0 -- a trend backed by the PTI survey findings. The federal government also has shown strong interest in Web 2.0 tools. Even the ever-secretive intelligence community has taken to social media, in one case setting up a wiki called Intellipedia for internal collaboration.

State governments appear to be taking a more cautious approach, based on anecdotal information. Perhaps because they have the dogged tasks of educating, medicating and incarcerating their citizens, states have been somewhat wary of throwing open their agencies to two-way communication and collaboration.

But as the California DMV has found, Web 2.0 can deliver immediate benefits when the right approach is taken. As one of the few agencies that nearly every state resident must contact, the DMV serves a broad demographic. "We put a lot of thought into who our customers are and how to reach them," said Soriano. Consequently the DMV knows that using a particular method to reach out to one demographic of customers might not work with another. "We found that teen drivers are especially open to communication via social media," he pointed out.

State tourism and parks agencies also have embraced Web 2.0 as a way to communicate with their audience. David Elwart, CIO of South Carolina's Department of Parks, Recreation and Tourism, said state tourism agencies already are adept marketers, so using social media is a natural extension. Elwart is an early adopter; he has been blogging personally since the concept first came on the scene a number of years ago. Elwart also uses Twitter and Facebook.

Currently the agency's state park division has a Facebook page with more than 6,000 friends and a Twitter account with 10,000 followers, according to Elwart. Along with providing updates and news about park and

tourist-related activities, the social media tools are opening up new services. For instance, Elwart's team of IT developers is working on an application for Facebook that will create an interactive map of South Carolina's parks. The map will eventually be linked to the agency's central reservation system so that visitors can use either the Facebook page or an iPhone app to book a camping site.

Encouraging Responsible Use

As CIO, Elwart sees it as his responsibility to stay abreast of new technologies, and to introduce and guide their potential use within his agency. He has adopted flexible guidelines for social media usage within the agency. After receiving feedback from administrators, especially those who were in charge of outlying field offices, the agency adopted guidelines for employee use. "We recognized people were going to use it, so we actually encouraged it be done, but responsibly," said Elwart.

That approach is more the exception than the rule in the public sector. So far, many agency guidelines and policies strictly control who can post updates on Facebook and send messages via Twitter. At the California DMV, messages and messaging via Web 2.0 are handled almost exclusively by the department's Office of Public Affairs. Rank-and-file employees aren't allowed use these social media tools from their work computers.

Most organizations -- public and private sector -- follow that restrictive approach. In fact, government might be slightly ahead of other organizations in adopting Web 2.0. A recent survey by Robert Half Technology found that 54 percent of business firms have company policies that prohibit employees from visiting social networking sites at work; just 19 percent permit it for business purposes only.

[Chris Curran](#), chief technology officer for consulting firm Diamond Management and Technology Consultants Inc., believes Web 2.0 is too big and transformative to be restricted in the workplace. "If you rewind to 1995, the attitude back then was, 'No Internet use at work.' Then it became, 'No Internet shopping during work hours.' But over time, the issue just went away because a majority of employees are good people, hardworking and productive. Some people are going to do stupid things whether they have access to social networking or not. But it doesn't make sense to ignore a social trend that is bigger than your organization because of a few bad workers."

Taking that inclusive approach is the consolidated city and county of [San Francisco](#), which has a social media center on its Web site that lists the various ways constituents can receive updates, follow activities and communicate. San Francisco boasts three YouTube channels, numerous Twitter feeds, Facebook pages and blogs.

CIO Chris Vein attributes the city's broad and liberal use of social media to Mayor Gavin Newsom's "understanding of how technology can transform government," he said. The philosophy in San Francisco is to "fail forward," which means new ideas and innovation are embraced, not frowned upon.

When it comes to guidelines for Web 2.0, Vein said the city's government is highly decentralized. "I set the vision," he said. "But the day-to-day decisions are done by the separate departments. I try to show the benefits and explain the risks." Control has been an issue, Vein admitted, and the city's legal counsel has probably suffered heartburn over some of the social media projects. But security is always a high priority and the risks are carefully calculated.

It's a Personnel Issue

How to set guidelines and policies around Web 2.0 continues to be a hot debate within the public sector. On one hand, the benefits of using social networking technology continue to expand as more agencies find new ways to use them. On the other hand, government agencies are held to a higher standard when balancing accessibility and transparency with privacy and security.

Increasingly CIOs are stressing that use and abuse of Web 2.0 in the workplace is not a technology issue, but a personnel issue. They advise approaching Web 2.0 from a risk management perspective, with the understanding that different agencies have different concerns about Web 2.0. For example, employees in a state tourism agency will have a more compelling need to use social networking than staff working for a corrections department.

Curran strongly urged CIOs to embrace Web 2.0 on a personal level by using the tools themselves. He recommended blogs as a way to keep both IT staff and government employees informed about all technology doings and their impact on how government operates.

"Trying to ignore this is like ignoring the Internet," he said. "CIOs need to embrace it as a tool and as an opportunity out there, and start thinking about how to take advantage of it."

While it may seem like there's a confusing number of platforms available -- providing more ways for things to possibly go wrong -- the industry appears to be integrating and consolidating. Twitter feeds are popping up on Facebook pages, for example. Curran noted that Google is introducing a new communications platform called Wave, which will combine various Web 2.0 tools with e-mail and collaboration tools. Not surprisingly, Microsoft is looking to jump into the waters with an integrated platform at some point, according to Curran.

"The innovations are going to continue," he added. "It's going to continue to get easier to use the [Web 2.0] platforms and for the common user to figure out where to go for certain kinds of social networking."

IT SECURITY: WHAT'S IN STORE FOR 2010?

MICHAEL KASSNER, DECEMBER 31ST, 2009

2009 WAS SIGNIFICANT, SECURITY-WISE. EXPERTS ARE PREDICTING 2010 WILL BE AS WELL. SEE IF YOU AGREE.

WHY WAS 2009 SIGNIFICANT? CRIMINALS FIGURED OUT THEY CAN MAKE A LOT OF MONEY IN CYBERSPACE. SO MUCH SO, THAT THEIR **UNDERGROUND ECONOMY** IS DOING BETTER THAN THE ABOVE GROUND COUNTERPART.

