Computers & Security (2005) **24**, 1–9

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Security views

Malware update

The Funner worm, one that targets Microsoft's MSN Messenger Instant Messenger, surfaced recently. It propagates by sending a copy of itself in the form of a file named "funny.exe" to every MSN Messenger contact it discovers. The worm changes the Registry in the Windows systems it infects and overwrites entries in the host's file that is used to uniquely associate each IP address with the name of a host. One reason that this somewhat destructive worm has not spread more extensively may be that it infects only a few types of Windows systems, of which Windows XP is the most vulnerable.

Another variant of the Mydoom worm started spreading on the Internet shortly after members of the black hat community announced a security-related vulnerability in the Windows Internet Explorer (IE). The flaw is in the way IE handles some attributes in the <IFRAME> and <FRAME> HTML elements. IE will process a malicious HTML document with excessively long strings in the SRC and NAME attributes of the previously mentioned elements; the excess input can overflow the buffer, resulting in execution of unauthorized code. This new MyDoom variant infects systems in which IE users click on a Web link within the body of an email message, resulting in a redirected connection to another Web site containing the malicious HTML document. Some of the email messages sent by this worm purport to be sent by eBay's on-line payment system, PayPal. Users are informed that their account has just been debited and that they need to click on an indicated link if they want to see the details of the transaction.

Yet another mutation of the Bagle worm, Bagle.AT, is also infecting Windows systems on the Internet. It reads email addresses from the Microsoft Outlook address book in systems that it infects and then sends copies of itself to the addresses that it finds. Additionally, it tries to disable security-related programs such as anti-virus software. Bagle.AT infects systems when users open the attachment that this worm sends; the worm writes itself into the system folder and then activates TCP port 81 to allow perpetrators remote back door access to the infected system.

A new worm, the Famus-F worm, appears to be a videogram by Osama bin Laden. This Windows-targeting worm sends itself in bi-lingual (Spanish and English) email messages that purport to include video clips of Osama bin Laden and contain a subject line that reads "More terrorism this year." The message itself reads as follows: "Last speech from Bin Laden. Please forwards this video to everybody". It also contains a password. If users of vulnerable Windows systems open the attachment, Famus-F creates numerous files and reads address books in the infected systems to find addresses to which to send itself. Famus-F has not been spreading nearly as fast as other worms such as MyDoom and Bagle.

The new Zafi.C worm differs from most other current worms in that it is intended to cause denial of service. This Windows-targeting worm creates a mail engine to transmit itself to addresses it reads on victim systems then sends a flood of mail to three sites, Microsoft.com, Google.com, and the site of the Hungarian Prime Minister.

Another worm that targets Windows systems, W32/Myfip, sends messages that appear to originate from eBay. The message text states that eBay is engaged in a market research effort and that if recipients agree to provide information, they could win a prize. Opening the attachment that arrives with each message causes the system to become infected. Myfip packs itself in an unusual manner, making it difficult to detect.

0167-4048/$ - see front matter.
doi:10.1016/j.cose.2004.12.001

A new version of the Sober worm recently surfaced. This Windows-targeting worm arrives in email attachments which if opened result in the system becoming infected. When this worm infects a system, it writes two copies of itself into the system and then creates a mail engine to send itself to email addresses that it gleans from address books in the infected computer.

Almost every worm that has been identified lately is programmed to infect Windows systems. With a few exceptions, most of these worms work in a very similar manner—they try to get Window users to open an attachment or to click on a Web link. There is thus nothing particularly original about most of these worms, nor are any of them nearly as successful as worms of the past, such as the MSBlaster worm. This makes me wonder why computer criminals even bother writing new variants of previously identified worms as well as a few more-or-less original, but uninteresting worms. One would think that they would find something "better" to do. The good news, at least, is that these worms are not very successful, in part due to bold initiatives by ISPs such as AOL, which now provides free anti-virus protection to their customers, as well as the increased use of anti-virus software by organizations.

