



THIS MONTH'S TOPIC...

In Enemy Hands: Data Security and the Insider Threat

Notes from our Chairman, Adam K. Levin

Think about all of the “private” aspects of your life that you’ve entrusted to organizations. Your name, Social Security number and address are held by countless banks, utility companies and other creditors. Your private medical history resides in your doctor’s office (if not several others). Many don’t think twice before handing over their “plastic” at a restaurant. And what about all that merchandise you’ve ordered online? It’s funny how our lives can be reduced to simple sets of numbers. And it’s scary how easily those numbers can be manipulated.

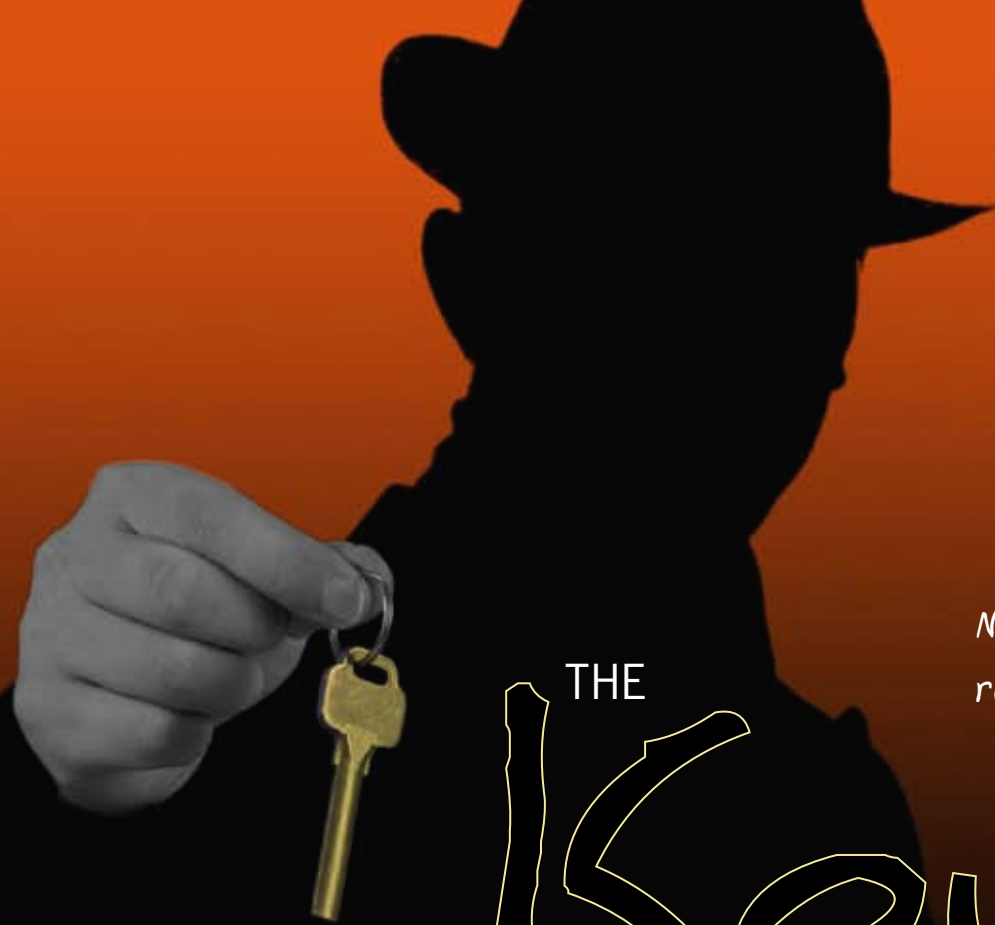
This month, in “[The Keys to the Kingdom](#),” we look at what happens when identity thieves infiltrate the very institutions entrusted with our most sensitive personal data. Thanks to a new study of closed Secret Service files, courtesy of Utica College’s Center for Identity Management and Information Protection, we have a better understanding of the criminal threat posed by “insiders.” This month’s editorial, “[Inside Traitors](#),” tackles whether anything really can be done to stop them.

