PROXIMAL CONSULTING WHITE PAPER 5
e-crime: The Vladimir Levin Episode

The sentencing of Vladimir Levin on 24 February 1998 brought to a conclusion the most high profile case of cyber crime to date. The saga - which almost resembles a Hollywood blockbuster - began in July 1994 when customers complained of $400,000 mysteriously "disappearing" from two Citibank accounts. It ended with Levin being tried in the Southern District of New York and pleading guilty to stealing $3.7 million from Citibank (the actual amount was far higher - the original charge specified over $10 million but Levin made a plea bargain). Levin, a graduate of the St Petersburg Tekhnologichesky University, who worked for AO Saturn, a trading company based in St. Petersburg was jailed for three years and ordered to pay back $240,015.

Reports at the time and documents filed in court accused Levin of stealing $400,000 and illegally transferring $11.6 million more between June and August 1994 by accessing the Citibank system breaking user identification codes and customers' passwords. The stolen funds were transferred to accounts in Finland, the United States, Germany and the Netherlands. Levin was arrested in March 1995 at Heathrow Airport as he stepped off an incoming flight from Moscow. Six months later that year he was extradited to New York - the extradition and the actual charges underscore the legal problems encountered with the multijurisdictional nature of cybercrime. In the UK at the extradition hearing Levin's lawyer claimed that no computers in the US were used to access Citicorp's accounts and thus extradition was unwarranted. When that ploy failed Levin's US attorney argued that none of the transactions technically passed through New York (where Levin was being tried) as Citibank's computer is over the river in New Jersey.

Levin was found guilty of routing wire transfers through Citibank's Cash Manager: a computer system which enables Citibank's customers to transfer their own funds in and out. Electronic transfers of money are simultaneously one of the most secure areas of bank operations (because so much money is at risk) and thus one of the prime targets for Hackers. Correct and current telephone dial in numbers to access such systems are regularly posted on hacker electronic bulletin boards.

This case was not only a serious embarrassment for the perceived integrity of global banking systems but more pertinently for Citicorp themselves. Citicorp is the largest bank in the US with a presence in more than 90 countries, which electronically transfers about $500 billion daily and a marketing strategy which stresses its technological competence which facilitates its global 24 hour service "The Citi never sleeps". Citicorp said it was the first time its payment system had been successfully compromised - but they deserve praise for the way in which they both reported it to the authorities and took the resultant adverse publicity on the chin. Turning potentially damaging publicity to their advantage Citicorp said the only reason $12 million was transferred from the New York accounts was because the bank cooperated with US authorities investigating the scheme. After the first $400,000 was stolen, the bank said, other illegal transactions were allowed to occur so an electronic trail could be laid that would identify all of the conspirators.

Yet there was a critical gap in security procedures at Citicorp that also helped allow the crimes to be committed. Before a corporate transaction is finally approved, most banks require users to swipe a credit-card-like pass smart card through a terminal. The card is encoded with an electronic signature unique to the user and if the signature isn't present the transaction is voided (bearing in mind the ATM story earlier this system is probably not as secure as promoted). Citicorp didn't make these cards available to clients before Mr Levin penetrated the bank's network, although it said it has done so since the crime was discovered.

Citicorp said that no current or former employees of the bank were involved in the scheme, but some bankers speculated that someone with inside knowledge of Citicorp's security procedures helped perpetrate the crime.

November 2003 – Adapted from "Hacked, Attacked & Abused: Digital Crime Exposed" by Peter Lilley (Kogan Page, 2002)

Proximal Consulting

Email: enq@proximalconsulting.com

Telephone: +44 (0) 1672 516725

Offices:

Poughcombe Barns
Ogbourne St Andrew
Wiltshire
SN8 1SE
UK

Rue Du Rhone 14
1204-Genève
Switzerland

Proximal Consulting have unrivalled experience in providing KYC enhanced due diligence background reports on individuals and companies on a global basis. We also offer a complementary range of services including AML training, country risk reports and bespoke investigations.

Our enhanced due diligence reports are tailor-made to our clients' specifications. They are totally different from the usual database-led reports that often fail to meet enhanced due diligence requirements. Our reports present clear, accurate and confidential findings which enable our clients to make informed business decisions and to fulfil their AML obligations.

We work with a variety of global clients including regulatory agencies, law firms, individual companies, private banks, trust companies and other firms in the financial sector.