

Security Trends Report

09/08

Internet fraud: lots of complaints, few repercussions

Washington, New York considered leading states in prosecuting online crimes

By Nancy Gohring

August 12, 2008 (IDG News Service) Despite receiving tens of thousands of online fraud complaints from consumers every year, U.S. states bring only a small number of Internet-related cases to court, according to research released Tuesday ([download PDF](#)).

The [Center for American Progress](#) and the [Center for Democracy and Technology](#) studied the number of complaints that state attorneys general offices receive and compared that with how many lawsuits the states bring against spammers, spyware creators and other online fraudsters. Not all states report such numbers, but the 20 that do said that they received 20,000 Internet-related complaints in 2006 and 2007, the research found. Most states included Internet-related complaints among the top 10 types of consumer complaints they receive.

During that time period, attorneys general brought 168 Internet-related cases to court, with 60% of those related to child pornography, the researchers found.

Although the [Federal Trade Commission](#) (FTC) also has a role in bringing cases against online offenders, states should do more, said Reece Rushing, director of regulatory and information policy at the Center for American Progress. "We see [the FTC] as absolutely critical, but the states should be partners in this as well," he said. "If we had all hands on deck, we could really make some progress in addressing this problem." Often, state laws against online fraud and abuse are tougher than federal laws, he said.

Washington and New York are considered leaders in prosecuting online crimes. There are a number of reasons why Washington has become a leader in prosecuting online fraud, said Paula Selis, senior counsel at Washington's state attorney general's office. "There must be a recognition that online fraud is a huge threat to consumers as well as a threat to online commerce," she said.

The Washington state legislature has funded a forensics lab and salaries for special attorneys and investigators to proactively look for fraud and investigate complaints, she said. In addition, Washington was one of the first states to issue antispyware and antiphishing laws, she said.

Complaints about Internet-related fraud continue to increase. In 2007, the FTC received more than 220,000 Internet-related fraud complaints, 16,000 more than in 2006 and 24,000 more than in 2005, the groups said in their report.

UK Government Depts. Lost 29 Million Records in One Year

(August 20 & 21, 2008) In the last 12 months, UK government departments have lost 29 million records containing personal data. The government asked for departments to include data loss on their financial statements after the loss of two disks containing personally identifiable information of 25 million child benefit claimants last year. The remaining four million lost records include those of three million driving test candidates reported by the Department of Transport and 620,000 on an unencrypted Ministry of Defence laptop. In a related story, the Home Office learned earlier this week that an outside contractor lost a memory stick containing personal information about thousands of criminals in England and Wales.

The Information Commissioner has been notified.

530M records exposed, and counting

By Jay Cline

September 9, 2008 (Computerworld) By my count, over half a billion records of personal information have been exposed or mishandled in the past eight years. And these are only from breaches where a record count has been publicly revealed.

That's more than the population of the [European Union](#), and more than the number of people living in the U.S., Canada, Mexico and all of Central America and the Caribbean combined.

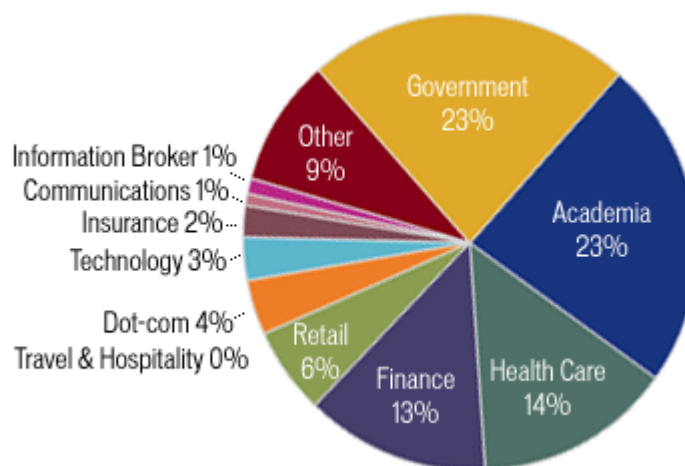
My count of 530 million is more than double the 244 million records cited on [Privacyrights.org](#). So how did I arrive at that figure?

There are a number of Web sites where you can find information about data breaches, including [Computerworld's privacy page](#), [Attrition.org](#), the [Identity Theft Resource Center](#), blogs, government agencies and privacy newsletters such as the International Association of Privacy Professionals' "[Daily Dashboard](#)". For my summer project this year, I tabulated the data from all of these sources. I added them to files I'd been keeping since 2000, which included data on breaches stretching back to 1995. An intern, Emily Prather, Googled the Fortune 500 companies for news of breaches that didn't make these lists. Add to these several dozen notification letters received by friends and family, and we tallied about 1,500 breaches.

