CYBER CRIME, FINANCIAL FRAUD AND MONEY LAUNDERING: UNDERSTANDING THE NEW THREAT LANDSCAPE

BY PHIL BUTLER

THE INTERNET: GOLIATH RISES
The race is on - throughout both the developed and the developing world - to become the new leader in digital enterprises.

It is estimated that, in the UK alone, the internet is worth over £100 billion and that 7.2% of the UK’s GDP is generated over the internet.

In 2009, the so-called BRICS nations, Brazil, Russia, India, China and South Africa, represented 45% of the world’s population and were responsible for 15% of global GDP. This figure is expected to rise over the years to come as these nations embrace the internet and the opportunities for enterprise and entrepreneurship which it offers.

While economic growth is good news, growth through ecommerce is vulnerable to the risk of cyber-attacks. Is enough being done to mitigate this risk? Close co-operation between governments, academia and businesses across the globe has seen our defences against cybercrime become more and more robust in response to rising crime levels.

CYBERCRIME: A GROWING THREAT
Let’s take a step back. The internet was first designed by a group of University professors who thought it would be an excellent way of sharing data, research and statistics amongst themselves within Europe.

Exponential growth over the last 15 years means that the internet now controls everything from where we shop and what we buy, to the way our transport system is co-ordinated.

Alongside this growth, crime has also burgeoned. In the UK, the cost of cybercrime is estimated at £27 billion per year, whilst global cybercrime is estimated at US$1 trillion per year - and growing.

Furthermore, research shows us that 23% of all UK web users have fallen foul of a phishing scam and 1 in 5 has been a victim of a scam email or website, with an associated cost of about £3.1 billion.

Experts believe that this makes cybercrime the number one strategic threat to the UK, overtaking the illegal import of drugs and illegal immigration. Over 20 000 hacking attempts on the government infrastructure of the UK are detected each week. Of major concern are Trojans, Worms and hackers infiltrating IT systems and stealing money and information. Fraud and the theft of intellectual property have become major phenomena throughout the world.

In the US, online industrial spying presents a growing threat. Tens of billions of dollars of trade secrets, technology and intellectual property are being siphoned each year from the computer systems of US government agencies, corporations and research institutions.

BORDERLESS CRIME
Think of the internet as a system or network of connections within which organized crime groups thrive. In the past, criminals were fairly indigenous to the towns and cities where they lived. They learned their trade in their immediate environment and very often be sent to prison where they would meet criminals with different skills and abilities. Once released, many would commit further crimes and stay in touch with those still behind bars, often on a national basis. Sometimes, very occasionally and particularly in the drugs war, criminals were able to cross territories and boundaries.

That has all changed. With internet access, a criminal based in a flat in London can commit a crime in, for example, Shanghai. The internet has made it easy for organized crime groups to commit crimes across borders, taking advantage of the obstacles which law enforcement officials encounter when trying to work across international boundaries.

SOME EXAMPLES OF CYBERCRIME
Many of us have experienced spam emails and phishing attempts with fake websites designed for us to be conned and to steal our money.

Cybercrime is fairly advanced. Criminals are able to track all of our movements and passwords via viruses and keylogger attempts and even via USB sticks that may have been infected with viruses.

Stuxnet was a program built to attack Iran’s nuclear program. It was a highly sophisticated computer worm that caused problems and hindered the Iranian nuclear program for months. There have been subsequent
adaptations of the Stuxnet worm, ones which could even allow hackers to open maximum security prison doors remotely. These new variations are also able to control engineering systems within organizations.

GLOBAL CYBER ESPIONAGE: WHAT'S BEING DONE?
The new National Security Agency data centre in Utah is a US$2 billion development to help protect US interests. The US, it is believed, can monitor all data and any information that flows over the internet within this new data centre – a very interesting development.

In the UK, the office for Cyber Security & Information Assurance (OCSIA) works across all sectors, including intelligence, defence and law enforcement. Furthermore, the country now has an international co-operation agreement with the USA and has established a National Crime Agency, incorporating a National Cybercrime Unit, designed to fight organized crime groups.

Organized crime has not changed much since the days of Al Capone. Criminals still commit the same crimes, but gangsters and armed robberies have morphed into cyber criminals using the internet to generate illicit funds. These groups have made millions and millions of dollars through cybercrime, but the funds have no value unless they can be channelled back into the mainstream financial system. Real estate, foreign land investment, smuggling, VAT fraud, investments such as rare art and wine, even investment in the energy and oil industries all provide opportunities to do this. The process through which this is done is known as money laundering. It is the process of concealing the source of money – and in fact all proceeds of crime - obtained by illegal means.

Anyone who works in the regulated sector – accountants, attorneys, banking officials, financial sector employees and even casino employees - may handle such money or proceeds and therefore has an obligation to report suspicious activity.

HOW DO ORGANIZATIONS PROTECT THEMSELVES?
Organizations need to achieve two primary goals: minimise regulatory risk and protect their reputations. Their first step is to examine existing policies and procedures and seek expert advice where necessary. Knowing who their customers are can go a long way towards reducing risk. It is also crucial to have access to a top quality database with global reach, which is able to identify high risk individuals and entities that are using the internet to commit crime.

