Overview of Cyber Security & Risk

By Mark Johnson

ICT Faculty
Introduction

Carl Sagan once said that we live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology. Society’s total dependence on the Internet and its related technologies is unprecedented and yet very few understand either the technology or its associated risks. This means that, even though most of these risks are entirely manageable, there is a dearth of people ready and able to do the managing, and even fewer to allocate the funds and make the necessary decisions.

This general lack of understanding is made worse by the confusing and all encompassing definitions for cyber crime and cyber security that abound at all levels. Essentially, most senior decision makers regard any unauthorised act involving even the most minimal use of IT or communications technology as some form of ‘cyber crime’. In today’s high tech society, this means that the vast majority of crimes have a ‘cyber’ element.

Our definition is narrower. We judge a crime to be a ‘cyber crime’ if the primary mechanism by which the crime was committed involved the use of the Internet, and/or World Wide Web, and:

1. The primary target of the attack was data, code or other digital material stored on an Internet connected device, or;
2. The primary motive of the attack was to disrupt remote systems or services, or the Internet itself.

Thus there is a distinction to be made between ‘cyber crime’ on the one hand and ‘eCrime’, which might merely involve someone sitting at your PC without your permission and stealing personal data, or using your credit card fraudulently to make an online purchase, having obtained it by picking your pocket; in neither case was the Internet an avenue for the attack, even though it might be used as an avenue for the exploitation of the proceeds of the attack.

Using these definitions, hacking and phishing, malware and Botnets are all examples of cyber crime for they all have an online component. Using Google Earth to plan entry to a home for the purpose of unlawfully removing the contents is not a cyber crime because the primary target is physical property. Neither is setting fire to a telephone exchange with the intent of denying service a cyber crime, because the attack in not technical in nature, not did it occur online. The first is a burglary and the last is arson. Naturally, there is a lot of gray in this picture.

A unique feature of the Internet is that it has grown to become a technology whose evolutionary direction was largely determined by consumers before it became a tool for corporate enterprises and government. So, we find corporate and government organisations, most of them directed by people with a very limited understanding of Internet technologies and services, jumping on the Internet bandwagon in order to keep pace with their customers and users.

As these bodies have recognised the cost-savings that can also be realised through the use of the Internet, their reliance on the technology has only grown, with the result that many vital services are now delivered or controlled almost exclusively online.
The United Kingdom Threat Assessment produced by the Serious Organised Crime Agency (SOCA) now includes cyber crime and related crimes as key threats.¹ So why do we still face huge cyber security challenges in what is now a very mature market for solutions? One simple explanation to this question is that large, complex and diffuse systems are more costly to defend than to attack. The defender must succeed everywhere, every time, while the attacker only needs to succeed once. This is the case with the Internet and all of its associated or dependent systems and networks; cyber attack is the ultimate form of asymmetrical warfare.

Cyber-security awareness should be one of society’s top priorities but it isn’t even close. Our educational system, government and corporate management systems all need to be exploited to ensure that this critical risk receives the attention it needs and that the necessary skills are available in abundance. Our aim at ICT is to raise awareness and understanding so that we can all become a part of the solution.

The Threat

Many leading thinkers and agencies have independently identified cyber crime as one of the main threats to the global 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.

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.

Cyber crime at a glance

‘Cyber Crime’ refers to any crime involving the use of a computer connected to the Internet. The motives may be financial, political, anarchical or other, but the basic attack and intrusion techniques generally remain the same regardless of motive. Cyber crime is becoming increasingly complex,

¹ http://www.soca.gov.uk/threats
reflecting both the increased complexity of our cyber technology and services mix, as well as improvements in security.

**Figure 1. Cyber security asymmetry**

It is estimated that two thirds of cyber attacks in 2012 will be launched via ‘Malnets’ (malware networks) and a 240% increase in such attacks has already been reported. Blue Coat defines Malnets as “distributed infrastructures within the Internet that are built and maintained for the purpose of launching a variety of attacks against unsuspecting users over extended periods of time. They gather users, typically when they are visiting trusted sites, and route them to malware, via relay, exploit and payload servers that continually shift to new domains and locations.” Blue Coat

---

2 Source: Blue Coat
claims to be tracking more than 500 unique Malnets although they admit that not all 500 will be active on any given day. The actual size of each Malnet varies from day to day depending on the current level of malicious activities and attacks.