Update in the war against cybercrime

Daniel Baas was sentenced to two and a half years of imprisonment after he pleaded guilty to breaking into computers without authorization. The computers were owned by law and business firms; Baas' intention was to obtain copies of legal documents, financial information and other types of information. Baas was also convicted of gaining unauthorized access to a computer owned by Acxiom Corporation and is awaiting sentencing for that crime.

John Denison, a New Zealand Health Ministry employee, has received a sentence of three years in prison for gaining unauthorized access to the Ministry's banking system and transferring the equivalent of over USD 2 million to his own account. Although most details of Denison's actions have been withheld, the fact that he created phony documents to help cover his actions is widely known.

The Cyber Terror Response Center of South Korea's National Police Agency has taken into custody a person who may have gained unauthorized access to over 1000 computers in less than a year. The accused man's last name is Lee and he allegedly worked at an information security company in the past; other details about his identity are still unknown. The motive for the criminal activity may have been profit; the accused may have sold the information he gleaned from the systems he accessed.

Four Eastern Europeans have been charged with phishing in London. According to the UK's National Hi-Tech Crime Unit (NHTCU), this is the first case in the UK in which individuals have faced phishing charges. The accused, who allegedly swindled financial institutions out of large sums of money, have already had a hearing and are awaiting trial.

Boston police have arrested Andrew Schwarmkoff, an alleged phishing scam perpetrator. He has been charged with fraud, identity theft, receiving stolen goods, and larceny. The accused is believed to be a Russian crime ring member; he has been denied bail.

Fifty-three people in four northern Brazilian states, one-third of whom have in the past been arrested for computer crime-related charges, were recently arrested on charges that they perpetrated phishing schemes. They may have bilked people out of as much as USD 30 million.

Hong Kong law enforcement officials have arrested 12 people on phishing charges. They allegedly engaged in a phishing scheme in Hong Kong in which people were reportedly swindled out of HKD 600,000. Six of the accused face theft charges that could result in sentences of up to 10 years of imprisonment if they are found guilty.

An Australian judge recently sentenced Nick Marinellis, an Internet scam artist, to a minimum of four years of imprisonment for his role as mastermind in a Nigerian 419-type scam. Marinellis may have swindled his victims of as much as AUD 5 million. He will not be eligible for parole until early in 2008.

DC Enterprises and its owner William Carson have reached a settlement with the state of Massachusetts in a case in which they were accused of violating the CAN-SPAM Act as well as the Massachusetts Consumer Protection Act. They sent unsolicited advertisement messages that did not provide suitable opt-out methods. Carson and his company will pay a fine of USD 25,000 and have agreed to quit violating the CAN-SPAM Act and the previously mentioned Massachusetts law. This is the first case in which a violation of the CAN-SPAM Act was tried in Massachusetts.

Three alleged spammers from North Carolina are on trial in Virginia for allegedly using bogus sender identities in millions of spam messages sent to AOL users. If convicted of the charges, they could receive up to 15 years of imprisonment.

Siblings Jessica DeGroot and Jeremy Jaynes have been convicted of sending massive amounts of spam messages to AOL customers via AOL's servers located in Virginia. Virginia has what is widely recognized as the strongest anti-spam legislation of any state in the US; Jaynes faces a possible sentence of nine years in prison, and DeGroot faces a fine of USD 7500. Richard Rutkowski, a third person accused of the same charges, was found not guilty.

A judge has issued a restraining order against Stanford Wallace, an alleged spammer, and the companies he owns at a recent hearing. Wallace, who is sometimes called the "Spam King," has been ordered to disable spam-generating software.