For a complete newsletter archive, visit: www.identitytheft911.org/newsletters

To learn about the latest scams on identity theft, visit: www.identitytheft911.org

Comments, questions? Contact us: newsletter@identitytheft911.com





*New identity theft study
reveals the insider threat*

THE Keys TO THE KINGDOM

Before four academics from upstate New York were allowed to set foot in the Secret Service's Washington, D.C., headquarters to begin their first-of-its kind identity theft study, they had to abide by a few rules. The first: a background check.



Donald Rebovich, Gary Gordon and two other researchers affiliated with Utica College's Center for Identity Management and Information Protection (CIMIP) did in fact clear the screening protocol. However, they still had to be escorted to and from their workspace each day by personnel from the agency's criminal investigative division as they conducted their systematic analysis of all 517 Secret Service identity theft cases closed between 2000 and 2006. Guests were strictly forbidden—namely, students whose research skills could have sped up the process of their ambitious project, which they began in September 2006 and finished more than a year later, in October 2007.

The Secret Service takes cases referred to it from businesses, local law enforcement organizations, or even everyday citizens who require greater investigative resources than local law enforcement can offer. "A lot of people associate the Secret Service with protecting the president, vice president and heads of state," says

As for the inmate who initiated the scheme, Rebovich asks, "What do you think she was in for?" The answer: "Identity theft."


Secret Service spokeswoman Kimberly Bruce. "They forget it started in 1865 to combat counterfeiting."

The agency declines to provide details on the number of agents assigned to identity theft cases, but a Feb. 25, 2006 U.S. Treasury-produced informational video places the cyber-crime unit alone at 200 agents.

Typically, Secret Service pursues the cases that are more extreme and amount to bigger dollar losses than most other cases. The median institutional or individual dollar loss in the Secret Service cases examined by CIMIP was \$31,356. Separate identity theft studies led by Javelin Strategy and Research and Gartner, Inc., both of which covered a wider range of identity theft cases through telephone polling, estimated losses of \$5,720 and \$3,257 per victim, respectively. While Secret Service data alone may not offer a complete reflection of the identity theft landscape, highlighting instead the more extreme end of the spectrum, it remains an important piece in a larger statistical puzzle. Paired with other studies, the data can help inform federal and local law enforcement in their efforts to coordinate high-level investigative and preventative efforts.

An eye-opening discovery

Instead of offering specific tactical suggestions for law enforcement, the CIMIP study illustrates and identifies issues to help agencies come up with directives of their own. However, by the time the group finished parsing data on the 517 identity theft investigations, Rebovich had come to his



own personal realization, inspired both by the findings and the rigorous internal security protocols imposed on the researchers by the Secret Service. Simply put: Insiders pose the greatest threat to an organization's data security.

"You can have all the best information and security to keep the bad guys away from the outside, but the greatest threat is from the inside," says Rebovich. "I wouldn't say it was surprising, but it opened my eyes a little bit."

In 176 of the 517 cases examined (34 percent) by the Utica College researchers, the "point of vulnerability"—that is, the point at which sensitive identifying data later used for fraudulent purposes was obtained—was the offender's place of employment. These included cases in which wait staff brought their own credit card "skimmers" to the restaurants where they worked in order to steal customers' account numbers; where employees of doctors' offices took advantage of extraordinary access to patients' personal data; and where car salesmen stole personal identifying information from loan applicants in order to "lend" themselves potentially lucrative identities.

"The commonality is that it's often the person who is inside the organization that has a legitimate reason for being there and uses that right to gain access to information that is [used for criminal purposes]," Rebovich says. "All of them eventually figure out that no one is looking—'I have access to this information, and I can make more money in this job'—some would say 'this miserable job'—and they decide to take advantage of it."

Insiders and their outside network

By virtue of their access, insiders can make their hits without the same barriers to entry as those trying to obtain sensitive data from the outside. In many cases, Rebovich says, the early successes of those perpetuating insider-based identity theft schemes caused them to bring others into the fray. "A person on the inside says, 'I can make it big taking advantage of personal information,' and it works," Rebovich says. "When we talk about small criminal groups, that's where they start."

