

## Enterprises Failing Social Media Test

### **Siemens study highlights the disconnect between the majority of consumers who want to use social media to connect with businesses and the few companies who are prepared to meet the demand.**

By [Alison Diana](#) [InformationWeek](#) July 19, 2010

Although 70% of consumers want to interact with businesses using social media, less than one-third of companies have the strategies, policies, and processes in place to meet this demand, according to a report.

The relative handful of organizations already addressing how to communicate with customers using social media could do a better job, finds the study, which was conducted by the Yankee Group for Siemens Enterprise Communications, which develops [unified communications](#) and contact center solutions. After all, average consumer satisfaction with current business interactions via social media is just 65%, the report found.

"Social media is changing the way businesses, customers, and employees interact, and this creates significant opportunities for contact centers and the enterprise as a whole to leverage the integration of these tools into business processes," said Zeus Kerravala, senior VP of enterprise research at Yankee Group. "As integration of social media improves within the contact center and with unified communications and collaboration, businesses can improve customer interactions and positively impact employee productivity and collaboration."

In fact, 58% of respondents credit regular communication via social media for enhancing loyalty to a business, the poll determined.

But social media is not only beneficial for consumer relations, according to Yankee Group's report. Corporations also can use the technology to improve internal operations and employee effectiveness: 67% of employees said they need more tools to track and manage their social communications for business reasons, the study said.

With the goal of meeting this customer and employee demand, Siemens Enterprise today began offering OpenScape Fusion Social Media Integrations for unified communications and contact centers. Available through channel partners and Siemens' professional services organization, the technologies are designed to help corporations incorporate social media -- ranging from Facebook and Twitter to internal social networking sites -- into day-to-day operations, Ross Sedgewick, senior director of large enterprise solutions marketing, told *Information Week*.

"The integrations are not necessarily pre-defined and plug-and-play. They're going to be driven by which media outlets have the business impacts -- professional or consumer," he said.

Midsized and large organizations can use OpenScape Fusion Social Media Integrations to automate and aggregate social media tools and contacts with their existing desktop communications, allowing users to easily collaborate and monitor customer and partner activities, according to Siemens Enterprise. To improve customer service, employees can escalate social media dialogs using one-click technology, moving into multi-party audio- or video-conferencing to resolve a customer problem.

The solution is customizable and adaptable, with businesses able to select as many or as few features as they want or need, then evolve and expand over time, said Sedgewick. Pricing varies, depending on the capabilities, services, and scope.

Since first unveiling a working prototype [at VoiceCon](#) in 2009, Siemens Enterprise has worked with several customers, including Henry Ford Health Systems and LateRooms.com. Dozens of customers have expressed interest in the technology, Sedgewick said.

"We see social media as a rapidly emerging interaction channel for our clients, and adding social media capabilities including web presence, web chat, and other tools, is another way we can deliver better and faster service to our patients," said Lefka Simeon, administrator at Henry Ford Health System Contact Center, an early user of OpenScape Fusion Social Media Integrations.

Initially, consumer-facing businesses are expressing the most interest in the technology, said Sedgewick. Geographically, North America and the United Kingdom are expected to lead adoption, he said.

## **Burgeoning mobile Wi-Fi hotspots present risks to enterprises**

Ajay Gupta July 23, 2010

Conventional Wi-Fi hotspot sites are fixed and are limited to restaurants, airports, hotels, hospitals, coffee shops, departmental stores, parks and other public places.

However, in the recent times, a new class of Wi-Fi hotspots, generally known as mobile hotspots, is getting popular. Mobile Wi-Fi (Mi-Fi) hotspots are personal devices which easily can be carried and set up at any convenient place, to provide internet access to a limited number of Wi-Fi users and devices.

Consumerization of portable Wi-Fi devices is the main driving factor behind increasing mobile Wi-Fi hotspot options. Some of these are standalone devices, whereas others can be set up in software on a PDA, laptop/netbook or a smartphone. Further, some provide hotspot functionality in Wi-Fi infrastructure mode, while others in Wi-Fi ad-hoc mode.

Mobile hotspots' growing popularity can be gazed from the fact that hotspot-creating applications are becoming popular on the web. Similarly, cellular carriers around the globe are providing and launching Mi-Fi-like devices. With 4G cellular networks now rolling out, mobile hotspot usage is expected to increase in coming times.

However, growing usage of mobile Wi-Fi hotspots is having detrimental effects on corporate security. Hardware options for mobile hotspots, such as Mi-Fi devices and USB Wi-Fi routers, easily can be brought into corporate premises lacking strict physical security. In addition, tools for soft hotspot creation on corporate endpoints and employee smartphones readily are available.

Mobile hotspots are generally set up by employees, visitors and guests for convenience. But such convenience leaves the enterprise security in the cold in one or more of following ways:

**Easy, unrestricted internet access:** Corporate employees will be able to bypass corporate firewalls and internet access policies when they connect their laptops and notebooks to an active hotspot (with uplink to a cellular data connection). With unrestricted access to the internet, not only is employee productivity at risk, but employees are more susceptible to installation of malware on their machines. Malware can result in disruption of the corporate network, theft of personal and corporate confidential information or improper functioning of the affected machine. Also, the malware can spread to other parts of the network.

**Malicious access to corporate endpoints:** Mobile Wi-Fi hotspots generally lack strong security controls, so if a personal hotspot signal reaches at places such as a parking lot or outside the premises, then a malicious hacker can connect to this hotspot and achieve access to corporate endpoints associated to the hotspot.

**Increased exposure to malicious attacks:** Even after the shutdown of a mobile hotspot, the network details are cached in to a connected corporate Windows machine, which causes the machine to search for the hotspot network at a later time. A seasoned Wi-Fi hacker (in range of searching signal) can exploit this in particular cases and can establish a connection with machine to compromise the same in various ways.

**Increased rogue AP risks:** Windows 7, USB Wi-Fi routers and smartphone-based hotspots operating over a corporate machine can result in a rogue access point (AP), if, by chance, these hotspots are configured to share the corporate network access available on the machine with their respective hotspot users. A rogue AP provides backdoor/unauthorized access to the corporate network.

**Increased interference to the corporate Wi-Fi network:** Operation of hotspots inside the corporate premises causes interference and drives corporate Wi-Fi network performance to lower levels. Very low values of performance occurring due to excessive interference from large number of operational hotspots is analogous to a denial-of-service attack on corporate Wi-Fi. Apple CEO Steve Jobs, at recent iPhone 4 launch, experienced such excessive interference from audience members operating a large number of personal Mi-Fi devices during the launch.

## Summary

Considering the effects on enterprise security, the need for 24-by-7 monitoring and scanning for various types of operational hotspots is apparent. To detect and prevent the operation of mobile hotspots, deployment of a wireless intrusion prevention system (WIPS) can be considered. Software mobile hotspots also can be prevented by installing a wireless security agent on to the machines on which these software hotspots are configured.

## How to steal corporate secrets in 20 minutes: Ask

By Robert McMillan  
July 30, 2010

IDG News Service - A few companies in the Fortune 500 need to upgrade their Web browsers. And while they're at it, a little in-house training on social engineering wouldn't be a bad idea, either.

Social engineering hackers -- people who trick employees into doing and saying things that they shouldn't -- took their best shot at the Fortune 500 during a [contest](#) at Defcon Friday and showed how easy it is to get people to talk, if only you tell the right lie.

Contestants got IT staffers at major corporations, including Microsoft, Cisco Systems, Apple and Shell, to give up all sorts of information that could be used in a computer attack, including what browser and version number they were using (the first two companies called Friday were using IE6), what software they use to open pdf documents, their operating system and service pack number, their mail client, the antivirus software they use, and even the name of their local wireless network.

The first two contestants made it look easy.

Wayne, a security consultant from Australia who wouldn't give his last name, was first up Friday morning. His mission: Get data from a major U.S. company. (IDG News Service has chosen not to report which companies fell for which attacks because of possible security risks.)

Sitting behind a sound-proof booth before an audience, he connected with an IT call center and got an employee talking. Pretending to be a KPMG consultant doing an audit under deadline pressure, Wayne got him to spill details, big time.

Wayne ignored a request for an employee number and launched immediately into a story about how his boss was on his back, and how he really needed to get this audit finished. He worked his Aussie charm on the worker,

who'd only been with his new employer for a month. Within minutes, it seemed he was willing to give Wayne pretty much any information he wanted -- at one point he even visited a fake KMPG Web page that Wayne had set up.

He ended the call promising to buy the employee a beer.

He ended the call promising to buy Ledoi a beer.

"What beer do you like?"

"Right now I'm on a Blue Moon kick."

In an interview after the call, Wayne couldn't believe his luck. "I was thinking they're a pretty big company and I know they did a lot of in-house security audits."

Later, contest organizers said his effort was the best of the day. But everyone who was targeted gave up information. Chris Hadnagy, one of the founders of the contest, believes the victims would have given away sensitive information such as passwords had they been asked. "They would have given pictures of their family if they'd asked for it," he said.

Contest rules prohibited asking for any sensitive information, or targeting certain types of organizations such as government or financial institutions. Even so, the contest rattled nerves even before it had started. Last month, Hadnagy [received a call](#) from the FBI asking about the contest.

Wayne, who has done this type of social engineering for 15 years in his day job as a security consultant, said he did about 20 hours of reconnaissance ahead of the contest. He knew how to reach the IT call center and what names to drop when he got through.

