The Enemy Within: The Challenge for Business from Cyber-attack

Michael Reynolds(✉)

GSM-London, London, UK
Michael.reynolds@gsm.org.uk

Abstract. This paper presents an overview of certain risks posed by cyber abuse in the business context. It does not in any way represent a definitive study of **this** very complex area which is in a state of constant flux to the extent that the laws of nations cannot keep pace with the challenges of today let alone tomorrow. This paper therefore gives warning of this phenomenon and focusses on the role of business to its management and staff and others affected by its IT structure. The paper gives some analysis of the threats from cyber-crime and abuse from a variety of government agencies and other bodies. The underlying theme is one of caution and warning of the enemy within organisations and outside who use cyber-attack as a means to an end.

Keywords: Cyberattack · Risk · Cyber law

1 Introduction

These days anyone with a computer is liable to cyber-attack. It can be extremely frustrating and costly for academics as well as businesses. Even worse it can damage the country's economy and in many respects cyber war when global organized cybercrime can be as deadly as actual military hostilities. Cyber-attack can steal your identity, steal the money out of your bank account, destroy final business information, breach client confidentiality, and even destroy State security and vital intelligence that becomes useless when made public.

Whilst everyone has got a computer very few people know how computers work and even fewer people are aware of the very real security risks they run whether they use a mobile phone, a laptop computer or an iPad.

In a society like the UK where shopping on line is the increasing norm and where in 2008 the value of on line retail sales was £48 billion and 57 % of individuals ordered goods or services on line £328m was stolen from credit card holders. Theft of copyright in music and film was estimated at £180m. and the loss to the economy in terms of non-delivery issues was £55m per year.[1]

[1] Consumer Survey, Office of Fair Trading.

© Springer International Publishing Switzerland 2015
H. Jahankhani et al. (Eds.): ICGS3 2015, CCIS 534, pp. 123–136, 2015.
DOI: 10.1007/978-3-319-23276-8_11

The best description of the risk is probably that expressed by NW3C[2] who recently reported:

Criminal Use of Social Media (2013)

> *Defining social media is difficult because it is ever changing like technology itself, but for the purposes of this paper, social media will be defined as any website or software that allows you to receive and disseminate information interactively.*
>
> *The tremendous rise in popularity of social media over the past seven years has led to a drastic change in personal communication, both online and off. Comparing to the world population clock, the total world population is around 7.06 billion. With that being said, the popularity of sites such as Facebook, (1.06 billion monthly active users). YouTube (800 million users), Twitter (500 million users), Craigslist (60 million U.S. users each month) and Foursquare (has a community of over 30 million people worldwide) has connected people from all over the world to each other, making it easier to keep in touch with friends, loved ones, or find that special someone. In addition to personal usage, businesses and the public sector use social media to advertise, recruit new employees, offer better customer service, and maintain partnerships. In fact, 65 % of adults now use social media. Social networking is the most popular online activity, accounting for 20 % of time spent on PCs and 30 % of mobile time. As social interactions move more and more online, so does the crime that follows it.*

In countering this threat the United States is the world leader. Unique amongst many countries the US has extra territorial jurisdiction to enforce many of its laws that other countries may not or are unwilling to extend their court's jurisdiction. This is a highly contentious area of international law and one which requires considerable review and development, a subject for a far more detailed analysis which is outside the scope of this overview.

A key player in the United States and in the world is the Federal Bureau of Investigation (FBI). An organisation which became famous in the 1930s depression fighting gangsters and in the 1960s under Attorney General Robert Kennedy fighting organized crime.

The FBI states that: *The FBI has the authority and responsibility to investigate and enforce all violations of federal law that are not exclusively assigned to another federal agency.*

- *Title 28, USC Sect. 533 & 28 CFR 0.85*
- "*The Department of Justice and the FBI lead the national effort to investigate and prosecute cybercrime.*"
- The President's National Strategy to Secure Cyberspace, 2003

The FBI further states that it:

> *"has a unique dual responsibility, to prevent harm to national security as the nation's domestic intelligence agency and to enforce federal laws as the nation's principal law enforcement agency. These roles are complementary, as threats to the nation's cybersecurity can emanate from nation-states, terrorist organizations, and transnational criminal enterprises; with the lines between sometimes blurred.*
>
> *The FBI's unified mission brings all lawful investigative techniques and legal tools together in combating these threats. This approach facilitates information sharing and ensures*

[2] The Internet Crime Complaint Centre. Partners: The Federal Bureau of Investigation, Bureau of Justice Assistance U.S. Department of Justice and the National White Collar Crime Centre.

responsible stewardship of resources by collocating talent, tools, and institutional knowledge in a single organization."