THAT'S GOING TO CHANGE IN 2010. THE PUNDITS SAY IT'S GOING TO GET WORSE. EVERY PREDICTION I READ, SUGGESTS THAT CYBERCRIMINALS ARE GOING TO CONTINUE LEVERAGING EXISTING VULNERABLE TECHNOLOGIES AND FIND NEW AND MORE EFFECTIVE (FOR THEM) VULNERABILITIES TO EXPLOIT. LET'S TAKE A LOOK AT SOME OF THE PREDICTIONS

EWEEK'S PREDICTION

MR. BRIAN PRINCE IN HIS **EWEEK ARTICLE** FORETELLS A CONTINUATION OF CURRENT BAD GUY SUCCESSES, PLUS A STRONG PUSH INTO THE CLOUD:

- *PIRATED SOFTWARE WILL DRIVE INSECURITY. USERS OF PIRATED SOFTWARE ARE AFRAID TO DOWNLOAD UPDATES, THUS EXPOSED TO SECURITY RISKS.*
- *SOCIAL ENGINEERING MEETS SOCIAL NETWORKS, UPPING THE ANTE FOR COMPROMISES. CRIMINAL ORGANIZATIONS ARE INCREASINGLY SOPHISTICATED IN HOW THEY ATTACK SOCIAL-NETWORKING SITES.*
- *CRIMINALS TAKE TO THE CLOUD. IN 2010, WE WILL SEE CRIMINALS LEVERAGING CLOUD COMPUTING, INCREASING THEIR EFFICIENCY AND EFFECTIVENESS.*

VERIZON SECURITY'S PREDICTION

MR. RUSS COOPER'S **VERIZON SECURITY BLOG POST** ABOUT 2010 SHOULD BE GIVEN SPECIAL ATTENTION. HE IS A HIGHLY-REGARDED SECURITY ANALYST AND FOUNDER OF **NTBUGTRAQ**. HERE ARE SOME OF HIS THOUGHTS:

- *SERVICES WILL PROTECT THEMSELVES. FACEBOOK, GOOGLE, TWITTER, TINYURL, AND THE LIKE WILL GAIN MORE CONTROL OVER CRIMINAL CONTENT.*
- *MALWARE WILL NOT EVOLVE. NO SIGNIFICANT CHANGES IN MALWARE WILL OCCUR IN 2010. BOTNETS WON'T GET MORE SOPHISTICATED, ALTHOUGH THEY MAY MAKE CHANGES IN THE WAY THEY WORK.*
- *CONSUMERS ARE GETTING SMARTER. THE BASE LEVEL OF "CLUEFULNESS" FOR CONSUMERS WILL RISE IN 2010.*
- *SERIOUS FINGER-POINTING AND FRUSTRATION OVER ESSENTIAL PROTOCOLS (SMTP, DNS) WILL OCCUR AMONGST GOVERNMENTS AND NON-TECHNICAL ORGANIZATIONS.*

HELP NET SECURITY'S PREDICTION

HELP NET SECURITY ENLISTED MR. MICHAEL SUTTON, VP OF SECURITY RESEARCH AT **ZSCALER** FOR THEIR PREDICTIONS. MR. SUTTON PROFESSES MANY OF THE SAME CONCERNS, BUT ADDED THE FOLLOWING:

- *APPLE'S INCREASING MARKET SHARE WILL FORCE THEM TO FINALLY INVEST IN SECURITY, DUE TO INCREASING ATTACKS TARGETED AT APPLE DEVICES.*
- *APP SECURITY TESTING IS LIMITED. DEVELOPERS ARE ABLE TO SLIP IN APPS WITH UNDOCUMENTED APIS. ATTACKERS WILL TAKE THINGS ONE STEP FURTHER AND GET MALICIOUS APPS ACCEPTED.*
- *THE ARRIVAL OF FINANCIAL DDOS ATTACKS. CLOUD-BASED SERVICES CHARGE BY ACTUAL CONSUMPTION. ATTACKERS WILL HOLD ENTERPRISES HOSTAGE BY ARTIFICIALLY INFLATING COSTS.*
- *CLICKJACKING HAS BEEN USED SUCCESSFULLY FOR SOCIAL-ENGINEERING ATTACKS AND IT WILL BECOME MORE PREVALENT.*

ITPRO'S PREDICTION

MR. STEPHEN PRITCHARD OF ITPRO CONSOLIDATED THE OPINIONS OF SEVERAL SECURITY FIRMS FOR HIS **2010 PREDICTION**. THAT CREATES AN INTERESTING PERSPECTIVE:

- *BIGGER BOTNETS ARE EXPECTED BY SYMANTEC, MEANING MORE SPAM E-MAIL. CAN IT GET WORSE? **SPAM IS ALREADY OVER 90% OF ALL DELIVERED E-MAIL MESSAGES.***
- *ACCORDING TO IT SECURITY FIRM **IMPERVA**, CYBERCRIME IS GETTING ORGANIZED. THE CRIMINALS ARE OPERATING CLEARLY-DEFINED SUPPLY CHAINS, SIMILAR TO DRUG CARTELS.*
- *GETTING USERS TO INSTALL **SCAREWARE** THAT CONTROLS THEIR COMPUTERS IS AN EFFECTIVE MONEY-MAKING TOOL FOR THE BAD GUYS. THAT SUGGESTS IT WILL BE MORE COMMON IN 2010.*
- *WINDOWS 7 IS A NEW OPERATING SYSTEM. THAT OVERRIDES ANY SECURITY IMPROVEMENTS. BEING NEW IS A LIABILITY, JUST ASK ANY SECURITY ANALYST.*

IN AGREEMENT

THE EXPERTS DID AGREE ON SEVERAL CONCERNS, THEY ARE:

- **CLOUD COMPUTING:** THE CLOUD OFFERS UNPRECEDENTED STORAGE AND PROCESSING POWER. IF MORE BUSINESSES START MIGRATING TO IT, SO WILL THE BAD GUYS.

- **DATA BREACHES:** DATA CENTERS CONTINUE TO GROW IN SIZE AND CAPACITY. YET, SECURITY IS NOT KEEPING UP. DATA BREACHES IN 2009 WERE MINOR COMPARED TO WHAT'S EXPECTED FOR 2010.
- **SOCIAL NETWORKS:** SOCIAL NETWORKS ARE RIPE FOR PLUNDERING. THAT'S UNDERSTANDABLE, CONSIDERING THE POPULARITY OF SOCIAL NETWORKS IN 2009. MOST, EXCEPT MR. COOPER, SAY WE HAVEN'T SEEN ANYTHING YET.

MY PREDICTION

WHAT I VIEW AS THE BIGGEST SECURITY HEADACHES FOR 2010 ARE THE PROBLEMS REQUIRING SIGNIFICANT EFFORT TO FIX, SUCH AS:

- VITAL, YET BROKEN SYSTEM PROTOCOLS, **DNS** FOR EXAMPLE.
- CONVINCING ORGANIZATIONS TO IMPLEMENT SECURITY/PRIVACY MEASURES ON BEHALF OF PEOPLE ACCESSING THE ORGANIZATION'S WEB PRESENCE.
- BALANCING USABILITY WITH SECURITY WHEN NEW TECHNOLOGY IS BEING DEVELOPED.
- Becoming proactive, we know mobile devices are on the bad guys' radar, but are doing little about it.

THE BIGGEST CIO CHALLENGE OF 2010: BYOT

PATRICK GRAY, 8 JANUARY 4TH, 2010

THE BIGGEST CHALLENGE ON THE HORIZON FOR TECH EXECUTIVES IS NOT GOING TO BE CLOUD COMPUTING, VIRTUALIZATION OR ENTERPRISE SYSTEMS. RATHER, IT'S GOING TO COME FROM THE GRASSROOTS OF AN ORGANIZATION IN THE GUISE OF A MOVEMENT TO BRING YOUR OWN TECHNOLOGY (BYOT) TO THE WORKPLACE. WE HAVE ALL HEARD OF HOW THE NEW GENERATION OF WORKERS WILL CHANGE THE WAY EMPLOYEES INTERACT WITH THEIR EMPLOYERS, AND WHILE MUCH OF IT IS OVERBLOWN, THIS IS A GENERATION THAT HAS A FUNDAMENTALLY DIFFERENT ATTITUDE TOWARDS TECHNOLOGY THAT WILL DEFINITELY RESHAPE CORPORATE IT.

