Hamilton JournalNews Sunday, June 30, 2013

Dayton Daily News Sunday, June 30, 2013

Hacking, data thefts put private info at risk

More than 600 million records have been breached since 2005.

By Tom Beyerlein, Ken McCall and Steven Matthews
Staff Writers

While the public has lately focused attention on a fugitive hacker and the government mass-surveillance programs he helped uncover, data breaches in recent years have exposed hundreds of millions of records containing personal information of the type often used by criminals seeking profit.

And experts say the data-breach problem is getting worse as an increasing amount of information is stored electronically, some of it living on a proliferating number of mobile devices like laptops and thumb drives that are targeted by ever-more-pervasive malware and easily lost or stolen.

Nobody has a precise count, but more than 600 million private records have been breached in nearly 3,800 incidents since 2005, according to a database of reported breaches maintained by the nonprofit Privacy Rights Clearinghouse of San Diego.

The stolen or lost records often contain personal identifiers like Social Security numbers that can be used for identity theft and private details like medical claims. Attacks by hackers and malware, loss and theft of mobile devices and improper disposal of paper records are some of the ways records are breached.

"It happens a lot," said David Salisbury, associate professor of information systems at the University of Dayton School of Business. "You can read the news and see the straight-up breaches are getting worse and worse and worse."

A Hamilton JournalNews analysis of the Privacy Rights Clearinghouse database shows that Ohio-based entities, mostly companies, have suffered 142 breaches of at least 6 million records collected on individuals. Each breach involved at least 10 records. Hacking and malware were the cause of almost 60 percent of them, with about a quarter stemming from loss or theft of portable devices.

Nationally, businesses dominated the types of organizations that experienced data loss, led by banks and insurance companies, which had 256 million breached records, 42 percent of the total. Not all of the breaches resulted in actual identity theft, but the breaches are putting more people at risk of having their identities stolen for criminal purposes.

Around the state, a number of breaches have topped 1 million or more records. This past October, a portion of the computer network used by Nationwide and Allied insurance agents was breached by cyber criminals, totaling 1 million records. Approximately 1.4 million records in DSW Shoe Warehouse's possession were hacked in 2005 when credit card information from customers in 25 states was compromised. And in June 2007, a backup computer storage device containing personal information of every state worker was stolen out of a intern's car, exposing 1 million records.

Twenty-three of Ohio's breaches, involving 938,000 records, involve companies, schools and government agencies headquartered in the Miami Valley. Among the local cases:

▨ In separate incidents over a period of four years, a criminal gang tied to the Mafia, a Nigerian scam artist and a group of young hackers broke into computer systems owned by LexisNexis of Miami Twp., stealing the personal information of 363,000 people. In the largest of the incidents, five men between the ages of 19 and 24 breached a Florida police department's computer system in a plot that led to the theft of personal information on 310,000 people. Among their reported targets were celebrities including Paris Hilton anc Arnold Schwarzenegger.

▨ Thieves broke into an office building of an Aetna vendor in Dayton and stole computer backup files containing personal identifiers and medical claims of 396,000 people.

▨ Officials of Miami University accidentally posted a report containing nearly 22,000 students' grades and Social Security numbers online, where it remained undetected by the university for three years.

▨ A laptop belonging to a state auditor was stolen from the official's car while it was garaged at home, exposing the Social Security numbers of almost 2,000 Springfield City Schools employees.

"Somebody breaking into your system can be very devastating," said Junjie Zhang, an assistant professor of computer science at Wright State University. "At the same time, the IT industry is working very hard to protect data privacy. It's sort of a war between the good guys and the bad guys."

Wise guys

Lee Klein's wife told him not to get mixed up with the Mafia, but he took the advice of a wise guy instead of a wise woman.

Klein, 43, of Boynton Beach, Fla., became a "crew" member of Thomas Fiore, an associate of the Bonanno organized crime family, federal court records show. In a criminal enterprise that included creating and cashing counterfeit checks, drug dealing and the sale of stolen consumer goods, Klein's niche was to illicitly access a LexisNexis computer system, pilfering personal information to help the mob identity police informants and find people to target for assault and extortion.

"I met the wrong person at the wrong time," Klein was quoted as saying in 2009 when he was sentenced to three years in prison for racketeering after the feds busted Fiore's operation. "I should have listened to my wife."

