

LLOYD'S



# DIGITAL RISKS

VIEWS OF A CHANGING RISK LANDSCAPE

LLOYD'S EMERGING RISKS TEAM REPORT

## **DISCLAIMER**

This document is intended for general information purposes only. Whilst all care has been taken to ensure the accuracy of the information, Lloyd's does not accept any responsibility for any errors and omissions. Lloyd's does not accept any responsibility or liability for any loss to any person acting or refraining from action as the result of, but not limited to, any statement, fact, figure, expression of opinion or belief contained in this document.

## **CONTACT DETAILS**

### **Director of Franchise Performance**

Rolf Tolle

020 7327 6743

rolf.tolle@lloyds.com

### **Head of Exposure Management**

Paul Nunn

020 7327 6402

paul.nunn@lloyds.com

### **Emerging Risks Team**

Trevor Maynard

020 7327 6141

trevor.maynard@lloyds.com

David Baxter

020 7327 6439

david.baxter@lloyds.com

### **Communications Team**

Bart Nash

020 7327 6272

bart.nash@lloyds.com

## **ACKNOWLEDGEMENT**

Our thanks go to the many experts who have given their views to inform this report. In particular, we would like to thank the Lloyd's Emerging Risks Special Interests Group, representatives of the Lloyd's market, for their comments.

© Lloyd's 2009

# CONTENTS

<b>Executive summary</b>	<b>3</b>
<b>Purpose</b>	<b>4</b>
<b>Emerging Risks Team</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
<b>History</b>	<b>6</b>
<b>Terrorism and crime</b>	<b>7</b>
<b>Mobile device vulnerabilities</b>	<b>14</b>
<b>Cloud computing</b>	<b>15</b>
<b>Web 2.0</b>	<b>17</b>
<b>GPS failure</b>	<b>18</b>
<b>Natural and man-made disasters</b>	<b>21</b>
<b>Conclusion</b>	<b>22</b>
<b>Sources of information</b>	<b>24</b>

# EXECUTIVE SUMMARY

## **1. NEW TECHNOLOGIES HAVE TRANSFORMED THE RISK LANDSCAPE AND BUSINESSES AND INSURERS NEED TO KEEP PACE WITH THE CHANGES.**

In less than fifty years, cyber space has profoundly changed all areas of modern society. Digital technology powers credit card transactions and basic services such as power and water supply. It enables hospitals to monitor and treat patients and defence systems to function. The staggering speed of development makes it difficult for managers to keep pace with risks. But the increasing level of reliance on digital technology means they must.

## **2. TRENDS SHOW A SHIFT FROM VIRUSES TO “SILENT” CYBER CRIME – MORE CRIMINALS ARE ATTEMPTING TO BREAK IN AND STEAL VALUABLE DATA WHILST REMAINING UNDETECTED.**

Many different types of people seek to carry out digital attacks: terrorists, hackers, cyber vandals, criminals, even disgruntled employees. These different groups have diverse motives ranging from financial gain to espionage, or even as a means of revenge. Businesses should consider who poses the biggest threat to them and ensure that they have adequate security measures in place.

## **3. THE IMPACT ON BUSINESS CAN RANGE FROM THE MERELY IRRITATING – A DISGRUNTLED EMPLOYER BLOGGING - TO THE DISASTROUS – THE LOSS OF MILLIONS OF POUNDS.**

The potential impacts of a digital attack or breakdown include: reputation damage, failure to comply with data security laws, loss of critical business data and intellectual property as well as loss of money and machinery.

## **4. ATTACKS ARE BECOMING MORE SOPHISTICATED – CYBER CRIMINALS WILL TARGET NEW DIGITAL TECHNOLOGIES, AS THEY ARE DEVELOPED.**

Risk Managers need to take a rigorous look at new applications to examine where their vulnerabilities lie. Cloud computing may mean that data is stored in jurisdictions with different legal requirements for data protection and it may transit many different countries networks – creating more opportunity for criminals to intercept data. Mobile phones could provide the means for criminals to access personal or business computers.

**5. ANY MACHINE OR SYSTEM CONTROLLED BY A COMPUTER IS AT RISK OF FAILURE.** GPS has transformed logistics, navigation, surveying and the mobile phone industry. The system is robust, and has arguably reduced risks in many areas, but like all technology, it can fail or be attacked. There are some concerns that industry is becoming over reliant on the system and back-up systems need to be in place.