He conceded that he'd lucked out by getting such a green employee. But new employees make the best sources. "If you pick someone who's a high-up person in the company, you'll get nothing," he said. "They've got a lot to lose."

Contestant number two, Shane MacDougall, decided to skip the call center and go right for the security staff at another well-known company. He took a more buttoned-down approach, claiming to be conducting a survey for CSO Magazine.

The first person he reached knew what he was doing, and firmly but politely shut MacDougall down after refusing to answer a few questions, saying, "These are specific questions that I don't feel comfortable answering."

Contestants were given only 25 minutes to work. So with the clock ticking, MacDougall lucked out on his next mark -- a contract employee in the security engineering department who had been with the company for two months. After a few softball questions about job satisfaction and the quality of the cafeteria food, he went for the hard data.

The mark delivered: operating system: Windows XP, service pack 3; antivirus: McAfee VirusScan 8.7; e-mail: Outlook 2003, service pack 3; browser: IE 6.

MacDougall then told him to visit a website to collect his US\$25 survey coupon, and Ryan complied.

## Cybersecurity mythbusting: Book smart vs. street smart

Charles Jeter, ESET cybercrime investigator  
August 03, 2010

Who would be better prepared to face off against cybercrime? A high school dropout or a Ph.D.? The answers will surprise you.

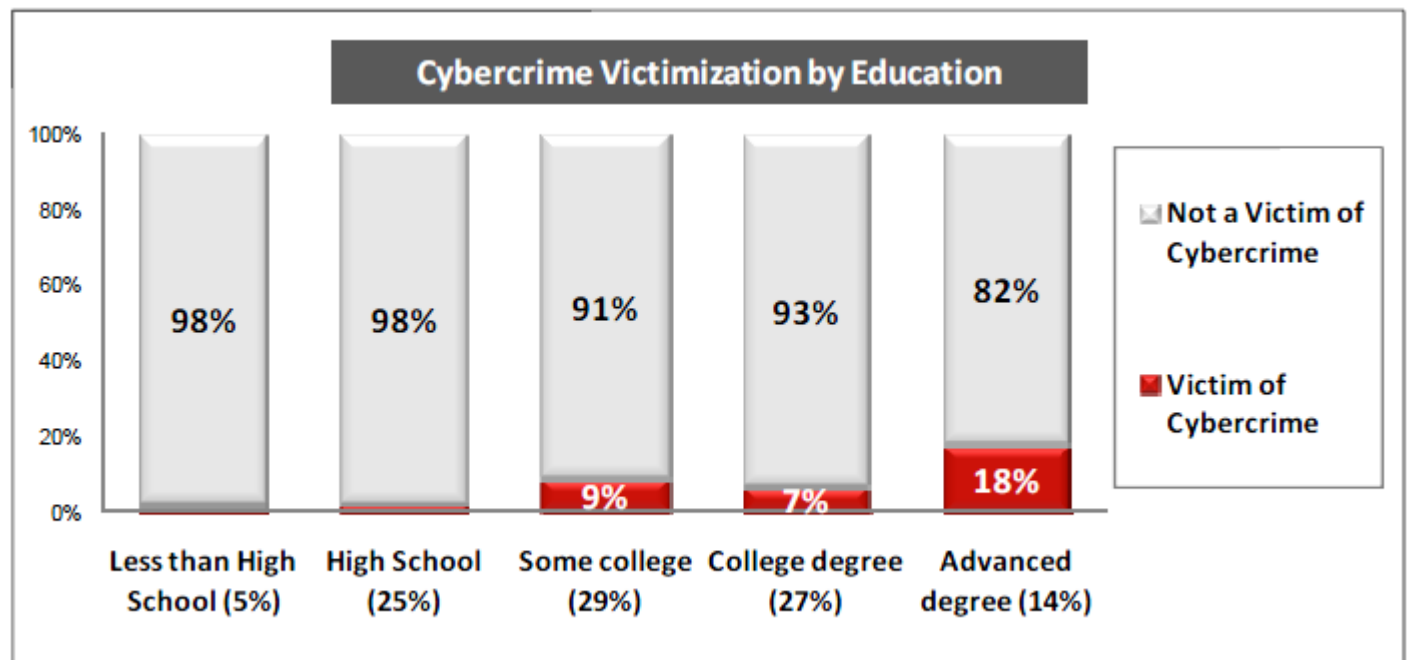
If the decision were based on a quick game of Three-card Monte in a back alley, conventional wisdom might favor the dropout – or at least provide even money between them. But what happens when it comes to recognizing computer crimes and scams which cost much more than pocket change? Will street smarts win out over book smart when it comes to cybercrime victimization?

### Perspective: Book smart vs. street smart quantified

Quoting from [a recent cybersecurity study](#) performed for ESET and [Securing Our eCity](#):

**Surprisingly, cybercrime victimization is also strongly related to education levels, and the more educated are more likely to be victimized.**

**As the chart shows, those who have not attended college are relatively immune to cybercrime.** Among those with some college or a bachelors degree, victimization is at moderate levels.



**But those with advanced degrees have really been hard hit: 18 percent in this group have been victims of cybercrime.**

Although cybercrime tends to be even more prevalent among highly educated Americans who spend more time online, **the victimization rate is high among those with advanced degrees – even among those who are on the internet less than three hours per week.**

This strong tie between education and victimization suggests that cybercriminals may more often target those who earn advanced degrees.

## **My perspective: Criminals usually take path of least resistance**

I could theorize that cybercriminals consider higher education to be where the money is that they want to steal; dot-edu's are considerably within the cybercriminal's purview. I disagree with the "targeted graduate" theory only because there is too much work involved and too many other willing victims to be reached through a broader approach such as phishing.

## **Perspective: Bulletproof monks**

Again, from CERC October 2009:

Also, some hubris on the part of well-educated people along the lines of "this can't happen to me" may occur and lead to riskier behavior.

I don't find this assessment to be complete, but it does have some truth to it. I recall one key cybersecurity discussion a few short years ago with a nameless defense contracting company. The topic was whether to implement internal controls and fundamental cybersecurity measures or not.

One example of the poor security observed was the insistence on sending interoffice mail through an external (and commercial) mail server with no domain security measures in place.

While this added vulnerability could be described as a theoretical risk, the "Admin-Admin" login/password combination found on all systems was not to be ignored.

Yet the cybersecurity risks were difficult to communicate and harder to put into place as practices. This took a surprising turn as the hardest sells on the concept and value of security turned out to be with the most educated members of the senior leadership – the academics.

The main objection to implementing proper network security adoption was upheld by two of the Ph.D-level senior leaders. Both also had significant personal risk as stakeholders. Along with being highly educated, the same two objectors were majority shareholders in the small, closely held business.

Yet both doctoral graduates cared little for the details around implementing proper network security – whether expressed as a duty and responsibility to their armed forces clients or expressed as a risk to their intellectual property and personal livelihoods.

Therefore, drawing from my personal experience, I must agree to some extent that book smart victims may indeed be falling prey to a "bulletproof genius syndrome" of academia. Partly, I find this to be responsible.

As a CIO, the challenge is in the human element – the more they know or think they know, the less your audience will want to hear from you. Finding ways to target the best teachable moments will become the longest challenge.

## Mobile malware: You will be billed \$90,000 for this call



Be it business or pleasure, most of us have our cell phones handy at all times. Those phones are full of vulnerabilities which are ripe for viruses. Some people change apps faster than their underwear; some of those apps act as a Trojan Horse carrying malicious code. Although some [software security experts](#) expect smartphones to be a tempting new target for hackers, F-Secure reported there haven't been more than 500 mobile phone viruses so far. What do we have to thank for staving off the upcoming smartphone attacks? Windows XP.

"There are more phones on the planet than computers. And it's easier to steal money from phones," stated Mikko Hypponen, chief research officer at security firm F-Secure Corp. In a [video interview](#), Hypponen explained there haven't been more mobile phone attacks, since Windows XP computers are still the "easiest" and most exploitable target. Even though Microsoft discontinued support, Windows XP is

still widely used throughout the world. It's currently "very easy" for online criminals to make money off of XP. As XP disappears, attackers will start to look around for another easy and popular target. Then online criminals will set their sights on smartphones which all have a built-in payment mechanism in the form of a monthly bill.

According to the above video, any mobile platform could be targeted. However, Hypponen guesses that the three main platforms for smartphone attacks will be iPhone, Android and Symbian. Most phone attacks are coming from Russia, South America, parts of Asia, and China where Symbian is king of the smartphones. Hypponen explained in the interview that so far all the attacks on smartphones have been, more or less, due to social engineering and tricking users into clicking on a link.

At his Black Hat presentation, Hypponen explained why attackers are starting to eye mobile platforms as targets. Criminals are finding ways to route money without leaving a trail for law enforcement. His talk was entitled, "[You will be billed \\$90,000 for this call.](#)"

We would be quick to report such an outlandish charge on our bill. If the calls totaled \$12, however, how many people would notice, admit to being scammed, and take the time to report it?

Hypponen told a tale of a hacker removing the copy protection from a [3D anti-terrorist shooting game](#) before offering the cracked version as a free app via a copycat site. Also free in the download was mobile malware. When users played the Trojanized game, their phones would secretly issue eight expensive international calls to places such as North Korea, Africa, and Antarctica. These special long-lining numbers didn't actually call the South Pole, but instead the call might end up routed to Canada while still billing the whole premium international expense to the South Pole. The billing difference between calling the premium international number (South Pole) and the less expensive location (Canada) goes to the virus writer.