What does the data say about the information risks facing your organization?

The biggest surprise to me was the sources of breaches. Many people within the information security profession refer to the insider threat as the primary source of risk, routinely saying that 75% of breaches are the work of employees.

This isn't exactly what breached companies are telling the press, though. The biggest line item we found was hackers, at 20% of all breaches. For their part, dishonest insiders garnered 3% of the blame. It's possible that a good number of the stolen laptops (19%) and other computers (8%) were taken by employees, but the cases we reviewed appeared mostly to be random criminal acts.



If you add up all of the mistakes employees make — such as losing laptops and backup tapes, improperly disposing of documents, inadvertently sending e-mails and packages, and misconfiguring Web sites — the employee category amounts to 39%.

A whopping 11% of publicized breaches were the result of an errors traceable to vendors.

Have these root causes changed over time? Many of us in the privacy profession know that organized crime is thriving in the stolen-information business and growing in sophistication each year. And maybe they're getting away with it more often. The share of intentional privacy breaches has fallen from 74% in 2005 to 55% this year. Conversely, unintentional data exposures rose from 25% to 40% over the same period, with unspecified causes accounting for the remainder.

There has also been some speculation that breach notification has peaked in the U.S., with more companies encrypting their laptops and doing better overall at applying lessons learned in breach prevention. The numbers don't support this assumption. From 1995 to 2004, I tracked 186 breaches, with an equivalent number in 2005 alone. In 2006 and 2007, and number of breaches topped 400, and it's on track to do so again in 2008. Each of the past three years has also seen more than 100 million records exposed.

Does risk vary by geography? The mandatory notification of privacy breaches in the U.S. has inflated the appearance of risk in America, with the U.S. accounting for 89% of the incidents we recorded. The U.K. (6%), Canada (3%) and Japan (1%) rounded out the top tier.

Within the U.S., the states with the highest number of breaches tracked closely with their relative populations, with California (133 incidents), New York (68), Ohio (58), Texas (57) and Florida (34) taking top spots.

But if you break down the incidents on a per-capita basis, our nation's capital tops the list at 75 breaches per million inhabitants. Montana (10 per million), Vermont (eight), New Hampshire (seven) and Rhode Island (seven) — with their handfuls of breaches and low populations — rounded out the top tier.

And what about industry sector? Some of the more infamous breaches — such as [CardSystems](#), [ChoicePoint](#) and TJX — may have given the impression that the privacy breach phenomenon is all about credit card number acquisition from private-sector companies.

But in terms of sheer number of breaches, government agencies (23%) and schools (23%) topped the charts. Health care (14%), finance (13%) and retail (6%) companies followed.

There were definitely limitations to our study. We're relying on what companies say or what gets reported about their breaches. Anyone familiar with doing forensics on a breach knows that these facts can be hard to pin down with certainty.

Moreover, many companies, especially smaller businesses, are experiencing breaches but not detecting them. Others are detecting them but not reporting them. And those helping companies in this area say there is a better-than-even chance that sending out a batch of breach letters will not result in press coverage.

What should privacy and security officers take away from this data? Stay vigilant of suspicious activity on the network, patch known vulnerabilities, train employees, keep locking down laptops and flash drives, and beef up your vendor oversight program. And get ready for mandatory breach notifications across the industrialized world.

Group to release uniform metrics to measure IT security

CIS also plans to launch services to help companies compare security efforts

By Jeremy Kirk

September 8, 2008 (IDG News Service) The Center for Internet Security (CIS) is set to release guidelines that enterprises can use to measure the state of their security, and it's also preparing to launch a service to help companies compare their security performance with that of their peers.

The latest CIS project is designed to resolve the confusion and lack of uniformity in ways to measure whether an organization's IT security is improving or not, said [Bert Miuccio](#), CIS's CEO.

"The problem that we've come to recognize is that information security professionals really are growing more confused on how to define success," Miuccio said. "They know that compliance with regulatory requirements, and audit frameworks do not necessarily result in improved security and are not the best measures of success."

CIS is a nonprofit group funded by a variety of organizations with an interest in security. Since it was formed in 2000, it has created 40 benchmarks for default security configurations for all kinds of software, including operating systems, middleware and network devices. The benchmarks, which are a free download on the [CIS Web site](#), are intended to help organizations reduce IT security risks.

Every security professional has different definitions of how to evaluate organizational security, Miuccio said. To try to find common ground, CIS assembled 85 information security experts who will work together to identify uniform ways to measure eight different metrics. The metrics should be released in late October or early November, Miuccio said.