## **6. THE GLOBAL NATURE OF THE INFORMATION TECHNOLOGY INDUSTRY MAY LEAD TO DATA BEING STORED IN PLACES VULNERABLE TO FIRE, FLOOD OR NATURAL DISASTER.**

The digital world is part of the natural world. Even if businesses no longer have warehouses or archive facilities, they still keep their digital files somewhere and the data is as vulnerable to catastrophes as it always was.

## **7. THERE IS NO ESTABLISHED METHODOLOGY TO MODEL COMPUTER SYSTEMS.**

Digital technologies are highly diverse and still developing. But businesses can and should look at what they can do to improve their security. The ISO 27000 series of standards provides advice on information security. Companies should identify who presents a threat, how an attack might be mounted, where their technical vulnerabilities lie and how they would deal with an attack. Insurance will also play a role.

**8. FEAR SHOULD NOT STIFLE INNOVATION.** Despite the challenges that information security presents, IT will continue to provide huge benefits to business. For example, the Web 2.0 phenomena of social networking, blogging and wikis cover practically every part of human activity. It creates new risks - people can use it to leak information or air potentially libellous views but it also helps business gather intelligence. If Google can predict flu outbreaks, how can insurers use the web to predict emerging risks? Companies who make a careful analysis of the risks, and identify how to manage them will be able to use digital communications with the most confidence.

## **PURPOSE**

This report investigates some of the trends and emerging risks posed by the revolution in digital and communications technology with the aim of raising the profile of these risks within the insurance industry and amongst risk managers in affected businesses. The information and views contained within this report are the result of consultation with knowledgeable industry figures and academics.

## **EMERGING RISKS TEAM**

The Emerging Risks team is part of the Franchise Performance Directorate at Lloyd's. We define an emerging risk as an issue that is perceived to be potentially significant but which may not be fully understood or allowed for in insurance terms and conditions, pricing, reserving or capital setting. Our objective is to ensure that the Lloyd's market is aware of potentially significant emerging risks so that it can determine an appropriate response to them.

The Lloyd's emerging risk team maintains a database of emerging risks which is updated regularly through consultation with the Lloyd's Emerging Risks Special Interests Group, consisting of experts within the Lloyd's market with support from the Lloyd's Market Association. The team also maintains strong links with the academic community, the wider business community and government. Contact with academia is often facilitated through the Lighthill Risk Network a not-for-profit organisation co-founded by Lloyd's, Benfield, Guy Carpenter and Catlin and open to subscribers from academia and within the financial services industry.

More details can be found at [www.lloyds.com/emergingrisks](http://www.lloyds.com/emergingrisks).

**DIGITAL RISKS PRESENT A  
CHANGING - AND  
CHALLENGING - LANDSCAPE  
AND THOSE WHO FAIL TO  
ADAPT RISK LOSING THEIR  
COMPETITIVE EDGE**

## **INTRODUCTION**

During 2007, Estonia experienced a cyberwar that targeted, slowed and - in some cases - disabled both public and private institutions. This was probably the first – and certainly the best documented cyber attack. And it has focused the minds of many governments on how to protect their own communities from digital threats.

Since the Estonian experience, the North Atlantic Treaty Organisation (NATO) has taken a hard look at its cyber defences, and, in the summer of 2009, both the US and UK Governments, published reports on cyber security. These reviews have prompted a debate between industry, governments and civil liberty groups with Governments calling for businesses to help them manage cyber risk. This debate will influence the direction of internet security.

Insurers need to take note of this debate. Cyber security is not simply something for governments and spies. It is a new reality for us all. The attack in Estonia was at one end of the spectrum. At the other is a disgruntled employee sending colleagues a defamatory email that could end up being seen by thousands of people across the world. And in the middle of the spectrum are the organised criminals, who steal, sell and buy credit card data from and on websites.

Cyber space is replacing physical space. It is where we shop, bank, socialise and work. Increasingly, it is where crimes are committed. If there is no cash box, where does your office's petty thief go to steal? If banks and shops need less cash on the premises, where does a bank robber go? Unsurprisingly, the current economic climate increases the threat of data theft.

This report looks at who is committing digital crimes and why. It identifies the current trends, the methods used and the potential impact of cyber crime on business. We also draw some conclusions on the best ways to mitigate the threat.