Operation Firewall, an undercover operation run by the US Secret Service, but also involving international law enforcement such as the Royal Canadian Mounted Police (RCMP), Europol, and the UK's NHTCU, resulted in the arrest of 28 people from eight states in the US. These individuals were allegedly involved in identity theft activity. The accused face charges of identity theft, computer fraud, conspiracy, and credit card fraud; they may have stolen and misused a total of 1.7 million or more credit card numbers, reportedly resulting in a loss of more than USD 4.3 million. Several groups of individuals targeted in Operation Firewall allegedly ran Web sites used to distribute fake credit card numbers and bogus information as well as advice on how to commit fraud. The pilfered information and tools used to commit the crimes were reportedly sold on these sites.

A federal grand jury has indicted former University of Texas graduate student Christopher Phillips on the grounds that he gained unauthorized access to the university's computer systems and gleaned personal information of more than 37,000 faculty, staff and students. Phillips's defense was based on the arguments that he did not intend to commit a crime, that he did not use hacking programs, and that he saw no warnings against unauthorized access to the university's computers.

US law enforcement officials have arrested William Genovese for allegedly unlawfully distributing trade secrets. He is accused of selling Microsoft Windows NT 4.0 and 2000 source code. If convicted, Genovese faces a prison term of up to 10 years and a maximum fine of USD 250,000. He has stated that Microsoft has singled him out because it has not been able to find the real perpetrators.

The Tokyo District Court has handed down suspended jail sentences to two men accused of pilfering personal information of customers of Softbank, an Internet service provider (ISP). These men reportedly gave the information they obtained to four other individuals who then allegedly attempted to blackmail this ISP by threatening to publish the information unless Softbank paid them a large sum of money (reportedly between JPY 1 and 2 billion).

Oxford University students Patrick Foster and Roger Waite are appealing a suspension ruling handed down to them by Oxford's Court of Summary Jurisdiction after they were found to have accessed the university's computer system without authorization, among other charges. Using a program they said was easy to download from Google, the two allegedly infiltrated the university's computer systems to view live closed-circuit material and access information concerning students' computer use without being authorized to do so. Their intrusions were meant to expose security lapses in Oxford's network so that they could publish what they found in the university newspaper. At the hearing, Foster, a second-year politics, philosophy, and economics student, admitted to all seven charges against him—two for using university facilities for unlawful activity, two for gaining unauthorized access, two for violating users' privacy, and one for wasting staff time by engaging them in activity unrelated to academics. Waite, a second-year history student, pleaded guilty to four charges—conspiring to breach the network, using facilities to engage in unlawful activity, gaining unauthorized access, and wasting staff time.

More encouraging news has emerged in the war against computer crime. Something to note regarding the above news items is that although a number of the arrests and convictions that were covered occurred in the US and the UK, many occurred elsewhere. Significant stories involving New Zealand, South Korea, Brazil, Australia (which has developed an excellent reputation for dealing with computer crime) and Japan were also in the news. Additionally, Operation Firewall could not have been the success that it was without considerable international cooperation. As I have said so many times before, computer crime is an international problem. Success in fighting this type of crime depends upon elimination of "weak links," countries that have weak computer crime legislation or none at all, and also upon international cooperation of law enforcement.

Microsoft submits revised anti-spam standard

Microsoft recently revised its Sender ID protocol in an attempt to make it work better with an existing

standard and narrowed the scope of its patent application to ensure that it does not overlap with other proposals. Microsoft's Sender ID is one of several proposals that would allow AOL and other ISPs to assure that a message from a sender address actually comes from mail servers within the indicated domain name. Messages that do not pass this check can be safely rejected as spam. Last May Microsoft combined its Sender ID proposal with another developed by Meng Wong and submitted them to the Internet Engineering Task Force (IETF) for approval. But several major industry representatives said they would not use the standard because Microsoft holds patents on the underlying technology, even though this software giant said it would not charge for using this technology. Microsoft said patents were needed to guard it from frivolous litigation. Sender ID and Wong's Sender Policy Framework proposal specify different methods for verifying the origin of email messages. SPF checks the ''bounce'' address provided to return undeliverable mail, whereas Sender ID examines another address buried deeper within technical routing records. Combining the two methodologies provides what is likely to prove a very effective way to combat phishing and spoofing. Microsoft said that it has resubmitted Sender ID to the IETF for approval. Meanwhile, AOL said that it will begin testing the Sender ID protocol again after it had previously rejected it.