To avoid detection after its \$12 payload was triggered, the mobile malware-laced app would work only as a game while the virus slept for 31 days. Then the virus would awaken and issue eight premium international calls again.

"Eventually, virus writers will realize it is easier to make money by infecting phones than it is by infecting computers," [Hypponen tweeted](#). According to the video, he expects to eventually see mobile smartphone worms that spread automatically to everyone listed in a phone's address book. When this happens, a worm could spread infection around the world in only a couple of minutes.

He advises cell phone owners to be wary of apps, install [anti-virus software](#) on your cell phone, and set strong passwords.

## **THE BARBARIANS ARE ALREADY INSIDE THE GATES: MITIGATING INSIDER THREATS**

AUGUST 2ND, 2010 TOM OLZAK

INFORMATION SECURITY. IT USED TO MEAN KEEPING THE "BARBARIANS" ON THE OTHER SIDE OF OUR WALL AND MOAT. YOU KNOW, THAT PERIMETER WE SO PAINSTAKINGLY BUILT WITH ALL THE NEWEST TECHNOLOGY. MOST OF US NOW UNDERSTAND THAT IT TAKES MUCH MORE. SO WE'VE BUILT INTERNAL CONTROLS TO STRENGTHEN SECURITY AROUND SYSTEMS, STORAGE DEVICES, ETC. BUT THIS IS OFTEN STILL NOT ENOUGH TO STOP A BREACH.

OUR SECURITY CONTROLS ARE TYPICALLY DESIGNED TO KEEP UNAUTHORIZED ENTITIES (HUMANS AND SOFTWARE) FROM REACHING OUR INFORMATION ASSETS. THE PROBLEM TODAY IS THAT MANY OF OUR TRUSTED USERS ARE BEHAVING IN WAYS THAT PUT OUR DATA, AND OUR ORGANIZATIONS, AT RISK.

### **THE CHALLENGE**

FIRST, LET'S PUT TO REST ANY DOUBT IN YOUR MIND THAT THIS IS A PROBLEM IN YOUR ORGANIZATION. ACCORDING TO DAWN CAPPELLI, TECHNICAL MANAGER FOR THE THREAT AND INCIDENT MANAGEMENT DIVISION OF THE SOFTWARE ENGINEERING INSTITUTE CERT PROGRAM, "...INSIDER ATTACKS CONTINUE TO BE SEEN AS A BIGGER PROBLEM THAN ANYTHING THAT MIGHT COME FROM THE OUTSIDE" (**BRENNER, 2010, P. 2**). DOLLARS SPENT TO PREVENT BREACHES AND OTHER INFORMATION ASSET RELATED INCIDENTS CAUSED BY EMPLOYEES MAY HAVE A LARGER ROI THAN THOSE SPENT ON TRADITIONAL CONTROLS.

THERE ARE THREE BASIC WAYS OUR EMPLOYEES PUT OUR ORGANIZATIONS AT RISK: DATA LEAKAGE, DATA THEFT, AND SYSTEM VANDALISM. DATA LEAKAGE IS A COMMON ENEMY OF SECURITY MANAGERS. IT ENABLES DATA BREACHES BY MOVING SENSITIVE INFORMATION FROM TRUSTED LOCATIONS TO STORAGE WITH INEFFECTIVE OR ABSENT SECURITY CONTROLS. FOR EXAMPLE, USERS OFTEN WANT TO TAKE DATA HOME TO MEET A TIGHT PROJECT DEADLINE. COPYING FILES TO A THUMB DRIVE OR OTHER MOBILE STORAGE DEVICE IS THE FASTEST WAY TO

GET WHAT THEY NEED AND MAKE IT HOME IN TIME FOR DINNER. IN MANY CASES, THEY JUST MOVED INFORMATION FROM HIGHLY SECURED LOCATIONS TO UNSECURED, UNENCRYPTED DEVICES. AND WE KNOW THESE DEVICES ARE NEVER LOST OR STOLEN...

DATA THEFT IS WHAT WE NORMALLY THINK OF WHEN WE HEAR ABOUT A BREACH. BUT WHY WOULD A TRUSTED EMPLOYEE, SOMEONE WHO HAS POSSIBLY WORKED FOR US FOR YEARS, DECIDE TO STEAL OUR DATA? THERE ARE A NUMBER OF REASONS WHY THIS MIGHT HAPPEN, INCLUDING:

- BEING PASSED OVER FOR PROMOTION.
- GETTING EVEN ON THE WAY OUT THE DOOR AFTER BEING FIRED, INCLUDING ACCESSING THE NETWORK FROM HOME BECAUSE TERMINATION PROCESSES FAILED OR DON'T EXIST.
- TAKING INTELLECTUAL PROPERTY TO A NEW EMPLOYER.
- BECAUSE THEY WILL BE PAID BY ATTACKERS WHO JUST DON'T WANT TO TACKLE THE REALLY NICE SECURITY FRAMEWORK YOU'VE CONSTRUCTED.

SYSTEM VANDALISM IS CLOSELY RELATED TO THE REASONS DISGRUNTLED EMPLOYEES STEAL DATA. IN SOME CASES, SYSTEMS ARE LOCKED DOWN, DATA ERASED, OR DESTRUCTIVE APPLICATIONS ARE LEFT BEHIND AFTER SENSITIVE INFORMATION IS COPIED TO THE THUMB DRIVE ALREADY SAFELY IN THE EMPLOYEE'S BACKPACK.

#### **THE SOLUTION**

CONTROLS ASSOCIATED WITH THE BASIC CONCEPTS OF LIMITING DAMAGE CAUSED BY EMPLOYEES SHOULD ALREADY BE IN PLACE; ALLOW THEM ONLY TO HAVE THE RIGHTS AND PRIVILEGES ABSOLUTELY NECESSARY TO DO THEIR JOBS (LEAST PRIVILEGE), RESTRICT THEM ONLY TO SEE INFORMATION NECESSARY FOR THEIR PIECE OF BUSINESS OPERATION (NEED-TO-KNOW), AND PREVENT ANY ONE EMPLOYEE FROM PERFORMING ALL THE TASKS ASSOCIATED WITH CRITICAL PROCESSES (SEPARATION OF DUTIES). I LIKE TO ADD TO THIS LIST SOMETHING THAT MANY ORGANIZATIONS ARE BEGINNING TO PRACTICE: ONLY KEEP SENSITIVE INFORMATION IN COMPANY SYSTEMS THAT IS ABSOLUTELY NECESSARY TO CONTINUE BUSINESS OPERATIONS. GET RID OF EVERYTHING ELSE.

THESE CONTROLS ARE A GOOD START, BUT HOW DO WE MAKE SURE EMPLOYEES PROPERLY HANDLE THE INFORMATION TO WHICH THEY MUST HAVE ACCESS? THIS GETS A LITTLE HARDER TO ENFORCE. SOME RECOMMENDED PREVENTION CONTROLS INCLUDE:

- **RESTRICTED USE OF MOBILE STORAGE.** MOBILE STORAGE DEVICES COME IN MANY FORMS, INCLUDING: THUMB DRIVES, PHONES, AND USB HARD DRIVES. IF YOU CAN'T CONVINCE MANAGEMENT TO USE TECHNOLOGY TO PREVENT USE OF THESE DEVICES, THEN AT LEAST MAKE SURE THEY ARE SECURE. ENCRYPTING USB DEVICES IS EASIER TODAY BECAUSE OF ADDITIONS TO OPERATING SYSTEMS (WINDOWS 7) AND SECURITY SUITES LIKE MCAFEE.
- **EFFECTIVE TERMINATION PROCESSES.** NEVER... LET ME SAY THAT AGAIN... NEVER ALLOW AN EMPLOYEE TO RETURN TO HIS OR HER DESK UNESCORTED AFTER THEY'VE BEEN

TERMINATED. IN ADDITION, TERMINATE ALL ACCESS TO INFORMATION ASSETS WHILE THE EMPLOYEE IS MEETING WITH MANAGEMENT TO GET THE BAD NEWS. IN SUPPORT OF THIS PROCESS, ENSURE ALL EMPLOYEES LEAVING ON THEIR OWN ARE LOCKED OUT OF REMOTE ACCESS AS QUICKLY AS POSSIBLE AFTER THEY LEAVE ON THEIR LAST DAY.

