Instructional Case of Insider Threat in the SDLC: The Case of InsureACure, Inc.[1]

CERT®[2] Program – Software Engineering Institute
Carnegie Mellon University

Introduction

An irate Oliver bounded into the plush office of Hugh, the director of HR, and demanded an immediate investigation of the Development Team's personnel for fraud. Their company, InsureACure, is responsible for processing medical health insurance claims by government workers.

"Someone on Danielle's team has corrupted our databases and allowed payment of thousands of dollars in false claims," complained Oliver.

"Calm down, calm down," said Hugh cautiously. "Tell me what has happened."

Trying to calm down, Oliver explained that somebody had changed the address of a legitimate medical service provider (MSP) and had been sending reimbursements for false claims to that address. "The total losses are in the thousands of dollars," explained Oliver. "No one in my department knows anything about it, but I'll bet one of those geeks in Danielle's group does!"

"Have you talked to Danielle," queried Hugh.

"You bet I have, but she's just stonewalling, claiming that it had to be somebody in my group who made the change. She won't even consider the possibility!" Just then Oliver's cell phone went off. Looking at the number of the incoming call, Oliver said, "Oh, this is IT, just a second …"

Oliver listened as the IT staff member reported that they had found an additional nine incidents in the audit logs of MSPs that had been inactive for more than two years followed by a change of address and frequent claims for reimbursement. In addition they discovered that the address changes in all of the cases were made by the Director of Operations.

"The Director of Operations," exclaimed Oliver incredulously. "But that's me!"

Background

InsureACure was established in 1993 to provide information and computing services to the burgeoning health care services community. Its first big contract was to process the

[1] The InsureACure organization and case example are fictional; any resemblance to a real organization or insider threat case is unintentional.
[2] CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

medical health insurance claims of government employees. InsureACure submitted checks for validated claims paid out of the government coffers.

InsureACure hired an experienced management team to support the business (see org chart at end of case). Critical support for InsureACure business processes was provided by the Health Insurance Claims Processing System (HICPS). The company's managers included:

- *Oliver* – the Director of the *Operations Department,* responsible for validating, entering, and managing claims using the HICPS application
- *Danielle* – the Director of the *Development Department,* responsible for the developing and maintaining the HICPS application
- *Hugh* – the *Human Resources* representative

Frank was hired in January 1994 by Danielle as a lead application designer and programmer for HICPS. Although Frank started a side business in 1998 selling custom-configured computer systems, he was a dedicated employee, proficient and productive developer, and personal friend of Danielle's.

The Initial Contact

In early December 2000, Johnnie called Frank at home. Johnnie had been Frank's roommate in college. Johnnie claimed that he was a consultant in the medical field, working with medical providers to determine optimal insurance plan participation. Johnnie explained, "If you could get me the names and addresses for MSPs that have not submitted claims in the last few years, it would provide very good leads for my business. I could then help those MSPs generate more business and that would help government employees get better rates and coverage. It would be good for everyone involved!"

Frank began to object, but Johnnie interrupted with, "Of course, this would be worth a lot to my business – and I'd certainly make it worth your while as an old friend."

Frank left Johnnie with a "Well, let me think about it." After Frank got off the phone Rose, his wife, asked who he was talking to. Frank explained the situation.

Rose shot back, "Well, I don't see what there is to think about. If this is going to help out people that you are supposed to serve, and we can make some money as well, there seems to be no downside. And besides," she continued to press, "your side business isn't exactly thriving, you know. If you can't make ends meet soon, you're going to have to give it up."

This hit a raw nerve for Frank. He'd hate to lose his business – and it didn't seem like helping Johnnie would really hurt anyone. People at work knew his business wasn't doing well, and his self esteem couldn't withstand actually losing it. In addition, the winter months were especially difficult with heating bills for the business and the holidays.

The Compromise

Frank accessed HICPS directly (no remote access was permitted to InsureACure's network) and emailed to Johnnie contact information for three MSPs that had not

submitted any claims in the last two years. The next day Johnnie mailed Frank $1000 with a thank you and a request for more addresses.

A couple weeks later, in mid-December, Johnnie called Frank at home and reported that he had just secured the business of two of the MSPs. “Thanks again Frank,” said Johnnie. “Would you be able to update their addresses in the InsureACure system so I could start serving them more fully? It would be worth over $10,000 dollars of business to me and I’ll certainly show my appreciation.”