When the Sender ID protocol was first proposed, there was relatively little enthusiasm for a variety of reasons. Many individuals did not see the need for such a protocol; another was widespread distrust of Microsoft. Now the spam problem is out of control to the degree that I predict that many, including the IETF, will start warming up to Microsoft's revised Sender ID protocol. Being able to reasonably determine whether a message actually comes from its indicated source is, after all, an excellent basis for determining whether to accept or reject messages that are sent.

Microsoft will deliver beta version of RMS Service Pack 1 soon

Microsoft will be delivering a beta version of its Windows Rights Management Services (RMS) Service Pack 1 (SP1) in the first half of 2005, and has started a partner validation program for its Internet Security and Acceleration (ISA) Server 2004 to assure customers of the interoperability of third-party products used in connection with ISA Server 2004. The RMS SP adds improved authentication via smart cards and the ability to be deployed without an Internet connection. The validation program is being run in conjunction with VeriTest testing services and caters to the propensity of Europeans to use more hardware security products than North American users.

If this new SP for RMS works as advertised, it should be extremely valuable from an information security perspective. Password-based authentication is a thing of the past, something that organizations and individuals should have abandoned a long time ago. Smart cards and other forms of third-party authentication are a much better alternative; the fact that the RMS SP adds the ability to authenticate using smart cards is thus an extremely valuable new feature of the SP. At the same time, however, after all the problems with previous Microsoft SPs such as Windows XP SP2, I shudder to think of all the things that will be wrong with this new SP by the time the final version is released.

Microsoft relaxes policy concerning advance notice of patches

Microsoft is now publishing on its Web site a summary of planned security bulletins three days before they are released in their entirety. The summary includes information on which products are affected by updates and severity ratings for security problems. This company normally releases security bulletins on the second Tuesday of each month. It previously offered advanced notifications to customers who signed up through support personnel, but the information was not available to all customers. With the security guidance, companies can get their IT staff ready for the update release day and should be able to prioritize their activities according to how critical the updates are. The bulletins will be available at http://www.microsoft.com/technet/security/default.mspx.

I am heartened to see that Microsoft has changed its policy concerning security patches that are soon going to be released. Sending advance information to some of its customers but not others deprived those who did not want to get entangled with Microsoft support people to obtain this information from being able to make reasonable judgments concerning each patch by the time the patch was released—something that was blatantly unfair. Now everyone should have an equal opportunity, which is increasingly necessary given the reality of ''zero-day exploits.'' Hopefully, Microsoft's change in stance will also influence other vendors who, like Microsoft did until recently, have unreasonable policies concerning the distribution of information regarding security patches.

AOL offers software that boosts security

America Online (AOL) has released a special edition of its Internet access software called ''AOL 9.0 Security Edition''. This release, which includes a wide range of features to defend against computer viruses, spyware, and spam, is the first version of AOL software to focus specifically on security. It is available as a free upgrade for existing AOL members in the US. Along with improved editions of parental controls and browser pop-up blockers that come with basic membership, AOL has AOL 9.0 Security Edition added McAfee VirusScan anti-virus protection, simplified spam controls, and instant-messaging spam protection. Other features in AOL 9.0 Security Edition include Money Alerts, a service that notifies consumers of unauthorized bank account or credit card activity and McAfee Personal Firewall Express. AOL's existing spyware protection has been enhanced with a SpyZapper feature that targets the most disruptive forms of spyware. Rather than expecting home users to purchase and install a number of packages, AOL has bundled basic protection against various threats into an easy-to-use package. Certain elements of this package, such as a free personal firewall and basic anti-virus protection, are already standard to its members in the US. The components of AOL's access package vary by geography and are being introduced at different times. Versions of the AOL 9.0 Security Edition for other countries may come later.