Whilst the FBI have oversight of such matters the specific IC3 is the partnering organisation that deals with cyber complaints in the United States and elsewhere.

In 2012 the IC3[3] reported that there were 289,874 consumer complaints when a loss of $525,441,110, an 8.3 % increase reported losses since 2011.The IC3 s success has led to the UK and other countries adopting similar centres.

Of those 289,874 complaints 114,908 reported losses. The average total loss overall to all complaints was $1,813. The average dollar lost to those reporting such loss was $4,573. What a United States the largest number of complaints was received from the state of California at 13.41 % and the lowest from Washington State at 2.72 %.

On a countrywide basis the percentage of victim complainants ranked as follows:

- United States: 91.2 %
- Canada:1.4 %
- UK: .9 %
- Australia: .7 %
- India: .6 %

2 Cyber-Crime Auto-Fraud

One key area of the cybercrime is auto-fraud. This is where criminals pose as car salesman selling stolen cars instructing their victims to send the payment to a third-party agent by wire transfer service. Usually the criminal pockets the money and does not deliver any vehicle. IC3 have reported that in 2012 there were 17,159 complaints where the victims lost the sum of $64,572,324.

2.1 Impersonation Email Scam

Government agencies in America do not send unsolicited emails. However IC3 received complaints at the rate of 47 per day resulting in victims losing more than $6,604 per day to this scam. These scams are dangerous and undermine confidence in the government agencies. The FBI identified this as including elements of Nigerian scam letters (419 scams) incorporating get rich inheritance scenarios, bogus lottery winning notifications and occasional extortion threats. In 2012, there was a total of 14,141 complaints with victims losing the sum of $4,672,985.

2.2 Frequently Reported Internet Crimes

(a) Telephone Calls

A number of victims received unsolicited telephone calls from foreigners posing as representatives of software companies. The victims were advised that malware had been

[3] The Internet Crime Complaint Centre. Partners: The Federal Bureau of Investigation, Bureau of Justice Assistance U.S. Department of Justice and the National White Collar Crime Centre.

detected on their computers and was an immediate threat. The fraudsters pressured victims into logging onto their computers where they were directed to a utility area which appeared to demonstrate how their computer was infected. The fraudsters' then offered to rid the computers of the malware the fees ranging from $49-$450. When the victims pay the fees they are then asked to complete Western Union authorisation so the money could be taken out of their account. Thus, the fraudsters gained access to the computers and all the information on the computers as well as pocketing the proceeds. This is a very common crime and the criminals have been known to operate from Africa and Pacific region.

(b) **Payday Loans**

The payday loan scam reported by IC3 involves victims receiving harassing telephone calls from fraudsters claiming the victim is delinquent in payment. These criminals have accurate information as to social security numbers, dates of birth, addresses, employer information, bank account numbers and names and telephones of relatives and friends. All this may be obtained from any social media that the victim may have innocently visited. The victim is harassed and often subjected to threat of assault or legal action and often this is directed at relatives, friends and employers.

(c) **The Grandparent Scam**

Here the scan involves quite elderly individuals claiming to be a grandson granddaughter or whatever who happens to be a young relative in a legal or financial crisis. It generally involves claims being arrested in a car accident another country. The caller's great sense of urgency and make a desperate plea for money making the grandparents agree not to tell the parents and consequently often preventing potential victims from discovering the scam. These criminals have often impersonated embassy officials or attorneys and ask the victims to transfer money to a special or a specified individual. These criminals have been operating from Canada, United States, Mexico, Guatemala Peru and the Dominican Republic. They use telephone numbers generated by free apps so the burgers telephone number appears on the recipient's caller ID.

IC3 reported that for 2012 the loss incurred in these cases amounted to $10,624,427 for 8,324 reported instances.

Other Internet fraud involves real estate and IC3 reported that in 2012 the sum of $15,418,734 was lost to fraudsters rental scams, timeshare marketing scams and loan modification scams[4].