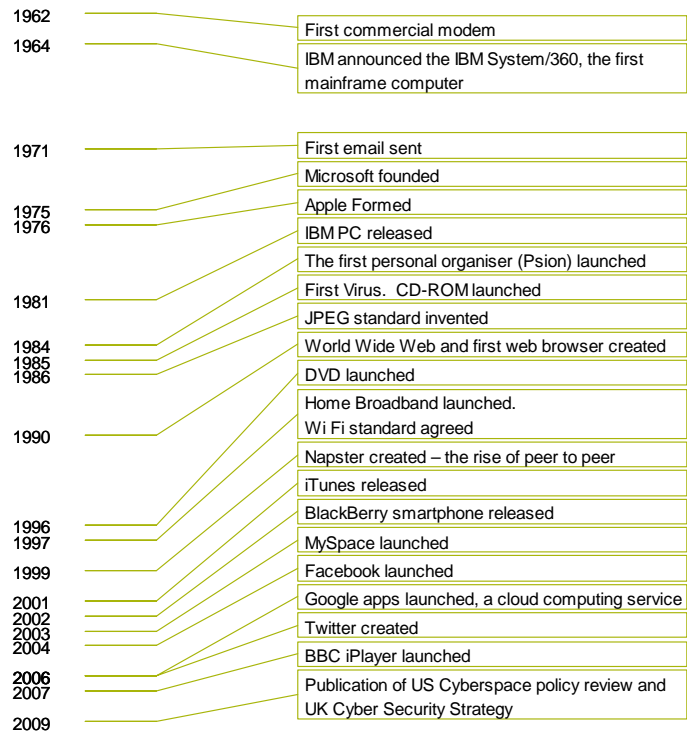
There are new difficulties in managing cyber threats. Modelling is difficult, not least because of the speed with which the industry is developing. Just forty years separate IBM's first main frame computer and the launch of Facebook. And the pace of development is, if anything, getting quicker, as IT firms continue to operate in an innovative and experimental environment. This presents a changing - and challenging - landscape for insurers and risk managers. Those who fail to adapt risk losing their competitive edge.

Ultimately, one thing hasn't changed. Businesses need to scrutinise their cyber security arrangements in a traditional way: are their most valuable assets sufficiently protected? And if not, how can they reduce the risk to themselves.

# HISTORY

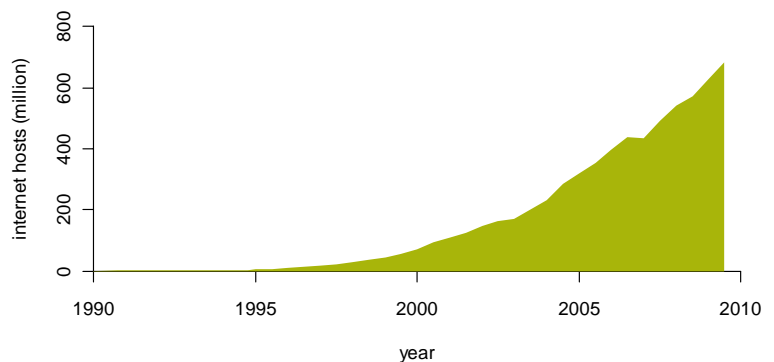
The information and communication technologies that make up the digital world have evolved substantially over the last 50 years, with the internet still under 20 years old. What follows are some selective dates that mark some technological and market breakthroughs to give context to the report.

## Timeline of technological landmarks



## Growth of the internet

The graph below shows the number of computers or applications connected to the internet, or internet hosts, in millions to indicate how quickly the internet has grown in recent years.



Source: Internet Systems Consortium <https://www.isc.org/solutions/survey/history>

# TERRORISM AND CRIME

## Overview

*"The UK is increasingly dependent on computers and the internet, but the very open nature of the digital network makes it vulnerable"*

**Ideas and Innovation , HM Government, August 2009**

The quote above comes from a report on countering the threat of terrorism. It notes that viruses can travel the globe in minutes, multiply more rapidly than physical risks and can originate from anywhere in the world. Many of these methods are not confined to terrorists. An organisation or individual may suffer a malicious attack from many different sources with differing motives, methods, impacts and mitigations, which are illustrated below:

### Attackers

- lone criminals, fraudsters and conmen;
- criminal organisations;
- state sponsored attackers;
- disgruntled employees;
- industrial spies;
- terrorists; and
- hackers, cyber vandals.

