



## WHITE PAPER: 06.09.11

### Cyber Security

Written by Paul Sexby

### Information (data) and cyber security

In its simplistic terms cyber security is about protecting sensitive information and allowing authorised people to have access to it, whilst keeping the unauthorised people and malicious data out.

High profile attacks (i.e. IMF, Sony) have helped demonstrate the fragility of some corporate systems; though many significant events have not been made public.

This paper aims to provide insight into some key areas of cyber security in the battle to maintain the integrity of organisations' intellectual property and brand.

*Cybercrime is big business, often conducted by highly sophisticated gangs*

#### What is cyber crime?

Cyber crime is a term used to define illegal activities undertaken by criminals for financial gain, whereby they use the Internet to attack electronic systems in order to extract information that they can sell elsewhere.

Cyber crime is big business, often conducted by highly sophisticated gangs. The criminal underworld has its own illicit economy and technical support structure offering assistance and information exchanges. If the gangs were to really organise themselves it might not be too long before they could potentially bring down a government (even a nation<sup>1</sup>) not just individuals or organisations.

It is estimated that the cost of cyber crime to the UK economy is £27bn<sup>2</sup> where the main losers are the businesses which suffer intellectual property theft. This sum incorporates the costs incurred as organisations investigate how their systems were breached, the implementation of additional measures to prevent reoccurrence, fines and penalties from legislators and regulators, and the compensation paid to the victims.

#### Risk of attacks

Internet based attacks continually grow in sophistication, and with the greatest show on earth (the Olympics) coming to the UK next year we must brace ourselves for an exponential rise in the number of incidents and potential disruption to our technology infrastructures. *(During the Beijing Olympics, China reported an 800% increase in cyber attacks; should we anticipate a greater level of such activities?)*

<sup>1</sup> Attacks against Estonia (2007) and Myanmar (2010) used 'conficker' botnet (a group of compromised computers) to conduct Distributed Denial of Service (DDoS). Estonia's financial operations were severely compromised and the government's communications networks were disrupted. Myanmar was cut off from the Internet for about 10 days ahead of general elections

<sup>2</sup> The Cost of Cyber Crime – Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, February 2011

Virus and malware attacks have changed considerably over recent years, from causing disruption to systems and services to more recently actively seeking out and facilitating the theft of personal or sensitive financial and business data.

Although an attack may not be directly focused at a specific business it may still suffer degradation in services beyond its control because we all share much of the same backbone connectivity and technology infrastructure.

Large corporations and government institutions have expended significant resources (time, effort, people and money) to prepare for and defend against malicious attacks though much of this effort has been expended on perimeter security and not always on a more strategic defence-in-depth strategy.

However, many Small to Medium-Size Enterprises (SMEs) appear at times to be blissfully unaware (or ignorant) of the risks they face; whilst others may be too overwhelmed by the potential risks that they cannot comprehend how to embark on a program to reduce them.

The interconnected, online and wireless world through which our personal and financial dealings are passed has created an enormous opportunity for the criminals, whilst reducing the potential for the perpetrators to be caught, let alone brought to justice.

*Industry experts  
claim a new  
website is infected  
every 9 seconds*

Assaults against organisations can be predominantly categorised as:

- An ex, often disgruntled, employee who believes they have a score to settle with an individual or the organisation as a whole;
- Persons committing various acts of theft and fraud for personal financial gain;
- Activist groups, such as Lulz and Anonymous who made the headlines recently. They are geographically and culturally dispersed body politics that do not align to any state or government but rather a set of ideals and have the ability to form and disperse at will, they are able to strike directly against those with which they disagree.
- Organised criminals and criminal gangs can perform sophisticated attacks with large dispersed systems and numerous resources. They frequently infect systems for later use in coordinated attacks against specific systems or mask their true intentions and activities.

## **Intellectual Property**

Data theft is not just confined to personal and financial information; Intellectual Property (IP) is often at considerable risk of theft. Given that IP is the backbone of many businesses (e.g. Coca Cola's drinks formula) having it stolen presents a substantial risk to a business.

Websites and corporate systems can be infiltrated in various ways; i.e. injection of malicious code – malware – and hacking tools that create 'back doors' into systems and applications. Once installed, these back doors are notoriously difficult to find and remove, and attackers use them to trawl internal systems in a bid to access and harvest sensitive data, commercial information, customer records, technology developments, mergers, acquisitions, draw-downs, i.e. anything that other people or organisations including competitors may be prepared to purchase. Most of this information has a good resale value if you know where to go!