Two are "outcome" metrics: the mean time between security incidents and the mean time to recover from security incidents. The remaining six metrics are related to process: the percentage of systems configured according to approved standards; the percentage of systems patched according to policy; percentage of systems with antivirus technology; percentage of business applications that have a risk assessment; percentage of business applications that have a penetration or vulnerability assessment; and percentage of application code that have a security assessment or code review before deployment.

Along with the metrics, CIS plans to launch around the same time a software-based service for companies to compare how they are doing in terms of security compared with other anonymous companies in their vertical market. This type of comparison is already commonly used for financial results and other aspects of business performance such as customer service.

"That's not done in information security today," Miuccio said. "We believe that this service will begin to enable that."

Identity thieves: Thanks for the bypass

September 8, 2008

The latest twist in identity fraud involves stealing your identity in order to use your health insurance.

Jennifer Barrett, global privacy officer at Acxiom, says the scam is the newest trend in identity fraud. That it's growing fast should come as no surprise, as health care costs - and the ranks of the uninsured - continue to rise. (Acxiom provides services to help insurers verify the validity of claims.)

With this type of fraud it's typically your insurance company, not you, that takes the financial hit. But you still might want to keep an eye on your medical claims history. The reason: if medical scammers steal your identity you may suddenly have a medical history that isn't yours. Left undetected, that might put you at risk for misdiagnosis or improper treatment, Barrett says.

Your own doctor isn't going to be fooled. But as the world moves to consolidated online medical records, you might find yourself in an emergency room somewhere with doctors reading someone else's medical history as they try to diagnose your problem.

The risk is that "You have things attached to your medical history that are not yours and you're not treated properly... They [might] think you had a bypass a year ago when you didn't," Barrett says.

The nightmare of medical identity theft

Excerpt:

One victim's record was altered with the wrong blood type. Another person's file was changed to include numerous psychiatric sessions that didn't occur and false diagnoses of severe depression. A Pennsylvania man discovered that an imposter used his identity at five different hospitals to receive more than \$100,000 worth of medical treatment.

Study: Weak Passwords Still Main Security Defense

New research finds most organizations still use passwords to protect important data. But the study also says they provide little protection against a breach

By [Joan Goodchild](#), Senior Editor

September 04, 2008 — [CSO](#) —

As a security manager, you know how easily passwords can be compromised -- and you are doing all you can to add extra layers of security, right?

If your answer is no, you're not alone. A new study finds most organizations are still relying primarily on passwords to protect important data.

The [research](#), titled "Strong User Authentication," was conducted by [Aberdeen Group](#) and commissioned by Quest Software, a provider of enterprise systems management products. It finds 52 percent of organizations require only passwords for employees to access critical data, rather than [augmenting passwords with stronger forms of authentication such as hardware tokens, digital certificates or risk-based scoring](#).

The research firm polled nearly 150 organizations around the world, according to Derek Brink, vice president and research fellow for IT Security, [Aberdeen Group](#).

"The fact that passwords are so predominant is probably not a surprise," said Brink. "But a high percentage use only passwords and that is bad because people don't practice really good policy with passwords."

Brink pointed to problems such as weak, short, word choices and poor policies in organizations as reasons why the password alone is now an out-of-date security protocol. In fact, the Aberdeen study found 64 percent of organizations do not even require users to change their passwords, 45 percent allow standard dictionary terms, like "password," and 29 percent of organizations have no requirements for password length.

Even those organizations trying to implement [good password policies](#) are running into problems, said Brink. The research found 88 percent of enterprise users have multiple work-related passwords, averaging between five and six.

"That becomes a management problem for users because they have to remember them all and keep them separate," said Brink. "And users typically solve that problem with bad practices, such as writing them down or choosing the same password for all systems."

Brink said more companies should be considering two-factor authentication processes that use software tokens, digital certificates or user biometrics as an additional layer of security.

"We have daily incidents now with regard to people gaining unauthorized access to data," said Jackson Shaw, a senior director of product management with [Quest Software](#). "With the recent, well-publicized incidents of network and identity theft, companies need to put security first and require more than just passwords for user authentication."

Feds finally put teeth into HIPAA enforcement

Three years after the federal law's rules on securing health care data took effect, HHS has issued its first 'corrective action plan.' And more may be on the way.

By Jaikumar Vijayan

September 8, 2008 (Computerworld) A data security audit that the [U.S. Department of Health and Human Services](#) conducted at Piedmont Hospital in Atlanta last year was widely viewed within the health care industry as a harbinger of [further actions](#) by the federal government to enforce HIPAA's security and privacy rules.