"Insiders" also remain an attractive commodity for criminals operating outside of organizations. In one Secret Service case cited in the study, a candy store employee who was caught skimming credit card numbers said that he was being paid by someone to do so. In 42 percent of the total cases examined by Secret Service, there was some "group activity" behind the crime, Gordon says, while the dollar loss tended to increase proportionally to the number of people involved.

In another case, Rebovich says, a state agency had outsourced the job of entering state workers' personal information into a database to a group of prison inmates. "They took every precaution to make sure inmates could not retrieve information and use it to steal identities," Rebovich says, referring to safeguards set up within the automated data entry system

itself. "One thing they didn't count on was searching prison inmates when they went into the computer area. One inmate decided to take a pencil and paper in." And that was all that was necessary to transform

In one Secret Service case cited in the study, a candy store employee who was caught skimming credit card numbers said that he was being paid by someone to do so.

an otherwise mundane job into a criminal enterprise. The inmate copied state workers' private identifying information, while an accomplice on the outside used the information to set up new credit card accounts, according to Rebovich.

As for the inmate who initiated the scheme, Rebovich asks, "What do you think she was in for?" The answer: "Identity theft."

The usual suspects

Identity theft committed by insiders occurred "most often among offenders employed in the retail industry—"stores, gas stations, car dealerships, casinos, restaurants, hospitals, doctors' offices, hotels and the like"—with such incidents accounting for 77 of the 517 documented cases, the CIMIP researchers found. Private companies were next, in 36 of the identity theft cases investigated by Secret Service. Interestingly, banks and credit unions clocked in third in the types of companies assessed, with 30 Secret Service cases between them.

In terms of fraud prevention, Utica College's findings underscored a key and perennially difficult challenge for organizations charged with safeguarding sensitive consumer data. How do businesses, educational institutions and government agencies ensure that Social Security numbers and credit card information don't go out the door with ill-intentioned employees? Is it even possible to monitor the use of sensitive data among workers without hindering day-to-day operations that require it?

Personal data as highly classified information

For starters, failing to adequately define what constitutes sensitive information and how it should be handled is a problem that, unfortunately for some businesses, is discussed only too late—after a security breach. Most insider-related data loss incidents reported by the FBI resulted

from “poor corporate policies or lack of organizational definition of what constitutes sensitive information,” according to an article published last September in E-Commerce Times by Anne Bonaparte, president and CEO of Tablus, a San Mateo, California-based data security consulting company.

Beyond that, the one obvious thing businesses can do better is to screen employees with access to sensitive data, just as the Secret Service screened the CIMIP researchers. “They wouldn’t have allowed us to set foot in that building [if] they didn’t have total trust in us,” Rebovich says.

And just as the Secret Service case files provided to the researchers didn’t include victims’ Social Security numbers—because, for one, that data had

no bearing on the Utica team’s study—businesses should maintain only the data that they absolutely require. Card retention policies dictated by the Payment Card Industry standard are an example of guidelines for determining what type of credit card

The one obvious thing businesses can do better is to screen employees with access to sensitive data, “They wouldn’t have allowed us to set foot in that building [if] they didn’t have total trust in us,” Rebovich says.

information to hang onto and for how long. Maintaining unnecessary data only adds to the risk.

Employees with such access should agree to other increased security protocols, experts say. Speaking to Identity Theft 911 last November, former Los Angeles Deputy Police Chief James McMurray, who also sits on Identity Theft 911’s advisory board, suggested that such “confidential” employees should agree to continued background monitoring—inquiries into current relationships and ties to those with criminal records, for example—and that they should be exempted from participation in labor unions.

McMurray and others recognize the inherent dilemma—that protecting the privacy of the many may require some infringement upon the privacy of the few. One way to mitigate this is to offer financial incentive for agreeing to more rigorous screening procedures. In other words, “confidential” employees could be offered more money.

