

Security Trends Report

07/20/07

Following are major trends within information security and some of their implications for state government.

Increased (black) market traffic in, and value of, information

Personal Identifiable Information (PII) and financial information has become increasingly valuable to the international black market. According to some reports an entire underground economy now exists in which criminals will pay between \$14 and \$18 for a single identity (for example, government issued identification numbers coupled with financial information).

Increased sophistication and organization of attackers

As a result, information security attacks have become big business over the past few years. As opposed to the scattered, automated “script kiddie” attacks of a few years ago, modern attacks are being perpetrated by international organized crime rings who are investing money in tools and training and coordinating their efforts to maximize profits. For example, a Russian company now markets a commercial-grade “attack kit” that has been responsible for compromising thousands of systems (including an epidemic of infections that hit Italian web-sites in June). The kit is sold for around \$1000 and includes a support contract and maintenance agreement. Increased investment in attack tools has increased the risk not only from external attacks but also from internal attacks as these tools become generally available.

Another aspect of the increased organization of attackers is the rise of “cyber terrorism” and “cyber warfare.” Although this has not yet become widespread, there have been several recent incidents of this type of activity. In June, Estonia suffered a wave of assaults on its computer networks that were attributed to Russia. The attacks were sustained, coordinated and focused and had “clear national security and economic implications.” Governmental entities may be at higher risk from this type of attack than other business types.

Decreased effectiveness of “traditional” technical defenses

Information security defensive measures are in an arms race with attackers. As attackers gain sophistication and develop better tools and attack methods, technical defenses become outdated and less effective. This, coupled with changing business needs such as greater connectivity requirements, makes maintenance of technical defenses a constant challenge. “There’s a new type of threat that traditional security measures are not designed to meet,” said Dan Hubbard, vice-president of California-based Websense Security. “Frankly, the attackers have out-evolved the solutions.”

Increasing penalties and cost associated with data safeguards

As repeated massive exposures of PII have hit the press, there has been an increase in government-legislated protective measures and legal repercussions. The penalties for exposures of PII have grown to include significant financial and legal risks [OR S.B. 583]. This has resulted in a trend for businesses to increase their expenditures to secure information rather than face increasingly costly penalties for failing to implement adequate safeguards.

Online business trend continues

The ongoing trend for businesses to put more of their mission-critical processes and applications online continues. Coupled with greater attacker sophistication, declining effectiveness of traditional technical defensive measures, and greater penalties for inadequately safeguarding information, this further increases the risk and costs that businesses are facing.

In summary, business owners attempting to meet demands for greater information availability are facing increased risk and cost because of a combination of interrelated information security factors. Increased and more effective criminal trafficking in personal identity information, coupled with greater challenges to protect it (at increasing costs) and greater legislated penalties for failing to adequately safeguard the information is raising information security costs across all industries.

Recent Incidents

Pfizer Breach Illustrates Risks of Sharing Files

Pfizer disclosed this month that the Social Security numbers and other personal data of about 17,000 of its current and former workers were exposed after an employee installed unauthorized file-sharing software on a company laptop provided for use at her home.

Data on about 15,700 of the workers was actually accessed and copied off the laptop by an unknown number of people on a peer-to-peer (P2P) network, New York-based Pfizer said in letters that it sent to affected employees and to state attorneys general.

Data Breach Affects Thousands of Ohioans (June 17, 2007) The state of Ohio has hired a data security expert to help "determine the likelihood of someone getting access to the data on a stolen backup storage device." The device was stolen from the car belonging to an intern at the state's Office of Management and Budget; the device contains the names and Social Security numbers (SSNs) of all 64,000 Ohio state employees, data belonging to nearly 54,000 people enrolled in Ohio's pharmacy benefits management program, 75,000 of their dependents, the names and case numbers of approximately 84,000 welfare recipients, records for nearly 160,000 Medicaid providers and their bank account information, and the names and federal tax identification numbers of approximately 1,200 vendors receiving payroll deduction payments from the state. Ohio governor Ted Strickland "has issued an executive order to change the procedures for handling state data."