Eighteen months after HHS quietly began [the Piedmont audit](#), there hasn't been much evidence of stepped-up enforcement. But now a stringent ["resolution agreement"](#) signed in July by the agency and Seattle-based Providence Health & Services is generating the same kind of buzz among health care providers that the Piedmont audit did.

On July 15, Providence agreed to adopt a so-called corrective action plan (CAP) and pay \$100,000 to settle what HHS described as "potential violations" of the Health Insurance Portability and Accountability Act's requirements for [safeguarding electronic patient data](#).

The resolution agreement — the first of its kind under HIPAA — stemmed from the [loss or theft](#) of laptops, optical discs and backup tapes containing the unencrypted medical records of more than 386,000 Providence patients. On several occasions in 2005 and 2006, equipment was reported missing after workers took it out of the office with them.

Under the CAP ([download PDF](#)), Providence has to revamp its security policies to include physical protections for portable devices and for the off-site transport and storage of backup media. It also is required to implement technical safeguards, such as encryption and password protection. And the not-for-profit health system, which has operations in five western states, must conduct random compliance audits and submit compliance reports to HHS for the next three years.

In addition, the agreement calls for Providence's chief information security officer to personally validate that all required policies have been put in place and that all employees have been trained on adhering to them. The CISO also has to attest that all backup media and portable devices containing health information protected by HIPAA are properly secured.

Significantly, the CAP precludes Providence Health from contesting the validity of or appealing any of its obligations under the agreement. The settlement is getting considerable attention within the health care industry because of the tough terms and conditions that the deal imposed on the provider.

"The CAP gives us some indication that the bar is being raised when it comes to HIPAA compliance," said Lisa Gallagher, director of privacy and security at the [Healthcare Information and Management Systems Society \(HIMSS\)](#) in Chicago. "This is a fairly serious corrective action plan."

Corrective Measures

The security action items that Providence Health & Services agreed to include the following:

- Revise policies and procedures for safeguarding patient data while it is stored at or being transported to off-site facilities.
- Train all workers on security policies and submit proof to HHS that the training has been completed.
- Update policies as needed, but at least on an annual basis.

- Ensure that a security risk assessment and management plan and a data breach notification policy are in place.
- Conduct reviews that include unannounced audits, spot checks and site visits at company facilities.

Source: U.S. Department of Health and Human Services

Gallagher added that the deal with Providence sends a clear message to other health care providers that HHS is finally cracking down on HIPAA violators, after having been accused of lax enforcement in the past.

The harder line is in keeping with an announcement in January that the Centers for Medicare & Medicaid Services (CMS), the HHS unit responsible for administering the HIPAA security rules, had hired [PricewaterhouseCoopers](#) to conduct audits on its behalf. At the time, the CMS said it planned to do 10 to 20 audits this year at organizations that had been the target of complaints about their data security practices.

According to Gallagher, the CMS is expected to release findings from those audits early next year. It also plans to highlight violation trends and provide guidance on the biggest problems that health care providers are having in implementing the controls required by HIPAA. "As far as I know, they are under way with these audits," she said.

Gallagher also expects the CMS to start working more closely on enforcement with the HHS Office of Civil Rights, which administers the data privacy rules set by HIPAA.

As of press time, the CMS had yet to respond to questions that were sent via e-mail, as an agency spokesman had requested. Providence officials also asked that questions be sent via e-mail but also hadn't responded.

Peter MacKoul, president of HIPAA Solutions LC, a consulting firm in Sugar Land, Texas, agreed with Gallagher that the Providence settlement was a dramatic example of the potential consequences of HIPAA violations.

"If you look at what they're being forced to do, it's scary," he said. "They have lost their ability to contest anything; there's no way of getting out of this agreement. And this is the best deal they could get."

MacKoul added that while Providence was audited for data security violations, many of the corrective actions it is being required to implement fall into the privacy realm, showing that HHS is making little distinction between privacy and security for [compliance purposes](#).

And based on the terms of the CAP, organizations that have to comply with HIPAA shouldn't be lulled into complacency by the previous lack of enforcement, MacKoul warned. "If I were a covered entity, I wouldn't want to roll the dice and get caught up in something like this," he noted.

The resolution agreement does appear to be a belated attempt by HHS to get the health care industry to take HIPAA more seriously, said Chris Apgar, president of consulting firm Apgar & Associates LLC in Portland, Ore. "I think it's about time they used somebody as an example," he said.

Even so, it's unrealistic to expect a large increase in the number of HIPAA enforcement actions in the near term, according to Apgar and other analysts. Such actions are triggered only when complaints are lodged against organizations. HHS has no HIPAA cops who are actively looking for violations, and health care providers aren't required to report internal violations themselves.

