

# Hacking

James L. Horton

The CIO was frustrated. The bank's credit card files had been hacked again, and this time 50,000 names and numbers were stolen. The CIO had struggled with a security breach for three months, since the loss of 100,000 names and credit card numbers. Computer security experts had discovered the initial intrusion when they found the credit card information offered for sale on a hacker's channel. The bank had sent notices to the 100,000 and assurances that the bank would make good losses from stolen data. Thus far the bank had paid out \$147,000.

Now, here was another theft. The CIO was certain the hack was the result of spear phishing. Someone, or a gang, was sending fraudulent e-mails to bank executives and getting them to click on an enclosed file laced with malware. The malware was exploiting the bank's security system internally. The CIO had ordered security training seminars and had reinforced the company's firewall. But, it was up to employees to check incoming e-mail headers and to avoid clicking on attachments until they checked with senders. The new attack would be another public embarrassment for the bank, which had lost customers from the earlier invasion.

The CEO had called the CIO into a meeting to discuss the issue. It was a meeting the CIO did not want. He met with his chief security officer and reviewed bank procedures. His CSO thought the hacks were the work of one person. He cited the case of Lin Mun Poo, a Malaysian man convicted of entering Federal Reserve computers. (Poo had been caught with stolen credit card numbers that he did not get from the Federal Reserve and was serving a sentence of 10 years in prison.)

"Someone is out to get us," the CSO said.

"Who?"

"We don't know but we've tracked him through computers in Russia and China. He covers his tracks."

"That doesn't help."

The CIO told the CEO what his department was doing to stop the attacks. The CEO was not mollified.

"I'm facing shareholders in 10 days, and they will ask about it. I need assurances that we've stopped this guy – or gang."

The CIO couldn't provide the CEO comfort, but when the bank announced the new breach, it had a lucky break. On the same day, a credit card company announced it had lost 400,000 customer numbers. The bank's disclosure was subordinated in news stories.

The CIO was aware of a torrent of hacking incidents. Thieves were targeting banks and credit card companies globally, and hacking had become a cost of doing business. The CIO was working with the FBI and consulting security services on the bank's incidents, but so far little was helping. The Internet Crime Complaint Center was registering nearly 27,000 intrusions per month, more than any law enforcement agency could handle, and the bank's breaches were small by comparison.

The CEO answered eight questions related to bank data security in the annual shareholder's meeting. All were hostile. The CEO assured everyone the bank was doing all it could to stop illegal entry, and he hoped to show progress through the remainder of the year.

"If you don't hear anything, that will be the best message," he said.

The CIO launched a new effort to prevent further data theft. Employees from senior executives to tellers were retrained. The corporate communications department conducted a campaign on the bank's intranet, and placed posters prominently throughout bank facilities urging employees to be wary of suspicious e-mail. It didn't work because customers were the next target. This attack was through phishing using e-mail, a lookalike bank web page and malware called Zeus. Zeus is a keystroke logger that steals a consumer's bank information and sends it to the hacker. The thief was sending official-looking bank notices with a link to the phony web page. When customers clicked on the link, the page appeared but Zeus was downloaded to their machines at the same time. The irony was the phony web page was a warning against hackers.

When the bank became aware of the Zeus attack, it sent notices globally to 300,000 customers but losses were heavy – at least \$7.4 million by the bank's estimate. The CEO was angry but there was little the CIO could do. The attack had taken place outside of the bank's security perimeter.

The CEO tasked the SVP of corporate communications with conducting an informational campaign to customers. The SVP and her team rolled out postal mailers (or bill stuffers), HTML-encoded e-mails, print and TV advertising. There were two messages -- be wary and the bank would not hold customers responsible for illegal activity in their accounts. The campaign, which ran three months, was a success in that reports of illegal entry dropped nearly 70 percent, but they didn't disappear.

Six months after the communications campaign, the hacker(s) attacked the bank again. This time he was foiled, but the CSO considered himself lucky. He knew there could be an intrusion that hadn't been discovered. As the CSO said, "It pays to be paranoid." The CSO was a daily reader of Bugtraq (<http://www.securityfocus.com/archive/1>) and frequently attended seminars on network security. He knew the bank's systems weren't sufficiently protected, especially after a merger with a smaller bank whose systems weren't compatible. He and the CIO were working daily on closing gaps.

The CSO was still stunned when the controller of a corporate customer called to ask why \$5 million had gone missing from its accounts and had been wired to Russia. It had been a hack that had run for weeks and siphoned money into 100 drop accounts in Moscow and St. Petersburg, all of which had been emptied within hours of the funds' arrival. The CSO and CFO were ordered to the CEO's office. They couldn't explain at first what had happened. In a matter days, however, it was discovered that someone had exploited the smaller bank's payment system. The exploit was stopped as soon as it was discovered.

The CEO was resigned as the FBI explained to him that the hacker(s) was beyond reach and likely somewhere in central Russia. The CEO ordered the CSO and CFO to review again the bank's security policies and procedures from top to bottom and to report within 30 days. Meanwhile, he had to disclose the new loss in a SAR (Suspicious Activity Report) to the US Treasury Financial Crimes Enforcement Network and to shareholders because it was material. He called in the general counsel and the SVP of corporate communications and asked their advice for how to make the disclosure.

# # #

Questions to answer:

1. How can the SVP portray the new hacking incident in a way that does not damage the bank's reputation for the long term?
2. What is the ongoing role, if any, for communications in bank security?
3. Write the announcement that discloses the bank's loss.
4. What would you do next to make the bank more secure?