Telltale signs

Rebovich, who previously served as research director for the National White Collar Crime Center in West Virginia, a Congressionally funded non-profit group that helps state and local law enforcement agencies tackle economic and cyber crimes, adds that it would be a mistake

for organizations to see a security breach as the “start” of a problem. Oftentimes, he says, employees who breach security internally are those who wear their disappointment and lack of enthusiasm for their job on their sleeve. Secret Service case notes revealed that in some cases, perpetrators were “either ready to get fired or ready to leave,” Rebovich says. “They can’t stand what they’re doing and they want to take a piece of the organization with them.”

But that’s not to say each was scraping by on minimum wage. “People in middle management commit these offenses as well. That was something that struck me,” Rebovich says.

Gordon says that he hopes that CIMIP, which he founded in June 2006 to conduct studies intended to help law enforcement agencies and policy-makers combat identity-related crimes more strategically, will be able to further study incidences of insider compromise.

Rebovich says the experience of poring over the files has made privacy issues more salient to him in his own life. “If you really want to be sure that

“It’s an outgrowth of our modernized society that there are so many places where we have personal information. We as individuals can try to prevent identity theft by shredding, etc. But, we’re at the mercy of organizations that have our personal information.”


the waiter or waitress is not taking a credit card to another swiper, you’d have to follow them and watch. But who’s going to do that?” he says. “It’s an outgrowth of our modernized society that there are so many places where we have personal information. We as

individuals can try to prevent identity theft by shredding, etc. But, we’re at the mercy of organizations that have our personal information. They’ve got the keys to the treasure...Sometimes, they give the keys to people within the organization and they don’t realize the value that it represents.” ■

More on the **CIMIP** Study

Beyond being the first systematic analysis of U.S. Secret Service identity theft cases, CIMIP's study also seeks to reconcile a shortcoming identified by the President's Identity Theft Task Force Report released this past April. Rather than focus on victims, the study presents a snapshot of offenders themselves.

Though not a complete picture (the report covers only 517 closed cases of identity theft over a six-year-period; the technology research company Gartner Inc., by contrast, estimates that 15 million Americans were victimized over a 12-month period alone), the CIMIP study does provide a fresh look at the perpetrators of identity theft, assessing their background, modus operandi and the disposition of their cases. **The study's key findings include:**

- 
- **47 percent of Secret Service cases are referred to by local and state law enforcement agencies. Corporate security and/or fraud investigators referred 20.4 percent. "That's one of the things we found very encouraging," says Gary Gordon, the study's lead researcher. "There's a great deal of cooperation already out there."**
 - **The median actual dollar loss to victims, which the study defines as individuals as well as organizations that incur losses, was \$31,356. "Again, we reported the median," Gordon says. "In some cases, the actual loss ends up being zero. In one case, the loss is 13 million."**
 - **In 42.4 percent of cases examined, groups of anywhere from two to 45 offenders were involved in the commission of the crime. "Interestingly enough, the dollar loss increases as the number of people involved in the crime increases," says Gordon.**
 - **In 50 percent of the cases, perpetrators used the Internet or technological devices to assist in their crimes**
 - **Most offenders (42.5 percent) were between the ages of 25 and 34 when the case was opened. The next biggest age brackets included 35 to 49-year-olds (33 percent), 18 to 24-year-olds (18.5 percent), and those over the age of 50 (6 percent). About one-quarter of the offenders were born outside of the United States, while 71 percent had no prior arrest history.**
 - **Half of the defendants were sentenced to incarceration, usually in combination with probation and restitution.**

So what's next for CIMIP, whose partners include investigative agencies like the Secret Service, U.S. Marshal Service and Federal Bureau of Investigation, research institutions like Carnegie Mellon, Indiana and Syracuse Universities, and private enterprises like the credit reporting bureau TransUnion, LexisNexis and IBM?

Gordon hopes to eventually probe more deeply into specific phenomena like insider points of compromise, and to examine data sets from other local, state or federal law enforcement agencies outside of the Secret Service. "We want to see if the trends we've found here are similar in nature." ■

Inside Traitors

By Adam K. Levin

As the national news media rightfully continues to home in on the dangers of hackers breaking into organizational databases, there remains one threat that businesses and other institutions often overlook, a challenge just as salient and, in some ways, more problematic. It's the risk posed by corrupt insiders.