In 2012, IC3 processed 289,874 complaints representing more than half a billion dollars in losses.

In 2013, IC3 processed 262,813 complaints the losses recorded for that year amounted to $781,841,611. [2013 Internet Crime Report IC3] 90.63 % 0f the complaints emanated from the US .85 % from the UK.

[4] 2012 Internet Crime Report IC3 p.15. www.ic3.gov.

3 EU/COE Joint Project on Regional Co-operation Against Cybercrime[5]

This report evaluated the cyber security policies of several countries in eastern Europe including Turkey Albania, Bosnia Herzegovina, Croatia, Kosovo, Serbia and the former state of Montenegro. Whilst some had taken effective steps to protect their networks many had not done so. Governments were encouraged to ensure that their national data protection legislation complied with the principles of the Council of Europe's data protection convention ETS 108 and to participate in the Convention's current modernization process. The same applied to the future data protection standards of the European Union. This could facilitate transborder sharing of data also for law enforcement purposes.

The report concluded (p.121):

> *In all countries and areas participating in the CyberCrime@IPA project, the creation or strengthening of police-type cybercrime units is in progress and the specialisation of prosecutors is under consideration in some. This process should be pursued. It is essential to understand that technology changes day by day and that the workload of cybercrime and forensic units is increasing constantly. The resourcing (staff, equipment, software) and maintenance of specialised skills and the adaptation of such units to emerging requirements is a continued challenge.*

It also recommended that:

> *All law enforcement officers – from first responders to highly specialised computer forensic investigators – need to be enabled to deal with cybercrime and electronic evidence at their respective levels. Elements of law enforcement training strategies have been identified, but not yet fully implemented.*[6]

Perhaps more importantly the report recommends the need for:

> *A Regional Pilot Centre for Judicial Training on Cybercrime and Judicial Evidence is being established. These achievements need to be institutionalised.*
>
> *Enabling all judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence in criminal proceedings should remain a strategic priority.*
>
> *Relevant authorities should consider the following actions:* ***Mainstream judicial training on cybercrime and electronic evidence****. Domestic institutions for the training of judges and prosecutors should integrate basic and advanced training modules on cybercrime and electronic evidence in their regular training curricula for initial and in-service training.*
>
> Whilst this may be recommended for Eastern Europe it is surely essential that the judiciary in all countries attain this level of competence in this vital area.

Another vital suggestion in the report was that there should be:

> *Memoranda of understanding between law enforcement and Internet Service Providers are a fundamental tool in this respect. Regional coordination of such MOUs would facilitate the ability*

[5] Strasbourg, 18 June 2013, Data Protection and Cybercrime Division, Council of Europe, Strasbourg. Data Protection and Cybercrime Division Directorate General of Human Rights and Rule of Law Council of Europe, F-67075 Strasbourg Cedex (France).

[6] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf.

> *of law enforcement authorities to conduct investigations across regional borders, with the knowledge that comparable standards have been adopted in other countries and areas. MOUs combined with clear rules and procedures may also facilitate the cooperation with multinational ISPs and other private sector entities including in the disclosure of data stored in foreign jurisdiction or on cloud servers that are managed by these ISPs. [p.127]*

Finally the Report concluded p.126:
"Governments should consider the following actions:

- ***Exploit the possibilities of the Budapest Convention on Cybercrime and other bilateral, regional and international agreements on cooperation in criminal matters.*** *This includes making full use of Articles 23 to 35 of the Budapest Convention in relation to police-to-police and judicial cooperation, including legislative adjustments and improved procedures. Governments (parties and observers to the Convention) should fully participate in the 2013 assessment of the international cooperation provisions of the Budapest Convention that will be undertaken by the Cybercrime Convention Committee (T-CY). They should follow up to the T-CY assessment of 2012 and promote the use of Articles 29 and 30 of the Budapest Convention regarding international preservation requests.*
- ***Provide for training and sharing of good practices.*** *Authorities for police and judicial cooperation should engage in domestic, regional and international training and the sharing of good practices. This should facilitate cooperation based on trust.*
- ***Evaluate the effectiveness of international cooperation.*** *Ministries of Justice and of Interior and Prosecution Services should collect statistical data on international cooperation requests regarding cybercrime and electronic evidence, including the type of assistance requests, the timeliness of responses and the procedures used. This should help identify good practices and remove obstacles to cooperation. They may engage with regional partners in an analysis of the issues adversely affecting international cooperation.*
- ***Strengthen the effectiveness of 24/7 points of contact.*** *Such contact points have been established in all countries and areas in line with Article 35 Budapest Convention, but their role needs to be enhanced and they may need to become more pro-active and fully functional.*
- ***Compile statistics on and review the effectiveness of 24/7 contact points and other forms of international cooperation on a regular basis.****"*

