

Telecom – The Terrorism Risk

Rohan Bedi, 26th Sept 2005

The telecommunications industry is exposed to significant risks from terrorism which require firms to take a hard look at their security, anti-fraud and know your customer controls, as Rohan Bedi¹ – Author of the PricewaterhouseCoopers Singapore publication “Money Laundering Controls and Prevention” and Senior AML Implementation Manager of a leading international bank, explains. This feature provides an overview.

Over the last few years, the telecommunications industry has faced many obstacles and challenges. Deregulation along with rapidly changing technology and weaker than expected demand for new services plus significantly increased competition, have altered the market and put pressure on margins. In order to survive, players need to be capable of attracting new customers, understanding their needs, and growing their relationships by expanding and upgrading their services.

In the midst of all this there is a whole new angle thrown in of possible usage of the services of this industry to facilitate terrorist activities/ vulnerability to terrorist attacks. In early March 2005, the New York Times reported that "Government agents have recently uncovered numerous calls from difficult-to-track prepaid cell phones, internet-based phone service, prepaid phone cards and public payphones in the US to known al-Qaeda locations overseas." Robert Mueller, Director, Federal Bureau of Investigation, at a 2005 conference in Washington, D.C said “The Internet has opened the doors to a new world of communication and commerce. But technology is a double-edged sword. Entrepreneurs and engineers are not the only ones who recognize the vast potential of the Internet. Criminals and terrorists do, too.”

The telecommunications industry has the following risks:

- Terrorists use mobile phones to detonate explosives. The terrorist attacks on Jakarta and Bali are reported to have been triggered by mobile phones. Many governments have the power, in a national emergency, to take over key infrastructure such as telecommunications networks. It was reported that the UK security forces were considering getting mobile phone networks disabled during President Bush's visit to stop terrorists using them to detonate bombs. In Thailand, every time a bomb goes off, the government closes down cellular networks to avoid the risk of a second device designed to hit security forces/rescue services rushing to the scene of the first explosion. However, there are ways around this to explode bombs in other ways.
- Cyber-terrorism is another dimension and involves the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population. If a terrorist group succeeded in bringing down telecommunications in a region, there would be cascading effects on all of the other infrastructures and the interdependencies are complex. The overall problem of the cyber threat and cyber vulnerabilities is a real one and a significant one. It is only a matter of time before we see traditional terrorist groups actually using cyber techniques to engage in

¹ Rohan Bedi is closely associated with the ICPVTR and has co-authored a July 2005 paper “AML/CFT – New Policy Initiatives” with Arabinda Acharya, Associate Research Fellow and Manager Strategic Projects, ICPVTR, IDSS, Singapore.

International Centre for Political Violence and Terrorism Research IDSS Singapore

attacks on their political targets. Some state sponsors of terrorism are believed to have cyber-warfare programs.

