C/M/S/

Countering the cybercrime threat – an historical perspective

A version of this article first appeared in the May edition of Fraud Intelligence published by Informa UK Ltd.

Introduction

My favourite bit – if I get the time to read a newspaper – is the Obituaries page. Inspiration, surprise and serendipity in an uneven and unpredictable mix. Each of these elements filled a book[1] which I read recently about Sir Isaac Newton (1642 – 1727). Newton was a brilliant Cambridge scholar, scientist and mathematician; famed for his writings about gravity and calculating the movement of planets. He also became, extraordinarily for a rather sickly farm-boy and academic from rural Lincolnshire[2], a successful, streetwise and ruthless detective and investigator as head of the Royal Mint. That at a time of war and national crisis when the currency was being systematically undermined by organised criminals. The book tells the story of Newton's personal battle against William Chaloner, the leading counterfeiter and forger of his day, a man whose long criminal career encompassed dealing in fake watches, knock-off Italian sex-toys and money laundering, as well as a successful phase as agent provocateur, bounty hunter and super-grass.

So, what possible relevance do the problems and challenges facing Newton in the London of the 1690's have today inhibiting the exponential growth of cybercrime? Can we draw lessons or adopt techniques from those used more than 300 years ago to help us in combating this threat, long before computers or the internet or even Sir Robert Peel's police force were ever conceived? This article examines some of the similarities and differences between the situation facing Newton compared with the issues of internet-based crime; looks at some of the principal barriers and inhibitors to an effective and co-ordinated response to e-crime, and suggests how Newton's analytical and practical methods might be a useful guide to our thinking and planning in this area.

Newton's challenges

There are some striking similarities between today and 1690's England[3]. The country was at war (as usual, with France); Government revenues were drastically down and there was massive opposition to the idea of increased taxes. The currency had also devalued significantly over the previous decade and was under further threat, partly as a result of speculation by traders, partly as a result of the undermining of the value of money in circulation by criminal activity. Rather than a mere General Election, '*regime change*' was a real possibility if King William III's army (then besieging the city of Naumur) remained unpaid and a Jacobite (Franco-Scottish) rebellion was fostered as a result of the financial dislocation and unrest.

The criminal threat to the currency arose as a result of the activities of 'clippers' and 'counterfeiters', filing or cutting off metal slivers from silver and gold coinage, then smelting the off cuts and pressing new, inferior coins – frequently adulterated with less valuable metals. The consequence over time

---

[1] Newton and the Counterfeiter by Thomas Levenson (2009 – Faber & Faber)

[2] Woolsthorpe, near Grantham

[3] The Acts of Union were not passed until 1707.

was that the value (and the actual physical size) of the currency drastically reduced. In 1662 the Government had attempted to stem this abuse by supplementing the older smooth-edged coins in circulation with specially 'milled-edged' coins produced by a then new and secret process by the Royal Mint, housed at The Tower of London. These new coins were harder (though not impossible) to copy, but milling (ie stamping of intricate patterns) around the edges made it much easier to detect and therefore to deter illegal clipping. However, the problem did not go away because the older, smooth-edged coins remained in circulation and continued to be abused. Newton's task upon his appointment as Warden to the Mint in 1696 was to restore the value of the currency first by re-issuing it in more secure form, then stamping out the abuse. Within 3 years the entire currency was recalled, smelted down and re-distributed (enhanced with the latest milling technology and special dyes), with minimal disruption to the economy or the King's taxes.