All these measures seem entirely sensible in the light of the threats described by IC3 and other agencies. It expresses good intentions and it is easier for governments to give vague expressions of intent and declarations, but actions speak louder than words and what is missing is enactment and enforcement.

4 Cybercrime in the UK

In its Cyber Crime Strategy Report of March 2010 the Home Office reported:

> *The number, sophistication and impact of cyber crimes continues to grow. These threats evolve to frustrate network security defences, and many business systems and home computers do not keep what protection they have up to date. "Hacking" has evolved from the activity of a small*

number of very technical individuals to an increasingly mature marketplace where technical skills and data can be purchased by criminal groups to carry out specific attacks. The trend therefore is for growth in the threat to internet security, as evidenced by the following figures:[7]

- *In 2008, 55,389 phishing website hosts were detected, an increase of 66 % over 2007.*
- *A 192 % increase in spam detected across the internet, from 119.6 billion messages in 2007 to 349.6 billion in 2008. The most common type of spam detected in 2008 was related to internet or computer related goods and services which made up 24 % of all detected spam.*
- *Active bot-infected computers – an average of 75,158 per day, showing an increase of 31 % from the previous period. In 2008, bot networks were responsible for the distribution of about 90 % of all spam e-mail.*

The Government's Serious Crime Bill, Part 2, Computer Abuse factsheet considers how the Government plan to tackle cyber-crime in the Serious and Organised Crime Strategy, published in October 2013.

The factsheet discusses The Computer Misuse Act 1990 ("the 1990 Act") which sets out the offences associated with interfering with a computer (i.e. hacking) and the associated tools (such as malware) that enable computer systems to be breached. It does not contain any powers. The 1990 Act makes unauthorised access to, or modification of, computer material unlawful, creating four offences.

Section 1 provides that the basic offence is of unauthorised access to computer material, for example by logging onto a system or accessing parts of a system for which additional authorisation is required by using another person's user ID and password. This offence is triable either in a magistrates' court or the Crown Court, with a maximum sentence of 2 years' imprisonment.

More serious offences are committed where the purpose of the unauthorised access is to commit or facilitate the commission of another offence (Sect. 2) or to impair the operation of the computer or hinder access to the programmes or data it contains (Sect. 3).

Section 2 offences would include, for example, unauthorised access to transfer money and so commit theft, or theft of sensitive data to be used for blackmail.

Section 3 offences include circulating viruses, deleting files, inserting a "Trojan Horse" to steal data or mounting a Denial of Service attack. Sections 2 and 3 offences are both triable either way, with maximum sentences of 5 and 10 years' imprisonment respectively.[8]

Section 3A deals with making, supplying or obtaining articles for use in offences under Sects. 1 or 3. This offence is also triable either way, with a maximum sentence of 2 years' imprisonment.(Section 3A has only had two prosecutions in England and Wales over the last three years. The problem is that Sect. 3A does not meet the EU Directive Article 7 requirement regarding "the intentional production, sale, procurement for use, import, distribution or otherwise making available "of tools with the intention that it is used to commit any further offences.[9]

[7] Internet Security Threat Report" – Symantec, October 2009.

[8] Home Office June 2014.

[9] Home Office June 2014.

Part 2 of the Bill amends the 1990 Act to:

1. Create a new offence of unauthorised acts causing serious damage;
2. Implement the EU Directive on Attacks against Information Systems; and
3. Clarify the savings provision for law enforcement.