Also, neither the CMS nor the HHS Office of Civil Rights has anywhere near the resources or the funding needed to investigate all of the complaints that are filed. As a result, examples such as the settlement deal with Providence will likely continue to be more the exception than the rule, Apgar said.

In fact, one of the primary reasons why Providence was investigated in the first place no doubt was [the publicity](#) generated by the incidents involving lost IT equipment, said Randy Yates, director of security at Memorial Hermann Healthcare System in Houston.

"Once something that large hits the media, the government is bound to do something," Yates said. "[The CAP] puts out a message that says, 'We see this thing, and we don't like it.'"

Often, enforcement actions are important because they get the attention not just of those in charge of implementing privacy and security policies, but also of those who control the purse strings within organizations. Last year, for instance, the audit at Piedmont Hospital contributed to the approval of a \$1.3 million budget item for data encryption at Memorial Hermann.

But if the investigations are as sporadic as they have been in the past, the buzz generated will fade away quickly, said Christopher Paidhrin, IT security officer at ACS Healthcare Solutions, a Dearborn, Mich.-based unit of Affiliated Computer Services Inc.

Paidhrin noted that the [Piedmont audit](#) last year initially raised a considerable amount of concern among health care providers. But most of that concern eventually melted away when the expected increase in enforcement actions failed to materialize. The same thing will likely happen in the aftermath of the Providence Health settlement, he said — unless HHS takes additional actions elsewhere and publicizes them to the same extent.

Chinese researchers use heartbeats against implant hacking

Wireless software updates for medical implants are gradually replacing incisions. Modern implants — from pacemakers to insulin pumps and sensors for bodily functions — have reduced the number of maintenance operations needed. They also allow doctors to use computer monitoring to track how a patient's health has developed. It is even possible in principle, to charge batteries through the skin. In telemedicine, Body Sensor Networks (BSNs) and Wireless Body Area Networks (WBANs) are being developed to improve care for the chronically ill.

But the opportunities also increase the risks. Wireless implants are vulnerable to [malicious attacks](#), which can be fatal. Experts say that signals must be securely encrypted. Now, researchers from the Chinese University of Hong Kong have presented their solution based on biometric features. The patient's individual heartbeat, which can easily be measured from the person's pulse, is used as the key for encryption. In their tests, 64-bit encryption works quite well, with the recognition ratio being nearly as accurate as with conventional fingerprint recognition systems. In the [journal *IEEE Transactions on Information Technology in Biomedicine*](#), the researchers argue that heartbeat encryption is even safer because the constantly changing heartbeat cannot be mimicked by a recorded copy.

As Carmen Poon and her colleagues from the [Chinese University of Hong Kong](#) explain, the constant minor fluctuations in the Interpulse Interval (IPI) make it impossible for attackers to use recorded data as a key at a later date. A sensor in the implant registers the rhythm of the heartbeat, while a second sensor records the rhythm at an index finger, where a person's pulse can be easily taken. Because the two measurements are taken at the same time on the same body, minor natural fluctuations in the pulse's rhythm play no role, but any earlier recordings of the pulse would not match. The implant and access devices only exchange encryption keys and communicate with each other when the details of the two measurements largely overlap.

In their tests, Poon's team did not use implants, instead recording the data on the right and left index fingers of their sample population of 99. An electrocardiogram (ECG) and a photoplethysmograph (PPG), which records fluctuations and light absorption under the skin, relative to the pulse, were used to analyse the data. The computer then used the interval between 16 successive heartbeats recorded down to the millisecond, to generate a calibrated 64-bit code.

Poon and her colleagues explain that this method has to be accurate enough to rule out incorrect data, but flexible enough to accept tiny biological differences between measurements taken at different parts of the body. In their tests, the system accepted most code pairs, rejecting only 6.5 per cent, which puts this approach close to the 4.2 per cent rejection rate generally found with fingerprint systems. As the

team put it, "the results suggest that easily accessible IPI data can serve as a good source for the generation of entity identifiers (EI) as node points in Body Sensor Networks (BSNs)".

Data Breaches Have Surpassed Level for All of '07, Report Finds

By [Brian Krebs](#)

Tuesday, August 26, 2008;

More data breaches have been reported so far this year than in all of 2007, according to a report released yesterday by a nonprofit group that works to prevent fraud.

Identity Theft Resource Center of San Diego found that 449 U.S. businesses, government agencies and universities have reported a loss or theft of consumer data this year. Last year, the center tallied 446 breaches involving 127 million consumer records. About 90 million of those records were attributed to a single retail chain, TJX, which operates [T.J. Maxx](#) stores.

Officials said they do not know whether there have been more breaches this year or if there is better reporting of the incidents.