**Malnet visualisation (2012)**

A Malnet is comprised of unique domains, servers and websites that work together to funnel users to the malware payload. This visual mapping shows the relationships between the trusted sites that act as the entry point, the relay and exploit servers and the dynamic malware payloads.

*Source: Blue Coat*

**Figure 2.** Visualisation of a Malnet.

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.

• **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).

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.

**Social media risks**

Notwithstanding the potential for an increase in complexity, many of today’s risks are remarkable for their simplicity. Indeed, we have seen a large percentage of them before and we ought to be able to deal with many of them quite easily. Take Social Media for example.

Social networking is an Internet within the Internet. Now the communications tool of choice for hundreds of millions of users, social media services such as Facebook\(^5\) provide unprecedented access and communications capabilities at almost zero cost for billions of people. They also introduce add a new dimension to some very old risks, 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 Facebook accounts and one LinkedIn account, we were able to attract an average of 120 friends per account.

---


\(^4\) [http://www.guardian.co.uk/technology/2012/aug/09/stuxnet-gauss-virus-kaspersky](http://www.guardian.co.uk/technology/2012/aug/09/stuxnet-gauss-virus-kaspersky)

\(^5\) [www.facebook.com](http://www.facebook.com)

• 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.

During the Second World War, Allied messages to citizens on the home front often included the phrase ‘Loose lips sink ships’, implying that by carelessly talking about vessel movements, or other sensitive information, people could accidentally pass information to the enemy. In the social media domain it’s more a question of loose clicks, but the impact on personal relationships, reputations and trust can be quite dire nonetheless.

Five percent of malicious incidents in cyber space now occur within or via social networking sites8 and this problem is compounded by the ease with which anyone can create and use a fake user profile on almost any of the social media services. Facebook claims to have 900 million users, but many in the sector, including yours truly, question the basis for this claim. In fact, in disclosures9 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, perhaps making social media an investment time bomb, an additional risk that financial services firms ought to bear in mind.

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 WebMoney10 and Bit Coin11, 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, someone 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.

---

8 Source: Blue Coat
9 http://www.sec.gov/Archives/edgar/data/1326801/000119312512325997/d371464d10q.htm#tx371464_14
10 www.wmtransfer.com
11 www.bitcoin.org
Firms are increasingly allowing staff to use their mobile devices for work. According to Gartner\textsuperscript{12}, personal device usage will be the hottest topic for IT Managers for the next 10 years.

\textbf{Figure 3.} The increasingly blurred boundaries between personal and corporate device use.

This is likely to add a number of risks as users engage in the following activities:

- Use of a single device for both personal \emph{and} business purposes.

\textsuperscript{12} Source: http://www.gartner.com/it/page.jsp?id=2048617
• 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 and laptops have long been a source of what IT support teams sometimes refer to as ‘Malware Mondays’ as devices come back onto the corporate network after having spent the weekend being used at employee’s homes, but as BYOD becomes standard practice, the risks arising can be expected to become even more commonplace.

4th Generation mobile broadband

4th generation mobile broadband, or ‘4G’, is the latest manifestation of the mobile data revolution and it looks set to accelerate the blurring of boundaries described above. Unlike 3G, which took several years to get off the ground, 4G enters a market already 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 this plethora of devices that the corporate employer hesitates to purchase for them and that are therefore the user’s personal property.
• It increases the scope for remote working and working while in transit, thus exposing ever more corporate data to interception and other forms of cyber attack or intrusions while simultaneously delivering huge increases in productivity and relative competitive advantage.

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.

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 don’t only ‘virtualise’ computing and data storage; they ‘virtualise’ cyber security risks and risk management but without removing your accountability for data protection.

Who secures your users’ networks?

In today’s networked world, you provide security for only a fraction of the time your user spends in cyber space.

Figure 4. Who secures the networks your users access in the course of a normal working week?

Cyber dependency

Our collective dependency on a single set of technologies for the operation of a very broad set of essential 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 priority.

**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 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.

**Particular concerns for regulated firms**

Regulated firms face a particular set of additional issues as a result of the increasing level of cyber security risk.

**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.