WE'RE WITNESSING THE END OF AN ERA AS WORKERS RETIRE WHO ENTERED THE WORKFORCE BEFORE COMPUTERS WERE COMMON IN THE HOME. THIS GENERATION INTERACTED WITH THE PC AS A BUSINESS TOOL AND LITTLE MORE, AND WAS UNFAMILIAR WITH ITS INNER WORKINGS AND MAINTENANCE, AND THEREFORE DEMANDED A "HIGH-TOUCH" IT STAFF TO MAINTAIN THE MACHINES. THE PC WAS A TOOL TO GET A JOB DONE, AND WHEN THAT JOB WAS DONE THE MACHINE WAS POWERED OFF AND LIFE WENT ON. THE NEWER GENERATION OF WORKERS GREW UP *WITH* THE PERSONAL COMPUTER. NOT ONLY WERE COMPUTERS INTEGRATED INTO THEIR LIVES, BUT THEY WERE A MEANS OF PERSONAL EXPRESSION, INTERPERSONAL COMMUNICATION WITH BOTH FRIENDS AND COLLEAGUES, AND A TOOL THAT BLENDED THEIR WORK AND PERSONAL LIVES IN ONE CONSOLIDATED WORKSPACE.

RECENTLY A SIMILAR TREND HAS OCCURRED WITH MOBILE PHONES. CORPORATIONS WERE THE EARLY ADOPTERS OF SMART PHONES, WITH THE EFFECTIVE AND CENTRALLY-CONTROLLED BLACKBERRY RULING THE DAY. SMART PHONES WERE TOOLS FOR EXECUTIVES OR THE PROVINCE OF A SMALL CADRE OF "PHONE GEEKS," BUT NOT SOMETHING THE AVERAGE PERSON WAS INTERESTED IN. THAT CHANGED IN THE LAST YEAR

OR TWO, AND THE SMART PHONE HAS BECOME MUCH LIKE THE PC, A SINGLE DEVICE THAT PEOPLE EXPECT TO USE TO MANAGE THEIR PERSONAL AND BUSINESS AFFAIRS IN ANY MANNER THEY SEE FIT. IN EITHER CASE, AN ENVIRONMENT THAT'S LOCKED DOWN AND RUTHLESSLY CONTROLLED BY IT SIMPLY WILL NOT CUT IT ANYMORE. AS COMPUTERS AND PHONES HAVE GONE FROM EXCLUSIVELY BUSINESS TOOLS TO A MEANS OF PERSONAL EXPRESSION, IT DICTATING MAKE, MODEL AND APPLICATION SELECTION WILL BE JUST AS ANATHEMA AS THE CEO DICTATING WHAT COLOR SHIRT, SHOES AND PANTS TO WEAR. USERS ARE GOING TO DEMAND AN ABILITY TO USE DEVICES OF THEIR CHOOSING TO INTERACT WITH CORPORATE INFRASTRUCTURE, AND I BELIEVE THIS TREND IS IRREVERSIBLE. IT ORGANIZATIONS CAN CHOOSE TO FIGHT A LOSING BATTLE AND MAINTAIN THEIR WALLED KINGDOM, OR ADOPT A BYOT APPROACH.

BRING YOUR IPHONE TO WORK DAY

IF YOU CONSIDER HOW PEOPLE USE THEIR COMPUTERS, BYOT IS FAR LESS THREATENING THAN IT MIGHT HAVE BEEN A FEW YEARS AGO. MOST PEOPLE INTERACT PRIMARILY WITH EMAIL AND DOCUMENTS, AND PERHAPS A FEW CENTRALIZED BUSINESS APPLICATIONS. LONG BEFORE ALL THIS **FANCY "CLOUD COMPUTING" TALK** ARRIVED ON THE SCENE, MOST CORPORATIONS HAD MOVED THEIR APPLICATIONS INTO A CORPORATE CLOUD OF SORTS, AND THERE ARE VERY FEW APPLICATIONS INSTALLED DIRECTLY ON A USER'S PC ANYMORE THAT ARE NOT COMMODITIES LIKE WORD PROCESSING OR SPREADSHEET APPLICATIONS. IN FACT, MANY REMOTE WORKERS ESCHEW CLUNKY CORPORATE LAPTOPS RUNNING OUTDATED SOFTWARE AND WORK ON MODERN DESKTOPS THROUGH WEBMAIL AND OTHER "CORPORATE CLOUD" PORTALS. WITH TECHNOLOGIES LIKE VIRTUALIZATION BECOMING MORE PREVALENT, IT MAKES FAR MORE SENSE TO PROVIDE EMPLOYEES WITH A HOSTED VIRTUAL DESKTOP, OR EVEN A VIRTUAL "WORK COMPUTER" ON A USB STICK THAT THEY CAN RUN ON THE HARDWARE THEY PREFER, WHETHER IT IS A DESKTOP WITH A MASSIVE LCD PANEL IN THEIR HOME OFFICE, OR A MACBOOK AT THE LOCAL COFFEE SHOP.

SMART PHONES ARE IN A SIMILAR BOAT. FOR THE VAST MAJORITY OF CORPORATE-TYPES, THE CRITICAL APPLICATION ON THESE PHONES IS CORPORATE EMAIL. AS VENDORS STANDARDIZE AROUND A MECHANISM FOR PROVIDING PUSH EMAIL, THE INFRASTRUCTURE FOR SOMETHING LIKE A BLACKBERRY LOOKS INCREASINGLY IRRELEVANT. GIVING UP THE CENTRALIZED CONTROL OF A BLACKBERRY-LIKE INFRASTRUCTURE WILL BE PAINFUL FOR IT DEPARTMENTS, BUT USERS ARE ALREADY REVOLTING AGAINST PHONES THAT ARE LOCKED DOWN AT THE CORPORATE LEVEL, AND DEMANDING TO KNOW WHY THEIR FRIENDS CAN INSTALL FACEBOOK AND READ THEIR GMAIL ON THEIR SMART PHONE, BUT THEIR IT DEPARTMENT REFUSES TO ALLOW IT. AS FUNCTIONALITY LIKE REMOTE WIPE AND EXCHANGE SYNC BECOME STANDARD, IT WILL STRUGGLE TO JUSTIFY SAYING "NO" TO USERS THAT WANT ONE PHONE OF THEIR CHOICE THAT INTEGRATES THEIR PERSONAL AND PROFESSIONAL LIVES, ESPECIALLY AS THESE USERS TAKE TITLES LIKE CEO.

BUT WHO WILL SUPPORT IT ALL?