Further measures include:
- Implementing risk-based robust and balanced anti-money laundering policies
- Appointing Money Laundering Report Officers (MLROs)
- Ensuring that reporting mechanisms are in place
- Training key individuals
- Periodically reviewing processes

WHAT ARE GOVERNMENTS DOING TO HELP COMBAT MONEY LAUNDERING?
Although there is currently no specific UN Convention on cybercrime, current anti-money laundering (AML) and Combating the Financing of Terrorism (CFT) legislation impacts on commercial activity that is facilitated through the internet.

UK: THE PROCEEDS OF CRIME ACT 2002 (POCA)
The Proceeds of Crime Act has undergone amendments. There is now no need to prove predicate or specific offences, so there is a lower burden of proof. There are new offences relating to negligence, failing to disclose and tipping off of offenders.

The following points are worth noting:
- Section 332 creates an offence of failure to disclose by nominated officers outside the regulated sector. It cannot be committed by negligence. The mental element of this offence is knowledge or suspicion.
- Section 333 creates the offence of making a disclosure likely to prejudice a money laundering investigation.
- Criminal property includes money as well as all forms of property, all real estate, things in action other intangible or incorporeal property, including shares, bonds and deposits.
- Individuals could face 14 years of imprisonment or 5 years if they are in the regulated sector and fail to disclose suspicious activity.

An offence is not committed if a person:
- makes an authorised disclosure
- has a reasonable excuse for not disclosing the information
- does not know or suspect that another person is engaged in money laundering
- has not been provided by his employer with relevant training
- did not know or suspect that the disclosure was likely to prejudice an investigation

Further defences include if the disclosure was made in connection with a function relating to enforcement or if the information is passed on in circumstances that amount to legal privilege, but not if the information is passed on to further a criminal enterprise.
THE USA PATRIOT ACT

The USA PATRIOT Act is a piece of legislation that affects every country in the world. Its purpose is to deter and punish terrorist acts in the United States and globally.

Key points of the Act are:

- To strengthen US measures, to prevent, detect and prosecute international money laundering and financing of terrorism
- To subject to special scrutiny foreign jurisdictions, foreign financial institutions and classes of international transactions or types of accounts that are susceptible to criminal abuse
- To require all appropriate elements of the financial services industry to report potential money laundering
- To strengthen measures to prevent use of the US financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong

It was introduced after 9/11 to protect the US financial system and US interests.

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force is the global standard for measures to combat money-laundering, terrorist financing and the financing of proliferation. Some of the main FATF changes, which occurred in February 2012 are:

- Combating the financing of the proliferation of weapons of mass destruction through the implementation of targeted financial sanctions
- Improved transparency to make it harder for criminals and terrorist to conceal their identities or hide their assets behind legal persons and arrangements
- Stronger requirements when dealing with politically exposed persons (PEPs)
- Expanding the scope of money laundering offences, to include tax crimes
- An enhanced risk-based approach which enables countries and the private sector to apply their resources more efficiently by focusing on higher risk areas
- More effective international co-operation including exchange of information between relevant authorities and conducting of joint investigations leading to the tracing, freezing and confiscation of illegal assets
- Better operational tools and better use of technologies for financial investigation units (FIUs)

What is key is both national and international co-operation and information sharing across regulators and enforcement agencies. These three key pieces of legislation are being rigorously enforced and all of them have application to cybercrime. The lowered burden of proof for regulators requires a consistent and thorough approach to compliance, along with heightened levels of transparency.

THE FUTURE - A BALANCED VIEW

The internet is changing the face of the future. For example, the retail experience is changing. More and more shops are closing as internet sales rise and technology drives consumer trends. Consumers are becoming less loyal, but still demand excellent service. They want to be engaged, but at a distance where they are in control. They expect an understanding of technological developments, will shop on line for basics, but want to shop in the right environment for those ‘special’ things or for ‘special events’. Technology needs to stay one step ahead to keep these virtual shoppers secure.

Keystroke Dynamics is touted as a potential solution to cybercrime: technology that allows one to identify anyone using a keypad or a keyboard within ten keystrokes. This can be applied to ATM devices, smart phones, iPads, laptops and computers. By adding an extra level of identification when individual’s log in to systems, security can be enhanced. This is just one example of work being done to safeguard the future and curb cybercrime in the years ahead.

Technologies are changing on an almost monthly basis and it is very difficult and expensive for law enforcement to keep up. So we have to look to the large agencies and institutions - the FBI’s of this world – to lead the fight against cybercrime.

The internet will continue to have a substantial impact on the future of almost every aspect of our personal and business lives. The opportunities for individuals, for companies and for countries are undisputed, but along with these opportunities come threats created by an ever-evolving criminal network. Staying one step ahead is crucial.

This Expert Talk has been adapted from the World-Check Webinar Series: “The Power Behind the Research” Cybercrime, financial fraud and money laundering – the new threat landscape presented by Phil Butler in September 2012.