### Motives

- financial gain, fraud;
- revenge by a disgruntled employee
- industrial espionage;
- state sponsored espionage;
- furthering religious or idealistic beliefs; and
- amusement or prestige.

### Methods

- viruses, Trojans, worms, spyware and crimeware;
- internal copying or destroying of data;
- manipulating or blackmailing an employee to commit malicious acts;
- hacking;
- key logging;
- electromagnetic interference; and
- denial of service attacks.

### Impacts

- vandalism, defacement of web sites and reputational damage;
- failure to comply with data laws or regulation;
- loss of key business or account data;
- loss of service to customers;
- loss of internal network, wired or wireless;
- interruption to supply chain;
- direct theft of money from accounts; and
- competitors gain intellectual property.

### Mitigation

- Using BS ISO/IEC certification system;
- Identifying vulnerabilities and risk management.

**"THREATS FROM INSIDERS  
WILL GROW, SPURRED ON  
BY THE ECONOMIC  
DOWNTURN"**

**CRIMINAL ATTACKERS SEEKING QUIET ACQUISITION OF DATA TO SELL ON MAY SEEK TO TARGET SMALLER BUSINESSES, WHICH MAY BE LESS LIKELY TO HAVE THE SAME LEVEL OF DEFENCES AS LARGER CORPORATIONS**

### Who carries out the attacks?

Cyber attackers take many different forms. They can be terrorists motivated by political beliefs, or thieves who stand to make millions by intercepting customers credit card details. But they can also be closer to home. A recent report by technology company McAfee [4] found that threats from insiders are expected to grow, spurred on by the economic downturn, as financially desperate or resentful employees turn to the valuable corporate information available to them for financial gain and to improve their future job prospects.

The level and frequency of attacks will depend on the motivation of the attacker. If the attacker is seeking defamation, the target could also be expected to be high profile. Criminal attackers seeking quiet acquisition of data to sell on may seek to target smaller businesses, which may be less likely to have the same level of defences as larger corporations. Attacks could potentially be aimed at services used by businesses rather than the businesses themselves, such as outsourced IT services, industry associations or market intelligence.

Companies should also keep up with the wider threat from cyber terrorism such as hybrid attacks. These are terrorist incidents which combine physical and virtual attacks to maximise effectiveness. For example the detonation of a bomb near a bank could be timed to coincide with a denial-of-service attack on their web-based services. Such attacks could also take advantage of physical or environmental vulnerabilities such as the state of the economy, ageing infrastructures, and political or commercial tensions. The impact of hybrid attacks is greater, as the target's ability to recover is hampered.

### Methods of Attack

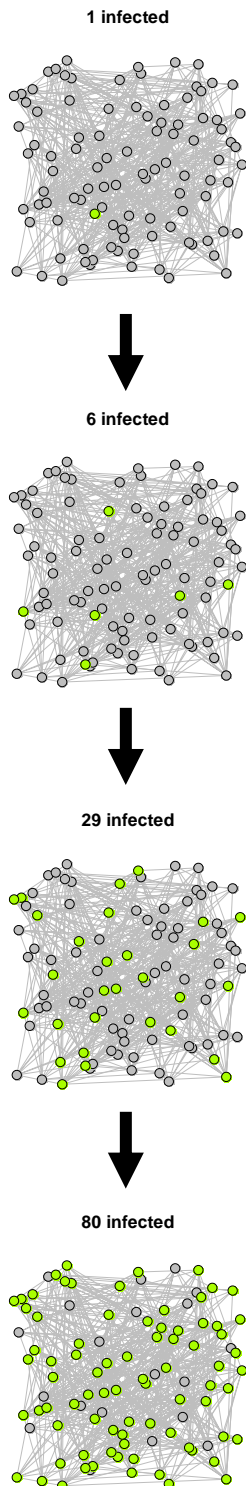
#### Malware and crimeware

Malware and crimeware can have differing definitions, however a common use of the word malware, or 'malicious software', is software that aims to cause damage or inconvenience to the target. Malware includes viruses, worms and Trojans. Viruses are computer programs that can continuously replicate themselves by infecting files, though they may or may not cause any damage to computers they infect; Worms also replicate, but unlike viruses exist as standalone programs and do not infect files; and Trojans do not replicate but pretend to be a benign program that when activated behave in an unexpected or unwanted manner. Crimeware on the other hand seeks to extract data from the target for criminal purposes, typically financial. There is a trend of attacks being less likely to be due to viruses and worms, and more likely to gather information through spyware or crimeware. Spyware is a general term for unsolicited programs that deliver unwanted advertising, monitor users' activities for marketing purposes and steal personal information. In terms of malicious activity over the internet, the most common method of attack in 2008 was web-based; especially via legitimate websites that have been compromised by attackers in obtaining user data [5, 6].