## **Is Cyber Crime Victimless?**

Historically criminals have been smart and at times worked together to form highly organised gangs to attack financial institutions or armoured cars transporting cash and bonds; or even raiding high value goods in transit (i.e. TVs, cigarettes). To counter this threat, institutions have employed sophisticated methods to protect their goods by using dyes and anti-theft devices, numerous serial numbers and codes making them easier to identify and trace later.

Over time criminals have adjusted their modus operandi; there has been a marked reduction in face-to-face fraud and theft whilst online illegal activities are rising.

Stealing (electronic) data poses less personal and direct risk to the criminal and cyber crime does not respect corporate or national boundaries. There are many legal restrictions that prevent deportation/extradition of (potential) offenders.

But who is the victim, the company whose data was stolen or the individual(s) whose data it is? If an attack and data theft goes unreported how does the individual find out and take appropriate measures to limit any risks and exposures to themselves, or obtain compensation for any damages or hold organisations accountable? Theft of personal data can cause an individual great distress, particularly if the data is used to fake an identity. This is a new crime 'vector' as it's the organisation that has lost the data, but the individuals that suffer directly.

### Third Party reliance

*Most third party contracts contain insufficient provisions for recourse, remediation or recompense.*

*They are not 'fit-for-purpose' at the time they are most needed*

One of the greatest challenges faced by businesses today is understanding the use and dispersal of the vast quantities of data which is replicated many times, in different forms – the 'data diaspora' (i.e. databases, spreadsheets, tape drives, hard copy, laptops/ USB devices, CD-ROM, DVD, BlackBerry, PDA, iPad to name but a few).

Businesses rely on third parties for numerous services in the processing of their data. Often with weak, almost non-existent, contracts or Service Level Agreements (SLA) that define the parties' responsibilities. Consequentially there is little obligation to provide any notification if they suffer a security incident which might affect and undermine the systems or data they process; furthermore there is no provision for recourse, remediation or recompense.

The following illustration captures the most common areas where organisations use third parties; and through whom sensitive and personal business/client data is processed on its behalf.

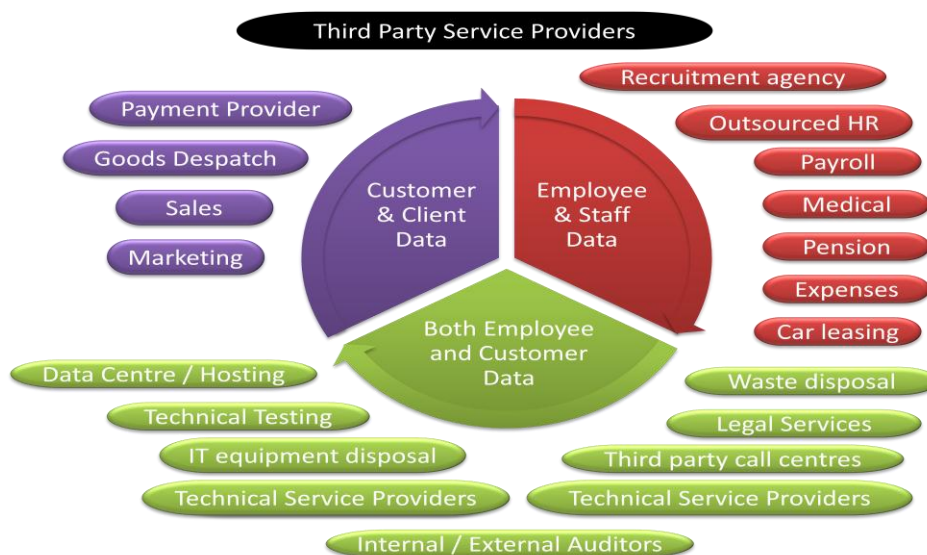


Figure 1 – Third Party Data Processors

At the critical time when companies most need to rely or call upon their contracts and SLAs they often find they are not fit for purpose, leaving them with all the costs and impacts of resolving the incident which may also include compensating the victims.

Third parties that process data or provide services and infrastructure through which another businesses' data is handled are required to align to a Data Processor Agreement. This agreement defines their responsibilities and obligations to safeguard that data, systems and infrastructure to the level mandated by the data/business owner, who in turn should conduct periodic due diligence to ensure such requirements are being adhered to.

### **Power of the consumer**

Consumers are growing increasingly frustrated and becoming more vocal in venting their anger relating to breaches and invasions of their personal data.