THIS HAS LONG BEEN THE "FINAL ANSWER" FROM IT WHEN ATTEMPTING TO KEEP BYOT FROM TAKING ROOT. WHILE "BUT THAT'S NOT SUPPORTED" HAS WORKED FOR THE LAST SEVERAL YEARS, THE EXCUSE IS WEARING THIN AS LARGE COMPANIES LIKE KRAFT AND UNISYS IMPLEMENT BYOT, AND A GENERATION OF WORKERS THAT SUPPORTED THEIR OWN TECHNOLOGY ENTERS THE WORKFORCE. RATHER THAN LOOKING LIKE THE BAD GUY, IT CAN ADOPT BYOT-FRIENDLY POLICIES AND INFRASTRUCTURE, AND MAKE USERS WELL-AWARE OF THE FACT THAT IF THEY WANT BYOT, THEN THEY ARE THE PRIME PROVIDERS OF HARDWARE SUPPORT AND MAINTENANCE UP TO A BASIC SET OF CORPORATE STANDARDS.

IN THE LONG RUN, BYOT IS ACTUALLY A VERY GOOD DEAL FOR IT. BYOT GETS IT OUT OF THE ROLE OF SUPPORTING HUGE FLEETS OF DULL GREY BUSINESS LAPTOPS, AND FOR THE RATHER MEAGER PRICE OF LETTING USERS CHOOSE A DEVICE THAT THEY FEEL A PERSONAL CONNECTION TO, ACTUALLY IMPROVES THE IMAGE OF CORPORATE IT. A COST-NEUTRAL APPROACH OF LETTING PEOPLE PICK THEIR OWN TECHNOLOGY EVEN BECOMES A BIG CORPORATE DIFFERENTIATOR, PRESENTING YOUR COMPANY AS FORWARD-THINKING WHEN ALL YOU'VE DONE IS REDUCE YOUR IT INFRASTRUCTURE AND "BOUGHT USERS OFF" BY LETTING THEM PICK THE HARDWARE THEY ACTUALLY CHOOSE TO SUPPORT THEMSELVES! GONE ARE THE HOARDS OF STEELY FACES GROWLING "UNSUPPORTED," AND ALSO GONE ARE THE IT HEADACHES ASSOCIATED WITH THE THANKLESS JOB OF SUPPORTING END-USER HARDWARE.

Strategic guidance for applying PCI-DSS tactics.

by [Steven Fox, Security Paradigms](#)

Mon, 2010-01-04 16:31

Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.- Sun Tzu

With the new year upon us, I reflect on all the "fun" security professionals had in 2009. With all the incidents that have expanded our catalog of war stories, I think that the misapplication of compliance standards is one of the themes that caused our eyes to twitch.

The [Payment Card Industry Data Security Standard](#) (PCI DSS), is "***a set of comprehensive requirements for enhancing payment account data security.***" In other words, PCI provides a set of tactics to protect the confidentiality and integrity of data. Great place to start – but it's only part of the picture. Applying them appropriately requires situational awareness and knowledge of the company's core values and strategy. Sun Tzu's approach at assessing an army's readiness for battle can be applied to the attaining this knowledge in a business environment.

The ground gives rise to measurements, measurements give rise to assessments, assessments give rise to calculations, calculations give rise to comparisons, comparisons give rise to victories.- Sun Tzu

1. Measure the Scope

"The number one PCI piece that companies don't do well is around scoping," said Verisign's Branden Williams. Given the limited resources available for *any* IT project, scoping is required in order to manage a project effectively and deliver on time and within budget.

Data flow diagrams and business case/process mapping is one way to determine scope. Williams cautions that many companies "assume they can apply PCI to their entire environment. This is a foolish assumption, especially in the case of legacy applications." Once the scope of the implementation is determined through measurement, the assessment of business risk can be performed.

2. Assess the Risk

"Regulations are not designed to handle the kinds of threats, the kinds of vulnerabilities, and the kinds of problems that organizations are facing today," said Edward Schwartz, CSO of NetWitness. He recommends that risk be assessed in the context of the processes that utilize the data being protected. Sun Tzu suggests a ***five-point risk assessment approach.***

1) **The Way** - refers to the culture of an organization. **A risk assessment must examine the impact of values and behavior on the overall security posture.** This information will be extremely useful when selecting effective controls.

2) **The Weather** – refers to seasonal changes in organizational priorities. **A risk assessment must take patterns of organizational behavior into account.** This steps in the process is facilitated by alliances with business stakeholders.

3) **The Terrain** – refers to the competitive landscape both within and without the organization. Most security professionals are used to examine through external terrain; focusing on the external threats. The internal landscape, however, presents greater issues, obstacles, and opportunities of which we must be aware. **Of particular concern are the behaviors that are incentivized by management priorities – they may focused on business expediency at the expense of security.**

4) **The Leadership** – refers to those who promote the corporate goals and enable those goals through tactical and operational initiatives. **We must assess what role those leaders will play in the PCI implementation and how they impact the overall risk posture.** By understanding our end-client – the business - you can architect a control strategy, and supporting tactics, that address risk while supporting management priorities.

5) **The Discipline** – refers to the enforcement of security policies and procedures. **A risk assessment must consider the human factors that enable threats.**

3. Calculate the Impact of Controls

After assessing the risks, we must review the benefits and constraints of control options in order to select the appropriate. According to Sun Tzu, **“those who are not thoroughly aware of the disadvantages in the use of arms cannot be thoroughly aware of the advantages.”** We must apply our knowledge of the corporate organism in order to select controls that will allow it to thrive.

If Generals do not know how to adapt advantageously, even if they know the lay of the land they cannot take advantage of it.

Standards like PCI serve an important role in creating a baseline for data protection and a common language for the discussion of the related issues. However, they are not designed to contribute to market responsiveness/agility. **The enlightened business creates synergies between the tactics communicated in these standards/regulations and their core competencies/strategies.**

Smartphones aren't just smart

Smartphones aren't just smart, they're personal computers. Unlike a desktop or even a laptop PC, those devices and other mobile phones can easily slip out of a pocket or purse, be left in a taxi, or get snatched off a table. They let you store photos, access e-mails, receive text messages, and put you one browser click away from potentially malicious Web sites.

In effect, gadgets like the Apple iPhone and those running Google's Android software can be as risky to use as PCs, except that the wide variety of mobile platforms has deprived malicious hackers of one dominant software element to target, such as they have with Microsoft's Windows operating system on desktops and laptops.

Here is a look at the different types of threats that affect smartphone users and what people can do to protect themselves.

What's the biggest security threat to my mobile phone?

Losing it. "You are way more likely to leave it in the back of a taxi than to have someone break into it," Charlie Miller, a principal analyst at consultancy Independent Security Evaluators, said in a recent interview. The best

way to protect data in the event of losing a device is to not store sensitive information on it, he said. If you must store sensitive information on it, use a password on the phone and encrypt the data. Devices can be configured so that they ask for a password every time e-mail or a VPN is accessed. Use a strong enough password that a stranger can't guess it. And back up your data frequently.

There are also ways to lock the phone remotely or wipe the data if it is stolen. AT&T spokesman Mark Siegel said users who lose their phone should call the company immediately and "with just a keystroke, we can prevent anyone else from using the phone--and from running up charges."

A number of companies offer software and services to protect mobile phones. One of them is a start-up called Lookout that offers a Web-based service that backs up the data, remotely wipes the data if stolen, can help locate the device, and includes antivirus and firewall protection.