- **PROVIDE A METHOD FOR EMPLOYEES TO REPORT SUSPICIOUS PEER OR SUBORDINATE BEHAVIOR.** MOST EMPLOYEES ARE HONEST AND ABOVE THE TYPES OF ACTIVITIES WE'RE EXAMINING HERE. MANY ARE ALSO WILLING TO REPORT UNUSUAL BEHAVIOR THAT MIGHT INDICATE THAT A PEER IS ABOUT TO DO SOMETHING YOU WOULD RATHER THEY DIDN'T. PROVIDE A WAY FOR EMPLOYEES TO ANONYMOUSLY REPORT THESE INCIDENTS. FURTHER, TRAIN MANAGERS ON HOW TO IDENTITY POTENTIAL PROBLEMS.
- **PERFORM INITIAL AND REGULAR BACKGROUND CHECKS OF EMPLOYEES IN SENSITIVE POSITIONS.** MANY ORGANIZATIONS PERFORM BACKGROUND CHECKS BEFORE SENDING AN OFFER LETTER. HOWEVER, ENSURING EMPLOYEE SUITABILITY TO HANDLE SENSITIVE ASSETS USUALLY STOPS THERE. RELATED TO THE PREVIOUS BULLET, ORGANIZATIONS SHOULD CONSIDER PERIODIC CHECKS FOR EMPLOYEES WITH ACCESS TO HIGHLY SENSITIVE INFORMATION.
- **BLOCK USE OF DATA SHARING SITES.** A LARGE NUMBER OF ONLINE SOLUTIONS EXIST THAT ALLOW EMPLOYEES TO SHARE LARGE FILES WHILE BYPASSING OTHER CONTROLS, LIKE EMAIL ATTACHMENT SIZE LIMITS. ONE EXAMPLE, AND A SERVICE I OFTEN USE, IS TRANSFERBIGFILES.COM.
- **LOOK FOR UNUSUAL ACCESS PATTERNS.** IN THE WHITEPAPER, *STOPPING INSIDER ATTACKS: HOW ORGANIZATIONS CAN PROTECT THEIR SENSITIVE INFORMATION*, IBM (2006, P.7) RECOMMENDS STARTING BY CREATING A BASELINE OF NORMAL USER BEHAVIOR IN EACH SYSTEM. THIS IS FOLLOWED BY INTEGRATING THE FOLLOWING INFORMATION INTO YOUR LOG MANAGEMENT SYSTEM AND ALERTING ON ANOMALIES:
  - INITIAL CONNECTION—DATE AND TIME OF LOGON, IP ADDRESSES INVOLVED, AND CONNECTION FREQUENCY
  - DATA ACCESS—REQUESTS FOR DATA, ORGANIZED ACCORDING TO SPECIFIC TYPE
  - APPLICATION USAGE—FREQUENCY AND DURATION
  - OVERALL USAGE—TOTAL SESSION TIME AND OVERALL DATA USAGE REQUESTS
- **FILTERING OF MOVING INFORMATION.** AND WHEN EVERYTHING ELSE IS IN PLACE, MAKE SURE YOUR TRUSTED AND HONEST EMPLOYEES ARE NOT MAKING MISTAKES ABOUT HOW THEY HANDLE INFORMATION, INCLUDING
  - SCAN AND FILTER OUTGOING EMAIL
  - USE **EXTRUSION DEFENSE** CONTROLS

- SCAN AND FILTER DATA COPIED ACROSS THE NETWORK
- SCAN ENTERPRISE STORAGE AND REPORT ON POSSIBLE INFORMATION STORED IN LOCATIONS LACKING THE RIGHT AMOUNT OF SECURITY

## KNOWLEDGEABLE HUMANS ARE STILL THE BEST SPAM FILTERS

DATE: JULY 26TH, 2010 RICHARD PERRIN

*SPAMMERS AND PHISHERS SPOOF THE ADDRESSES, SUBJECT LINES, AND CONTENTS OF LEGITIMATE EMAILS FROM POPULAR SERVICES. A SIMPLE RULE OF THUMB CAN HELP SPOT THE FAKES.*

---

BOTH SPAM FILTERS AND INCREASING AWARENESS OF THE MOST SIMPLE FORMS OF TRICKERY ARE ALLOWING MANY USERS TO MORE EASILY DETECT AND AVOID OPENING SPAM AND PHISHING EMAILS. WHILE AUTOMATED SPAM FILTERS ARE FAR FROM PERFECT — ONE MUST EFFECTIVELY CHOOSE BETWEEN A FILTER THAT DOESN'T CATCH EVERYTHING IT SHOULD OR A FILTER THAT CATCHES THINGS IT *SHOULDN'T* — THEY ARE GETTING BETTER AT FILTERING OUT THE SIMPLE STUFF.

THE SPAMMERS AND PHISHERS ARE NOT TAKING THIS LYING DOWN, HOWEVER. AS WITH THE **COLD WAR** BETWEEN THE UNITED STATES AND THE SOVIET UNION, THERE IS AN ARMS RACE GOING ON BETWEEN MASS UNSOLICITED EMAILERS AND THE PEOPLE TRYING TO DETECT, AND DEFEND AGAINST, THEIR EFFORTS. EVERY TIME A NEW SOLUTION IS AVAILABLE THAT PROVIDES BETTER DETECTION AND PROTECTION, IT TURNS OUT THE SPAMMERS AND PHISHERS HAVE ALREADY DEVELOPED AN EVEN BETTER WAY TO GET AROUND YOUR DEFENSES AND HAVE ALREADY BEEN USING IT FOR A WHILE. UNFORTUNATELY, THE DEFENDERS ARE ALWAYS A COUPLE OF STEPS BEHIND IN THE TECHNOLOGICAL ARMS RACE. IT TAKES HUMAN JUDGMENT TO REALLY BEAT THE SPAMMERS AND PHISHERS.

THE MOST KNOWLEDGEABLE AND CAREFUL AMONG US TEND TO BE FAIRLY IMMUNE TO THESE PROBLEMS. FOR INSTANCE, BY READING ALL EMAIL IN PLAIN TEXT, WITH ZERO MARKUP PARSING AND NO IMAGE DISPLAYING, SOME OF US HAVE RENDERED OURSELVES EFFECTIVELY UNTOUCHABLE BY THE EFFORTS OF PHISHERS: IT TENDS TO BE SAFE TO OPEN EMAILS FROM SUCH MISCREANTS AS PLAIN TEXT, SINCE THE SCRIPTING AND MARKUP TRICKS PHISHERS USE TO GET COMPUTERS TO DO THEIR DIRTY WORK FOR THEM WITHOUT THE PERMISSION OF THE USER ARE RENDERED INERT AND INEFFECTIVE WHEN THE EMAIL CLIENT DOES NOT PARSE THE CONTENT AS MARKUP. THE DAY MAY COME WHEN SOMEONE FINDS A WAY AROUND EVEN THAT LEVEL OF CAUTION, BUT BY THEN THE MOST KNOWLEDGEABLE ABOUT EMAIL SECURITY WILL PROBABLY HAVE COME UP WITH AN EVEN BETTER WAY TO DEAL WITH THE ISSUE.

THE FACT REMAINS, THOUGH, THAT NO MATTER HOW WELL THE MOST KNOWLEDGEABLE (AND CAREFUL) AMONG US CAN DEFEND OURSELVES AGAINST PHISHERS AND SPAMMERS, THE MAJORITY OF EMAIL USERS HAVE NEITHER THE UNDERSTANDING NOR THE TOOLS TO SIMILARLY DEFEND THEMSELVES. MORE DEPRESSINGLY, MANY PEOPLE WHO SHOULD KNOW BETTER REFUSE TO USE SUCH TACTICS AS VIEWING EMAILS ONLY IN PLAIN TEXT AT LEAST UNTIL THE SAFETY OF THE EMAIL IN QUESTION HAS BEEN DETERMINED TO BE SAFE AND GENUINE WITH CERTAINTY. ONE OF THE KEYS TO PROTECTING YOURSELF IS TO AVOID ACTING IMPULSIVELY WHEN IT COMES TO EMAIL. ANOTHER IS TO MINIMIZE THE TENDENCY TO LET THE COMPUTER DO YOUR THINKING

FOR YOU, ESPECIALLY CONSIDERING HOW BAD COMPUTERS ARE AT APPROXIMATING “THINKING”. RELYING SOLELY ON SAFETY RULES IMPOSED BY AN APPLICATION DEVELOPER IS A RECIPE FOR FAILURE, IN PART BECAUSE BY THE TIME THE NEWEST VERSION OF AN APPLICATION GETS TO THE END USER THE CHANCES ARE GOOD THAT THESE RULES ARE ALREADY OUT OF DATE. IT IS EVEN WORSE WHEN USING EMAIL WEB CLIENT SOFTWARE SUCH AS ONE OF MICROSOFT’S FLAGSHIP OFFERINGS, WINDOWS LIVE HOTMAIL. SUCH SERVICES TYPICALLY “HELP” YOU BY DEFAULTING TO OPENING NEW MESSAGES WHEN USERS TRY TO SELECT A MESSAGE OR EVEN WHEN THEY SIMPLY DELETE ANOTHER MESSAGE IN THE SAME “MAILBOX”. FROM A SECURITY PERSPECTIVE, THIS KIND OF EMAIL INTERFACE BEHAVIOR IS SIMPLY UNACCEPTABLE, BUT IT IS ESSENTIALLY THE NORM FOR WEBMAIL.

GOING BACK TO ACTING IMPULSIVELY, HOWEVER, A CONSTANT PROBLEM FOR PHISHING AND SPAM EMAIL IS THE TACTIC OF SPOOFING, OR TAKING ON THE APPEARANCE OF, LEGITIMATE EMAILS FROM POPULAR WEB SERVICES. IT IS A CONSTANT PROBLEM, RATHER THAN A SOLVED PROBLEM, LARGELY BECAUSE THE EFFORTS TO SPOOF LEGITIMATE EMAILS ARE BECOMING MORE SOPHISTICATED. THIS IS AN ATTACK NOT ONLY ON THE ABILITY OF SPAM FILTERS TO WEED OUT THE BAD APPLES, BUT ALSO ON THE ABILITY OF END USERS TO RECOGNIZE SOMETHING “PHISHY” ABOUT THE MALIGNANT EMAILS — AT LEAST UNTIL IT IS TOO LATE, AND MOST USERS HAVE ALREADY OPENED THE EMAIL.