- Most terrorists would not like to coordinate their work from a home or cell phone they obtained using their own name, driver's license, address and other identifiers. Identity theft is one way a terrorist can establish an anonymous phone service to use for their terrorist activities. With a new identity backed by a phone number, credit-card fraud is also facilitated for financing lodging, transport and supplies.
- Telecommunication fraudsters can also be terrorists: Hired hackers, once broke into major telecommunications companies to harvest calling-card numbers that eventually were sold to organized crime in Italy who used this anonymous time to perpetuate their crimes. There are also other ways to steal telephone time which the fraudster can then sell to a terrorist. In the summer of 2002, a sleeper cell was detected that had an expert in the fraudulent use of telephone calling cards. The terrorists responsible for Madrid's March 2004 train attacks "used stolen telephone and credit cards for communications back to Pakistan, Afghanistan, Lebanon, etc." Mohamed Atta and his group used prepaid wireless and prepaid phone cards while planning the September 11 attack. With regard to credit card fraud, incidents of account data compromise are increasing, represented by 'phishing' and by web sites and internet service providers (ISPs) which have had their credit card lists hacked. Terrorists use subscription fraud where they obtain a subscription to a service, typically by applying in the normal way but by using counterfeit or false documentation.
- Organised crime also uses corrupt owners of telecommunications businesses or corrupt employees in such businesses.
- Terrorists use the internet in different ways to raise funds, collect resources, plan attacks, spread propaganda and recruit adherents. These days the internet is also being use to train terrorists given the closure of the larger training camps in Afghanistan. Terrorist-affiliated entities and individuals have also established internet-related front businesses as a means of facilitating communications among terrorist cells and raising money. A terrorist group may also gain control of a legitimate charity and use it to accept electronic value held in bearer smart cards as donations which in reality could be the proceeds of drug trafficking.
- Terrorists use the internet as a "pervasive, inexpensive, anonymous means of communication"² through which they can plan and orchestrate other fund raising activities. Terrorists use online banking and other financial services. They also use internet-based alternatives to the banking system such as internet payment services and e-cash.
- Anonymity of the internet is enhanced by the fact that many servers do not use 'log files' to trace the origin of the computer through which the transaction is made. Thus, the internet-protocol number of the server and the date and time of connection are not kept in an electronic file. The roots of the transmissions are effectively kept private and virtually untraceable.
- Terrorists web-sites can be made anonymous by using anonymisers which replace the Internet-Protocol (IP) address for the user's home computer with another IP address that cannot be traced back to the user because anonymisers generally do not maintain logs. An anonymiser can also provide the ability to simply browse the web or send emails without the

Terrorists use the internet as a "pervasive, inexpensive, anonymous means of communication"

² Todd M. Hinnen, 'The Cyber-front in the War on Terrorism: Curbing Terrorist Use of the Internet', Science and Technology Law Review, December 15, 2003

International Centre for Political Violence and Terrorism Research IDSS Singapore

website host or the email service operator knowing the source of a web page request or email message. Anonymiser services are free in some cases.

- A common method to communicate safely is for the terrorist to save a draft of a message on a free e-mail service which is read by someone in another part of the world. Because the draft was never sent, the ISP does not retain a copy of it and there is no record of it traversing the internet. Another common method involves providing basic electronic mail services in conjunction with a terrorist-sympathizer web site. Imagine a secure web site that supports basic e-mail services. An e-mail can be sent from one of its e-mail accounts to another without ever leaving its servers. To further add to the burden of law enforcement, by the use of something called Unicode, messages can be written in Cirilic, Hindi, Japanese, Chinese, Korean, Arabic, Hebrew or in just about any other alphabet. In addition, terrorists may use encryption and steganography to conceal the content of electronic communications regarding raising and moving funds. A website can also be used to carry encoded content or hidden messages. Because the actual server that houses a website can be located anywhere, the ability of law enforcement to track illegal activity is further complicated.
- Cyber laundering is another huge area which exploits the speed, security and anonymity of the internet payment systems coupled with the volume of electronic payments in e-space to make tracking and monitoring very difficult. The efficiency of the internet makes it easier to “layer” transactions and fund transfers, routing money through a number of accounts across different countries using a number of different instruments and transfer mechanisms within a short period of time. Online auctions, gambling, banks and other businesses are at risk. With the increased focus on charities, terrorists are also using money laundering techniques to launder the proceeds of drug trafficking and criminal activities to be used in terrorist financing. The controls in this regard are mostly by the payment services provider (eg, the internet bank) albeit the ISP also has a role (discussed ahead).
- There can also be a link in fraud and money laundering. In the Bank of Sicily case in October 2000, a group of about 20 people, some of whom were connected to Mafia families, working with an insider, created a digital clone of the bank’s online component. The group then planned to use this to divert about US\$400 million allocated by the European Union to regional projects in Sicily. The money was to be laundered through various financial institutions, including the Vatican bank and banks in Switzerland and Portugal. The scheme was foiled when one member of the group informed the authorities.³