In July 2009, LexisNexis notified 13,329 people whose information was compromised. Company officials said Klein worked for a client of LexisNexis subsidiary Seisint and misused his access to a computer system that is used by companies, government and law enforcement to access personal information for background checks. Sentenced to three years for racketeering, Klein was released from federal prison in January 2012, records show. Fiore remains in prison.

Klein's thievery was just one of three bizarre episodes that breached LexisNexis systems. The month Klein and Fiore were indicted, May 2009, the U.S. Postal Inspection Service warned more than 30,000 people that thieves used a LexisNexis system to access personal information to obtain fraudulent credit cards. CBS News reported it was the work of a Nigerian scam artist.

The largest of the LexisNexis breaches, involving 310,000 people, came to light in 2005. A year later, federal authorities indicted five young men on charges of conspiracy and computer fraud.

A federal indictment charged Timothy C. McKeage, then 21, of Woonsocket, R.I., of using a Trojan Horse program to hack into the Port Orange, Fla., police computer system. "McKeage utilized this unauthorized access to fraudulently obtain usernames, passwords and other information, which he subsequently used to create additional usernames and passwords to access the (LexisNexis) Accurint database," according to the indictment.

The indictment identifies some of McKeage's targets by initials only, but the Washington Post reported they included the heiress Paris Hilton, then-California Gov. Arnold Schwarzenegger and actors Laurence Fishburne and Demi Moore. A juvenile friend of one of the co-conspirators admitted to hacking into Hilton's cell phone, obtaining revealing photos. McKeage pleaded guilty to conspiracy to commit computer fraud and aggravated identity theft and spent eight months in federal prison.

LexisNexis officials did not return phone calls seeking comment.

It doesn't necessarily take a computer genius to be a successful hacker. In its 2013 annual report on data breaches, Verizon said 78 percent of cyber attacks it studied had difficulty levels of "low" or "very low."

"Very uniformly there's a high percentage of these breaches that could be prevented by really easy fixes," said Mark Eichorn, assistant director of the Federal Trade Commission's Division of Privacy and Identity Protection. "So there's room for improvement (in safeguarding information)."

Old-fashioned crime

Hacking is prevalent, but sometimes thieves get hold of personal information the old-fashioned way: through burglary.

For example, a burglar broke into the car of a state auditor's employee, parked in a home garage, in 2007 and took a laptop containing 1,950 personal records of past and present Springfield City Schools employees.

On Oct. 26, 2006, thieves broke into the Dayton offices of Concentra Preferred Systems and stole a lockbox holding 396,279 medical claim records of health insurance customers of Aetna, Nationwide, Humana Medicare and Anthem Blue Cross Blue Shield. Concentra officials said at the time they were probably garden-variety crooks instead of sophisticated identity thieves, because they also stole cash and "pawnable items of value."

Aetna spokesman Tim Willeford said employees are required annually to complete data security training, and all member information must be stored securely on approved company equipment. Aetna vendors are required each year to complete a comprehensive security test designed to determine if they have thorough enough IT controls.

"Aetna takes data security and the protection of personal information very seriously," Willeford said in a written statement. "We have a strong track record for protecting member and provider information. Despite this, sometimes mistakes happen. When they do, we take prompt action and notify affected individuals as appropriate."

Experts say not all companies are conscientious about reporting breaches, and there is no central repository for reporting data breaches.

"There is a patchwork of laws," said Craig Spiezle, executive director and president of the nonprofit Online Trust Alliance. "Wouldn't it be great if I could go to 'databreach.gov' (to report and learn about breaches)? That would be a great benefit for consumers. It would also give us good aggregate data. But today it doesn't work that way."

Unintentional exposures

Private information isn't always breached by theft. Sometimes it's inadvertently released by the organization charged with safeguarding it.

In fall 2005, a Miami University graduate was Googling her name when she discovered that the university had posted 21,762 student records, including names, grades and Social Security numbers, to a public folder online. The information was publicly accessible for three years.

During the same academic year, a staff member at Miami University-Middletown lost a device holding private information, including Social Security numbers, of 851 students enrolled between July 2001 and May 2006. Social Security numbers shouldn't have been stored on the device, said Joe Bazeley, Miami's information security officer.