Malware can directly affect an organisations ability to function and hence impact earnings. However, such attacks would in most cases occur over the short term and be obvious in their effect and hence could be either quarantined or removed. Crimeware however, due to its differing motivation, can generate a greater return on investment for the criminal if their attacks go unnoticed so that they can continue to generate revenue.

**THERE IS A TREND OF ATTACKS BEING LESS LIKELY TO BE DUE TO VIRUSES AND WORMS, AND MORE LIKELY TO GATHER INFORMATION THROUGH SPYWARE OR CRIMEWARE.**

The diagram below demonstrates how quickly a virus can spread. Each of the 100 dots represents a computer, which in turn has the email addresses of five other computers represented by lines. In the top image one computer becomes infected with a virus. The second image shows how the virus replicates to new computers via the five email addresses contained within the originally infected computer. The subsequent diagrams show the continuation and speed of the infection.



### Attack sophistication

It can be increasingly difficult to recognise ‘fake’ websites. “Cross-scripting” is where a contaminated website changes a legitimate website so that data entered by the user (for example into an online shop) is redirected to criminals. The fake is often only done on the local instance of the website (i.e. the one loaded onto the users own machine), hence the original site is untouched and the operators may not be aware that their website is being altered at the end user’s computer.

Loss of productivity can also occur even if the attack is not direct or even targeted. For example, a self-replicating spam (unsolicited emails) attack could use up a large amount of internet bandwidth. Bandwidth is the amount of data that can be transmitted at any one time. However other systems, such as cash machines and payment systems use the same physical connections (copper cables or optical fibre) and hence they could be brought to standstill when the bandwidth limit is breached by the spam attack. This occurred within the internal systems at the Bank of America in 2003, when their network became infected with the Slammer worm and the resultant congested network traffic meant their ATMs could not communicate with their central databases and hence could not dispense money. [10]

### Impacts of a digital attack

The impacts of an attack are as varied as the attackers themselves. They include:

- **Third party information** – Data entrusted to an organisation may be stolen by criminals who can use it to extract money from the third party. Companies who do not take appropriate care of the customers’ data can be a target for litigation. For example, when TKMaxx lost 45.7 million credit card details in 2007, a number of lawsuits were filed by customers against them. This led to its parent company paying \$6.5 million in attorney fees alone and the class counsel estimated over \$200 million was provided in benefits to the class action [7]. According to one report, attackers are concentrating more and more on collecting data for financial gain, with 76% of phishing targeting financial brands [5]. Phishing is where the attacker attempts to convince the target to hand over confidential or personal data, most commonly credit card or bank account details.
- **Extortion** – Criminals could threaten to release data they have collected.
- **Espionage** – Criminals could sell stolen data and intellectual property to an organisation’s competitors.
- **Regulatory** – If the organisation is shown to be in breach of its regulatory requirements, it could face a fine or sanctions.
- **Reputation** – Once criminal activity is discovered, particularly if the discovery is public, a company’s reputation could be damaged, potentially affecting its share price.

**INCREASINGLY, COMPUTERS CONTROL MACHINERY AND SYSTEMS. INTERFERENCE, EITHER ACCIDENTAL OR INTENTIONAL, CAN RESULT IN PHYSICAL DAMAGE.**

**A COMPLEX, EXTENDED SUPPLY CHAIN PROVIDES MORE OPPORTUNITIES TO MODIFY THE SOFTWARE FOR MALICIOUS ENDS.**

### **Indirect Impacts:**

- **Lost productivity** – It is possible to attack a web based application by simultaneously (and automatically) making many requests for information – this slows down the response time and reduces the level of services to the intended users of the website. This is often called a “Denial of Service” attack. Through denial of service a company will be unable to conduct business and may lose money as a result.
- **Data retrieval** – In many circumstances data can be retrieved through the use of back up or recovery systems, for example from hardware failure or stolen physical media. Where the media is still available, but the data it contains has become unreadable by normal means, methods are available to retrieve the data, although at a higher cost than recovery from a back up system.
- **Irrecoverable data loss** – In some circumstances, such as a major natural disaster or malicious destruction, data will be permanently lost. The value of data can vary enormously, but for some organisations it could mean bankruptcy.

