Risks faced by financial services & other commercial institutions arising from the misuse of technology

Mark Johnson
The Risk Management Group

August 2012

I. Introduction

Both the UK Cabinet Office[1] and the Serious Organised Crime Agency (SOCA)[2] have independently identified cyber crime as one of the main threats to the UK economy. This is a challenge that affects most major economies and while the true cost of high technology crimes is difficult to calculate, the number of reports and news media stories appearing daily on the topics of hacking, data loss and similar cases serves to support the notion that this category of risk is indeed of special importance.

In an era of absolute dependency on the cyber technologies for most economic, commercial, political and social systems and processes, attacks or exploits that target or transit these technologies, and which may deliberately or accidentally bring said services to a halt, represent an existential threat to our globalised systems of trade, supply chain management, finance and the financial markets, governance and security.

In this short paper I will describe some of the key risks we have encountered while working with clients, as well as listing other emerging issues on the high-tech crime front. In so doing, I will briefly describe the risk landscape, highlight some specific issues for regulated firms and summarise a few of the countermeasures that should be considered.

II. The Technology Risk Landscape

Modern information and communications technologies ('ICT') permeate the fabric of our daily lives. Your morning paper, the television news, the journey to work, the traffic light that delayed you, your cup of coffee, the report you browsed, the phone call you made, even this paper itself, were all delivered to you via or with a contribution by ICT. While ICT is not the only way in which such goods and services can be delivered, it has become the de facto mechanism for delivery, with the result that other solutions, such as manual or paper-based operations, are largely redundant. There is no readily available fall back system for most of the ICT operations that now govern our daily lives.

It is therefore very important that we develop a sound appreciation of the range of current ICT risks and the countermeasures required.

i. Cyber crime

Often conflated with eCrime, 'Cyber Crime' refers to any crime involving the use of a computer and a network.

Typical cyber crime attack methods include:

- **Hacking**, or breaking into computer systems and networks using highly skilled 'manual' techniques.
- **Code injection** attacks designed to access logon data tables of user names and passwords, such as those allegedly perpetrated against Sony Online Entertainment[3] in 2011.
- **Cross site scripting (XXS)** attacks that launch attacks on a target site via a malformed webpage.
- **Man-in-the-Middle** (and man-in-the-browser) events wherein an attacker interposes themselves between two parties in order to intercept their communications.

[1] UK Cabinet Office Report - The cost of cyber crime, 2011
[2] United Kingdom Threat Assessment, Home Office
[3] http://www.channel4.com/news/sony-networks-hacked-again

- **Spyware** that captures key strokes, personal data and logon information.
- **Trojans, worms, viruses** and other malware that can deliver a payload or disrupt and even damage systems, such as Gauss[4], or the Stuxnet and Flame attacks centred on Iran over recent years.
- **Denial of service (DoS) attacks** that attempt to bring down selected services or even whole networks, normally by flooding them with traffic or signalling messages.
- **Botnet exploits** involving networks of thousands, or even millions, of infected computers that might broadcast SPAM or be used to facilitate distributed denial of service attacks (DDoS).