So far this year, at least 22 million consumer records have been the target of data breaches, according to the report. But resource center founder Linda Foley cautioned that the true number of records affected is likely far higher, noting that in 41 percent of the cases the number of consumer records affected was not disclosed. What's more, Foley said, many businesses are not reporting data breaches or are not aware of them.

In addition, she said, a single breach report often involves data belonging to multiple businesses.

In April, software vendor SunGard Higher Education disclosed that a lost laptop exposed the names, Social Security numbers, birth dates and driver identification numbers of students from at least 18 colleges in Connecticut and New York. The company has not yet disclosed the full scope of the breach, but has since notified a number of schools from other states, including Maryland and Virginia, that their students also have been affected.

"We're still hearing about colleges that have been affected," Foley said.

About 44 states and the District have laws requiring entities that suffer a data loss or breach to alert affected consumers. But only three states -- Maryland, New Hampshire and Wisconsin -- routinely publish those reports online, Foley said.

According to the identity theft center, malicious attacks were the leading cause of data breaches this year. Nearly 13 percent were attributed to hacking, while customer data theft by company employees accounted for 15.6 percent. Lost laptops and other digital media containing consumer data comprised 21 percent of the breaches. Fourteen percent involved the accidental publishing or dissemination of sensitive consumer data, while breaches attributed to subcontractors made up 11 percent.

Kevin Mandia, founder of Mandiant, an Alexandria firm that helps companies investigate and respond to data breaches, said the spike in disclosures this year may be related to the recent arrest of several cyber criminals thought to be responsible for some of the most high-profile theft of data to date.

"The number of cases referred from law enforcement in years past was much smaller," Mandia said.

Earlier this month, federal prosecutors announced indictments against 11 people alleged to have taken part in stealing more than 40 million credit- and debit-card account numbers from nine nationwide retailers, including TJX, [BJ's Wholesale Club](#), [OfficeMax](#), [Barnes & Noble](#), [Sports Authority](#), [Boston Market](#) and Dave & Busters restaurant chain.

Studies Find Web Sites Rife With Unpatched Vulnerabilities

Government Computer News (08/28/08) ; Jackson, William

New reports by WhiteHat Security and Cenzic expose consistent vulnerabilities in the vast majority of Web sites. Two-thirds of all vulnerabilities identified by WhiteHat in its most recent Security Statistics Report were mitigated; conversely, 70 percent of Web applications analyzed by Cenzic involved unsafe procedures that could have jeopardized a user's personal information. Sixty percent of analyzed sites were vulnerable to cross-site scripting, and new SQL injection attacks are gaining ground and showing up in about 20 percent of sites, according to WhiteHat. Cenzic identified Web-enabled applications such as ActiveX controls, QuickTime, Flash, and other media players as prime targets for hackers looking to embed malicious code. "Attacking client-side applications or browser plug-ins is increasingly becoming a means for distributing malware, rootkits, and backdoors," Cenzic's report says.

Will Exiting Employees Steal Data?

Access Control & Security Systems (09/02/08)

Companies should be careful when firing or laying off IT administrators, concludes Cyber-Ark Software annual "Trust, Security & Passwords" survey, which found that 88 percent of IT administrators would take valuable and sensitive information such as the customer database, merger and acquisition plans, and their company's list of privileged passwords if they were let go. The survey, which polled 300 IT security professionals, also found that of those that said they would take information, 33 percent said they would take the company's list of privileged passwords, which contains keys that would allow them to access all the information on the company's network. In order to protect themselves from former employees, companies should secure their privileged passwords and identities in a digital vault that gives individuals access to the information if and when they actually need it, says Cyber-Ark's Udi Mokady. Mokady says companies also should be sure to routinely change and manage their privileged passwords and identities.

Zombie Plague Sweeps the Internet

BBC News (09/04/08)

Botnets are successfully carrying out more Web attacks and have increased the number of zombie computers under their control by threefold, reports the Shadowserver Foundation. The organization identified more than 100,000 machines that were part of a botnet in June 2008, but that figure has now tripled to almost 450,000 computers. Experts say these attackers insert malicious code into a Web site that exploits a vulnerability in one of the Windows-based programs the visitor is running on his computer. This code then puts the compromised computer in touch with a command and control (C&C) server, which can fully control the victim's computer. These webs of zombie computers form various botnets that are run by a consolidating group of C&Cs, the foundation says.

The Challenge of Securing Virtualization Operations

Network World (09/02/08) ; Antonopoulos, Andreas M.