Regulation and Law Enforcement

Kwok Wui San, Partner and Head of the Regulatory Advisory Services at PricewaterhouseCoopers Singapore states "The e-space has not really been an area of focus from an AML regulations standpoint. It is probably because the internet is normally regulated by non-financial services regulators which may be less aware of AML-linked risk issues. They are generally more focused on consumer care and the functioning of telecommunications. It is also not easy to regulate transactions in e-space. Extra-territorial issues come to mind. Which law applies? Which supervisor is responsible for monitoring an e-transaction? This makes

³ Phil Williams, 'Organized Crime and Cybercrime: Synergies, Trends, and Responses', US Department of State Global Issues journal, August 2001

International Centre for Political Violence and Terrorism Research IDSS Singapore

supervision, enforcement and prosecution quite difficult. Criminals and terrorists benefit because of difficulties in identification/authentication of parties and a lack of audit trails, record keeping or suspicious transaction reporting by the technology providers. There is also the long-standing matter on the need to manage privacy concerns of consumers.”

Furthermore, from a terrorist financing perspective, in most countries, there is no central government authority that reviews the content of web sites before they are hosted online. Moreover, most ISPs have neither the resources nor the desire to monitor the content of their customers’ web sites. Although law enforcement may search the internet for public sites soliciting donations to terrorist organizations, they too lack the resources to maintain constant vigilance over the vastness of the internet.⁴ An expert says “We can expect to see the emergence of ‘jurisdictional arbitrage’ (ie. cybercrimes will increasingly be initiated from jurisdictions that have few if any laws directed against cybercrime and/or little capacity to enforce laws against cybercrime). Jurisdictional voids remain allowing criminals and hackers to operate with impunity.”⁵

The ability of a criminal to transmit information across the internet in a way that is unlikely to be noticed by law enforcement is growing rapidly. Clearly, the ability of terrorists and other criminals to keep up with the changing face of technology continues to far surpass that of investigative and law enforcement personnel. To add to the problems facing law enforcement agencies, there are billions of instant messages transiting the internet daily. Governments should be under no delusions that they can magically filter all internet traffic to separate the innocent from the guilty. The technologies that permit information to be hidden in various ways will continue to grow in sophistication and availability. The technology of governments will have to find ways to keep pace with the knowledge and capabilities of those who use the same technology to perpetrate crime.

Regulatory Measures

Governments and telecommunications regulatory authorities are sensitive to these issues and many are considering new regulatory measures:

- Mobile phones are the most efficient devices for detonating bombs because of their digital technology and the quality of the network. There is a push by the EU Justice Commissioner to ban unregistered pay-as-you-go mobile phone cards to increase the possibility of phone communications being tracked. The Thailand government wants mobile phone operators to register the identity of people buying prepaid SIM cards, the so-called subscriber identity module that identifies a phone to its network. That means collecting data on close to one million people a month. Current users will need to contact their network operators to provide ID information. Telecommunication analysts point out that companies will get more client data with which to refine their marketing strategies. However, operators criticize the plan

⁴ Todd M. Hinnen, ‘The Cyber-front in the War on Terrorism: Curbing Terrorist Use of the Internet’, Science and Technology Law Review, December 15, 2003

⁵ Phil Williams, ‘Organized Crime and Cybercrime: Synergies, Trends, and Responses’, US Department of State Global Issues journal, August 2001

International Centre for Political Violence and Terrorism Research IDSS Singapore

stating that terrorists could evade identification measures by using false identities to buy them, using stolen SIM cards or mobile phones or phones from other countries, or activating bombs by other means (reports suggest for example, remote garage door openers and family walkie-talkie sets – anything with a wireless signal). Furthermore, call tracing only establishes approximate location. Nonetheless, Switzerland has already introduced registration in 2004 and Singapore is also considering following suit.