The first some companies know of a data breach is when a customer has tweeted or posted information online somewhere, rather than from their own monitoring systems. Consumers are turning technology and 'people power' to hit back at organisations. This can very quickly damage a brand globally because the notification of a data breach has the potential to go 'viral' in minutes.

### **Risk Analysis**

Businesses have to take appropriate ownership of customer, stakeholder, partner, investor, shareholder and employee data held and processed in their systems or on their behalf by third parties. It's essential that companies exercise their governance responsibilities through the dissemination of the appropriate policies (rules) to be followed by employees or in contracts and SLAs with their service providers.

In its simplistic form a Risk Assessment comprises a process that:

- **Identifies Assets** – determines exactly what data/information (including IP) is critical to business operations, where this data resides, in what form, how and with whom is it shared or used (internally and externally), how and when is it subsequently removed, archived and/or destroyed.
- **Assesses the Risks** – the various threats to which the business, systems and data are likely to be exposed, both external and internal against the likelihood of specific event or series of events causing a threat to materialise.
- **Mitigates the risks** – through the application of appropriate and proportionate controls to reduce and mitigate highest risks first.
- **Monitors and maintains** – conducting regular reviews to ensure the appropriate controls are applied and functioning as required, and that no new threats or business requirements/exposures have emerged.

Effective risk management should be aligned with appropriate information security controls that result from a risk assessment based upon the organisations' risk appetite.

Whilst companies may delegate tasks to other third parties they retain ownership and responsibility for ensuring appropriate controls are applied and adhered to.

### **Cyber crime reporting**

The UK does not have disclosure laws (unlike the USA) but this is gradually changing and as a direct result of recent high-profile attacks legislation is being drafted in the European Union<sup>3</sup> (EU) that could significantly change reporting requirements for businesses.

Businesses and law enforcement agencies must work better together to tackle cyber crime, however companies will not (willingly) declare they have had any security issues or breaches because of the potential reputational and brand damage that might ensue.

---

<sup>3</sup> EU Justice and Rights Commissioner (Viviane Reding) speaking at the British Bankers Association (BBA) Data Protection and Privacy Conference 22 June 2011

Reporting such crimes can be a challenge in itself as many police forces lack the skills and resources to investigate such activities. If the police are fortunate enough to identify a perpetrator, unless they are located in this country actually being able to extradite and convict them through the protracted legal system only adds to the challenge; to many organisations it is just not worth the effort.

### **Cost of cyber crime**

As previously stated the cost to the UK economy last year from cyber crime is estimated to have been a staggering £27bn. To the organised criminal gangs, or individuals who wish to make an impression upon them, this can be a highly lucrative business. The relative ease of access into many systems and the ability of the attacker to hide their tracks through cyber space make the likelihood of them being caught quite low.

The cost of cyber crime does not fall evenly across business sectors. Organisations, irrespective of sector must prevent haemorrhaging their valuable intellectual property or the costs of cyber crime and the impacts upon them will undoubtedly rise even further and faster than they are currently.

### **Synergy of controls**

Effective cyber security is a synergy and balance of controls that embrace the People, Policy and Processes through which data is handled and that is underpinned by appropriately configured technology with regular monitoring, reviews and testing to ensure the necessary controls are in place to provide a level of assurance that they have not been tampered with, bypassed or superseded.

There are numerous regulatory and best practice guidance available to assist organisations assess and align appropriate controls to their business sensitive data and systems but many organisations tackle cyber security tactically rather than strategically.

The majority of organisations most at risk of cyber crime fall outside the umbrella of the Critical National Infrastructure<sup>4</sup> (CNI) with the exception of finance. Contributing factors to this are that those within the CNI do not rely on the Internet to sell their products and services and they are more heavily regulated and audited to ensure they have appropriate controls in place.

### **Conclusion**

As companies rely upon technology and the use of cyber space to interconnect their systems, it has become increasingly clear that the criminals have obtained the tools and developed the skills to access and exploit these systems almost at will and are able to use the information obtained for financial gain.

Both private and public sectors have a significant role to play in reducing the risks and likelihoods of these crimes being successful, as a minimum by complying with security regulations and industry standards as well as conducting regular technical checks of their systems to better protect themselves from exploitation.

Underreporting cyber crime also plays a part in the perception of businesses as to the wider risks and potential of such activities affecting them; because they have not heard about it sufficiently they believe that it is overhyped and an unrealistic threat. That is until they suffer a breach.

---

<sup>4</sup> For a definition of CNI visit the Centre for the Protection of the National Infrastructure website at [www.cpni.gov.uk](http://www.cpni.gov.uk)