The new offence in clause 37 addresses the most serious cyber-attacks, for example those on essential systems controlling power supply, communications, food or fuel distribution.[10]

The new offence applies where an unauthorised act in relation to a computer results, directly or indirectly, in serious damage to the economy, the environment, national security or human welfare, or a significant risk of such damage (where damage to human welfare encompasses loss of life, illness or injury or serious social disruption). A significant link to the UK is required, so that at least one of the accused or the target computer at the time of the offence or the damage must have been in the UK, or the accused must be a UK national at the time of the offence and the conduct constitute an offence under the law of the country in which it occurred. The accused must have intended to cause the serious damage, or to have been reckless as to whether it was caused. This offence is more serious than the existing Sect. 3 offence and is triable only on indictment (in the Crown Court). Where the attack results in loss of life, serious illness or injury or serious damage to national security the maximum sentence is life imprisonment, where the attack results in serious economic or environmental damage or social disruption the maximum sentence is 14 years' imprisonment.[11]

The EU adopted a Directive on attacks against information systems in August 2013. The aim of the Directive is to establish a set of minimum rules within the European Union on offences and sanctions relating to attacks against information systems. It also aims to improve cooperation between competent authorities in Member States. The Government has until 4 September 2015 to transpose the Directive into UK law.

In 2013, the government introduced the Cyber Essentials Scheme providing a set of controls that organizations could implement demonstrating that they had met a recognised baseline.[12]

4.1 Common Forms of Cyber Attack

Cyber attacks coming for stages:

1. Survey
2. Delivery
3. Breach
4. Attack.

[10] Home Office June 2014.

[11] Home Office June 2014.

[12] Cabinet Office https://www.gov.uk/government/organisations/cabinet- office. Accessed: 10/02/15.

In 2013 the government reported 81 % of those companies that reported a breach of security suffered losses or between £600,000 and £1.15 million.[13]

When it is considered that the cost of IT is excessive and in many cases a scandalous waste of public money in terms of the IT systems provided for the Ministry of Justice and the NHS where the providers were paid millions of pounds of taxpayers money and the systems proved completely unworkable is learning how to ensure that many more millions of pounds are not wasted because the systems are totally insecure. What is worse is the amount of time and money that is expended with IT which is increasingly perceived as being manipulated by the manufacturers and so-called geeks who run the systems.

The time has come, if not long passed to stop this nonsense and produce systems that are not all things to all men, not play toys or gimmicks, and are specifically designed for business to satisfy its real needs and no other. Similarly for academics systems must be designed which are capable of precise measurement of statistics and scientific analysis meeting the demands required by science and industry. Today's computers and IT systems are just not up to this task and they are not fit for purpose. The dangers of all this and the lack of awareness are highlighted in the research undertaken by Professor Jahankhani.[14]

The measures one is advised to take seem pitiful when compared to the sophistication of global organized crime and states that sponsor cyber terrorism and attack.

The measures one is advised to take appear to be the only measures that can be taken and these include:

1. Risk management education outlined in the governments paper 10 Steps: User Education and Awareness;[15]
2. Patch management; this applies patches purchased at the earliest possibility to limit exposure to know software new vulnerabilities; therefore simpletons to keep software updated to deal with the potential of software bugs;
3. Secure configuration; it is advised to remove unnecessary software and default user accounts. It is advised that default passwords or changed and that automatic features that could activate malware are turned off.
4. Restrictions on user access to applications, privileges and data;
5. Monitoring and analyzing all network activity to identify any malicious or unusual activity; security monitoring will be necessary where the organisations more likely to be attacked to identify any unexpected suspicious activity; businesses should also having place and effective response to reduce the impact of an attack on the business.

[13] 2014 Information Security Breaches Survey sponsored by the Department for Business Innovation and Skills.

[14] Jahankhani, H., Al-Nemrat, A., Hosseinian-far, A. (2014) "Cybercrime classification and characteristics" in Cybercrime and Cyber Terrorism Investigators' Handbook, Elsevier, ISBN 978-1447126829. And in Jahankhani, H. (2013) "Developing a model to reduce and/ or prevent cybercrime victimization among the user individuals", in Strategic Intelligence Management, Springer, ISBN 978-0124071919.

[15] Cabinet Office https://www.gov.uk/government/publications/ 10 steps to cyber security advice sheet. Accessed: 10/02/15.