Mobile device users should also be careful about leaving the phone unattended, or loaning it to people. Spyware can be installed without you knowing it. For instance, the PhoneSnoop program can be used with BlackBerry devices to remotely turn the microphone on to eavesdrop on nearby conversations.

Can mobile phones get viruses?

Yes. Mobile viruses, worms and Trojans have been around for years. They typically arrive via e-mail but can also spread via SMS and other means. Mobile phone users should be diligent in installing security software and other updates for their devices. All the major desktop security vendors have mobile antivirus and related offerings.

In November, several worms hit the iPhone, but only devices that had been jailbroken so they can run apps other than those approved by Apple. One worm changes the wallpaper on affected devices to a photo of 80s pop singer Rick Astley of "Rickrolling" fame. The second, more dangerous worm attempts to remotely control affected iPhones and steal data such as bank login IDs. Jailbroken iPhones have also been directly hacked via SMS, including by one Dutch hacker who was demanding \$7 from victims for information on how to secure their iPhones.

Miller says: "Don't jailbreak your phone. It breaks all the security, basically." If you simply must jailbreak it, you should change the default root password and not install SSH (Secure Shell network protocol).

What are other types of attacks?

Just like with computer users, smartphone users are vulnerable to e-mail and Web-based attacks like phishing and other social-engineering efforts. All attackers have to do is create a malicious Web page and lure someone to visit the site where malware can then be downloaded onto the mobile device. People should avoid clicking on links in e-mails and text messages on their mobile device. (For more anti-phishing tips read "FAQ: Recognizing phishing e-mails.")

SMS offers another avenue for attack. Last year, researchers demonstrated several ways of attacking phone using SMS messages. In one, they exploited a vulnerability in the way the iPhone handles SMS messages. Researchers also showed how an attacker could spoof an SMS to make it look like it comes from the carrier to get the target to either download malware or visit a site hosting it. In another proof-of-concept attack, a text message was used to launch a Web browser on a mobile device and direct it to a site that could host malware. When the attack is used to phish for personal information it is referred to as "SMiShing."

Is it safe to use Wi-Fi and Bluetooth?

Yes and no. If you are doing something sensitive on your phone, like checking a bank account or making a payment, don't use the free Wi-Fi at a coffee shop or other access point. Use your password-protected Wi-Fi at home or the cellular network to avoid what is called as a man-in-the-middle attack in which traffic is intercepted. Pairing a mobile phone with another Bluetooth-enabled device, like a headset, means any device that can "discover" another Bluetooth device can send unsolicited messages or do things that could lead to extra fees, data being compromised or corrupted, data stolen in an attack called "bluesnarfing," or the device being infected with a virus. In general, disable Wi-Fi and Bluetooth unless you absolutely need to use them.

Which is safer: the iPhone or Android?

Apple vets all the apps that are used on the iPhone, and that tight regulation of the Apps store has kept users safe from malicious apps so far. Nothing is foolproof, however. Once apps are approved they can do any number of things. For instance, Apple removed free games in November developed by Storm8 that were found to be collecting users' phone numbers.

From an architecture standpoint, Android offers more granular access control. But the open-source nature of the Android platform means apps aren't as controlled as they are on the iPhone and holes can be introduced by any number of parties. For instance, Miller found a vulnerability in the Android mobile platform last year that could have allowed an attacker to remotely take control of the browser, access credentials, and install a keystroke logger if the user visited a malicious Web page. The hole was not in code written by Google, but was contributed by a third party to the open-source Android Project. However, any risk was mitigated by an application sandboxing technique Google uses that is designed to protect the device from unauthorized or malicious

software that gets onto the phone, Google said. Miller recommends that Android users only download software from trustworthy vendors and reputable sites.

Are standard mobile phones safe?

Obviously regular mobile phones don't pose the Web-based threats that smartphones do. But they are still used to store sensitive information that can be accessed by gaining access to the device. For instance, the inbox and outbox for text messages can contain information that can be used for identity fraud, said Mark Beccue, a senior analyst for consumer mobility at ABI Research. "Regardless of what type of cell phone, the most dangerous current threat is through a cellphone's in/out message boxes," he said. "Clear (them) out regularly. Do not transmit full account numbers, PIN or passwords within a text message unless you immediately delete the out box message."

Standard phones that support Java can be susceptible to certain threats that smartphones are. For instance, scammers in Russia and Indonesia are hiding a Trojan in pirated software that surreptitiously sends SMS messages to premium rate numbers - costing as much as \$5 each, thus racking up huge bills, said Roel Schouwenberg, a senior antivirus researcher at Kaspersky Lab.

Phishing attacks soar in December

December 30 2009

Network Box stats show over half of all web-based threats this month were phishing attacks.

Phishing attacks soared in December as cyber criminals looked to capitalise on the higher number of online shoppers in the run up to Christmas, according to new research from managed security firm Network Box released today.

The firm's analysis of web-based threats in December 2009 shows that just over 57 per cent of all threats were phishing attacks, compared to 28.3 per cent in November.

"The run up to Christmas is traditionally a time for hackers to strike the vulnerable. A higher proportion of shopping is done online, with more money spent than at any other time of year," warned Network Box internet security analyst Simon Heron.

"Christmas offers rich pickings for phishers. This is likely to continue through the sales in January, and we urge online bargain hunters to be vigilant."

The firm also found that the greatest source of viruses and spam during the same time period was Brazil, which accounted for 20.9 per cent of all viruses and 9.1 per cent of all spam in December. This is up from 14 per cent and eight per cent respectively in November.

Network Box also warned that India is playing an increasingly significant role in the world's threat landscape, with 6.8 per cent of all spam coming from the sub-continent, up from 4.2 per cent in November; and 4.1 per cent of viruses – the same as in November.

TSA document release show pitfalls of electronic redaction

By Jaikumar Vijayan

January 4, 2010

Computerworld - The inadvertent exposure of a sensitive [Transportation Security Administration security manual](#) last month serves as a sobering reminder about the pitfalls of trying to redact, or hide, electronic text.

The lapse occurred when a contract employee posted the improperly redacted security manual -- which described TSA airport screening methods that are designed to thwart terrorists -- on a public Web site for federal procurements.

Other organizations, such as [HSBC Bank](#) and [Facebook Inc.](#), have also had embarrassing incidents in which text in electronic documents that they thought was unreadable was revealed.

Such lapses often result from a simple misunderstanding of how electronic redaction works, said Barry Murphy, an analyst at [Murphy Insights](#), a Boston-based consultancy specializing in e-discovery and records management.

"Obscuring portions of text in a word processor by placing black boxes over it, for instance, does nothing to redact it," Murphy said. The text may not be viewable, but it still can be indexed, making it very searchable and easily retrieved by copying and pasting the blacked-out portion to another document, he said.

Another common mistake is to overlook the metadata and revision histories that are often automatically embedded in Microsoft Word documents and PDF files, Murphy noted. Blacking out or deleting the text doesn't get rid of this metadata. The only way to ensure that sensitive data isn't simply visually hidden is to remove it using redaction tools, he explained.