BY CURBING THE TENDENCY TO ACT IMMEDIATELY AND IMPULSIVELY WHEN DEALING WITH SUCH EMAILS, A SIMPLE RULE OF THUMB CAN HELP DEFEND AGAINST THE ATTEMPTS TO TRICK US INTO TRUSTING AN EMAIL WE SHOULD NOT, IN FACT, TRUST. THE RULE IS SIMPLE: HAVE PATIENCE. SPECIFICALLY, WHENEVER YOU GET AN UNEXPECTED EMAIL FROM SOMETHING LIKE AMAZON, PAYPAL, FACEBOOK, EBAY, OR EVEN CHASE BANK, WAIT A WHILE BEFORE OPENING IT. WAIT AT LEAST 12 HOURS, IN FACT. THE THEORY IS QUITE SIMPLE: WHEN BOTNETS START SENDING OUT PHISHING AND SPAM EMAILS TARGETING USERS OF SPECIFIC SERVICES OR CUSTOMERS OF SPECIFIC BUSINESSES, THEY TEND TO SEND EVERYONE SEVERAL SUCH EMAILS IN A SHORT PERIOD OF TIME. IF YOU GET ONE SUCH EMAIL NOW, CHANCES ARE GOOD THAT YOU WILL GET A COUPLE MORE IN THE NEXT TWELVE HOURS OR SO, WITH THE SAME SUBJECT LINE, OR AT LEAST AS SUBJECT LINE THAT IS RECOGNIZABLY SIMILAR. EVEN IF A LEGITIMATE EMAIL OF THE TYPE BEING SPOOFED INVOLVES SOME KIND OF REQUEST FOR CONFIRMATION, SUCH REQUESTS TEND TO TAKE AT LEAST 24 HOURS TO EXPIRE (USUALLY LONGER), MEANING THAT WAITING SOMEWHERE

IN THE RANGE OF TWELVE TO SIXTEEN HOURS GIVES YOU PLENTY OF LEEWAY. EVEN IF YOU LET REQUESTS IN LEGITIMATE EMAILS EXPIRE, THE DEFAULT TENDS TO BE TO LET THINGS REMAIN HOW YOU SET THEM UP IN THE FIRST PLACE, SO THAT THERE IS PROBABLY NO HARM DONE BY MISSING THE DEADLINE.

THIS SIMPLE TECHNIQUE OF HAVING PATIENCE, AND LOOKING FOR DUPLICATE PHISHING ATTEMPTS, IS ESPECIALLY EFFECTIVE IF YOU HAVE MULTIPLE EMAIL ADDRESSES. IN THAT CASE, MORE THAN ONE OF YOUR EMAIL ACCOUNTS MAY WELL RECEIVE SUCH SPAM OR PHISHING EMAILS SPOOFING LEGITIMATE COMMUNICATIONS FROM POPULAR WEB SERVICES, MAKING THE CLUMSY DECEPTION EVEN MORE OBVIOUS.

KEEP IN MIND THAT THIS IS NOT A FOOLPROOF METHOD OF DETECTION. THERE MAY BE CASES WHERE ONLY ONE SUCH EMAIL ARRIVES IN YOUR INBOX IN THE FIRST TWELVE HOURS, LEAVING YOU STILL UNCERTAIN, SO THAT OPENING THE EMAIL TO READ IT IN ALL ITS HTML- AND JAVASCRIPT-PARSED GLORY CAN STILL BE DANGEROUS. AS ALWAYS, YOU SHOULD ENGAGE YOUR BRAIN BEFORE DEALING WITH ANY UNEXPECTED EMAILS, AND EXERCISE YOUR BEST JUDGMENT. WAITING BEFORE EVEN CONSIDERING OPENING SUCH EMAILS, HOWEVER, MAY WELL HELP YOU IMPROVE YOUR EFFECTIVENESS AND ACCURACY IN IDENTIFYING SPAM AND PHISHING EMAILS THAT TRY TO SNEAK IN PAST THE BS FILTER IN YOUR BRAIN.

## **Cybercrime costs a business \$3.8 million/year, study finds**

Ponemon Institute researchers tallied response time, business disruptions, revenue loss and property destruction

By [Ellen Messmer](#), Network World  
July 26, 2010

A new study of 45 U.S. organizations found that cybercrime -- including Web attacks, malicious code and rogue insiders -- costs each one of them \$3.8 million per year, on average, and results in about one successful attack each week.

"First Annual Cost of Cyber Crime Study," conducted by Ponemon Institute and sponsored by ArcSight, entailed seven months of research and visits to each of the 45 organizations. The participating midsize and large organizations (from 500 to more than 105,000 employees) represent a mix of industries and government agencies. Researchers talked to IT security personnel, as well as network, [forensics](#) and management staff, to determine the costs of responding to and mitigating cybercrime attacks. The researchers spent about four weeks with each participating organization, according to Larry Ponemon, director of Ponemon Institute.

The \$3.8 million annual cybercrime tally represents an average; organizations reported from a low of \$1 million to a high of \$52 million per year, according to the study.

The \$3.8 million average cost represents not what companies or government might routinely spend each year on say, antivirus software, but the direct cost of coping with the attacks. In the event of a Web-based application attack, such as Web-based SQL injection, "say they bought a Web Application Firewall to respond to that, we'd amortize it," Ponemon says.

Types of cybercrime reported include: stealing intellectual property, confiscating [online bank accounts](#), distributing viruses and other malware, posting confidential business information on the Internet, and disrupting a company's infrastructure.

Researchers tallied the time spent responding to attacks, the disruption to business operations, revenue loss, and the destruction of property, plant and equipment. Sometimes cybercrime attacks came in fast waves against an organization, and financial institutions seem to be targets of the stealthiest types of cyberattacks, such as [botnets](#), Ponemon says.

Defense, energy and financial services companies experienced higher costs than organizations in retail, services and education, according to the report.

Ponemon says those organizations that had invested in defensive technologies, including security information event management, and had a chief information security officer on board, appeared to be better prepared to respond and took less time to remediate problems. But only about 40% could be considered to have invested in this way, he adds.

The study found it took 14 days on average to respond to a successful cyberattack, with an average cost to an organization of \$17,696 per day. Malicious insider attacks took up to 42 days or more to resolve.

While the number of companies involved in the study is only 45, and thus the data can't be considered statistically weighty enough to characterize entire industries, the "First Annual Cost of Cyber Crime Study" provides a look at how cybercrime is dragging down U.S.-based companies and government.

"The eye-popping thing we found is a lot of organizations are very disorganized in even understanding the environments they're dealing with," Ponemon says. Ponemon Institute intends to do further studies of this kind in the future, he adds.

## **Most Breaches Caused by Crime Gangs**

### **New Verizon Report Cites Organized Crime, Insiders Among Top Trends**

July 28, 2010 - Linda McGlasson

Organized crime was responsible for 85 percent of all stolen data in 2009. And stolen credentials were the most common way to gain unauthorized access into organizations.

These are among the headlines of the [2010 Verizon Data Breach Investigations Report](#), just released by Verizon Business.

Conducted for the first time in collaboration with the U.S. Secret Service, this year's report takes a broader look at the types and causes of data breaches. The USSS investigated 84 data breaches in 2009; Verizon investigated 57. Over the past six years, this annual report has reviewed over 900 data breaches, encompassing more than 900 million compromised records.

The latest report finds 2009's breaches of electronic records involved more insider threats, greater use of social engineering and the persistent, troubling trend of organized crime involvement. Of the 143 million records breached in 2009, 85 percent of them were attributed to financial service incidents. The one good piece of news: The overall number of breaches declined from those cited in [2008's report](#).

Wade Baker, director of risk intelligence at Verizon Business and primary author of the report, says working with the Secret Service and combing data sets "offers a wide angle lens look at the data breach, trends and new types of attacks." As in earlier reports, about two-thirds of the breaches in the report have not been disclosed or never will be.

Another key point made in the report: Most of the breaches were considered "avoidable" if only security basics had been followed. Verizon Business investigative experts found that only 4 percent of breaches required difficult and expensive protective measures.

## Inside the Numbers

Data breaches caused by insiders add up to 48 percent of all breaches investigated -- an increase of 26 percent over 2008. Conversely, breaches caused by external sources were down slightly to 70 percent, dropping from 2008's 79 percent.

Another change: 48 percent of the breaches occurred because of privilege misuse, up 26 percent over the previous report. Malware and hacking held top spots in earlier reports, Baker says.

In terms of industries impacted, financial services made up 33 percent of the cases investigated, followed by hospitality at 23 percent and retail at 15 percent.

Other key takeaways:

- 98 percent of the data breached came from servers;

- 61 percent of the breaches were discovered by a third party;

- 96 percent of the breaches were avoidable via simple or intermediate controls;

- 85 percent of the attacks weren't considered highly difficult;

- Nearly 80 percent of victims subject to the payment card industry data security standard were not compliant.

## Global Outlook

Looking at global trends, [Chris Novak](#), Verizon Business' managing principal of investigative response, says under-reporting of breaches is common outside the U.S.