6. It is important that all staff are properly trained in reducing the risks of successful social engineering attacks;
7. Malware protection within the Internet gateway which can detect malicious codes in imported items;
8. Network perimeter defences which can block insecure or unnecessary services what only now permitted websites to the access; this can be achieved by establishing web proxy, web filtering, content checking, and firewall policies to detect and block executable downloads, blocked access to known malicious domains, and prevent users computers from communicating directly with the Internet.
9. Malware protection which can block malicious emails and prevent malware from being downloaded from websites;
10. Password policy which can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts;
11. Device controls within the Internet gateway can be used to prevent unauthorized access to critical services or inherently insecure services that may still be required internally;
12. Secure configuration and restricted System functionality to devices used in the business.
13. White listing and execution control can prevent unknown software from being able to run or install itself including auto run on USB and CD drives.

4.2 Business at Risk

Business can be at risk where does not establish clear security guidelines for employees. For example, many employees may download material from insecure sites, may use USBs or portable hard drives for their own uses which might potentially important malware and compromise business data.

Confidentiality is essential in most businesses. In the legal profession all client information and data, the Instructions to counsel, advice to client and any advice given privileged from disclosure. If such information comes into the public tonight there are serious consequences for the law firm not only is it a preacher client confidentiality, a breach of obligation to the client but a disciplinary matter.

4.3 Types of Cyber Attack Exposure

There are several types of attack to which businesses may be exposed. These may include:

(a) Connection to and trusted network;
(b) Denial of access to services and information;
(c) Compromising the system or the service.
(d) Unauthorised access compromising confidentiality, integrity and availability of systems, services and information.

A number of measures may be taken to reduce the risk of these attacks has referred to below in the security policy measures.

4.4 Security Policy

Each firm should adopt a security policy and special operating procedures with security control. Regular surveillance and monitoring is therefore essential to maintaining security and keeping client confidentiality. Government has reported that some individuals may release personal sensitive commercial information, or abuse the system or their privileges in gaining unauthorized information, they may also steal or damage the computer system.

4.5 Security Policy Measures

The government recommend that all businesses follow the network design principles of ISO/IEC 27033-1:2009 to help define the necessary security qualities for the perimeter and internal network segments and ensure that all networked devices are configured to the secure baseline build.[16]

Businesses should limit access to network ports, protocols and filtering, inspecting all traffic at the network perimeter to ensure that only traffic which is required to support business is being exchanged. Technical controls that should be implemented to scan for malware and other malicious content.

Businesses should install firewalls to form a buffer zone between interested external network and the internal network used by the business. A white list should be applied that only allows authorized protocols, Ports and applications to communicate with authorized networks and network addresses. This should reduce the exposure of the ICT systems to network-based attacks.

The government have warned in their 10 Steps: Network Security that untrusted networks expose corporate networks to attacks that can compromise confidentiality, integrity and availability of Information and Communications Technologies (ICT).[17]

Anti-virus and malware checking solutions should be utilized to examine both inbound and outbound Data at the perimeter in addition to antivirus and malware protection deployed on internal networks and on host systems.

There should be no direct network connectivity between internal systems and systems hosted on trusted networks. The business should identify a group and isolate critical business information assets and services and apply appropriate ductwork security controls to them.

Wireless devices may be especially vulnerable and therefore wireless devices should only be allowed to connect to trusted wireless networks. Wireless access points should be secured. Security scanning tills should have the ability to detect and locate unauthorized wireless access points.

The government further advises that the anti-virus and malware solutions use of the perimeter should be different to those used to protect internal networks and systems in order to provide some additional defence in depth.

[16] Cabinet Office https://www.gov.uk/government/publications/ 10 steps to cyber security advice sheet. Paras 3 and 3.1. Accessed: 10/02/15.

[17] Cabinet Office https://www.gov.uk/government/publications/ 10 steps to cyber security advice sheet. Accessed: 10/02/15 Summary.

4.6 Training

All staff should be trained, monitored, and given further periodic training in security. Staff should be aware that the users of the system are the weakest link as they are always the target for phishing attacks, social engineering etc. In many instances a successful cyber attack only requires one user to divulge log on credentials or open an email with malicious content. Ideally new staff should be inducted into the company's security policies and also made aware of their employment obligations with regard to information and cyber security whilst in the course of their employment. This should be subject of contract terms of engagement and also supervisory control and disciplinary sanction.

Regular briefings from the company's IT experts or updates with regard to current threats should be given.