In a 2005 document Merck & Co. sent to a publisher, the drug giant deleted information linking its drug Vioxx to an increased risk of heart disease. But the deleted information was included in the document's metadata and was later recovered.

"The major, major thing is: Do not use your word processing programs for redaction," said John Pescatore, a Gartner Inc. analyst. There are "very strong, usable software tools that can be used for electronic redaction," he added.

Examples of automated redaction tools include [Redact-IT from Informative Graphics Corp.](#), [Rapid Redact](#) from Onstream Systems Ltd. and [ID Shield from Extract Systems Inc.](#)

Lawmakers and Consumer and Industry Groups Respond to HHS Interim Breach Notification Rule

(December 31, 2009)

Health industry representatives and members of the US Congress have sent letters of comment to US Department of Health and Human Services (HHS) Secretary Kathleen Sebelius regarding her agency's interim final rule regarding data breaches of protected health information. The rule allows organizations in possession of protected health information (PHI) to decide not to notify patients of a breach if the organization determines that it presents no significant risk of harm. Leaders of the House Ways and Means and Energy Committees strongly urged the removal of the substantial harm standard as did consumer advocacy group Consumer Watchdog. The American Hospital Association praised the inclusion of a "risk threshold" in the rule and suggested including identification of "other situations in which inadvertent use and disclosure does not compromise PHI and warrant a breach notification."

http://www.information-management.com/news/data_breach_security-10016802-1.html?zkPrintable=true

[Editor' Note (Pescatore): Just think: all those banks we bailed out had judged that their investments did not present any "significant risk." The power of breach disclosure laws has been "if you lose control of information people trusted you to keep safe, you have to tell them." Allowing risk loopholes just means people will be notified only after their information is misused, not before.

(Schultz): Realistically, how can organizations that have protected health information and that barely know what the words "security risk" mean possibly determine what "significant risk of harm" and "risk threshold" mean?]

ADOBE TO SURPASS MICROSOFT AS HACKER TARGET

McAfee says Adobe Reader and Flash will top Microsoft Office as the favorite target of cybercriminals in 2010.

By [Antone Gonsalves](#)
[InformationWeek](#)

December 30, 2009

Adobe Reader and Flash will surpass Microsoft Office applications as favorite targets of cybercriminals, a security vendor predicted Tuesday.

In unveiling its 2010 [Threat Predictions report](#), McAfee said the growing popularity of the Adobe products has attracted the attention of cybercriminals, who have been increasingly targeting the applications. Adobe Reader and Flash are two of the most widely deployed applications in the world.

As a result of Adobe's success in client software, McAfee Labs believes "Adobe product exploitation will likely surpass that of Microsoft Office applications in 2010."

Security experts for quite a while [have warned](#) of the potential security risk posed by Flash. In November, Foreground Security identified a flaw in the way Web browsers handle Flash files that could be used to compromise Web sites that have users submit content.

Beyond Adobe, cybercriminals are also expected to step up efforts next year to crack social networking sites, as well as third-party applications in general. Internet users can expect crooks to use more complex Trojans and botnets to build and execute attacks and to take advantage of HTML 5 to create threats. HTML 5 is the next major revision of hypertext markup language, the core markup language of the Web.

"We're now facing emerging threats from the explosive growth of social networking sites, the exploitation of popular applications, and more advanced techniques used by cybercriminals, but we're confident that 2010 will be a successful year for the cybersecurity community," Jeff Green, senior VP of McAfee labs, said in a statement.

Facebook, Twitter, and the third-party applications that incorporate the social networks have given criminals new technologies to target and exploit. In 2010, users will be most vulnerable to "rogue apps" distributed by criminals across the networks and to crooks that use the names of people on friends lists to get victims to click on unfamiliar links they might otherwise avoid, McAfee said. In addition, the use of abbreviated URLs on sites like Twitter will make it easier for cybercriminals to mask and direct users to malicious Web sites.

The technological advancements of HTML 5 are expected to shift more computing activity from the desktop to online applications. The technology's cross-platform support will make it easier for attackers to reach users across all mainstream browsers, McAfee said.

More sophisticated Trojans will make it possible to make unauthorized withdrawals from online banking accounts that stay below transaction limits, thereby making those withdrawals more difficult for banks to spot. E-mail attachments are expected to remain the most widely used Trojan distribution method, so users can avoid infection by checking on the safety of an attachment before clicking on it.

Regarding botnets, McAfee expects attackers in 2010 to adopt peer-to-peer control, a distributed and resilient botnet infrastructure, rather than the centralized hosting model seen today. The additional cost of the peer-to-peer model is expected to be outweighed by better success against the security community's increasingly aggressive techniques in shutting down and denying access to botnets.

Botnets typically refer to networks of computers that contain malicious software that places the host computer in the control of cybercriminals. The applications, called bots, are secretly deployed through Trojans or exploiting vulnerabilities in Web browsers and other Internet-enabled applications.

Compliance and Cloud Computing: Do They Even Belong in the Same Sentence?

The Open Group's Jim Hietala says issues are being addressed, but at the moment it's buyer beware

By *Jim Hietala*

January 06, 2010 — [CSO](#) —

There is no doubt that cloud computing is dominating today's IT conversation among C-level security executives. Whether it's due to the compelling cost saving possibilities in a tough economy, or because of perceived advantages in provisioning flexibility, auto-scaling, and on-demand computing, CSOs are probing the capabilities, costs and restrictions of the cloud. At the same time, security and compliance concerns are at the forefront of issues potentially holding large enterprises back from capitalizing on the benefits that cloud computing has to offer.

Some of the most frequently asked questions among CSOs today about the cloud include: "Is using cloud computing services advisable for applications and data that are subject to compliance requirements? Is compliance in the cloud even possible? And what standards are in place already to avoid the stormier implications of cloud?"

Not surprisingly, any answer to these questions right now has to start with "It depends...."

Coming to a meaningful answer requires an understanding of the context in which the question is asked. The kind of cloud service under consideration □ public or private? IaaS, PaaS, or SaaS? - matters greatly in meeting compliance requirements. The individual compliance regulations and specific requirements are also key to understanding whether compliance can be achieved in a cloud computing deployment. This article examines the closely related compliance challenges that organizations face when contemplating cloud computing.

"The Cloud"

Blanket statements regarding compliance and cloud computing aren't possible, because there is no such thing as "the cloud". There are a number of different types of cloud computing services, and there are varying types of cloud infrastructures that can be created for single enterprises, and for groups of similar organizations. A recent NIST paper [recognizes three service models](#): Infrastructure as a Service (IAAS); Platform as a Service (PAAS); and Software as a Service (SAAS). Under this, NIST further describes four different deployment models. These include private cloud, community cloud, public cloud and hybrid cloud.

The different service models and deployment models allow varying degrees of customer control, and place different obligations and responsibilities upon both customers and service providers with respect to security and compliance. In private clouds, for example, the organization building them is free to apply whatever set of controls they see fit. In public, community, or hybrid clouds, the customer or user organization does not typically have this degree of control. In addition, the degree of control flexibility afforded the user organization for an IaaS service will generally be a lot higher as compared to a SaaS service. With the higher degree of flexibility offered to the customer organization by an IaaS service comes a higher degree of responsibility for security and compliance for the customer as well.