Although AOL is a huge ISP, AOL is not all that popular in the circle of professionals with whom I associate. The reason that I repeatedly hear is that AOL does not offer sufficient functionality. Although it is true that other ISPs often allow users to access and run more services than AOL does, I keep thinking that AOL's limited services are the result of this ISP's superior level of understanding of and commitment to information security. After all, the fewer services that are run, the safer the environment. Now AOL is offering a wide range of free features designed to make home computers more secure and spam-free. AOL deserves to be recognized as a leader among ISPs; if all ISPs approached security as AOL does, the Internet would be a much safer place.

Study shows home computer users are ignorant about security

According to a recent joint study by AOL and the National Cyber Security Alliance, most consumers (66 percent) think they are safe from on-line security threats, but their computers lack basic safeguards against worms, viruses, spyware, remote attackers, and other Internet security threats. The survey revealed a wide gap between users' perceptions and the prevalence of actual security-related threats on the Internet that causes many home computer users to neglect security countermeasures such as anti-virus software and personal firewalls, and could pose a threat to the integrity of sensitive personal and financial data, which survey respondents said they were increasingly using their computer to store and manage. In the study technical staff examined 329 home computers connected to the Internet with either broadband or dial-up connections over two months. Participants were interviewed about their awareness of on-line security threats. After the interviews, technicians examined the firewall and anti-virus settings on participants' computers and looked for worm and virus infections as well as for spyware and adware. More than 70 percent falsely believed they were safe from worms, viruses and on-line threats, even though almost 20 percent had systems that were currently infected by a worm or virus. Sixty-three percent acknowledged having such infections in the past. The spyware/adware problem was even more common and overlooked. Spyware or adware programs were found on 80 percent of the computers analyzed in the study, with an average of 93 pieces of spyware or adware on the infected machines. About 90 percent of those whose computers were infected with spyware did not know about the infections and were not even aware what spyware programs are. In addition to finding widespread ignorance about computer threats, the AOL technicians found poor security on many of the systems they inspected. While 85 percent of people who were interviewed had installed anti-virus software on their computer, 67 percent of those surveyed lacked up-to-date anti-virus signatures that could stop the latest malware threats. About 67 percent of users also failed to run personal firewall software. Confusion about the purpose and necessity of security programs may be a large part of the problem. Most users said they did not understand what a firewall is or how it works, and 58 percent could not even explain the difference between a firewall and anti-virus software. Users surveyed were also generally confused or unaware of the symptoms of infections by spyware and other types of undesirable code. For example, 63 percent of those with pop-up blocking software said pop-up messages still appear on their displays. Approximately 40 percent reported that their Web browser's home page or search results had been changed

without their permissions all perfect symptoms of the presence of spyware or worm or virus infections.

I found the results of this study to be both fascinating and entirely believable. How can home users defend their systems against Internet security threats when they do not even know what these threats are and what consequences they can cause? Why would someone want to install a personal firewall on a home computer when the person does not understand what the personal firewall does? These results strongly reinforce the need for security awareness and training, not just for employees of large corporations, academic institutions, and government agencies, but also for home users. We now need to change our mode of operation from assessing the problem with home users to doing something about it. Unfortunately, those involved in public awareness efforts know more than anyone that the problem will not be easy to solve, but a good first step would be for countries to pass legislation that allocates money to develop strategies for dealing with the problem.