"If people think the breach landscape is bad here, the outlook is worse in Europe, Middle East and Africa and Asian markets," he says. "Many of them have much more pervasive and long term breaches, and it is common to sweep them under the rug."

Around the globe, many of 2009's data breaches were driven by economic desperation. "A lot of people with great IT skills are out of work and go to the dark side because they have to live and pay bills," Novak says.

Novak's prediction: Sophistication of malware and "laser-type" attacks on high value targets will only increase. Likewise, he expects that organized crime involvement -- and the sophistication of their attacks -- will increase, and they will be more successful. "It is definitely not going to diminish," Novak says.

## Industry Response

Long embraced as an industry benchmark on data breach investigations, the Verizon report gets extra attention this year because of the collaboration between Verizon Business and the Secret Service.

"I like this combination and collaboration between Verizon Business and Secret Service on data breaches," says [Linda Foley](#), founder and chairman of the Identity Theft Resource Center. "This report is remarkable. It confirms what we saw in the breaches we monitor. It goes much deeper in analysis and provides a lot of insight into criminal behavior in terms of breaches, including insider (sometimes just written off as human error)."

Rick Kam, CEO of ID Experts, a data breach response provider, says the latest report mirrors his own group's finding -- particularly an increase in "hybrid attacks" where external organized cybercriminals work with insiders to implement an effective breach.

Kam adds that cyber criminals are using advanced data mining data techniques to create more complete identities. "They are stealing data from public and private data sources that contain both sensitive financial data,

as well as other identifiers like health insurance numbers, diagnosis, personal information from social websites like Facebook, to accomplish this." A cyber breach that looks benign may only be a piece of the identity puzzle organized cyber criminals are creating, he says.

### **Breach Prevention Tips**

Given that 96 percent of the breaches were considered avoidable by simple security controls, the Verizon Business experts recommend these fundamental measures for organizations to ensure protection:

**Back to the Basics** -- Make sure your firewalls and routers are configured securely. Set the essential controls, and check them regularly.

**Use Layered Security** -- For most organizations, the idea of security architecture resembles a piece of chocolate candy -- crunchy and hard on the outside, and soft and chewy on the inside. "Those soft, chewy centers make it easy for the hacker to move around and collect data undetected," Novak says. Think "jawbreaker" security instead of "chocolate cream crunch" security, he says.

**Monitor and Mine Event Logs** -- This is where a breach is uncovered. "Now the discovery of a breach is taking too long, and trends show on data breach timelines that the time to discovery isn't getting better," Novak says. **Watch Privileged Activity** -- Don't give out excessive rights to your own employees and contractors. "Most give people too many privileges than are needed," Baker says. "Go back to appropriate permissions, and monitor insiders, rather than just trust them," says Baker. One tell-tale sign of possible future insider abuse is that many insiders have a bad history of minor policy violations.

**Watch Outbound Traffic** --It's not just what's hitting your firewall from the outside that should concern you, but what's leaving the organization, too.

**Be Prepared to Respond** -- Novak compares a data breach incident response plan to a company's fire exit plan, "When the building is on fire, you don't start planning who the fire marshal is, or what the exit strategy is," he says. "You have to have those plans before the fire happens."

## **A Tale of Three Breach Reports**

July 30, 2010 - Linda McGlasson

This week a trio of reports came out on data breaches. Talk about information overload! I decided to take a look at these reports to compare commonalities and distinctions.

One of the best and most comprehensive of reports, the annual [Verizon Business Data Breach Investigations Report](#), slams home some really scary statistics for financial services, hospitality and other industries prone to data breaches. Its two top headlines: Organized crime was responsible for 85 percent of all stolen data in 2009. And stolen credentials were the most common way to gain unauthorized access into organizations.

“ **When boiled down to the basics, each of these reports says the same thing: Expect a data breach.** ”

Next, the first annual [Cost of Cyber Crime Study](#)" by the Ponemon Institute shows the enormous cost that data breaches have on victim organizations. This study doesn't look at types data breaches per se, but rather the costs. Web-borne attacks, malicious code and insiders are the most costly, making up more than 90 percent of all cybercrime costs per organization per year. An average web-based attack costs \$143,209; malicious code,

\$124,083; and malicious insiders, \$100,300. The report doesn't paint a rosy picture about the average length of time to resolve a data breach. An incident incurred by a malicious insider, for instance, takes an average of 42 days or more to resolve.

Then there is the aptly named report, [The Leaking Vault - Five Years of Data Breaches](#) from the Digital Forensics Association, which shows that of the 2,807 publicly disclosed data breaches worldwide over the past five years, the cost to the victims was \$139 billion. The sectors studied in this report were business, government, education and medical. These areas on average lost 395,000 individuals' data every day. Those numbers work out to every person in the United States having their data breached not once, but twice.

Here's what stands out when comparing the Verizon Business and Digital Forensics Association reports:

Both reports agree that outside "agents" or criminals cause more harm and data loss than insiders.

Digital Forensic Association's report says stolen or missing laptops were the leading cause of data breach incidents. Verizon Business' report says data stolen off of servers made up 96 percent of its breached data. I think Digital Forensic Association's analysis is studying a much larger number of incidents, so this may be why they're seeing laptops at the top. Their report does say that hacking accounts for 45 percent of all the records taken.

On the insider threat, Verizon's report shows that 90 percent of the insider cases were result of "deliberate and malicious" activity. The Digital Forensic Association's report says when an incident involved insiders, it was more than twice as likely to have been an "accident." These two data points are going in opposite directions, but most of the insider cases I'm aware of are malicious and deliberate.

One interesting point that Verizon's report makes about insiders: If you look at past history, most insiders were cited in the past, prior to their incidents, for other minor forms of misuse.

Verizon's report sees no evidence that the economic conditions are causing people to steal data. I will bet my house, though, that next year they'll find a trend pointing toward economic failures, foreclosures and the poor economic conditions here and abroad are making some folks turn to the dark side.

When boiled down to the basics, each of these reports says the same thing: Expect a data breach to happen to your organization. Don't be surprised when it does happen; be ready; and have an incident response plan in hand to mop up when the incident does occur.

## US Secret Service shows business how to fight cyberthreats

[Warwick Ashford](#)

Wednesday 28 July 2010

**Business needs to be more proactive in its approach to security in the face of increased insider threats and customised malware, says [Verizon Business](#).**

Both types of attack have increased in the past year, according to the 2010 Verizon Data Breach Investigations report in partnership with the US Secret Service.

This is the first time private and commercial data has been combined in a data breach report, said [Matthijs Van der Wel](#), head of the EMEA forensics team at Verizon Business.

The data from the financial crime investigations from the Secret Service has enabled a broader and deeper perspective on cybercrime, he said.

"Most breaches are caused by external sources, but we now see a lot more cases that involve insiders combined with social engineering that we did not see in our previous data set," said Van der Wel.

The data also highlights an increased use of customised malware in smaller attacks to avoid detection by anti-virus and intrusion detection software, he said.

"Detection is extremely difficult, especially when mixed with stolen credentials, which enable attackers to mimic legitimate traffic," said Van der Wel.

The report recommends a more proactive approach to security in which businesses actively monitor log files for anomalies.

A sudden increase in the size and volume log files is usually a good indication of malicious activity, according to Van der Wel.

In most cases, businesses have a small window of opportunity of about a day between the compromise and the theft of data, which should not be missed, he said.

Cases involving insiders show data theft is often preceded by a series of minor policy violations, the research shows.

Keeping track of minor policy violations is another way businesses can identify potentially malicious activities, said Van der Wel.

Businesses also need to move away from authentication methods that rely on usernames and passwords. Instead they should move to two and three-factor authentication, he said.

"The time for passwords is gone because they can be captured easily by password sniffers, no matter how long and complex they are," he said.

The breach report includes a list of recommendations for businesses to improve their information security and background information on how the cybercrime world works.

Key findings of the 2010 report:

Most data breaches (69%) caused by external sources

Many breaches (48%) involved privilege misuse

Nearly all data is breached from servers and online applications

Most breaches (85%) were not difficult to carry out

Most victims (87%) missed evidence of security breaches in their log files

Recommendations for enterprises:

Restrict and monitor privileged users

Watch for minor policy violations

Implement measures to stop the use of stolen credentials

Focus on the size and volume of log files

Share incident information with other organisations

## Search engine optimization techniques for hackers

At DefCon, Barracuda Labs will explain how malware pushers use search engine optimization techniques to push their poison to the top of those Google rankings.

By [Bill Brenner](#)

July 27, 2010 — [CSO](#) —

Any company that does business online knows the importance of mastering search engine optimization (SEO) techniques to get their content atop the Google rankings. It turns out [malware pushers care about SEO](#), too, and at [DefCon](#) later this week researchers will show just how big a deal it has become.

The full findings won't be released until mid-week, but CSO got a preview in an interview Friday with Paul Judge, chief research officer and VP of cloud services for Barracuda Networks, and Dave Maynor, research scientist with Barracuda Labs and CTO-cofounder Errata Security.

The findings are based on a five-month study in which Barracuda Labs observed and measured attackers' use of search engine results to host malware or redirect users to malicious sites. Data was collected several times a day and checked for malicious content across [Google](#), Yahoo!, Bing and Twitter.

"We realized that attackers are trying to get in front of as many eyes as possible. They take advantage of popular search terms and we wanted to see exactly what they're doing," Judge said. "We set the system crawlers to look at Google, Yahoo! and Twitter, figure out the popular search terms, then we searched for those pages and analyzed them in search of malicious content."