Ohio

Stolen Backup Tape Costing State Millions

Costs to the state resulting for the theft of a computer backup tape containing Social Security numbers and other sensitive data from a state intern's car could soon reach \$2.2 million, after officials said that the number of those affected has more than doubled. The total now includes more than 770,000 taxpayers, along with nearly 259,000 businesses, vendors or other entities.

MORE: [Columbus Dispatch](#)

Other News:

Drip, drip, drip goes the data as leakage threat rises

<http://cwflyris.computerworld.com/t/1675416/101582/68378/0/>

A new survey from IDC reminds us not to attribute to malice what can be explained by inattention. According to the survey, corporate data is more at threat of exposure from leakage (and a number of other causes) than from intentional theft by employees. That's the most surprising finding of a study <http://www.idc.com/getdoc.jsp?containerId=206750> titled "Worldwide Information Protection and Control (IPC) 2007-2011 Forecast and Analysis: Securing the World's New Currency." This inadvertent leakage threat has risen to fourth in importance behind viruses, spyware, and spam, while intentional theft by employees with a criminal or otherwise malicious agenda has actually fallen in rank, and now sits in seventh position.

Can 'cyberinsurance' protect you from data breach catastrophe?

Insuring companies for costs related to data breaches used to be a slow business, but after the multimillion-dollar TJX case, companies are suddenly scrambling for coverage -- and some are being rejected by insurers for inadequate policies and procedures.

<http://cwflyris.computerworld.com/t/1669405/1138972/68239/2/>

Hackers Target Execs and Their Families"

IDG News Service (07/02/07) ; Kirk, Jeremy

MessageLabs reports that about 10 emails per day containing malware were targeted at individuals in senior management positions in May. In addition to targeting executives, families of those targeted also received phony executable code files in email attachments with the executive's name in the subject line. MessageLabs chief security analyst Mark Sunner says sites such as MySpace and Facebook facilitate the ease of finding out detailed information about an individual. CIOs, CFOs, and CEOs have all been targeted, MessageLabs reports, when they tracked over 500 targeted messages. Sunner says hackers are employing single messages as opposed to mass-spam because of the former's success rate of being overlooked. IP addresses from such messages come from all over the world and botnets, or computer networks that are already controlled by hackers, are also being used to send such email.

[\(Link to Source/Publication\)](#)

"Nearly 30,000 Malicious Web Sites Appear Each Day"

InformationWeek (07/02/07) ; Gaudin, Sharon

Sophos security consultant Carole Theriault reports that the incidences of Web malware have burgeoned on the Net recently, reaching roughly 30,000 per day. In June, malicious sites online skyrocketed from 9,500 daily to 29,000 daily--a sizeable increase from only 5,000 new malicious sites per day in April. Theriault said the considerable increase can be attributed to hackers opting for taking over Web sites over sending malicious email, and as more security analysts discover infiltrated sites, hackers have upped the sophistication of their techniques. Eighty percent of the sites that researchers discover on a daily basis as being compromised are legitimate sites. The IFrame malware has been the most notorious kind of malware, encoding Web pages with erroneous HTML, infecting about two-thirds of the world's hacked sites. "The Italian IFrame attack should certainly act as a wake-up call to ISPs across the globe," said Theriault. "Web sites should be as secure as Fort Knox, but at the moment, too many web pages are easy pickings for cybercriminals."

[\(Link to Source/Publication\)](#)

"Cyber Security Report Released" Computing Research Association (06/28/07)

Cybersecurity is the focus of "Toward a Safer and More Secure Cyberspace," a new report from the National Research Council of the National Academy of Sciences. The report identifies three broad areas of concern about security, with the first being that a lack of security will enable enemies to launch a cyberattack, in conjunction with a physical attack, to cause an enormous loss of life and billions of dollars in other damages. Secondly, the report draws attention to the potential for billions of dollars in losses due to fraud and extortion if businesses are unable to shore up their cyberspace systems and networks. Finally, the report warns that a lack of cybersecurity may curb the use of technology in the years to come and lead users to discount the positive impact that IT can have on national competitiveness, in addition to national and homeland security. The report also includes a potential Cyber Security Bill of Rights that offers a set of 10 provisions. The points include availability of system and network resources to legitimate users; easy and convenient recovery from successful attacks; and control over and knowledge of one's own computing environment.