Frank replied, “That would be difficult because addresses can only be modified by authorized accounts, but I’ll see what I can do.” The initial $1000 was nice, but more money would help get his business to a point where he could really make it a success.

Frank knew that only certain members of the Operations Team were authorized to change information about MSPs in HICPS, and that an email notification was sent out to a supervisor for online approval when such a modification was made. Therefore, there were several hurdles to overcome:

a. *Overcoming role-based access controls in HICPS application* - Since Frank had access to the DBA account, it was a simple matter for him to insert a row into the role-based access controls table giving the DBA account the additional privilege needed to access the HICPS application. Frank chose to insert the DBA account rather than his own, since the shared DBA account would not be traceable directly to him.

b. *Disabling the email notification to the supervisor* - Because Frank had written the programs in HICPS used to add and change MSP data, he knew how to modify the *ChangeMSPAddr* program to disable the email notification, and that’s exactly what he did. He then released the modified code as the production version.

c. *Performing the online approval process* – There were several alternatives for getting around the approval process. The cleanest way would follow the normal process, and therefore avoid arousing suspicion, and also conceal Frank’s identity in the system logs. For this plan, Frank would need the password of an authorized Operations Team supervisor. Since passwords were required to be changed every three months, he was able to determine that one of the supervisors would be required to change their password within the next two weeks. Frank modified the “change password” program so that after the supervisor entered their new password, it saved the password to a file in clear text before proceeding with the usual encryption process.

Frank’s plan worked. On December 20th, Oliver changed his password and the plaintext password was saved to a file on Frank’s machine. The following week, while most employees were away on the holiday break, Frank went into the office, used the DBA account to change the MSP addresses, as requested by Johnnie, and then logged in as Oliver to complete the online approval process.

With the modified *ChangeMSPAddr* program, no one was notified of the change of address. However, Bob, one of Frank’s co-workers, happened to notice in the transaction logs that someone had accessed the database using the DBA account. Bob queried Frank, “Hey Frank, why did you access HICPS over the holiday?”

"What makes you think it was me?" Frank replied defensively.

Rather cowed by Frank's negative tone, Bob stuttered, "Well … as far as I know, you were the only one at the office that day."

"Yeah, well I was just debugging a problem, that's all" replied Frank, curtly ending the conversation.

Bob was suspicious, but didn't report it since he didn't want to be seen as "telling on" a co-worker.

Over the next six months, Frank continued to provide Johnnie with inactive MSPs, and to change addresses when requested using the same method described above. He supplied Johnnie a total of 15 MSP addresses, changed 10 of those 15 to an address provided by Johnnie, and received a total of $10,000 for his effort. During this period Johnnie submitted nearly $1 million in fraudulent claims, cashing reimbursement checks at organizations that didn't require identification. Frank frequently considered getting out, stopping his dealings with Johnnie, but felt that he was in too deep to quit. Frank was able to pay off the debts that his business had accrued and took a nice family vacation to the Caribbean to boot.

After his vacation, Danielle dropped by Frank's office to ask about his vacation. "Hi Frank, How's it going? How's Marlin doing in college?"

"I'm fine. Our vacation to the Caribbean was great! Marlin's doing great as a senior now, and Gil just entered as a freshman last August," replied Frank.

"Wow! That must be tough having two kids in college at the same time!" Danielle thought it was a bit strange that Frank had taken such a lavish vacation with two children in college, but thought it was none of her business, and put it out of her mind as she went on to deal with the everyday pressures of her job.

The Discovery and Cover-up

On July 9, 2001, an MSP called the InsureACure customer support line with a question about the appropriate codes to use for a procedure for one of its patients. "Sure, I can help you. Let me pull up your file on my computer." The help desk attendant reviewed recent transactions for the MSP, "It looks like you had several claims filed over the past quarter, but they look to be very different codes than what you are asking about."

The MSP nearly leapt out of the telephone, "I have WHAT filed? I haven't filed a claim for eons! I've been on leave from my clinical practice to conduct research at a university. What do you mean I have filed claims? How can that be?"