E-voting in recent US election gets mixed reviews

E-voting got its first major test in the recent US elections. Many felt that e-voting technology worked according to expectations, whereas others such as voter and activist groups reported significant problems, such as machines failing to boot or freezing while in use. Some voters using touchscreen systems said the machines refused to accept their votes for particular candidates or failed to offer complete ballots that included candidates in local races. Other problems included voting machines that failed to start, forcing polling places to turn voters away, and machines displaying summary screens showing different vote tallies from the ones that were actually cast. One Ohio precinct in which only 638 ballots were cast, reported 4258 votes for President Bush. Officials who found the error said Bush actually got 365 votes to John Kerry's 260. Dr. Aviel Rubin, computer science professor at Johns Hopkins University and a strong critic of e-voting, co-authored a 2003 report detailing security vulnerabilities in one version of Diebold Election Systems' voting machine software. Rubin supports having the machines create paper records to allow voters to verify their votes before leaving. Polling places could also use the records if a manual recount is needed. Currently, only Nevada requires a paper trail on touchscreen machines; but that may soon change, given the problems in the recent elections.

In a study conducted by doctoral students and faculty from the University of California—Berkeley's sociology department, the researchers claim to have discovered statistical irregularities associated with the electronic voting machines used in three Florida counties that may have given President Bush 130,000 or more votes than the actual tally. According to the study, counties with electronic voting machines were significantly more likely to show increases in support for Bush between 2000 and 2004 compared to counties with paper ballots or optical scan equipment. This change cannot be explained by differences between counties in income, number of voters, change in voter turnout, or size of the Hispanic population. In Broward County, for example, Bush received about 72,000 excess votes, a result not attributable to chance. The other two counties experiencing unexplained statistical discrepancies in the vote were Miami-Dade and Palm Beach counties. The three counties revealed the most significant irregularities and were the most heavily Democratic counties in the state. Smaller counties in which there was strong support for Bush did not produce any statistical anomalies. The study used a widely accepted method known as multiple regression analysis, a widely used statistical method in the social and physical sciences to distinguish the individual effects of many variables, which in this case included number of voters, median income, Hispanic population, change in voter turnout over the last four years, support for President Bush in the 2000 election, and support for Republican candidate Robert Dole in 1996. Electronic voting results in Ohio, a state that Bush also won, were also studied, but no anomalies were found there. A spokesman for the research team stated that embedded software flaws or hardware problems could have caused the irregularities.

I have discussed e-voting extensive in previous issues, so I will not belabor the point here. I will just say that e-voting provides an almost too ideal opportunity for unscrupulous individuals to throw off the results of elections. I strongly agree with Dr. Rubin—paper trails are the only reasonable way of validating the results of elections. I cannot understand why so many states in the US oppose paper trails. Election fraud does happen—consider, for example, what just occurred in the elections in the Ukraine. What happened there could happen in any free country. To the rest of the world's credit, countries other than the US have been much more cautious about proceeding ''full steam ahead'' with e-voting.

BSA keeps pressure on organizations with illegal software

During last months of last year, the Business Software Alliance (BSA) has doubled (from UKP 10,000 to UKP 20,000) the reward for individuals who report the use of illegal software within organizations in the UK. The use of illegal software in the UK, regardless of whether it is deliberate or accidental, is soaring. According to a 2004 IDC survey of 2180 workers in the UK, 29 percent of software used in the UK is illegal. The availability of software on-line and the rapid growth in spam-selling software have made purchasing or downloading illegal software much easier than ever before. At the same time, identifying illegal software usage has become more difficult than ever. Research performed for the BSA found that 47 percent of UK workers said they would be bothered if they knew illegal software was being used where they worked. When queried why the use of illegal software would bother them, 57 percent said that they believed illegal software use indicated poor company governance practices. Twenty-one percent reported that they were worried about being found personally guilty of illegal use of software. The BSA provides free software auditing tools, tips, and advice to assist companies in complying with copyright laws and implementing effective software asset management (SAM). This organization also provides software licensing and software management guides, free software auditing tools, and a list of SAM providers. Anonymous reports of illegal software usage can be recorded at http://www.bsa.org/uk/report.