Newton inherited 30-year old machinery, housed in decrepit sheds propped against the walls of The Tower, a hopelessly inadequate budget and a demoralised workforce working to targets which most regarded as impossibly ambitious. Sound familiar? Worse, the person in command of the workforce was a renowned gambler and socialite; lazy and lacking in any expertise or motivation save to maximise his personal profit from the Mint's turnover of new coins each year. Newton was also appointed Magistrate to the Mint, policing the coining process and responsible for investigating and prosecuting any criminal tampering with the currency. For this part of his job he had no legal training or experience, no police force, a nominal budget and no manual or predecessor's model to follow. He succeeded by applying the same dedication and scientific method as for his mathematical studies and his hobby as an alchemist. He mastered every aspect of the technological process employed at the Mint. He observed each stage, measured and analysed it, then tinkered with the process to achieve optimum performance. He also made it his business to find out exactly what counterfeiters were up to and how their business worked. Newton built an extensive network of informants, runners and thief-takers. He personally immersed himself in interrogations and recorded and cross-referenced as many details as practicable. He developed and extended a generous system of incentives, reward payments and 'stings' to elicit incriminating information from informants in taverns, prisons and brothels across the capital. Albeit in a different age, Newton proved ruthlessly efficient in using the threat of execution, deportation and financial ruin to further his aims and to obtain confessions and convictions. Amongst those he sent to the gallows was William Chaloner; it is a fascinating tale.

Nature, scope and common elements of the modern cybercrime threat

Are the problems facing us greater than those facing Newton? There are striking parallels: war, financial dislocation, unrealistic targets and budgets, a sense of societal breakdown and the impotence of authority. London, then as now, was the crowded, wealthy centre of a global trading network. Fear, greed and the survival instinct still motivate and drive criminal activity. Religious fanatics embrace new methods of communication and new weapons to disrupt and attract attention, and to make money on the side. Technological advances and the ubiquity of computerised machines engage and seduce us in developed countries, but at the same time make us more vulnerable. Innovation and the drive to reduce cost year on year, combined with migration, outsourcing and the shifting balance of global trade patterns means that the range and pace of change appears ever-faster. In Newton's London the lack of any police force and the bustle of a trading city without modern identity tools meant that criminals could operate relatively freely. Today's sophisticated criminal seeks to exploit the same anonymity through the use of cyber cafes, unregistered servers and by operating remotely from safe-haven jurisdictions where government and law enforcement is either weak or non-existent or part of the problem.

Part of the challenge of devising defence strategies for cybercrime[4] is the range and scope of such activities, plus the degree of State involvement or tolerance of those who perpetrate it. Examples include denial of service attacks preceding military incursion (S. Ossetia, 2008) or the recent hacking of Google in China to identify Tibetan activists. Ideological and political extremists also use the internet to transmit funds or encoded instructions to terrorist groups. States naturally engage aggressively to subvert them. Beneath that level are the individuals and organised crime groups ("OCG's") with which you, as readers, will have most contact and experience. In practice there is a complex pattern of interrelationships between these categories which is ever shifting, sometimes rapidly so. The increased connectivity and penetration of personal computers means that individuals can move with greater ease within and across these categories. Thus entrepreneurial individuals have built powerful OCG's very quickly[5]. The story of the development of a global one-stop cybercrime superstore (DarkMarket) by an itinerant 33-year-old pizza delivery worker is an instructive one. The reduced cost and accessibility of DIY cybercrime kits (e.g. 'Zeus' - £1500 and 'Spy Eye' - £320) has stimulated a massive upsurge in the last 12 months in the number of 'phishing' and 'key-logging' attacks. These no doubt further clog up your in-box as well as mine because of the clever 'mutating' features which reduce the effectiveness of anti-virus software and firewalls.

In 'McMafia'[6], Misha Glenny describes how these various forces and drivers have combined to create global cybercrime hubs wherever chronic poverty, a decent level of education and established OCG's coincide, most notably in the emerging BRIC countries[7]. At the same time as law-abiding organisations are striving to 'go paperless' and outsource various non-core functions to lower-cost (and less secure) jurisdictions, each element of the cybercrime threat is increasing. The criminal mind was in Newton's time, and is today, ingenious and adept at monitoring and exploiting the vulnerabilities created by a dynamic changing environment. The IT tools and skills to enable them to do so are increasingly sophisticated and inexpensive for the criminal to acquire. There is a constant battle to try and anticipate, recognise, communicate and counter these abuses, and to mitigate loss and damage in the meantime.