The type of cloud computing service and the deployment model have impacts beyond security and compliance. A recent whitepaper from the Jericho Forum entitled [Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration](#) identifies some other critical dimensions for analyzing the security of cloud computing, including: internal/external; perimeterised/de-perimeterised; proprietary/open; and outsourced/insourced. Some of these dimensions bring additional concerns such as vendor lock-in, portability of data and applications, interoperability, data privacy, and data repatriation. These dimensions also affect the capability of a given cloud formation to satisfy compliance obligations.

While many of the benefits of cloud computing apply across different cloud service models and deployment types, the ability of the various kinds of cloud computing to address security concerns and to meet compliance obligations varies widely. For private clouds, building controls into the cloud that are necessary to enable compliance is fairly straightforward. For public cloud services, however, compliance is a more challenging endeavor.

Compliance Regulations and Cloud Computing Services

Another significant consideration when thinking about compliance and cloud computing are the specific laws and regulations, and the related regulatory guidance and requirements that affect an organization.

For some of the key compliance regulations, including HIPAA, GLBA, and PCI DSS, careful analysis of the specific requirements is required, along with a solid understanding of the security controls put in place by the cloud service provider. Herein lies a challenge, as many public cloud service providers are not very transparent in providing information to their customers describing the specific security controls deployed.

This means that organizations considering using cloud services should perform a gap analysis between the specific requirements identified in relevant regulations, and the set of controls provided by the cloud service provider. For IaaS cloud services, customers may be able to close gaps by deploying specific security controls on their virtual infrastructure. For example, software firewalls and anti-malware software may be deployed as needed by customers in IaaS virtual machine instances to satisfy compliance (and security) requirements. In the case of SaaS cloud services, customers generally have far less ability to implement specific security controls, and must instead use the set of controls delivered by the cloud service provider.

It is also worth noting that satisfying many compliance requirements will require regularly assessing the control state for the cloud service at periodic intervals. For example, PCI DSS requires quarterly vulnerability scans be conducted for systems. Even performing vulnerability scans on public cloud services may be an issue, as some cloud services limit the customer's ability to do this in their contract language.

The [Cloud Security Alliance's](#) forthcoming version 2 guidance will provide extensive discussion of compliance and audit concerns related to cloud computing, along with many other areas of security concern.

Conclusions and Guidance

Using cloud computing services for data and applications subject to compliance regulations requires a high degree of openness and transparency on the part of the cloud service provider. Customer organizations considering the use of cloud services need to really think through what use cases make sense today, closely review contracts and service level agreements, really understand the compliance requirements and how they are met (or not met) by the cloud service. They should also insist on "right to audit" clauses and general transparency on the controls in use.

Perhaps in the future cloud services will emerge that are tailored to meet the compliance requirements of specific regulations and industries, but for now—caveat emptor!

FTC to examine cloud privacy concerns

Agency to hold discussion Jan. 28

By Jaikumar Vijayan

January 6, 2010 04:32 PM ET

Computerworld - In a development likely to be closely watched by Google Inc., Amazon.com, Microsoft Corp. and other vendors, the Federal Trade Commission is examining potential threats to consumer privacy and data security posed by [cloud computing](#) services.

The agency will hold a [roundtable session on Jan. 28](#), and [another later this year](#), to gather information from industry stakeholders and to study ways of protecting consumer privacy in cloud environments.

The FTC plan was also detailed in a letter sent last month to the Federal Communications Commission. The letter was filed in response to a request for comment on a national broadband plan that is being drawn up by the

FCC. In its letter, the FTC said it wants to be sure the FCC pays attention to technologies such as cloud computing and identity management in drawing up its plans.

The letter, signed by David Vladeck, director of the FTC's Bureau of Consumer Protection, highlighted some of the cost benefits of cloud computing services but also expressed concerns at the associated risks. The letter, dated Dec. 9, was dug up by [The Hill](#) blog, which reported the story earlier this week.

"The ability of cloud computing services to collect and centrally store increasing amounts of consumer data, combined with the ease with which such centrally stored data may be shared with others, create a risk that larger amounts of data may be used by entities in ways not originally intended or understood by consumers," Vladeck warned.

The FTC is also considering how businesses can strengthen identity management practices, such as user authentication and credentialing, to protect consumer privacy on the Internet, Vladeck wrote in his letter.

The roundtable scheduled for Jan. 28 is the second the agency is holding on online privacy issues. The first one was held in December and focused on the risks associated with online information collection and use, behavioral advertising, consumer expectations relating to privacy on the Internet and the adequacy of legal mechanisms.

In addition to the daylong roundtable discussions on consumer privacy and data security in cloud environments, the FTC will also seek comments and original research on the topic from industry stakeholders, Vladeck said.

The FTC's interest in cloud computing comes even as companies such as Google, Microsoft, Amazon and social networking sites such as Facebook are rushing to offer an array of cloud-hosted applications for consumers. The trend has triggered alarm among privacy advocates who are concerned about increased consumer tracking and data collection by the service providers.

At the December roundtable many privacy advocacy groups called on the FTC to stop relying on industry privacy self-regulation. The groups asked the FTC instead to issue a comprehensive set of Fair Information Principles for the Internet for the digital era, and to abandon its previous notice and choice model for companies. Among those calling for such changes were the Center for Digital Democracy, the Electronic Privacy Information Center, the Consumer Federation of America and the World Privacy Forum.

VA, Kaiser Permanente launch e-health records exchange

Integrated eHealth Records system will be offered to 5.4 million veterans

By Lucas Mearian

January 6, 2010 05:40 PM ET

Computerworld - In a first-of-its-kind public-private partnership, health-care network giant Kaiser Permanente and the U.S. Department of Veterans Affairs today unveiled a pilot program they've been using to share patient electronic health records over the past several months.

The program connects the VA's VistA (Veterans Affairs Health Information Systems and Technology Architecture) and Kaiser Permanente HealthConnect electronic health records systems. VA beneficiaries and Kaiser Permanente members in the San Diego area were the first to be offered the opportunity to sign up for the pilot. The VA is the nation's largest integrated health care system, serving 5.4 million veterans out of 7 million eligible current and former service members.

The information, which the patient must agree to share, includes any previously diagnosed health problems, medications and allergies.

At a San Diego press conference, Dr. Robert M. Smith, chief of staff of the VA San Diego Healthcare System, compared the importance of the electronic health information program to the first moon landing, saying "much like President Kennedy's charge, we're going to take President Obama's charge [to create a nationwide EHR system] and move forward quickly."

Dr. Stephen L. Ondra, the VA's senior policy adviser for health affairs, said three out of four U.S. veterans and active duty service members receive some portion of their health care outside of the VA or Department of Defense facilities. Interoperability between federal agencies and the private sector is essential to provide the best care for veterans, service members and their dependents, Ondra said.

With the new health data exchange capability, when a veteran visits a clinician, previous medical history data will be available instantly to help guide treatment in any Kaiser location that participates in the program. Before this project, patients frequently consented to sharing this information, but it could take weeks or even months, for doctors to receive the paper documents.