In total they reviewed 8,000 search terms and 5 million search results. Not surprisingly, Maynor said, "Google is pretty full of malware." In fact, 68 percent of the malware found was on Google. To Judge's surprise, only 1 percent of it was found on Twitter. Yahoo! Accounted for 18 percent of the malware found.

Like Microsoft in the first part of the last decade, Google is a major target these days because it accounts for so much online market share, Judge said. Though Twitter's growth has exploded in the last couple years, it isn't focused on search rankings as Google is.

The researchers also studied the times of day and days of the week where malicious activity was strongest. The period between 1 and 5 a.m. represented more than half the malware generated. Maynor said the working theory is that hackers in Europe are up and about at that time. Meanwhile, Mondays have turned out to be the busiest day of the week, accounting for about one third of malicious activity.

"People get back to their office on Monday and they don't feel like working yet, so they visit other sites and that's when they fall in the trap," Maynor said.

## Malware openly available in China, researchers say

### Developers sell subscription programs, upgrade services for hacking

By [Jaikumar Vijayan](#)

July 29, 2010

Computerworld - LAS VEGAS -- China's rapid emergence as a hotspot for criminal hacking activities is enabled by the open and unfettered availability of sophisticated hacking tools, according to security researchers attending the Black Hat conference here this week.

Many of the hacking tools are inexpensive, highly customizable, and easy to use.

Most of the early users of the malware products have sought to steal has been from from online gaming accounts inside China. But now experts are seeing much broader use of such tools.

Hackers in China are developing malicious software "almost like a commercial product", said Val Smith founder of Attack Research, a Los Alamos, N.M.-based security firm. The products come complete with version numbers, product advertising, end-user license agreements and 24-hour support services, he said.

They are "rapidly deploying very easy to use tools for cutting edge exploits," Smith said at a Black Hat presentation on Wednesday. "Their community is huge because [the malware] is easy to use," while at the same time many of the exploits are very advanced, he added.

Unlike in the U.S, the buying and selling of hacker tools in China takes place mostly in the open, said Anthony Lai, a security researcher with Valkyrie-X Security Research Group (VXRL) a Hong Kong based non-profit firm. Often, all that's required to find and purchase a malware program often is the ability to use a browser and search engine, he said during a talk at Black Hat.

Most of those selling malware products make little effort to conceal their activities. In fact, many openly advertise their wares and their capabilities through search engines like Baidu.com, he said. Customers can buy the malware they need for less than \$20 or sign up as subscribed members and get regular updated supplies of the tools, Lai said.

The hacking tools run the gamut and are often designed for off-the-shelf use. Many offer exploit generators that allow more sophisticated hackers to carefully customize malware for specific needs by using graphical user interfaces, Lai said. The GUIs let wannabe hackers specify what they want the program to do, for instance, whether they want it to steal data, capture screens, log keystrokes, remotely control a system or undertake any other task.

Some check boxes lets malware purchasers decide what kind of obfuscation and hiding methods they want to use to evade detection by security tools, while others walk them through the deployment and updating process, Lai said.

It's not unusual for those selling malware programs to let buyer's first test out the products before buying it and to offer regular product updates and phone numbers to call for support services. Statistical tools are also available to help buyers keep track of the systems they have infected.

China's hacking abilities has received increasing scrutiny following [Google's disclosure](#) earlier this year that it's servers had been hacked apparently by hackers based out of China.

# The quiet threat: Cyber spies are already in your systems

By Bob Violino

July 27, 2010

InfoWorld - Is your company's data under surveillance by foreign spybots looking for any competitive advantages or weaknesses they can exploit? This might sound farfetched, but such electronic espionage is real. It's an insidious security threat that's a lot more common than you probably realize.

As an IT or security executive, determining whether your organization is under attack via this seemingly undetectable threat -- and putting in place adequate technology and procedural safeguards -- should be a high priority. The stakes are too high to ignore the problem.

Security experts believe that [a growing number of companies are being spied upon electronically](#) by sources from other countries, [most notably China](#). What makes these attacks so troublesome is that their techniques are often undetectable by the usual security tools. Electronic spies try to get into systems without causing disruptions, so they can quietly gather information over a period of time.

These types of threats are much harder to deal with than untargeted attacks because they never become widespread enough for security vendors to observe reliably. As a result, security software and other tools that detect known attacks don't identify these threats. Also, an attack that's aimed at a particular target can be designed to get around whatever combination of defenses is in place. And the people who launch electronic spying attacks go to great lengths to prevent the targets from detecting the threat.

Although the problem is largely hidden, it is real and serious. In this special report, InfoWorld.com answers the key questions on who's spying, what they're looking for, and what you can do to protect yourself.

[How common is e-spying? Observers say electronic spying is becoming more common. Neil MacDonald, a vice president at research firm Gartner who covers computer security, maintains that as many as 75 percent of enterprises have been or are being infected with undetected, financially motivated, targeted attacks that evaded their traditional perimeter and host defenses.](#)

"Any government or commercial organization with sensitive information is being targeted," MacDonald says. The [highly publicized attack on Google's network](#), in which the company was a target of what it called a highly sophisticated and coordinated assault originating from China, was just the beginning. MacDonald says multiple Gartner clients have reported being attacked during the same timeframe via similar methods. InfoWorld's editors have learned of repeated attacks at major companies, described in several off-the-record conversations.

Others say it's hard to determine how widespread this type of activity is because the attacks are so difficult to identify and track.

"While we know it's a serious problem, the secrecy of these kinds of attacks makes it impossible to know how common they are," says Paul Kocher, the chief scientist at Cryptography Research, a security consultancy.

Spying organizations consider any effort that gets detected by the victim to be a massive failure, so the only information available relates to attacks that failed, Kocher says.

"Because the whole point is for the espionage to be stealthy, there is truly no way to know the size and scope of the issue," says Mark Lobel, advisory principal at PricewaterhouseCoopers. But don't let that quiet nature fool you, he adds: "In conversations with people in the industry, they are confident that it is a larger problem than most people recognize or understand."

[Who's doing the espionage? Even when electronic spying is detected, it's often impossible to know the real source of the attack. For example, if you trace an attack to an IP address in a given country, it's likely the machine is simply a compromised computer that's acting as a proxy or relay.](#)

[Today, most security vendors track threats such as viruses in a signature-based detection setup, looking for parts of known viruses. But for countries such as China that have the budget and expertise, it's not hard to exploit advanced code and other zero-day attacks that security vendors don't have on record to catch, says Brandon Gregg, a San Francisco-based corporate investigator who plans to teach a law-enforcement class on electronic espionage in the fall.](#)

Although China is often cited as a source of electronic spying, it's hardly the only place from which such attacks originate. "It's human nature that you need one entity you can blame. But from the data I've seen and from what I've heard it's a little more complex than that," says Nils Puhlmann, CSO at online game producer Zynga Game Network and co-founder of the Cloud Security Alliance. While Puhlmann wouldn't provide details, he indicates that electronic spies operate from multiple countries and are not necessarily state-sponsored.

Sites such as Hackerforum.com feature content about remote access tools that allow hackers to not only control a computer completely in a few steps, but to hear and see a user without the user knowing about it.

[How do the cyber spies infiltrate your systems? A typical targeted attack will exploit multiple weaknesses to achieve its ultimate goal: usually to steal information or compromise a specific account. A particular user in an organization might be targeted via a well-crafted, believable email \(a technique called "spearphishing"\) and might inadvertently help install spyware via his or her PC.](#)

Some attacks can originate by hackers gaining access to publicly available information and correlating it. While not every piece of information posted on the Internet is sensitive, when combined with other data on the Web as well as additional information posted by other companies, a pattern can begin to emerge.

"You are able to put together pieces of nonsensitive information to figure out or to deduce sensitive information," notes PricewaterhouseCoopers' Lobel.

Perhaps an attacker might exploit a security or configuration weakness of an externally accessible system or application, with the aim of gaining user credentials or establishing a surveillance point.

Attackers can also exploit publicly known or nonpublicly known technology vulnerabilities. And to access truly sensitive information, they can resort to tactics such as bribery.

During a targeted attack, more than one system or application-level vulnerability could be directly exploited. Once a single system or account is compromised, virtually the entire environment can be gradually traversed until the ultimate goal of the attack is achieved.

Often, the attackers place monitoring software in out-of-the-way locations and systems, such as log servers, where traditional IT security methods aren't looking for intrusions. They collect the data and send it out, such as via FTP, in small amounts over time, so they don't rise over the noise of normal traffic and call attention to themselves.

[Who are the data thieves targeting? If you think your company is not a likely target of electronic spying, don't be so sure. Although military systems and government contractors will always be major targets, services that carry information for many types of organizations are also extremely attractive because a single intrusion can provide information about a large range of targets, Kocher says. For example, Webmail services, telephone networks, shippers' databases, and social networking sites are all likely targets.](#)

[Any company with advanced intellectual property or sensitive research and development data is of interest to spies, notes Paul Kurtz, COO of Good Harbor Consulting and a recognized cyber security and homeland security expert who has served in senior positions on the White House's National Security and Homeland Security Councils.](#)

["Adversaries will look up the supply chain too in order to gain access to more sensitive data, so those organizations supporting sensitive government and private sector groups should also monitor for espionage activity," Kurtz says.](#)

[What risks do you face? What's at risk for your organization if it doesn't at least look into whether it's being spied upon electronically? Quite a bit.](#)

["It's the worst-case scenario at stake: the loss of competitive advantage," says PricewaterhouseCooper's Lobel. For instance, a government entity that's doing the spying could hand over intellectual property to one of your biggest competitors. This could allow the competitor to avoid the research and development cost and time that your company has spent, or tip them off to future products in your pipeline.](#)

Kurtz says private-sector firms have the most to lose today, as the federal government is doing little to help them and they are "hemorrhaging intellectual property, which will lead to loss in market share, investor confidence, and ultimately their ability to compete and survive as a company."