- Another proposal being put to the EU by British Foreign Minister Jack Straw is for records of emails and mobile phone calls to be kept for at least a year albeit, the European Parliament considers this too intrusive and too costly. Some mobile telephone operators and some ISPs already keep this data. These communications logs would be useful for police and intelligence agencies. Mobile telephone records reveal numbers called and give the geographical location of crime suspects. Internet logs would yield up names and addresses, and the source and destinations of emails and websites used. For example, Italian investigators say the police used cell phone records to track down one of the suspects in the failed suicide bombings in London on 21 July 2005. The suspect was traced using call records from two cell phone numbers, supplied to the Italians by the UK police.
- Cyber terrorism is really more a question of risk management than prevention, because there is no way to prevent attacks one hundred percent. Experts stress vigilance about computer security: patching security flaws quickly once they're detected, designing systems to withstand attacks, backing up systems off-site so they can bounce back quickly from a disruption, watching for disgruntled employees who might help terrorists penetrate a system. Law enforcement agencies and military branches have programs to defend the national information infrastructure. Individual computer owners can become unwitting accomplices to denial of service attacks. Technology linked recommendations for businesses include firewall protection in 128-bit encryption format (the highest level of protection) and monitoring software for breaches of identifying details. Good security also includes virus protection software, avoiding suspicious email and programs.
- Focusing on telecom fraud is important for organizations and regulators. If industry can stop telecom fraud, many criminals and terrorists would find their anonymous communications for planning, funding, recruiting and procuring supplies severely restricted. The better and quicker the clamps on subscription fraud, the more exposed are those who require anonymity. The public should associate stealing telephone time with the crimes that accompany it including terrorism. Some of the new security measures recently introduced to combat fraud include biometrics, which directly measures physical characteristics for example, thumbprints as a means of identifying an individual. There is also address verification, which checks whether the person is who they claim to be by comparing known facts about them. There are also smart cards or chips (with or without biometrics) which add intelligence. These measures do not offer 100 per cent coverage and the fraudster is always looking for a chink in a companies' armour. Other techniques include forensic data mining used to look through the huge volumes of transactional and operational data to spot the hidden patterns, trends and clusters that reveal fraud. Neural networks are used to build profiles of a customer's unique behaviour so that radical changes to this behaviour, which may indicate fraud, can be detected.
- Telecom regulatory authorities have to do a proper scrutiny on the standing of parties before according any approvals. Furthermore, know your employee controls are an important aspect of preventing corruption in the ranks of telecom companies.

Focussing on Telecom fraud is essential to control terrorism

International Centre for Political Violence and Terrorism Research IDSS Singapore

- To combat cyber laundering, the FATF report in 2000-2001 suggests that - ISPs establish log files with traffic data providing IP numbers of subscriber and telephone numbers used for server connection; information collected through the servers be shared with enforcement agencies; information collected be maintained for up to a year; and ISPs keep records, including identification information, on those who transit through their servers.
- The May 2002 FATF 40 consultation report states that ‘some regulators believe that people should be identified when they receive smart cards (electronic purses) with a stored value capacity over a certain amount and/or when they acquire or re-load electronic money in excess of a certain amount by means other than debiting an account held with a financial institution that is subject to customer due diligence requirements’.
- Internet payment services and e-cash companies should log traffic on their web site and retain those logs (although in rare cases, companies proactively destroy business records to protect their customers’ privacy, most of them retain logs so that they can investigate customers’ claims of fraud or theft), it should, at the very least, have a record of the date, time, and IP address from which the account was accessed for every transaction.
- Online businesses need to adopt transaction trend monitoring software and name recognition technology in order to effectively manage their money laundering and terrorist financing risks.
- Managing the risk of fraud and linked money laundering is another area that banks have to invest in.

The KYC Angle

Jay Jhaveri, Director Asia, World-Check, says “The process of identification is always accompanied by the concomitant process of verification. The shopkeeper selling SIM cards can at the most do identification checks. Verification is a pending process that the telecom company must then do and file STRs for suspicious transactions. For the purposes of verification a key control is to review transactions against data-bases of terrorists, money launderers, drug traffickers and other high-risk categories such as politically exposed persons (PEPs), using a good name recognition technology. PEPs from high-risk countries have also been known to have links with terrorists. Automated filtering is essential.”