Feeling the heat, the help desk attendant said, "OK, let me get your contact information and we'll investigate this issue and get back to you." After writing down the MSP's address, he realized it was not the same as the address in HICPS, but decided not to mention this to the caller. "We'll get back to you as soon as possible."

Later that day, Frank overheard a conversation in the lunchroom about the discrepancy with the MSP. He panicked! To cover his tracks, he recompiled the *ChangeMSPAddr* program with the email notification re-enabled, and released the change into production. Frank also removed his account from the role-based access controls table.

In order to wipe out all record of the altered *ChangeMSPAddr* program, he then instructed Tim, the Development Team's backup manager, to initialize the backup tapes, stating that "they won't be of any use in the future since we're changing to a new data format." Tim began to initialize the tapes, but stopped when Danielle became aware of what he was doing and told him to stop. Tim explained that Frank had instructed him to do so. Danielle knew that made no sense, and had meant to confront Frank about it, but never got around to it.

At the end of the week, at the Operations Team meeting, the help desk personnel described the problems with the MSP's transaction history to Oliver. "Why did you not inform me of this problem right away?" asked Oliver.

"We have small glitches with HICCUPS all the time," said one help desk attendant flippantly. "A problem with one MSP doesn't seem like a major emergency."

Obviously not amused by the derogatory reference to the system as HICCUPS, Oliver shot back, "Well how do you know that the problem isn't more pervasive!" Dealing with the immediate problem, Oliver asked Tina, an Operations Team staff member, to investigate the discrepancies in the MSP's claim history and to report back to him by the next day.

The Investigation

The next Monday, July 16th, Tina used a screen in HICPS to review all claims for the MSP under question. That afternoon she met with Oliver to report her findings. "There was a total of $95,000 in claims paid for that MSP over the last year. I don't see anything out of the ordinary with the MSP claim transactions," reported Tina. "But to review the change of address transactions, we'll need to look at the database logs, and for that we'll need to go directly to IT."

Looking at the claim history, Oliver noticed, "The claim codes for this MSP do not even match the MSP's specialty." Oliver called Danielle in IT asking to see the database logs for changes to the address information for that MSP.

For the rest of that week, Oliver went around and around with IT trying to get the database logs, but IT said, "It is going to take some time to extract the transactions of interest. We've got a lot of pressing work, with the new upgrades of our Windows machines."

When IT finally provided the logs, it became clear that the suspicious claim transactions for the MSP immediately followed a change of address for the MSP. Oliver commented, "This looks pretty suspicious; please review the transaction logs for similar patterns of activity as soon as possible." That was Friday afternoon, July 21st.

Oliver scheduled a meeting to follow-up with Danielle first thing Monday morning. Bypassing any exchange of pleasantries, Oliver got right to the point, "How could changes to the MSP addresses have been made without someone knowing about it? Nobody in my group knows how or why these changes were made."

Danielle pulled up the program to modify MSP addresses. "This program looks fine but the *ChangeMSPAddr* program was just recently updated." Mumbling under her breath,

she added quietly, “Unfortunately the backups of previous versions are not available to be able to see what changed.”

At that, Oliver blows up, “WHAT? How is that possible? Why in the heck don’t you have backups?”

Realizing the difficult spot she was in, Danielle added defensively, “We are in the process of upgrading our backup system and had a mix up with the backups and they were accidentally overwritten.”

Clearly perturbed, Oliver asked pointedly whether there was anybody on staff who had motive to tamper with the backups – clearly implying criminal actions by one of Danielle’s Development Team members. Danielle said “That is out of the question; an Operations Team member must have done it since they are the only ones authorized to change an address of an MSP.” Danielle knows that Frank has been acting strangely, but is reticent to talk more to Oliver because of his temper and for fear of violating the privacy of her team members.

It was after the meeting with Danielle that Oliver decided that he needed to go directly to HR for help. He scheduled a meeting with Hugh on July 31st. After finding out about the additional nine cases of suspicious MSP address changes in his phone call with IT, he told Hugh with great urgency, “It looks like we may have hundreds of thousands of dollars in fraudulent claims that we have paid out over the last year, and according to the logs, my account was used to approve the address changes associated with the fraudulent charges. The address changes were made by someone using HICPS, but we don’t know who. You have to believe me Hugh … I know nothing about this. Please help me track down who did this and how they did it, so that we can prevent it happening again.”

InsureACure Organization Chart