[\(Link to Source/Publication\)](#)

July 06, Associated Press — **Illegal workers turn to ID theft.** Fictitious Social Security numbers and green cards are cheap and widely available, and getting them is the first step for many undocumented immigrants arriving in Oregon. But workers and federal officials say increased immigration enforcement -- such as June's raid at a produce plant in North Portland and the detention of 167 workers -- has pushed some undocumented workers to shift from forgery to identity theft. "Enforcement is deterring people, but it's also having another effect," said Kevin Sibley of U.S. Immigration and Customs Enforcement. "Aliens are finding it more difficult to find jobs using the traditional counterfeit documents. So they're willing to commit the extra step to beat the system and get a job. The next step is using someone else's identity." During one stretch last year, American Staffing Resources -- which supplied temporary workers to the Fresh Del Monte plant -- employed 596 workers there, of whom 463, about 78 percent, were using someone else's Social Security number. Only 48 employees had valid, matching Social Security numbers. Federal authorities attribute the proliferation of fraudulent documents to a rise in multinational criminal organizations branching out into the documents market and the misuse of Social Security numbers by employees.

Source:

<http://159.54.226.83/apps/pbcs.dll/article?AID=/20070706/STATE/707060333&template=printart>

Report: Data breaches don't often result in ID theft

Cold comfort for those that do, of course

July 05, 2007 (IDG News Service) -- Most large data breaches don't appear to lead to identity theft, and proposals that would require companies to notify customers of most breaches may lead to increased costs without significant benefits, says a report from a U.S. government agency released Thursday.

The report ([PDF format](#)), from the [Government Accountability Office](#) (GAO), said only four of the 24 largest data breaches between January 2000 and June 2005 appear to have resulted in identity fraud.

Wide-ranging data breach notification laws that would require nearly all breaches to be reported could lead to notifications that "present little or no risk, perhaps leading consumers to disregard notices altogether," the report said. While a breach notification law would have several benefits, a law that requires notification for nearly all breaches could also create significant costs for businesses, the report added.

Congress is currently considering several breach notification bills, including some that would require notification for nearly all breaches.

Instead, Congress may want to consider a notification rule based on the potential for the risk of ID theft, the report said. The president's Identity Theft Task Force has recommended a national standard for determining when government agencies and private companies should report breaches, the report pointed out.

A risk-based standard "could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk," the report said.

A data breach law would create costs for businesses, including the cost of developing incident response plans and notifying customers, the report said. While it's difficult to determine costs, a [Ponemon Institute LLC](#) study in 2006 found that 31 companies with breaches incurred an average cost of \$1.4 million per breach for notifying customers, staffing call centers, paying legal fees and other expenses, the report said.

The GAO researched 24 large data breaches reported in the media between 2000 and 2005, and found that 18 of them had no ID theft or fraud identified. Three of the breaches, at [CardSystems Solutions Inc.](#), DSW Inc., and CD Universe, had reports of fraud associated with existing customer accounts.

And a breach at [ChoicePoint Inc.](#) had reports of unauthorized new accounts opened. In the remaining two breaches, GAO was unable to determine if there had been ID fraud.

It's difficult to track ID theft resulting from data breaches, the report said. In some cases, thieves don't attempt to use the data until a year or more after the breach, the report said.

A breach notification law could be beneficial because it would encourage organizations to improve data security, the report said. "Care is needed in defining appropriate criteria for data breaches that merit notification," the report said. "Because breaches vary in the risk they present, and because most breaches have not resulted in detected incidents of identity theft, a notification that is risk based appears appropriate."

[Alan Paller](#), director of research at the SANS Institute, a security research and training company in Maryland, praised the report, saying some in Congress have focused too much on data breaches. Some lawmakers have "dropped the ball on the far more important area of attack-based defenses," he said.

The report is important because it gives Congress more information about data breaches, said Thomas Lenard, senior fellow and acting president at the Progress and Freedom Foundation, a conservative think tank.

"It's very good to have more data on this issue," he said. "[The report] reinforces my view that we should only adopt new regulations in this area if it can be shown that their benefits are greater than their costs."