Organizations need to not only fear the loss of propriety information, but the public backlash from lost personal data as well. The 2007 [security breach suffered by retailer T.J. Maxx](#), in which data from millions of customer credit cards was stolen, "was a PR nightmare," says corporate investigator Gregg.

[What can you do to stop the cyber espionage? There's probably no way you can completely protect your organization against the increasingly sophisticated attacks by foreign and domestic spies. That's especially true if the attacks are coming from foreign governments, because nations have resources that most companies do not possess.](#)

But there are steps you can take to at least reduce the chances of an attack being successful or doing significant damage.

One strategy many experts agree on is to practice "defense in depth." By having multiple layers of defense, the failure of one layer does not have to result in a compromise. This strategy includes not only deploying some of the latest technology but also educating employees about the risk and showing them how they can help prevent spying incidents.

If resources allow, consider hiring people who specialize in uncovering and defending against the methods electronic spies use to get into networks.

Gartner's MacDonald recommends that companies get the basics right. For example, sharpen patch management discipline in both breadth and depth, establish and track configuration management standards, and train users about the threats from social engineering attacks.

Because most attacks come via email and the Web, it's a good idea to beef up your email and Web security gateway capabilities to next-generation protection platforms that provide multiple styles of protection, including URL and Web reputation services.

Also, move from antivirus and antispymware to [endpoint protection platforms](#) that provide multiple styles of protection (such as antivirus, antispam, firewalls, and host-based intrusion prevention systems) in an integrated framework and management console.

"Assume you will be compromised," MacDonald says. "Beef up your detection capabilities by performing detailed monitoring of system, network, application, and data transactions looking for behavior that falls outside normal parameters." Most security event and information management ([SEIM](#)) products are adding these types of capabilities.

Cryptography Research's Kocher says the most reliable defense is to run small, physically isolated networks. As networks grow, the likelihood of a malicious attack increases. "In my company, we manage a completely offline network with separate PCs, network cabling, and printers," he says. Employees have laptops for email and Web browsing, but these don't carry highly sensitive data. The systems with critical data have no Internet access whatsoever.

While it's expensive and cumbersome to duplicate hardware and eliminate connectivity with the outside, it's the only way the company can be confident that its data stays where it should, Kocher notes.

New and more powerful security tools, such as network forensic products, are emerging to help defend against electronic spying threats. For example, [NetWitness Investigator](#) is an interactive threat analysis application that can perform free-form contextual analysis of raw network data.

These tools don't look for actual malicious code, but rather patterns of network traffic that resemble that of hackers lurking in your network and taking data, says corporate investigator Gregg. Once Social Security

numbers, credit cards, or other file types are seen moving out of your network, alarms not only warn the user but help identify and track where the data is going.

If your company has the resources and the expertise, consider developing your own specialized tools to help thwart attacks. Some experts believe this will become more common as companies find that off-the-shelf software doesn't account for their specific information, information movement, and other needs, nor the often custom-tailored threats against them. In other words, because the threats are often custom-made to get specific information from a specific company, your defenses may need to be customized as well.

Ignorance is not at all bliss Unfortunately, most companies remain blissfully ignorant of the problem of electronic surveillance, says Gartner's MacDonald, taking false comfort in antivirus software and network scans that continue to show zero infections. They'll remain blissfully ignorant until they stumble upon the fact that they've been compromised and that it's been going on for months.

"Denial works until it doesn't," he says.

## **Beware Phishing via Fax**

### **IRS, Anti-Phishing Group Team up to Fight Fraud Trend**

July 29, 2010 - Linda McGlasson

Imagine a small business owner receiving a fax, purportedly from the Internal Revenue Service, saying the business owes back taxes. Not wanting to tangle with the IRS, the owner fills out the appropriate financial information requested and faxes it back to the number provided.

Unfortunately, this individual has just fallen for a classic offline [phishing attack](#) -- "fax phishing."

Traditional phishing happens exclusively via the Internet with emails and attachments, but offline phishing involves sending direct faxes to consumers or businesses. A growing public threat, fax phishing is a reaction to improved spam filters, and a result of free IP fax services, says phishing researcher Markus Jakobsson.

"The IRS component though is an old one," Jakobsson says. "It seems to work. You do not mess with the IRS; you do what they say. And if they say you have a refund coming, everybody wants to believe that is so."

To help educate consumers and businesses about these offline attacks, the [Anti Phishing Working Group](#) has stepped in to create a new consumer fax education initiative in conjunction with the IRS.

The average loss incurred in offline phishing scams range from a few thousand to tens of thousands of dollars -- "Losses that victims don't realize they have sustained until long after the crime is complete," says Peter Cassidy, secretary general at the APWG. The new education program called "Fax Back Phishing" provides telecommunications companies and Fax over Internet Protocol (FoIP) hosting firms with links to educational sites to educate consumers and businesses the moment they are scammed.

The IRS's Online Fraud Detection and Prevention (OFDP) group, under the Office of Privacy Information Protection & Data Security, has been tracking and disabling offline phishing incidents since early 2009. The OFDP identifies fax numbers from complaints sent to its phishing alert address. Before OFDP became involved in offline phishing, these numbers would remain active for months, Cassidy says. Now the group works with

telecommunications providers and is able to take down the majority of these fax numbers within 12 hours. This response greatly reduces the potential window of opportunity for phishers to harvest credentials. Approximately 250 numbers have been disabled in under 18 months.

The IRS turned to the APWG to help with the development of a response utility to advise consumers who've fallen victim to offline phishing scams. A fax coversheet with APWG's education resources site is now faxed to victims when the fax number is discovered. The FTC Sentinel, a consumer complaint database owned by the Federal Trade Commission, also gets the victim's information for further law enforcement investigation and takedown of other phishing operations.

The cooperation between the IRS and APWG is encouraging, says Laura Mather, Ph.D., co-chair of APWG's Internet Policy Committee. "The phishers continue to find compelling mechanisms for contacting consumers and having the IRS work with us to create a program for protecting people who have been contacted by this type of scam shows that the crime fighters cooperate as well as the criminals," she says.

A social engineering expert says people are all used to fax-based spam. "But phishing via this medium is a newer trend," says Rohyt Belani, CEO of Intrepidus, a social engineering training vendor. He says that the work required to respond by the recipient makes the traditional online phishing attack a much more dangerous threat.

Jakobsson agrees with Belani's view, adding, "In my view, it is an attack that is not going to have a huge impact: there simply is not a huge number of consumers who have faxes, so that leaves corporate fax numbers."

Jakobsson believes that SMS-based phishing, also known as [smishing](#), or text phishing, "is going to grow much faster than fax-based."

Even so, education of consumers and businesses is key to beating the phishers, says Belani. "People need to be educated that their banks, the IRS, or anyone else will never ask them to provide sensitive/confidential information via electronic means."

## Should IG Reports be Treated as Gospel?

July 26, 2010 - Eric Chabrow

John Gilligan doesn't think that inspector general audits of agencies' IT security should be treated as gospel. The flaws they identify may be factual, he says, but they're not always put in the perspective of the agencies' overall approach to cybersecurity.

Gilligan is the former chief information officer of the Air Force and Energy departments, and for the past couple of years been the major force in getting government agencies to adopt the [Consensus Audit Guidelines](#), 20 key automated controls that when implemented could go a long way in securing agencies' IT systems.

His basic gripe about the IG information security audit is that it's not placed in context. In a conversation I had with Gilligan late last week, here's what he said about the process:

"The whole IG review process is one that has not really provided a lot of value because the IGs come in without criteria, and all they do is that they have to find potential problems. So, the agency says, 'It doesn't matter what I do; the IG is going to find some problems.' But the Consensus Audit Guidelines says, wait a minute, you can define a subset and focus on them (steps to secure IT), and here are the criteria, here's how you evaluate how you're going to be successful. The IG may say this other stuff, but the response could be, 'Yes, I'm focused on the most important things.'"

Gilligan doesn't contend the IG audits are valueless. If anything he says, some agencies IGs do a better job than others in identifying problems with IT security. "I don't cast all of them with the same brush," he says, adding:

"But I think that a lack of objective criteria to some extent is a lack of experience in many of the IG shops and that serves to create a situation where even well-performing organizations can find that their IG gives them a poor report. On the other hand, sometimes you can find there's an organization that is not really doing so well gets a good IG report, not because there's an objective evolution against consistent criteria, just this particular IG organization perhaps is not as experienced or not as focused."

Gilligan says government IGs as a group need to provide better IT security training to government auditors and develop consistent criteria in evaluating the security of IT systems because many constituencies, including Congress, give significant weight to their findings:

"They're looking for independent corroboration; it's an important part of our governing system. But right now I don't think it's often adding the value it could if we mature it a bit more."