The company should have on its staff persons who are qualified in information assurance (IA) skills such a system administrators, incident management team members, and forensic investigators. If there are any serious incidents investigation should be carried out in accordance with the companies security procedures. The incident needs to be fully recorded and reported and then properly investigated. Where serious information has been late all systems have been damaged in legal proceedings maybe necessary and therefore important that any hard or software be examined and produced in evidence.

Staff should be tested on their knowledge and asked what steps they vaguely take to prevent risk.

Staff should report any untoward incidents and to voice their concerns about poor security to senior managers and senior management should accept their responsibilities accordingly.[18]

All the above advice he Is critical to running a safe and secure business. In 2011 Ernst & Young published a report entitled: Ever-increasing fraud risks in the IT and ITeS sector. They looked at the reasons for fraud hand blazing means of preventing and deterring employees/vendors from committing fraud. One of the problems they found that although certain businesses had policies in place they were not communicated to staff.[19] Alarmingly they pointed to:

> *"an absence of dedicated efforts/specialised skill sets to prevent/detect fraud under pressure situations. The internal audit teams may not be equipped with the necessary skills/tools required to prevent and/or detect frauds by employees/others."*

They also pointed to the fact that over the last five years i.e. from 2006 to 2011 they had detected and noted:

> *that senior/middle management employees, who have obtained a higher level of trust and responsibility within a company, are more likely to commit fraud by misusing the authority and trust bestowed on them."*

[18] Cabinet Office https://www.gov.uk/government/publications/ 10 steps to cyber security advice sheet. Accessed: 10/02/15.

[19] Ernst & Young. Ever-increasing fraud risks in the IT and ITeS sector. (2011) p.4.

This is pretty much an indictment of business organisations in the UK is a dangerous time when the economy was on the brink of collapse. It is it begs the questions not only about corporate governance, not only about business efficacy, and not only about management efficacy, but also about professional and ethical standards in the UK at that time and even now.[20]

What Ernst & Young advise and what is entirely sensible is that businesses create an antifraud environment. Each business should have a code of business conduct and ethics policy and describe what will be considered as unethical or unacceptable behavior. Employees should be free to report any unethical behavior, misconduct, or criminal or fraudulent activity without fear of victimization or oppression or other disciplinary action or retaliation of some kind. The business should undertake a comprehensive fraud risk assessment and insure it has an effective framework and in place.

They also recommend that there should be adequate monitoring procedures in place to review and improve the effectiveness of anti-fraud programs and controls. The measures they suggest are:

(a) Employees annual declaration of 100 % compliance with the code of business conduct and anti-fraud policies;
(b) Adequate review/monitoring process to ensure that tipoff's/complaints made through fraud hotlines are investigated/I dressed appropriately;
(c) Oversight by audit committee of the risk of override of controls by management.

The questions that need to be asked are whether there is sufficient documentation relating to the full policy, code of conduct and ethics. Has the coping communicated, is there an effective whistleblower mechanism, is the management team trained sufficiently, is there a full prevention health check, does the risk assessment process specifically cover the risk of fraud, is the internal audit team adequately equipped to cover the risk of fraud, other adequate tools to detect suspicious unfortunate transactions, and does the business have the necessary skill sets to investigate fraudulent/dishonest acts?

5 Conclusions

In this paper we have noted that cyber-attack is an ever resent problem and that despite all efforts of various agencies to counter this phenomenon it remains an ever present danger to business. We have also noted however the concerted efforts and declarations of intent by many states, including those in Eastern Europe to act in concert against these threats. Regulation is being reviewed and revised, new laws are being introduced and judges are encouraged to have specialist training in this area. Be that as it may the fact is that according to the UK Home Office in 2010 there were 75,158 computers bot infected. In the 21st century it must therefore be asked whether business can afford such systems when so much time is wasted sorting out IT problems. Have we not reached the point where each profession should have its own system? Most computers are designed

[20] For an example of the concerns raised at the highest levels of international arbitration see; Michael Reynolds PhD (LSE) Ethics in International Arbitration. Legal Ethics December 2014.

for public use with entertainment a key component, social media etc. Does business require all this? Do academics? Perhaps the time has come for a critical re-evaluation of what we need these systems for and to limit their use for specific defined purposes which may be more secure. The rate and extent of abuse cannot be sustained in terms of time or cost because the preventative measures that were successful yesterday and which succeed to day may not succeed tomorrow.