"What we have achieved with this pilot is that process of taking weeks to get stale paper records now occurs in seconds," he said. "So the net effect is clearly an improvement in quality, an increase in patient safety and a tremendous improvement in efficiency in how we share information and deliver the best possible care. This is the first of many steps to come."

Ondra said that if any physician was asked to choose three things he could know about a patient from an outside institution, he would pick health problems, medications and allergies. "That's why these things were selected for the first three," Ondra said.

Although the data exchange is Web-based, the pilot program has less to do with proprietary technology and more to do with using a set of standardized protocols for displaying patient information on a common network that allows two computer systems to view data no matter the underlying software or computer systems.

The organizations are using the [Nationwide Health Information Network](#) (NHIN) to exchange data. The network was developed over several years by the U.S. Department of Health and Human Services [Office of the National Coordinator](#) (ONC). In June, the VA and the DOD agreed on a single NHIM standard.

Almost [two dozen public and private health care entities](#) are testing the NHIN. In February of 2009, the U.S. Social Security Administration [started receiving EHRs](#) from MedVirginia, the Regional Health Information Organization for Virginia.

According to Smith, of 1,144 recent VA patients who were asked if they would be willing to participate in the information exchange, 40% said yes. "We think we can get a higher number by following up and making sure they know what kind of an opportunity this is for them," he said.

The NHIN provides a technology "gateway" to support standards and a legal framework for the secure exchange of health information between physicians treating a patient who has authorized the release of his medical information. Clinicians from the participating organizations can electronically, securely and privately share authorized patient data, ensuring around-the-clock access to critical health information, the DHHS said. This immediate electronic access supports increased accuracy, efficiency and safety. It also helps to avoid redundant care and testing.

Smith said the same NHIN framework that allows information exchange also enables accountability. "Any retrieval of information also results in the recording of [data] to track who pulled up that information," he said.

A [national effort is underway](#) to promote the use of e-health records that can be shared between multiple health care facilities, eliminating the need for patients to physically carry their health records with them from one doctor's office to another.

As part of the American Recovery and Reinvestment Act, \$19 billion has been earmarked for health IT spending, \$17 billion of which is designated for incentive payments for e-health records use beginning in 2011. To date, however, only about [25% of the nation's 5,000 hospitals](#) have rolled out EHR systems, and only a small fraction of physician practices have done the same.

Part of the problem has been a lack of standardized methods for sharing patient data between disparate computer systems as well as the government's slow progress in establishing what will constitute ["meaningful use"](#) of EHR technology for the purposes of federal reimbursement monies.

Smith said that similar to financial institutions' securely and seamlessly sharing customer information from different locations and systems, EHRs from different systems can securely provide access to health data from multiple sites of care.

The next phase will add the DOD's health care system to the exchange in the first quarter of this year. The program will eventually be made available to all 5.4 million veterans who receive benefits from the VA and all military service members.

Tweeting for the Public Good

Utah allows employees to use social media on the job, but lays down the rules.

By [Steve Towns](#) | January 2010

State and local agencies may be embracing Web 2.0 to interact with citizens and constituents, but they're struggling with social-network use among their own employees. In too many instances, the first inclination of public-agency managers still is to restrict access to popular social-networking sites such as Facebook and YouTube for rank-and-file employees.

That is ironic when you consider some of the terrific uses that state and local governments have found for these tools. Motor vehicle departments post driving instruction videos on YouTube, a practice that's proven hugely popular with young drivers. Transportation and public safety agencies use the Twitter micro-blogging service to broadcast real-time updates on emergency situations and road conditions.

As productive ways of using these tools keep emerging, you have to wonder what potential uses governments are missing out on. Could social networking promote regional collaboration between workers performing similar tasks in neighboring cities? Could it reinvent relationships between social services caseworkers and benefits recipients? It's hard to say unless public-sector workforces are given some freedom to experiment.

Sure, social networks pose legitimate security and privacy concerns for public agencies. They also blur the line between working and simply goofing off. And if government agencies have been restrictive about employees using these sites at work, they're not alone. A survey released earlier this year by Robert Half Technology found that more than 50 percent of private businesses contacted completely prohibit social networking during work hours.

Luckily, the landscape is beginning to change. And as with many things in technology, the state of Utah is leading the way. In September, the state's Department of Technology Services released guidelines that give thoughtful advice to state employees who participate in social networks. The guidelines offer tips for creating interesting and valuable content. They also warn employees to be honest and respectful in their online postings, urge them to think before replying to comments, and remind them to follow state privacy laws. "We want to make sure that when our agencies use social media, they do it responsibly," says Utah Chief Technology Officer Dave Fletcher. It's important to "recognize the difference between social media as a private individual and social media as a public or government representative — that's not clear to some people."

Fletcher, himself a prolific blogger and microblogger, says guidelines are vital as governments increase their use of Web 2.0 networks. Utah's Web portal includes more than 30 blogs from public entities and more than 200 Twitter feeds from state and local agencies within the state. "More and more, our agencies are using social media," Fletcher says, "and there are increasing expectations from citizens that agencies will interact with them when they have issues and questions."

To create its guidelines, Utah borrowed ideas from businesses and the few available government social media policies. The document also includes the state's own hard-won experience, Fletcher adds. "I started blogging in 2002, so I've observed the evolution of social media. And I've watched as people have gotten fired from their jobs for using social media incorrectly."

What Utah's guidelines acknowledge is that the use of social media at work isn't strictly a technology issue. It's also a management issue. The guidelines don't say which employees belong on social networks and which ones don't — that determination is up to individual agencies. But the guidelines do make the issue easier for agencies to address. And that's a step in the right direction.

Heartland to pay up to \$60M to Visa over breach

By Grant Gross

January 8, 2010 12:00 PM ET

IDG News Service - Heartland Payment Systems will pay up to \$60 million to issuers of Visa credit and debit cards for losses they incurred from a [2008 data breach](#) at the large payment processor.

The settlement between Heartland and Visa, announced today, will offer card issuers "an immediate recovery with respect to losses they may have incurred from the Heartland intrusion," Ellen Richey, Visa's chief enterprise risk officer, said in a statement.

Heartland disclosed the breach a year ago. The U.S. Department of Justice has charged Albert Gonzalez and several other accomplices with the data breach, and Heartland was one of several companies they broke into using [SQL injection attacks](#). Gonzalez and his associates stole more than 130 million credit card numbers from Heartland, prosecutors alleged.

Gonzalez [pleaded guilty](#) in the Heartland case and in two other data breach cases. In the Heartland case, he pleaded guilty in December to two counts of conspiracy and will receive a prison term of at least 17 years.

Heartland's settlement with Visa is the second the company has announced in the past month. Heartland agreed to pay [American Express \\$3.6 million](#) in a settlement announced in December.

Bob Carr, Heartland's chairman and CEO, called the deal with Visa a "fair settlement." The company is committed to helping card issuers reduce data breach risks, he said in a statement.

The Visa/Heartland settlement agreement will go into effect after 80% of the eligible card issuers accept the deal, the two companies said in a press release. U.S. and international card issuers are eligible for the settlement money. By participating in the program, card issuers release Heartland and Visa from any additional liability.