The BSA has also been very active in the US. This organization has, for example, collected $2.2 million in out-of-court settlements in its yearly software piracy sweep in the US. The BSA asserts that 22 percent of all commercial software used in the US have not been purchased, costing the software industry more than USD 6.5 billion in lost revenue every year. The BSA's latest piracy sweep led to settlements with 25 companies; the proceeds were used to fund educational initiatives, such as its campaign to discourage young people from using peer-to-peer networks to swap software, games, music, and other copyrighted material.

Although the illegal software problem is rampant in the UK and US, it is even worse in other countries. While in one unnamed country a few years ago, I could hardly walk a block in this country's capital city without being offered the opportunity to buy cheap copies of a variety of Microsoft software. It is of little wonder, then, that companies such as Microsoft are doing everything they can do to prevent illegal copying of software. Lamentably, information security professionals too often turn their heads when cases of illegal software usage within the workplace surface unless an organization has a very well-defined policy against the use of software accompanied by prescribed punishments for the violation of the policy. The BSA is doing the best it can to combat the illegal software problem, but I fear it is making only a small splash in what has proven to be a very large pond.

Intrusions occur at UC—Berkeley and Purdue University

The names, home addresses and phone numbers, social security numbers, and dates of birth of 1.4 million Californians who provided or received care under California's In-Home Supportive Services program since 2001 were compromised when a UC-Berkeley research computer system that held these data was broken into. The data were given to University researchers under a special confidentiality agreement with the state's Health and Human Services Agency. This agency recommends that all people who were involved in the program since 2001 contact major credit reporting agencies to have a fraud alert placed in their credit profiles and also to start monitoring credit reports for possible indications of identity theft. The intrusion may be the largest public disclosure so far under California's law (SB1386) that requires companies and state agencies to inform Californians of any security-related incident in which certain types of personal data may have been compromised. In cases involving over 500,000 people, the organization can inform potential victims by putting appropriate postings on a Web site and also by reporting the compromise to the media. The incident has prompted the agency to review agreements it has made with researchers and to think of ways to confirm that security safeguards have been put in place. In an unrelated incident, an intrusion into several of Purdue University's computers was recently detected. University administrators reacted by urging all faculty, students, and staff to change their passwords. Purdue staff has not yet been able to determine whether personal information was stolen, downloaded, or changed; computer users were urged to watch for signs that their personal data might have been stolen.

A reporter with whom I talked several weeks ago told me that intrusions into computing systems have become so commonplace that they are not interesting any more. The UC—Berkeley break-ins

are a huge exception. A unconfirmed report indicates that the administrator of the system that stored the personal data was aware that the system was wide open to attacker and wanted tighter controls placed on the system, something that the lead researcher opposed. University administrators reportedly ruled in favor of the researcher; not long afterwards, the catastrophic intrusion occurred. I am not really sure who is most at fault in this case, the researcher who reportedly opposed something he did not understand, University officials who reportedly quickly dismissed the concerns of the system administrator, or the California state agency that so naively supplied personal data to the researcher. The only consolation is that potential victims of identity theft received some warning, even though it was very general. Hopefully, this incident will motivate California lawmakers to go well beyond the provisions of SB 1386 by passing a bill that requires adequate protection of personal and other types of sensitive data.

H + BEDV Datentechnik—Secure Point partnership is terminated: Jaschan is the issue

German anti-virus software vendor H+BEDV Datentechnik ended its partnership with firewall company SecurePoint because SecurePoint hired Sven Jaschan, the alleged author of many worms and viruses, including the Sasser worm. H+BEDV Datentechnik had planned on integrating its anti-virus software into SecurePoint's firewall. Jaschan was hired by SecurePoint last year shortly after he (who is awaiting sentencing) was released on bail after he admitted that he created the Sasser worm. H+BEDV Datentechnik became concerned that a malware writer was an employee of SecurePoint and ended the relationship between the two companies.