Security operations in a virtual environment can be very challenging for a number of reasons, writes Andreas Antonopoulos. For instance, IT professionals have to look behind the virtualization layer when looking for the root cause of a fault or security alert. This can be very challenging because virtual infrastructures undergo a great deal of change on top of the abstraction layer. For example, virtual machines can move from host to host in near-real time in response to a hardware failure or to rebalance a load or reduce power consumption. In addition, the virtual storage environment, storage re-allocation, and the network also see similar dynamic moves—particularly in large virtual server pools. Meanwhile, servers in a virtual environment are created and decommissioned at a rapid pace. This makes it difficult to forensically analyze a server or to find its logs and its configuration. Antonopoulos notes that many of these challenges are only seen after virtualization technology has been adopted in production and deployed throughout a data center. Instead of waiting for these challenges to appear, Antonopoulos says they should be discussed in the early stages of planning and implementation of virtualization technology.

MIT Lincoln Laboratory Software Aims to Thwart Cyber Hackers

MIT News (08/27/08)

Researchers at the Massachusetts Institute of Technology's Lincoln Laboratory are developing the Network Security Planning Architecture (NetSPA), software that will identify the most vulnerable points in a computer network. NetSPA uses information on networks, individual machines, and any programs running to create a graph that displays how hackers could infiltrate the network. System administrators can examine the graph and determine the best course of action. NetSPA relies on vulnerability scanners to identify known weaknesses in network-accessible programs that could allow an unauthorized person to access a machine. NetSPA also analyzes complex firewall and router rules to determine which vulnerabilities can be reached and exploited by attackers, and how attacks can spread within a network by moving from one vulnerable host to another. Richard Lippmann, leader of the development effort, says NetSPA enables network administrators to see which vulnerabilities pose the greatest threat to the network, allowing them to fix those problems first instead of patching or fixing vulnerabilities that are not accessible to attackers. NetSPA also can account for unforeseen avenues of attack, such as if a network had to share data with an outside vendor years ago, and now someone is forging that IP address to try to exploit the forgotten permission.

Public, Private Sectors at Odds Over Cyber Security

Los Angeles Times (08/26/08) ; Menn, Joseph

Cybersecurity experts say that three recent, significant computer security breaches highlight how badly the Internet needs a major overhaul, and exposes the rift between corporate America and the U.S. federal government over who is responsible for fixing the Internet. Over the past few months law enforcement officials busted an international ring that accessed customer databases and trafficked tens of millions of credit card numbers, a researcher discovered a major flaw that could allow hackers to redirect Web users to fake versions of popular Web sites, and computer attacks have been used to cripple the country of Georgia's Internet capabilities. However, these incidents have done little to make cybersecurity a more prevalent issue on a national scale. "Nothing is happening," says Jerry Dixon, former director of the National Cyber Security Division at the Department of Homeland Security (DHS). "This has got to be in the top five national security priorities." The U.S. government has primarily argued that the private sector is better positioned to handle the problem, but corporations say the problem is too large for them to manage. Industry professionals say the Internet's technical underpinnings, which are loosely administered by the U.S. Commerce Department, need a major overhaul to eliminate vulnerabilities. The disagreement is largely because cybersecurity issues touch on so many different areas, with DHS overseeing the protection of government networks, the FBI and Secret Service pursuing cyber crimes, and the U.S. State Department following up on cases that lead to other countries. The U.S. government has assembled taskforces that called for increased cooperation and communication between public and private sectors, but experts say their efforts have yet to yield tangible results.

Latest Cybersecurity Threat Lies in Trusted Software and Hardware

NextGov.com (08/25/08) ; Nagesh, Gautham

A new trend that security experts are seeing more of involves a supply-chain attack, in which a piece of hardware is infected before it attaches to a user's personal computer. Employees from one federal agency were recently victimized by such an attack after finding and opening two tainted USB drives, which surreptitiously retrieved sensitive data and sent it to a remote location. A majority of these attacks originate in China, where much of the hardware used by Americans is produced, and can be perpetrated through a device as innocuous as a digital projector. The threat is especially menacing since a user cannot know ahead of time if an outside device has been tainted, but the SANS Institute's Alan Paller offers some risk management techniques. Federal agencies must first standardize their desktops and applications to reject any unauthorized users who attempt to access their systems, as mandated under the Federal Desktop Core Configuration rule. Next, agencies should alert their employees to the dangers and instruct them to treat any unidentifiable or new hardware as a potential threat that must be scanned before using.