### **Virtual threats to the physical world**

Impacts from terrorists and criminals may not be limited to the virtual world of data and the internet, but could manifest in the physical world. Increasingly, computers control machinery and systems, for example cars, ships, planes, train signalling and gas pressure regulation. Interference, either accidental or intentional, can result in physical damage.

A NASA review of electromagnetic interference illustrates how accidental interference can affect physical machinery:

*“During the early years of Anti-lock Braking System (ABS), Mercedes-Benz automobiles equipped with ABS had severe braking problems along a certain stretch of the German autobahn. The brakes were affected by a near-by radio transmitter as drivers applied them on the curved section of highway. The near term solution was to erect a mesh screen along the roadway to attenuate the electromagnetic interference. This enabled the brakes to function properly when drivers applied them”*

The placing of malicious code in vehicle controlling software at the design stage, for example the software used to control planes in flight, could have a devastating effect. This code could be activated at a predetermined time to disrupt the vehicle’s systems and cause it to crash. Malicious code within software in computerised medical equipment could also potentially kill. These threats could multiply if manufacturers outsource software creation to other companies, who in turn could outsource the creation of parts of the software to further companies. This complex, extended supply chain provides more opportunities to modify the software for malicious ends. Having identified a problem, companies are starting to review the code written for them by outsourced companies to ensure that no hidden surprises remain.

## Management and mitigation

### Uncertainties and modelling cyber security

Unlike economics or actuarial theory, there is no standard model on which IT and information security is based. There are no agreed 'engineering' tools or formal methods to build software. Innovation has led to great diversity and the quality of implementation of security measures varies greatly. One could compare this situation to that faced by the engineers of the nineteenth century. There was a great deal of innovation and growth, but standards evolved over time, for example railway track gauges today are largely identical, but in the early days of rail they varied from region to region and therefore didn't allow trains to cross certain boundaries. Structures such as bridges also had to be built and materials like iron and steel had to be tested for their limits of endurance and application for the first time. Today this knowledge is well documented and engineers can build structures with confidence thanks to the innovation and experimentation of their predecessors. Digital security is still in this innovation and experimentation stage.

The ability to rigorously test a digital security system against the many and varied threats does not currently exist. It is exceptionally difficult to create a model of a digital security system and throw scenarios at it, either physical or virtual in nature due to the sheer complexity of the system and the environment it sits within. This will no doubt change in the future as standards evolve and the sophistication of modelling digital security systems increases. Until then, estimates of the probabilities, and to a lesser extent the impacts, of risks to such systems and their security will mostly be of a qualitative nature.

However, while it is difficult to determine probabilities of attacks, it is possible to assess the capabilities of an organisation to defend against attacks and vulnerabilities. This focuses on the maturity of the risk management and thought processes within an organisation and its approach and ability to respond to change.

The ISO 27001 standard (see case study on page 15) outlines a risk management framework that can assist organisations in managing cyber threats. However, many of the threats to an organisation's cyber security are from vulnerabilities that exist in their software, which malicious programs can exploit. Therefore, an important part of cyber risk management is vulnerability management. This consists of several distinct stages such as:

- identifying vulnerabilities;
- assessing the impact of a potential attack in order to prioritise the application of software patches; and
- confirming the patch has fixed the vulnerability.

A business that demonstrates appropriate vulnerability management should be at lower risk than those who do not. In terms of mitigation it is important to consider "what is the criminal's view of my system?" Data that may not be considered essential to a business operation, and hence lower in relative value, could be of great worth to another malicious party. When insurers are developing scenarios to test their portfolio of risk this can also be a good approach, whereby the assumed intent of a variety of attackers can be used to judge what sort of attacks can be expected and what the impact might be.

**IN TERMS OF MITIGATION IT IS IMPORTANT TO CONSIDER "WHAT IS THE CRIMINAL'S VIEW OF MY SYSTEM?"**

**THE ISO 27001 STANDARD OUTLINES A RISK MANAGEMENT FRAMEWORK THAT CAN ASSIST ORGANISATIONS IN MANAGING CYBER THREATS.**

## **Security is a business opportunity**

The UK Government is calling [10] for relevant high-tech and other industries to help them mitigate the terrorist threat. The areas highlighted include:

- development of biometrics to validate identities;
- methods to quickly restore services after an attack;
- tools to identify the source of an attack;
- secure sharing of data;
- high speed data mining; and
- presentation of data and “information assurance”.