Bravo, H+BEDV Datentechnik! Hiring members of the black hat community for mainstream information security positions as well as other positions is a bad idea, as shown by H+BEDV Datentechnik's loss of confidence in its now former business partner. We as information security professionals need to maintain a clear separation between the white hat and the black hat community; if we do not, we strongly threaten not only security, but also our own reputations.

Provisions of Sarbanes-Oxley Act go into effect

Section 404 of the Sarbanes-Oxley Act (SOX) has recently gone into effect. Provisions in this section require publicly-traded companies to implement policies and controls that secure, document, and process material data that affect their reports of financial standings. Vendors helping companies with integrating SOX compliance initiatives into the business process will potentially generate USD 5.8 billion in business this year, with 28 percent going to technology companies. Last year over USD 1 billion was spent on technology that was implemented to comply with SOX provisions. Security technology providers will get a large share of this business.

As I said in an earlier editorial, SOX has been a boon to auditors, but it also has been a catalyst to the practice of information security in the US. Regulatory compliance is one of the best motivators for adequate funding and management support of sound information security practices. SOX has motivated publicly-traded companies to examine and improve their security practices and has at the same time raised the proverbial bar for the practice of information security in sectors outside of the publicly-traded company arena. Vendors and consultants have also benefited in that SOX compliance generates a considerable amount of business for them. There is a great financial cost that goes with SOX compliance, but the benefit of a much improved governance process over IT will be well worth it.

India, US discuss information security in India

At a conference of IT experts and senior government officials hosted by NASSCOM and the Information Technology Association of America, US Under Secretary of Commerce Kenneth Juster urged India to strengthen its laws to better guard intellectual property rights and ensure that computer criminals do not steal sensitive information. India's current laws dealing with electronic commerce and patent and copyright protection are insufficient to deter computer crime; Indian officials say they are trying to make appropriate legal changes. The conference concentrated on how both countries can counter threats to their information infrastructure in coordination with each other. Juster said India must safeguard the privacy of personal and financial data, because an increasing number of US corporations rely on Indians to run their technical operations and develop software.

The organizers of this conference should be commended for their efforts in launching discussions concerning information security in India, a country to which the US is outsourcing a growing proportion of IT work. In some cases US companies

have required that third-party business partners in the US, Europe and the Far East adhere to rigorous security standards, but have not done so for relationships with companies in India. The discussions at this conference were thus an important first step in dealing with the security implications of outsourcing.

Seoul Metropolitan Government bans Internet messenger

In an effort to better protect information, the Seoul Metropolitan Government (SMG) has banned all of its employees from using Internet messengers, chat services, and other connections to potentially dangerous sites during working hours. The SMG cut connections to these sites and also to other affiliated organizations in an attempt to boost work efficiency. Harmful sites designated by the SMG include sites with sexual explicit content, violence, on-line gambling, games, movies, and animation. Chatting and messenger sites introduce the risk of leaking internal information and were thus treated as harmful sites. SMG employees are not happy with the new system because they had been using messaging services during the day to interact with their colleagues on business-related matters. The SMG trade union added that disconnecting networks from harmful sites is another way of controlling workers.

Virtually every organization that has high levels of Internet connectivity wrestles with the problem of the particular services that should be available to employees. Many services, such as email and Web services, are necessary for a large proportion of employees, but others have dubious value because they present a golden opportunity for cyberloafing and leakage of sensitive and proprietary information. Instant messaging is, for example, often used much more for personal—than for work-related reasons. The same is true of Internet relay chat (IRC). Some organizations have taken the same approach as the SMB, namely cutting off potentially harmful services altogether and limiting sites to which employees can connect. This approach, although effective in dealing with the problem, can have an unfortunate byproduct, however—causing hostility within the workplace. Numerous vendors have also developed reasonably effective technical solutions that can be used to minimize cyberloafing without alienating employees to the degree that SMG's approach so often does. Regardless of the approach an organization takes, the approach should be described in a clearly stated policy that communicates the employer's specific expectations and admonitions to employees.

Eugene Schultz
Editor-in-chief