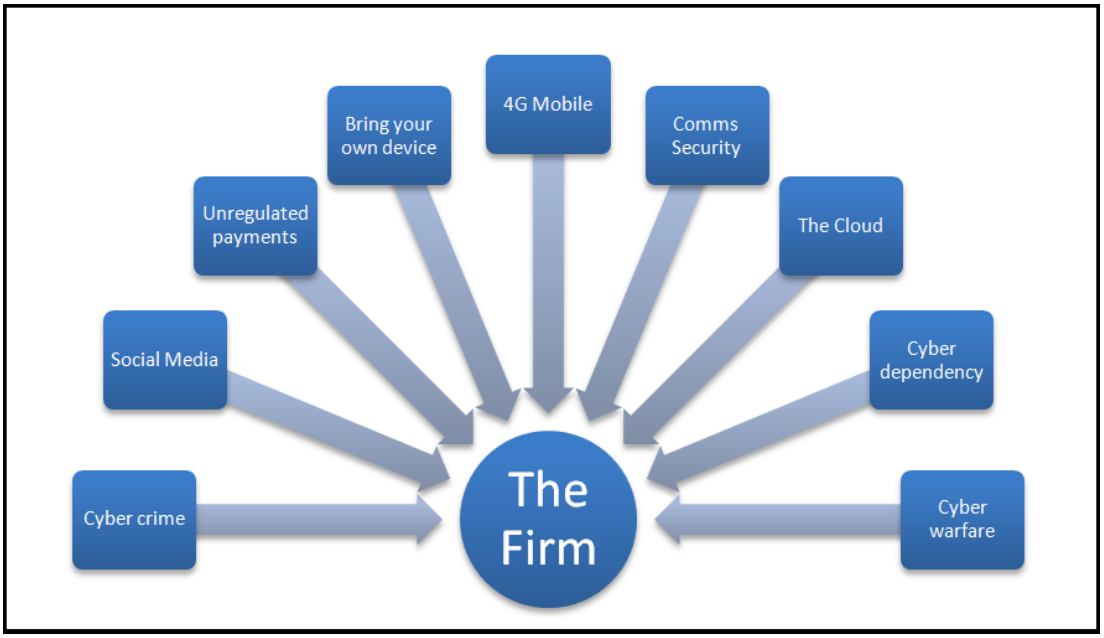

Image 1 Key Risk Areas

The list goes on, but the point to be made is that increasingly complex technologies are, by their very nature, exposed to increasingly complex sets of risks. Many of these risks can manifest themselves in combination, with one case involving, for example, a code injection attack designed to steal passwords, followed by a fraud attack on selected accounts, or even the insertion of a Worm to infect a system or network.

ii. Social media risks

Now the communications tool of choice for hundreds of millions of users, social media services such as Facebook[5] introduce several new risks into the high-tech mix, including but not limited to:

- **Data protection risks** in relation to user's account and profile information, which often includes dates of birth, addresses and telephone numbers. LinkedIn recently suffered a hacking attack[6] that is thought to have exposed 6.5 million user names and passwords.
- **Identity verification risks,** demonstrated by the ease with which fake social media accounts can be created and 'friends' found. In our own tests using five faked

[4] http://www.guardian.co.uk/technology/2012/aug/09/stuxnet-gauss-virus-kaspersky
[5] www.facebook.com
[6] http://www.bu.edu/today/2012/linkedin-hacking-what-you-need-to-know/

Facebook accounts and one LinkedIn account, we were able to attract an average of 120 friends per account.

- **Harassment, grooming and targeting,** whereby criminals and others are using social media to identify, locate and investigate potential victims[7].
- **Reputational harm,** particularly from events such as 'Twitter Storms' where users target a brand and generate thousands of negative messages that are read by millions of consumers in a very short period of time.

Facebook claims to have 900 million users, but many in the sector, including yours truly, question the basis for this claim. In fact, in disclosures[8] made in its SEC filing prior to the recent Facebook IPO, the firm admitted that approximately 4% all accounts are known to be fakes or duplicates. The true figure may well be much higher, although facebook in all probability can't assess this, making social media an investment time bomb, an additional risk that financial services firms ought to bear in mind.

iii. Unregulated payment risks

A number of online sites exist that allow users to transfer value across borders without going through the regulated sector and with no anti-money laundering, terrorist funding, sanctions or trafficking checks. Examples range from WebMoney[9] and Bit Coin[10], both of which offer cyber currency options, to numerous sites that trade in the 'currencies' used by players inside online games such as World of Warcraft and Eve Online.

On these trading sites, dozens of which can be found with a quick Google search (using the search term 'buy world of Warcraft gold', for example) it is possible to buy and sell both game funds and game accounts via a credit card transaction, meaning that by secretly transferring a set of game account usernames and passwords to you, I can transfer value which you can sell online for real money. Some accounts retail online for over USD 1,000 and significant funds, in terrorist funding terms at least, can be transferred across borders without any identity verification or transaction monitoring taking place. Bribery and corruption, as well as tax evasion, are additional risks arising from this model.

iv. Mobility and Bring Your Own Device (BYOD)

Firms are increasingly allowing staff to use their mobile devices for work. According to Gartner[11], personal device usage will be the hottest topic for IT Managers for the next 10 years. This is likely to add a number of risks as users engage in the following activities:

- Use of a single device for both personal *and* business purposes.
- Use of devices across public, home and corporate networks, with increased potential for man-in-the-middle attacks.
- Transportation of devices to and from work and on personal trips.
- Storage of sensitive corporate data on personal devices.

These behaviours already occur, but if BYOD becomes standard practice, the risks arising can be expected to become even more commonplace.

[7] http://www.legalandgeneral.com/_resources/pdfs/insurance/digital-criminal-2012-report.pdf
[8] http://www.sec.gov/Archives/edgar/data/1326801/000119312512325997/d371464d10q.htm#tx371464_14
[9] www.wmtransfer.com
[10] www.bitcoin.org
[11] Source: http://www.gartner.com/it/page.jsp?id=2048617

v. 4th Generation mobile broadband

4th generation mobile broadband, or '4G', is the latest manifestation of the mobile data revolution and unlike 3G, which took several years to get off the ground, 4G enters a market dominated by smart phones or PDAs, laptops and tablet devices such as the iPad.