While the possibility of systemic risk arises and will need careful definition and limitation, it seems likely that insurers can be one of the partners to help manage this risk.

# CASE STUDY: INFORMATION SECURITY AND THE BS ISO/IEC 27000 SERIES

## Information security

Increasingly organisations see information as an asset that adds value, and like physical assets it must be protected against damage, corruption or loss. Information security is the process by which information in all its forms is protected through established controls such as policies, guidance and usage of software. [11]

## Importance

Information security enables robust business continuity, reassurance to investors, confidence to be able to deliver services and a control against reputational risk. Attacks from computer viruses, hacking and denial of service are becoming both more common and sophisticated, and accidental damage or loss can also occur through employee actions or physical damage such as fire or flood. Increasingly interconnected software and devices, such as mobile phones and laptops, also increase organisations vulnerability to information security breaches through greater access to their systems. Given that organisations are increasingly relying upon digital and computer systems the role and importance of information security cannot be denied. [12]

'... nearly 90% of those companies that had adopted BS 7799 [the precursor to the BS ISO/IEC 27000 series] said that formal certification had improved their business continuity; 85% said it had minimized damage from security incidents; and 53% said it had led to a higher return on investment ...' - *Computer Weekly, May 2004, as based on the DTI Information Security Breaches Survey 2004* [11]

## Assessing risks

Organisations will have differing requirements with respect to information security and differing vulnerabilities to threats. As money and time are finite resources the vulnerabilities must be balanced against the impact to the business, prioritised, and then acted upon through controls. Information security risk management is also not a one-time exercise but a continuous evaluation and implementation/modification of controls to combat new threats and vulnerabilities as they appear. [13]

## Standards available

A useful guide to insurers as to whether insureds have a good approach to information security is whether they adhere or are certified to the BS ISO/IEC 27001 standard [14, 15, 16].

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) have produced the ISO/IEC 27000 series of standards that deal with information security. Within this series are several standards and documents that can be used by organisations to manage their information security. One of the standards, BS ISO/IEC 27001, is auditable and organisations can become certified by a suitably accredited third party. Insurers who wish to assess information security risk may want to investigate whether potential insureds are BS ISO/IEC 27001 certified or whether they follow the best practices laid out by the standard.

## BS ISO/IEC 27001

The BS ISO/IEC standard is suitable for all types of organisations, though the finance, health, public, IT sectors and any other organisations that manage data on behalf of others will find it particularly relevant.

The BS ISO/IEC 27001 standard can be used by organisations to:

- Outline their security requirements and as a framework to implement and manage controls to meet those requirements in a cost effective manner;
- Ensure compliance with laws and regulations, as well as standards required for internal and external auditing; and
- Provide relevant information regarding information security to third parties such as trading partners, customers, insurers and other organisations they interact with who might require reassurance.

## BS ISO/IEC 27002 to BS ISO/IEC 27006

There are several other standards and documents that assist organisations in meeting the BS ISO/IEC 27001 standard, namely:

- 27002: Outlines further controls and control mechanisms that organisations can implement
- 27003 (not yet published): Guidance on how to implement an information security management framework
- 27004: (not yet published): Covers metrics and measurements, enabling organisations to gauge how effective their information security management is.
- 27005: Provides guidelines on how to manage information security risk, and is designed to be read in conjunction with BS ISO/IEC 27001
- 27006: Lays out the requirements and provides guidance for any body wishing to audit and certify organisations using BS ISO/IEC 27001

## MOBILE DEVICE VULNERABILITIES

**WE COULD SEE A RISE IN THE NUMBER OF DIGITAL ATTACKS OR THREATS SPECIFICALLY TARGETING MOBILE DEVICES.**

Another revolution is taking place in mobile technology. People own mobile devices such as phones or personal digital assistants (PDAs) that connect to the internet, their home and work computer and other mobile devices. This gives malware embedded within the mobile device greater access to any personal or work data. It may also increase the possibility of becoming infected with malware due to mobile devices' greater connectivity. Mobile devices are remotely accessible and potentially kept on for a longer period than static devices, which can increase the likelihood of becoming infected or providing data. We could see a rise in the number of digital attacks or threats specifically targeting mobile devices.