"When unintentional exposures happen, we usually don't find out until someone notices it or reports it," he said. Miami's situation isn't unusual: 69 percent of the breaches in Verizon study were detected by an outsider, not the keeper of the information.

As part of Miami's efforts to control data, officials regularly scan university websites in search of nine digits in a row or with dashes. None of the searches has uncovered Social Security numbers, but they have found student ID numbers, which Miami also treats as confidential. Staff and faculty are expected to follow university policies on the handling of confidential data, Bazeley said, but training is mandatory only for employees who handle credit cards.

"It's a legal obligation, and at its core, it's just the right thing to do," Bazeley said. "When you entrust information to an organization, the expectation is that they will take very strong steps to protect that information."

Nonetheless, Miami has had a half-dozen small breaches in the last five years.

Bazeley said the proliferation of online services gives thieves plenty of opportunity, but that too many individuals are careless with their personal information, leaving themselves vulnerable. "With the trend toward social media, people put ridiculous amounts of information on the web," he said.

Consumers, however, have little protection against thefts of data from a third party, such as a business or government office. The FTC's Eichorn said those employers can better protect consumers by keeping computer safeguards and employee training up to date, limiting the amount of information they collect and periodically purging old records that aren't needed.

"A lot of businesses, it's cheaper to keep the information into perpetuity" than to review it, he said.

UD's Salisbury expects the data landscape to continue to evolve.

"We're in kind of a period of time when (personal information) is kind of easy to get at," he said. "But it's always been somewhat easy to get at if you're imaginative enough. It's a real threat. (But) at the end of the day, it's all risk management: Do you understand the risks and do you have a plan to deal with it if the risks are realized?"

Data breaches

These tables show the types of organizations that most often have been the target of data breaches since 2005, and the types of breaches that have occurred.

TYPES OF BREACHES, NATIONWIDE

Description	Data breaches	Total records breached	% of total breaches	% of total breached records
Hacking or malware	840	358,244,664	22.3%	58.9%
Portable device (lost, stolen or discarded)	959	171,544,533	25.5%	28.2%
Insider (intentional breach by someone with legitimate access)	446	32,458,070	11.9%	5.3%
Unintended disclosure	652	25,151,335	17.3%	4.1%
Stationary device (lost, stolen or discarded)	223	7,381,190	5.9%	1.2%
Payment card fraud	57	7,202,735	1.5%	1.2%
Physical loss (lost, stolen or discarded non-electronic records)	471	3,169,581	12.5%	0.5%
Unknown	114	2,930,762	3.0%	0.5%

TYPES OF ORGANIZATIONS BREACHED NATIONWIDE

Description	Data breaches	Total records breached	% of total breaches	% of total records breached
Businesses - financial and insurance services	503	256,217,888	13.4%	42.1%
Businesses - retail/merchant	448	152,224,788	11.9%	25.0%
Government and military	637	148,119,954	16.9%	24.4%
Healthcare - medical providers	920	24,643,419	24.5%	4.1%
Businesses - other	479	14,210,307	12.7%	2.3%
Educational institutions	682	10,695,778	18.1%	1.8%
Nonprofit organizations	93	1,970,736	2.5%	0.3%

SOURCE: Privacy Rights Clearinghouse

PROTECTING AGAINST IDENTITY THEFT

Nearly everyone is vulnerable to identity theft, and there is little an individual can do to protect against third-party data breaches. But there are steps you can take to limit your exposure. Here are some tips:

▨Ensure all portable devices have up-to-date security protections.

▨Use unique passwords.

▨Exercise caution in clicking on pop-ups, advertisements and links in email.

▨Limit the amount of personal information you share.

▨Monitor credit card statements and regularly review credit histories.

▨Alert credit card companies and banks immediately if you suspect identity theft.

TOP 5 DATA BREACHES IN OHIO SINCE 2005

DSW Shoe Warehouse, Retail Ventures	1.4 million
Ohio state workers	1 million
Nationwide Mutual Insurance Company and Allied Insurance	1 million
Ohio State University	750,000
Concentra Preferred Systems	396,279

SOURCE: PRIVACY RIGHTS CLEARINGHOUSE