A Hacker Breaks In—Lessons Learned
From a True Story

By Zhu Wenming, CISA, Hu Hanhui and Wang Hao

This is a true story about an investigation in which the authors are involved. Due to the complexity, volume and vulnerability of the nature of business, it could happen again in the future. Therefore, it is important to arouse people’s awareness and start to reconsider, review and redesign the risk management system. (For privacy reasons, the names of the parties in the article have been altered.)

The Story

On 13 January, the Sunday before the Chinese Spring Festival, people in Shanghai were enjoying the last weekend of the lunar year. A week later, they would have a one-week vacation to celebrate their most important holiday of the year. However, the call center of SOME Bank, a mid-sized bank in the city, was busier than ever. People were preparing the New Year foods, clothes and gifts, and they needed help when using bank services. Miss Rosie, a young representative, had just finished the 20th call of the morning, during which she successfully taught a grandmother how to extract money from an automated teller machine (ATM). The busy lamp turned to red again, and Rosie pushed the connect button.

“Hello! May I help you?”
“I lost all my money!”

Rosie tried to comfort the customer:
“Don’t worry. We will look into it right now and see what happened. Please believe me that your money will be safe. Now tell me what happened.”

The customer, Mr. Rich, said that in checking his account through Internet banking, he was astonished to find that the account balance had shrunk to several dollars, when, a week ago, the balance had been more than US $100,000. Rosie wrote down all this information, as well as Mr. Rich’s contact information. She comforted the anxious man again, telling him that everything would be fine.

The Investigation

Within 15 minutes, Mr. Rich’s case was escalated to Mr. Simpson, operations vice president of the bank. After a short call to the CEO, in which he briefly explained what had happened, he launched the contingency management process. Though it was still the weekend, he had to call together the head of related functions, including IT, internal audit, Internet banking, customer service, security and law. He explained what had happened and set up a committee. Members of the group came from each of the functions. The responsibility of the group was to find out what happened and how, evaluate possible loss, take quick action, and minimize the negative impact.

All the members were included in a mail group to enable instant communication during the investigation. Tasks were assigned to each member as follows:
• Internal audit—Investigate when, where and how the money disappeared, report possible loss, and work with police (if involved) to find the perpetrator.
• Information security—Conduct a health review of the Internet banking system, find possible loopholes, and make a quick fix.
• Customer service—Soothe the customer and minimize the involvement of the media. All service channels, including the call center, were told to be extra vigilant and to send any similar cases directly to the group.
• Public relations—Evaluate the necessity to report the incident to the police and regulatory body, and make proper response to all parties involved.

Two days later, the findings of the investigation team were finalized:
• The computer records showed that the money was transferred to another account in the same bank two days earlier. The odd thing was that the transaction code of the transfer was “Internet transfer between same holder’s accounts,” which meant that the transfer occurred between accounts registered under the same holder, while the actual account holders were different people: Mr. Rich and Mr. Thief. Obviously, Mr. Thief’s information was falsified. It seemed that the perpetrator had bypassed the “same person’s accounts” verification control.
• All transfers took place at midnight for US $10,000 per day (the daily maximum for Internet transfers). The first transfer began with many failed attempts and ended with a successful one. The following transfer succeeded easily with fewer attempts. A full search showed that the same thing happened to four other customers, with a total loss of about US $1 million.
• The day after the money transfer, the money was extracted from Mr. Thief’s account (as well as other destinate accounts) through ATMs throughout the city and at branch counters. It appeared that was done because ATM extractions are limited to US $5,000 per day, while counter service sets no limit.
• Every branch was equipped with continuously running video cameras. The archived video recorded a young man taking the money. However, because of the man’s intentional disguise (cap, glasses, wig) and quality of the video, it was hard to tell his exact appearance.
• By analyzing the web server’s access log, the auditor found that the attack came from several IP addresses. According to the router table, these IPs belonged to a network café. The frequency of visits to a certain page was as high as thousands of times per hour.
The security officer who conducted a health review of the Internet banking system reported the following serious security weakness:

• Though the system locks the account after five successive wrong password attempts, it sets no limit for wrong account number input. For example, one could enter a possible password, such as 123456, to guess different account numbers, until a corresponding account was found. The system could not identify and report this exception.
• On the login page, no artificial verification code was used, which meant one could employ a robot (a specially designed program to perform functions automatically) to conduct brutal cracking.
• Poor session management resulted in the same session ID being shared among all web pages during one’s connection. One could copy and reuse a previous ID before it expired to bypass the account verification and log in to the system.
• The validation of “same holder’s accounts” did not take place on the server end, but on the front end through an HTML page, making it easy to be compromised.
• No process was in place to analyze and monitor transactions. The investigators could now determine how the break-in likely happened:
  • Step 1—Someone connected to the Internet banking server and ran robots to discover the account and password combination.
  • Step 2—The attacker then logged in to the Internet banking system with the cracked account/password combination and launched the “transfer between same holder’s accounts” module. (He noted how a session was established between the local computer and the Internet banking server, and a session ID was available on the local computer.)
  • Step 3—The attacker saved the page from step 2 and modified the script’s program logic to bypass the “same holder’s accounts” validation, so the unexpected operation data (accounts of different people) could be accepted.
  • Step 4—Before the session ID expired, the session was still active. The altered page submitted the transfer instruction with the unexpected data, and the server accepted and executed.

How to React

Now the bank management had enough information to make a decision—before a final decision was made, some factors needed to be taken into consideration:

• It was hard to estimate the risk of a potential attack. Since the perpetrator had successfully cracked five accounts, theoretically he could have cracked more, which could be used to launch more attacks. With account/password combinations, there are other ways to steal money besides through Internet banking.
• The perpetrator chose the timing of the attack because with the upcoming Spring Festival, the bank would cease operation for a week. He would have abundant time to steal money without disturbance.
• The Spring Festival is the high time for business. Unwarranted banking service could ruin customer experiences and damage the bank’s reputation seriously.
• External regulation needed to be considered; modification and termination of any banking service should be subject to the approval of the China Banking Regulatory Commission (CBRC).

After a balanced consideration, the committee announced the following action list with due approval:

• Report to the police and regulatory body immediately, and ask for their assistance and suggestions.
• Identify and freeze all possible violated accounts. Violated accounts were defined as those showing recent password change, abnormal access frequency, etc. The holders were asked to change the password immediately.
• Apply quick fixes to all loopholes detected in the system. Until then, some functions were closed with the approval of CBRC.
• Compensate the customer’s loss since the loss was not the customer’s fault.
• Require those in security and transaction monitoring to be on duty when normal operations cease during Spring Festival.
• Create a public relations management plan and develop standard announcements.

Luckily, bank management had a peaceful holiday. No more bad news was reported. A month later, the police arrested the perpetrator, a young engineer of an Internet company and a former employee of the Internet banking system vendor—which explained how he knew about and exploited the loopholes.

Lessons Learned

The particular story is over, but the risks still exist. What this story teaches is that a comprehensive management policy should exist to mitigate the risk. The policy should include:

• Risk awareness at all levels, reminding us that any business is subject to vulnerabilities. The awareness should be part of the organization’s culture and fostered through education.
• A process to define, monitor and identify abnormal events from all channels, including customer service, transaction monitoring, internal audit and security. Exception monitoring should be part of daily work.
• A standard report and escalation procedure, to ensure that management knows what happened.
• Emergency procedures and quick responses. High management commitment and cooperation among functions are important.
• Provisions for a team with strong investigation and analysis skills. The members may come from IT audit, information security functions, etc.

Zhu Wenming, CISA

has nine years of experience in information systems audit. He is pursuing a Ph.D. degree from Southeast University (China) and is an IT audit project manager with Pingan Insurance Group. Prior to Pingan, Wenming worked for e-government and private sector organizations. He can be reached at mzhw@gmail.com.

Hu Hanhui

is a professor of management at Southeast University. He can be reached at huhu@seu.edu.cn.

Wang Hao

is an associate research fellow at Nanjing Audit University (China). He can be reached at why@nau.edu.cn.