Mobile broadband has two primary effects that drive risk:

- It increases the pressure for BYOD to be permitted, as workers become increasingly reliant on a plethora of devices that the corporate employer hesitates to purchase for them.
- It increases the scope for remote working and working while in transit, thus exposing ever more corporate data to interception.

vi. Communications security

Communications service providers (primarily telephone operators and Internet service providers) have long struggled with internal and external fraud challenges. As everyone goes online and as the boundaries between different types of network and service become blurred, the security issues that once remained hidden within these homogeneous networks now become issues for all of us.

Of particular relevance are:

- The communications interception risks already mentioned, which are compounded when a single call or data session passes across local WiFi, then the Internet and finally across a global corporate network.
- The risk of remote database access, attacks that bypass authentication (e.g. 'man-in-the-browser' attacks) and malware-triggered denial of service attacks.

vii. The Cloud

The Cloud introduces yet another set of issues. Firms may unknowingly share platforms with competitors. Auditors and IT managers need to establish where data is stored and how data classification schema should be applied in relation to remote storage or data processing. Third party employees need to be trained and vetted to standards that comply with those of the business responsible for data protection. ICT security controls also need to be operating at the same level. Cloud services do not only 'virtualise' computing and data storage; they 'virtualise' cyber security risks and risk management.

viii. Cyber dependency

I have already made the observation that our collective dependency on a single set of technologies for the operation of a very broad set of key activities constitutes a serious risk. It is certainly not an exaggeration to say that any catastrophic cyber event that resulted in a long term (meaning days rather than hours) termination of ICT services at a national or continental level would have the potential to trigger a global economic collapse.

If our dependency on ICT/Cyber is the most important risk factor we face today, then the security of our ICT/Cyber infrastructure, systems and processes should become our top managerial and political priorities.

ix. Cyber warfare

One of the most likely scenarios for the widespread disruption to, or termination of ICT services is a cyber warfare attack. Conventional thinkers[12] describe this in terms of a form of 'cyber bombing raid' on the enemy's systems, akin to a World War Two strategic bombing campaign against centres of production and "worker's housing".

As with any attack of this kind, however, whether kinetic or digital, the potential for collateral damage is immense. Amongst the numerous challenges facing cyber warriors are two that deserve special mention:

- **Entanglement**; in our globalised world, separating one part of the cyber infrastructure from another might prove challenging. How can any protagonist be sure that in a wholesale cyber war the collateral damage caused will not do as much harm to the globalised economy of the home nation as to its enemies?
- **Attribution**; given the capacity for sophisticated state-sponsored cyber attackers to mask their true location and the origin of an attack, or even to route their attacks through a third country, those responding to such incidents will face difficult choices when it comes to attributing any attack to a particular source.

A number of other challenges exist and it seems possible that a major cyber warfare event will not necessarily be a clean affair, characterised by precision attacks on pin point targets, but that it has the potential to cause widespread harm to friend, foe and innocent bystanders alike.

III. Particular concerns for Financial Services firms

Financial Services (FS) firms face a particular set of additional issues as a result of the increasing level of cyber security risk. These are summarised here:

i. Compliance

Operating in a very tightly regulated space, while simultaneously touching networks and technologies that are often inherently vulnerable, FS firms need to be especially wary about cyber security risks as their exposure is two-fold; they will suffer all the harm that a cyber security breach can bring to any business, but they may also be exposed to regulatory fines or other measures.

Furthermore, because consumer confidence is such an important consideration in FS, and because the particular customer data held is so sensitive, the scope for reputational harm is also multiplied several times over when compared to most other sectors.

ii. Anti-money laundering, Anti-trafficking and Countering Financing of Terrorism

Modern communications technologies introduce two more challenges for in terms of adherence to mandated responsibilities[13] for spotting and reporting suspicious transactions:

- **Big data**. Big data refers to data sets that are too large to be efficiently processed by conventional data processing platforms. As increasing numbers of financial transactions go online, driven in large part by the evolution of the mobile data

[12] www.defense.gov/cyber

[13] http://www.worldcompliance.com/en/resources/white-papers/third-eu-directive.aspx

service mix, the volume of transaction records that will need to be collected and assessed is also likely to rise. We have already experienced this in the conventional telecoms sector, where daily traffic volumes across all services have risen dramatically around the world over a twenty year period. The Big Data challenge is likely to affect FS teams over the coming years, leading to requirements for new and bigger data processing solutions and new approaches to data analytics.