The phenomenon spans the history of human drama—from the Biblical narrative of Judas Iscariot to Shakespeare's *Macbeth*, to filmmaker Martin Scorsese's more recent gangster epic, "*The Departed*."

For institutions that warehouse sensitive data, employees who steal are a disastrous wild card. A business or government agency can do everything within its power to fortify its databases against outside intruders, but if it fails to take the same defensive measures against insiders, any potential intramural schemes bent on exploiting those weaknesses can enable criminal employees to raid databases with relative ease. Then, unsuspecting consumers are left to salvage their credit and identities largely on their own as organizations struggle to mend their customers' broken trust.

For institutions that warehouse sensitive data, employees who steal are a disastrous wild card.

Consider the numbers from the recent study by the Center for Identity Management and Information Protection: of the 517 identity theft cases investigated by the U.S. Secret Service between 2000 and 2006—among the worst identity theft cases under investigation—176 of them (that's 34 percent) were perpetrated by someone working within the organization. Not surprisingly, restaurants and gas stations, where credit cards are constantly switching hands, stand among the most vulnerable establishments, as do doctors' offices and car dealerships, where an abundance of private identifying data is readily at a corruptible employee's fingertips.

This brings us back to the mantra familiar to those working in the trenches of identity theft protection: an institution's security is only as good as its weakest link. While a twenty-foot-high electric fence may keep the bad guys out, it does nothing to dissuade the criminals working within. Data security is no different. Protocols designed to mitigate foul play internally are just as important as those designed to prevent hacking from abroad.

The circumstances may seem outside of many business administrators' purviews—how can one employee prevent another from running off with potentially valuable customer information?

While it's true that short of a crystal ball, there is no surefire way to predict or completely prevent employee-related identity theft (or any type of identity theft, for that matter), there are ways to mitigate it. And it doesn't need to involve Orwellian systems of internal surveillance. As with any good business strategy, a combination of pragmatism and emotional tact can provide a solid foundation for data security protocol.

Store only the data your business needs

Consider first the factors that exist within an organization's control. This would include the information that is itself being collected. Earlier this January, after TJX experienced its monumental data security breach that left approximately 94 million credit and debit card accounts exposed to computer hackers, one of the more troubling questions the company found itself being pressed to answer was why it was storing unencrypted debit and credit card numbers in the first place. According to Payment Card Industry standards, the self-regulatory guidelines advised by Visa and MasterCard, unencrypted data should never have been maintained. Keeping only the information that your business needs on a day-to-day basis is the critical first step.

Limit internal access to data

Limiting employee access to sensitive data, and performing stringent background checks on those who do have access to it is a logical follow-up safeguard. Temporary workers should be similarly screened if they'll have access to sensitive personal data. Some may argue that such measures seem excessive, but background screening of employees who handle financial and private data is no different than screening a pilot for sobriety before takeoff. The risk to the greater populace justifies a minor intrusion on the privacy of the individual. For those handling sensitive private information, we should expect and *demand* a baseline of moral competency. Unfortunately, in a marketplace of increasingly disposable minimum-wage tasks, for some the

most direct route to material accumulation is through the quick and immediate strike of identity theft and credit fraud.

Evidence from the CIMIP study suggests that employees who are dissatisfied with their jobs are more likely to steal from employers without remorse. And while this would imply that more attention ought to be paid to employees who seem disgruntled or unmotivated, the inverse of the statement should also be considered—that a positive, reinforcing work environment, paired with proper security training, can be a great deterrent to employee crime. It's not difficult to understand why somebody would have a harder time ripping off somebody they like. Likewise, employees who care about their jobs may be more likely to act as whistle-blowers when they spot suspicious behavior among co-workers.

While a twenty-foot-high electric fence may keep the bad guys out, it does nothing to dissuade the criminals working within. Data security is no different.

If nothing else, the CIMIP study should serve as a stern reminder to businesses and institutions that they must establish clear-cut rules in the workplace—uncompromising policies concerning data storage, disposal and equally important, access. In fact, they should pay attention to how the Secret Service treats personal data—as highly classified information—and follow suit. ■