Monitoring the Enemy Within: Reflections on a New Internal Data Theft Study

CSO Online (08/12/08) ; Bachman, Cooper

ID Analytics' "Analysis of Internal Data Theft" study examined more than 12 cases of internal data theft at government agencies, educational institutions, and corporations. The incidents involved the theft of more than 5 million identities from consumer and employee files and resulted in eight cases of identity fraud and more than 1,300 cases of attempted fraud targeting bank card, store card, and wireless service providers. In analyzing the incidences of fraud, ID Analytics researchers discovered four patterns that were common to all of the cases. First, the study found that the fraudulent use of the stolen data occurred within 20 miles of where the data was stolen. In addition, the study found that data stolen in an internal breach was more likely to be misused than data lost in an accidental breach, since internal breaches are carried out with malicious intent. The study also found that criminals are increasingly using data stolen in internal data thefts to apply for wireless phones. Finally, the study found that identities stolen in internal breaches and identities stolen in breaches committed by individuals outside an organization were primarily used online for less than two weeks at a time. The study concluded that organizations need to take steps to improve data security, including continuously monitoring customer and employee data in order to detect any misuse early.

Study Alludes to Government Mishandling Social Security Numbers

Government Security (09/08)

Approximately 44 million consumer records were accidentally lost or exposed by the government between 2005 and mid-June 2008, according to a report in the September issue of Consumer Reports. The records contained Social Security numbers, driver's license numbers, and other personal data. The report was based on 230 publicly reported data breaches by federal, state, and local governments that was compiled by the nonprofit Privacy Rights Clearinghouse. "At the government level, leaks of identifying information useful to thieves occur on a grand scale," says security expert Robert Siciliano. "This is largely because municipal governments continually fail to update their antiquated processes, which results in officials posting Social Security numbers and more online, for all to see."

Data Security Now 10% of IT Operating Budgets, Forrester Says

Network World (09/04/08) ; Brodtkin, Jon

Forrester's recent survey of 1,255 security decision-makers at North American companies has found that IT security budgets are growing. According to the survey, 10 percent of IT operating budgets is allocated for security this year, up from 8 percent in 2007. The survey also found that 21 percent of respondents plan to increase IT security spending next year, while 73 percent plan to maintain their current level of security spending. Just 6 percent said they planned to reduce security spending in 2009. In addition to examining IT security spending trends, the survey also looked at the relationships IT security professionals have with business executives. The survey found that 30 percent of respondents had a "dotted-line relationship" with their company's board or CEO, while 19 percent had such a relationship with their company's executive committee. Forrester analyst Khalid Kark attributed the increased influence IT security professionals have with their company's executives to several factors, including data breaches and the resulting media coverage and lawsuits, as well as the fact that CEOs are agreeing with IT professionals' argument that IT security deserves more attention.

User Ignorance Begets Internal Threats

Computerworld Australia (08/28/08) ; Meckbach, Greg

Most security threats come from inside organizations, not from hackers on the outside, concludes an IDC survey. The survey found that 56 percent of participants said that email was a source of confidential email links, while more than 33 percent of participants cited Web mail or posts to Web sites as the source of breaches suffered by their organizations. In addition, the survey found that 19 percent of participants believed iPods and other electronic devices that plug into a computer's USB port were used to take information in security breaches

suffered by their organizations. It is only now that organizations are becoming aware of such insider threats, says IDC's Brian Burke. "Three or four years ago, companies simply did not know, didn't have visibility to the fact that employees were committing these errors," Burke says. "The fact that they're actually aware of it now and they see it as a major driver signifies a major shift in the level of knowledge out there that this insider threat really exists." Although organizations are increasingly becoming aware of threats posed by their own employees, most employees still do not know that they are doing anything wrong when they are told that are breaking information security rules, says Starla Rivers, the technical security architect at San Diego-based Sharp HealthCare.

Secure by Design

CIO Insight (08/08)No. 96, P. 22 ; Raikow, David

Perhaps the most important part of securing an organization's network is implementing a realistic security policy. Failing to do this renders even the best security technology virtually ineffective. The process of developing a security policy begins by assessing risks and setting clear priorities. When assessing risks, organizations should try to determine how likely it is that they will suffer the different types of security failures, as well as how much each of those failures would cost. When trying to answer these questions, organizations should be careful not to fall into several common errors, such as focusing too much on quantitative detail and concentrating on hardware and software while ignoring risks created by user behavior. Organizations should then begin developing a policy that will address the threat priorities that were clarified or identified for the first time during the risk assessment. During this process, organizations should select a set of strategies that will help them mitigate the threats they identified in the risk assessment while keeping in mind relevant business needs and budget limitations. The final step is to implement the security policy, a process that conforms to a variety of different schedules and is done in different chronological orders and phases. This step consists of two elements: Educating users about the security policy and initiating the appropriate changes in corporate culture, and installing and configuring hardware and software. An important thing for organizations to keep in mind is that the implementation of the security policy needs to be done gradually, since it is counterproductive to force organizational changes and changes in user behavior to happen all at once.