CYBER CRIME IN THE FINANCIAL SECTOR

A few months ago, I encountered in an article by Ian Rowan at Switched.com reporting the news of a computer consultant that siphoned $1M USD from a Utah Bank. Also Mementosecurity commented the article on April 27th explaining how “An IT contractor hired to fix some bugs in a recent computer upgrade used his system access to make fraudulent electronic transfers into accounts under his control. He allegedly used the funds to remodel his home, pay off his two car notes, and cover a few mortgage payments. The fraud came to light when his business partner reported the suspicious transactions.”

We are talking about “the same old story” that plays over, again and again. Infosec ’s[1] portals are totally filled by this kind of news, ranging from the highly orchestrated organized-crime actions up to the “one-man crime” approach.
Let’s take in consideration a couple of cases, one very recent and the other rather old. This latter one is the LGT case, also known as “The Lichtenstein Tax Affair”.
Mr. Kieber, an employee at LGT Bank, allegedly stole customers’ financial data and sold them to an Intelligence Agency. The peculiar aspect here is that Mr. Kieber was already sought by an international warrant issued by Spain back in 1997 for running a 600.000 CHF check-fraud. A bank, where privacy is the fundamental value to be assured to its customers shouldn’t have hired a man with that kind of “background” in the first place. We may also discuss IT procedures and checks, as well as Counter-Fraud and Privacy security policies and rules used by the violated institution. But that’s not the real point.
The second example I would like to talk about is even more peculiar. In October 2008, a US Payment Gateway(2), RBS WorldPay, was hacked. The attackers hacked into the credit cards (CC) database and, apparently, were able to own it completely. No one noticed the break-in and nothing happened, until a few months later. On January 9th, 2009, a 24-hour withdraw operation was run among three continents (USA, Asia, Europe). One hundred “mules” withdrew $9 million USD in a 24-hour timeframe, leaving no traces behind, except in some cases, where pictures were shot from the ATM’s themselves (http://media2.myfoxny.com/pdf/atmwantedposter.pdf). More than 130 ATMs in 49 cities (from Moscow to

Atlanta, to get the idea) were affected by the attacks.
Curious to say, a nearly identical attack happened in 2007, when iWire (a payment card company) encountered losses of $5 million USD.
Obviously, if a world-wide known bank, a payment gateway and a payment card company have all been somehow "violated", this means that no one can be totally secure: nothing is 100% secure.
Nevertheless, I would like to bring the reader's attention towards other points and thoughts, far from the IT Security's standard approaches. These kinds of crimes will continue, they will never stop. They will increase in number daily, reaching unimaginable amounts of money. Cybercrime, intended as all the various sorts of e-crimes, is the most profitable criminal activity ever seen, much more than international drug dealing and human trafficking. Cyber crime usually involves a few risks, and typically doesn't require the authors to "show up" and physically expose themselves. Also, the de-facto international approach and MO (Modus Operandi) of these crimes complicates the law enforcement agencies' investigations, information exchange, dialogues and collaboration, while the laws and the international agreements among different legislation systems would not always work out, especially in some countries. These countries, obviously, are among those ones preferred by e-criminals.
Just to give the idea, the 2007 "financial turnover" for RBN (Russian Business Network), one of the most important and distributed criminal organizations in the Internet area, was more than $2 Billion USD. RBN has been credited for creating nearly half of 2007's phishing incidents worldwide, being also specialized in the distribution of malicious codes, hosting malicious Web sites, developing and selling specialized malware and 0-day exploits. This means money, a lot of it too.
That's why cybercrime will constantly represent an issue, now and in the upcoming future. That's why I do get amazed when reading news about IT consultants who stole money from their clients, customers or companies they worked at. Frankly speaking, rather than getting shocked, I get angry. Today's world is already filled with bad guys, meaning those people that belong to the well-known criminal world. It has always been like this, since the very ancient past. Then, particularly since the 80's, we started learning about a new type of criminals, involved in the so-called "white-collar crimes". They were a few, highly specialized people, that decided to bid over their own life, and try to get "the big one" to fix all the rest of their lives.
Today the situation is changing, again. We are experiencing white-collar crimes linked with organized crime. Every day we learn about somebody that has been arrested for e-crime actions: young people, students, consultants, "hackers", and criminals. I think those are just the tip of the iceberg. The key difference that apparently no one has realized yet is another one: it doesn't matter whether the bad guy is "the IT consultant" rather than an anonymous teenager.
Today many more people know about IT security and hacking. Resources are available in a really easy and accessible way. The Internet is everywhere, allowing attacks to spread worldwide. People should realize that just like Social Networks exist thanks to the Internet, similarly, we also have a kind of "Criminal Network(s)" thanks to the Internet. It's a process that evolved along the years, and this is the current scenario. There is close to nothing we can do against it, but we can carry on our efforts in raising awareness, training and education. Every new technology opens the doors to new criminal approaches. This should be our first thought whenever using a new technology, along with all the good things and enhancements the technology itself will surely give us.

* Raoul Chiesa is Senior Consultant on cybercrime issues at UNICRI. He is also member of the board of Directors at CLUSIT, ISECOM, Telecom Security Task Force, and honorary president and co-founder of @ Mediaservice.net.

(1) InfoSec: Information Security, often also referred as "IT Security" or "ICT Security", though a light difference exists among those terms.

(2) Payment Gateway: it is usually referred to that entity to which each merchants (meant as a shop, gas station, etc) relies for the electronic payments. It can be a bank (specialized in on-line financial transactions) rather than a credit card dedicated on-line gateway, used by most banks and merchants.

(3) In the so-called "underground economy" organized crime business model, the "mules" are the last link of the chain. Typically we are referring to homeless and/or very poor people, belonging to ethnical minorities.