Four Types of Terrorists

- 1) Unknown persons (who could also be lone operators) who are inspired by a cause and want to become terrorists but can’t find a more experienced mentor. Such persons often get caught early because of the sheer incompetence of their schemes.
- 2) New terrorists indoctrinated at some religious school preaching extremism who commit an act shortly after being brainwashed and trained. There are also persons who get indoctrinated through the internet and somehow find themselves a mentor and self-train using the urban-warfare training that al-Qaeda has made readily available on the internet.
- 3) “Sleepers” in touch through family and friends’ connections with experienced terrorists who act as their mentors and train them in small groups. Sometimes sleepers are small groups embedded in the migrant settler community that due to incomplete integration into the host society may have hidden cells engaged in terrorist and criminal activities with or without a mentor. The police have insufficient proof (if at all) to lock them up/ put them on a public black-list albeit they may be monitoring some of them.

International Centre for Political Violence and Terrorism Research IDSS Singapore

4) Known hardcore terrorists on the most wanted list of the FBI and other black-lists.

With the focus on anti-terrorism in the West, the first category is increasingly being foiled at an early stage with limited damage.

The second category of terrorists, for example, the recent London July 2005 bombers included a young Pakistani boy from a good family who unfortunately got swayed under the influence of some person(s) he met at a religious school. Or, the example of Mohammad Momin Khawaja indoctrinated through the internet, who was arrested by the Canadian police collaborating with the UK in March 2004, in connection with a large UK plot. He was a Canadian citizen of Pakistani origin, a contract computer software operator with the Canadian Foreign Affairs Department earning a decent income. He never got any formal training albeit he did manage to get himself an al-Qaeda mentor and probably trained himself using the internet. Such cases are naturally tough to spot on any database.

The third category of terrorists are for example, the Madrid bombers who may not have been on the US OFAC black-list when they did the event but there may be a news report somewhere that associated them with a more known figure ie, a good commercial database of a third party vendor may throw up the link thereby raising a red flag. The Madrid Bombers had ties to a ring of petty criminals that smuggled drugs and others who were involved in bank ATM fraud and robbery. The masterminds were al-Qaeda trained.

The fourth category is obviously the easiest to spot albeit they would avoid doing transactions in their names ie, they would use identity theft to help them conceal their identities. People in this category include individuals who had been to the al-Qaeda training camps in Afghanistan prior to 2001. For example, as many as 3,000 British born or based people are thought to have been trained in the camps and may since have trained others.

Arabinda Acharya, a Fellow with the International Centre for Political Violence and Terrorism Research, IDSS Singapore states “Estimates of persons trained in Afghanistan varies between 50,000- 100,000. Unfortunately there is no way to trace all the people who went to the camps. Governments need to backtrack on the movement of people during the period that the camps operated but this requires a huge amount of international cooperation and logistical coordination which is not happening as per UN reports.”

The recent London and Madrid bombings have highlighted that terrorists have developed extensive support networks inside major cities in Europe and more al-Qaeda type attacks are likely.

A key and effective tactical measure is for undercover operations using the internet to reach out to terrorists, establish contact, train-with and bust these terrorist rings. Similarly, more specially trained agents need to be sent out to religious schools to try and establish contact with extremists in order to infiltrate and destroy their operations.

Conclusion

The industry needs to focus its efforts on the adequacy of their overall risk management processes and also specifically their identification and verification processes, in order not to fall foul of regulators. On the latter, early adoption of non-documentary verification processes and even emerging technologies like biometrics, should be considered. The issue is less of whether regulations spell out clearly what needs to be done. Proactive behaviour as a good corporate citizen requires a focus on the best risk management practices, which ultimately will also protect the organization against reputation damage and real losses in these very uncertain times.

Disclaimer: the opinions in this article are the authors own and do not represent the organisation in which he works/ was associated with.