- **Unregulated payments**. As described earlier, the unregulated payments sector (Bit Coin and others) poses an additional challenge, if not for FS firms directly, then for their regulators.

iii. eCrime

A purist might tell you that eCrime includes:

- Computer intrusions
- Distribution of malicious code
- Denial of service attacks
- Internet-enabled fraud

While technically correct, this definition is confusing to the lay person as it represents a 100% overlap with 'Cyber Crime', a term that is probably more widely used and better understood. In fact, some UK Police eCrime Unit websites[14] discuss the topic of cyber crime interchangeably with eCrime. I prefer to break these subjects down because a great deal of high-tech cyber crime is not financially motivated. I use 'eCrime' to denote those electronic crimes that have an economic (primarily fraudulent) set of drivers and 'Cyber crime' to refer to computer or network crimes with a technical focus. Be prepared to hear that I am wrong!

Online banking and credit card service providers are particularly exposed to eCrime. The main risks they face are:

- **Card not present fraud**, when card details are stolen and then used for online or telephone transactions.
- **Man-in-the-browser** attacks in which infected web pages hijack online banking sessions after customers have logged in and authenticated themselves, in order to change the amounts and destination accounts of payments and transfers.
- **Denial of Service attacks,** designed to bring down bank services.
- **Database intrusions,** intended to steal, edit or delete sensitive data.

Although Chip and Pin technologies have reduced some types of credit card fraud, the general trend towards more and more remote transactions is likely to keep this class of risks alive.

IV. A summary of the main countermeasures

It would require a book (and indeed, there is one on its way!) to describe the full range of countermeasures available to the modern firm. This is in fact good news and I have cherry picked my top five topics and summarised them here.

[14] http://www.met.police.uk/pceu/

i. Authentication

In today's environment, traditional username and password techniques are no longer effective and many firms have already moved away from them. Usernames and passwords can be intercepted or retrieved from insecure tables, they are frequently written down, and in some cases they are re-used on other sites, such as social media pages, by people who don't want to have to remember more than one logon in their lives.

Enhanced approaches normally involve what is known as two or three factor authentication; something you **know** (perhaps a password), plus something you **have** (such as a security dongle) and something you **are** (such as a biometric measurement). Even this approach is likely to evolve and solutions have already been developed that take authentication to even higher levels.

ii. Data Classification and Encryption

As we enter the world of Big Data, it is increasingly important that we make sure that security does not become an inefficiency that inhibits our operations. One tool for achieving this is data classification, which involves scoring different types of data based on its sensitivity. Good data classification can support the following:

- **Different authentication levels** for different roles and data types, so that even someone with a sensitive role can quickly logon and view unclassified data, such as an intranet page, only going through the higher levels of authentication when the type of data to be viewed justifies it.
- **Sound decisions** about Cloud strategies and off-shoring, consistent with compliance rules and other guidelines.
- **Economically sound choices** with respect to data storage, encryption and security in general.
- **Proper risk assessments** that reflect the true value of various data assets and which do not treat all data as equal.

iii. Social Media Policies

New social media challenges require organisations to develop workable social media guidelines that reflect real world conditions while still helping to keep the firm secure. We have developed a freely available 10 point plan[15] to help address this need.

iv. Disaster preparedness

This is the big one. Is your firm ready to deal with a complete cessation of Internet services over a period of several days or weeks? Can you assure the survival of your business, and those of your customers, in such circumstances? I do not know how many will answer this question with a confident 'Yes', but I fear that the number is very low.

If you accept that such a service disruption is a realistic possibility, then I suggest that Cyber Disaster Preparedness and Business Continuity should be amongst your top priorities going forward.

[15] http://trmg.biz/app/download/5781092122/TRMG_Social+Media+Risk+Control+10+Point+Plan.pdf

v. Awareness

Finally, everything falls apart if we are not risk aware. In the modern world, it is not sufficient simply to educate employees; we need to educate their families and their children, many of whom will be sharing the portable device that the employee brings, or will soon bring, into the workplace.

Awareness of cyber security and guidelines for safe behaviour need to be taught in school from the age of four. I have produced a simple 'A to Z' guideline[16] that is intended to support this process. Like all of the reading suggested in this article, it is free to download and share as you see fit.

V. Conclusion

Risk in the high-technology era, where our economies are knowledge-based rather than industrial, and where data-centric business models, such as the financial services model, are our main focus, orients itself towards that data and towards the systems that hold it, the networks that carry it and the people who use or depend on it.

Data is today one of our greatest assets. Any risks that affect the security, integrity, completeness or timeliness of delivery of that data are consequently our greatest risks.

About the Author

Mark Johnson is the founder and Chairman of The Risk Management Group, a high-tech risk control consultancy specialising in the delivery of training, advice and solution design to firms and vendors in the financial services and communications sectors.

[16] http://www.trmg.biz/the-a-to-z-guides/