Common inhibitors to an effective response

Newton would have recognised each of the following constraints on an effective, co-ordinated response:

(1) Resources: fighting the technological criminal consumes resources, which are always in short supply. The speed of technological change means that equipment needs to be regularly updated and replaced to avoid becoming obsolete and ineffective;
(2) Competition: whether between countries or within markets or government agencies, competition (in a free market) arguably can be an important protection against crime and corruption because a corrupt entity will usually become exposed because of its inefficiency compared with rivals. However, natural reluctance to publicly expose or share embarrassing lapses or admit to weaknesses often leads to delays in identifying a general problem and increases overall exposure;

---

[4] Cyberspace and the National Security of the United Kingdom: threats and responses (March 2009)

[5] Welcome to DarkMarket by Caroline Davies: Guardian.co.uk 14/01/10

[6] McMafia: crime without frontiers (2008) Faber & Faber

[7] Brazil, Russia, India and China

(3) Diverse political objectives: whether due to poor or divided leadership, or just woolly thinking, different political aims, goals and values generally undermine effective cooperation in this area;
(4) Fear of penetration and compromise: if the existence of my (secret) investigation or informant is disclosed then all the time and resource invested is potentially lost irretrievably (for the benefit of others, especially galling if they are criminals);
(5) Legislative constraints: the speed of technological change combined with the inertia of the morass of national, international and developing human rights law frequently leaves crime-fighters with an overwhelming feeling of frustration at fighting an agile opponent with limited resources and 'one's hands tied behind one's back'.

In the face of such obstacles many abuses are simply not cost-effective to pursue; '*twas ever thus*' Newton would agree.

Newtonian countermeasures

Newton's tried and tested approach is just as valid today for our threats as it was for his. He would immerse himself in the subject; then observe, record and act as aggressively and decisively as possible on the basis of his analysis. I suggest that he would have embraced a wide range of measures but endorsed, with enthusiasm and conviction, the following trio: -

First; engaging with the honest citizen and user of the internet, whether individual or corporate, both to protect and preserve the massive benefits which computers bring, but also to act more positively when abuse is detected. There is a need for much greater awareness for all users on the signs of abuse and the encouragement of relevant reporting regimes. Primarily these efforts should be designed to promote self-help. Survival of the (technologically) fittest is the essence of this message. In practice that means: devoting adequate time and resource to technical defences; to maintaining a basic level of spare capacity which can be relied on in the event of catastrophic breakdown, which includes maintaining alternative non-IT systems. No system and no data are absolutely safe: minimum standards of IT security and protection should become elevated board-level concerns because failure threatens the future of the entity.

Second; building, financing and maintaining as comprehensive as practicable anti-cybercrime networks, working within the relevant constraints: technical, cost, legal, diplomatic. A global view and approach is essential, even though there will be large chunks of the network which will remain problematic; perhaps impenetrable or subversive from time to time. There are some encouraging signs. In the UK the FSA's recent initiative on insider share-trading blends the best of public and private sector techniques. The proposed creation of a National Crime Agency is a step in the right direction. At an international level, recent co-operation between US and Russian authorities[8] may be significant or may just indicate that shifting allegiances have made joint working expedient to achieve a particular result. There will always be political barriers to overcome but every success at every level acts as both an example and a deterrent to others.

Third; innovation, guile, better awareness and stamina on our part remains essential, especially since technology provides the cybercriminal with many natural and novel advantages. Intrusive legislation directed at ISP's, individuals and corporate users; voluntary or compulsory 'inoculation' of PC networks; aggressive forensic investigations which link up cross-border entities and institutions with co-operative and robust law enforcement; all such measures should be considered and have a positive role to play.

---

[8] FT.com 21.03.2010-Moscow cracks down on Cybercrime

In 2009 the estimated value of online data theft globally for the first time outstripped the estimated value of the entire illicit drugs industry. The harm that drug abuse wreaks is more visible and has been with us for much longer. The pernicious harms caused by cybercrime are less visible but no less real. They feed into and support existing organised crime groups. Every individual and every business has to take this threat seriously in order to avoid becoming a serial victim, whether directly or by paying higher costs, taxes and insurance premiums.

Simon Chandler is a partner at CMS Cameron McKenna LLP and can be contacted at simon.chandler@cms-cmck.com