A rapidly expanding area of mobile attacks is in the form of text message scams that aim to get users to hand over personal information such as credit card or banking details [9]. Attackers even include a telephone number which connects to a very realistic, but fake, automated customer service line to further convince users of its authenticity. The iPhone operating system was recently patched to close a vulnerability that could be exploited through SMS texting.

Text messages have also been used to exploit vulnerabilities within mobile phones, which can result in the phone service becoming disrupted or even the execution of malicious code, potentially allowing others to gain control over the mobile device.

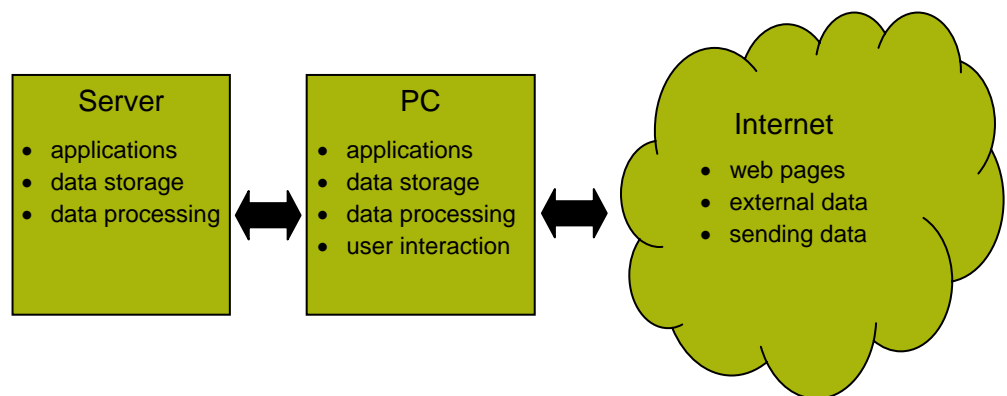
# CLOUD COMPUTING

Cloud computing, also referred to as internet computing, is an increasingly popular way of using computer applications by accessing them, and storing data, over the internet. The illustration below shows how cloud computing differs from 'traditional' computing. Instead of using programs that are installed on the user's desktop computer or internal network, programs are run over the internet, typically using web-based technologies. Data is also no longer held on the user's computer but sits on a web server in a remote data centre.

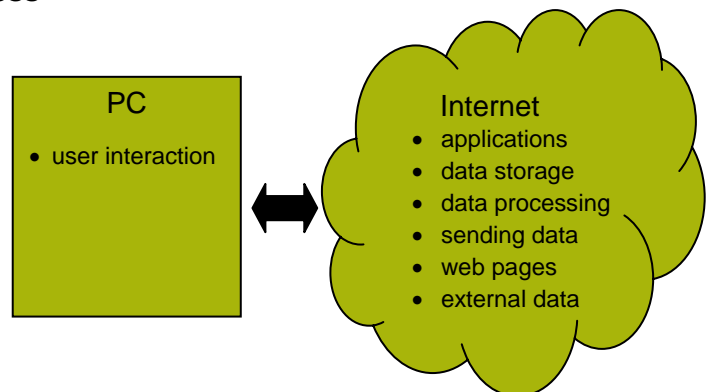
## Illustrative differences between cloud and 'traditional' computing

---

### 'Traditional' process



### Using a 'cloud' process



The data is physically stored in data centres, although their geographical location is unlikely be near the end users. Indeed, the end user typically has no knowledge or control of the systems behind cloud computing applications. The advantages of using cloud computing lie in the easy sharing of information, low maintenance overhead, easy access to new versions of applications, and availability of data. One example of cloud computing already available is Google Docs where users have access to a suite of applications, such as word processing, spreadsheets and databases, where the data is 'saved' online. The documents can be easily shared and edited by others as they are accessible by any machine that has an internet connection and a modern browser. Such applications are becoming more popular as they can potentially reduce costs and

**INFORMATION TRANSMITTED FROM ONE COUNTRY TO ANOTHER MAY GO THROUGH A THIRD OR INDEED MANY COUNTRIES, WHERE IT MAY BE INTERCEPTED, COPIED OR MODIFIED OR CORRUPTED**

increase flexibility for businesses and individuals due to economies of scale and the centralised nature of the applications. For example, the local government in Washington D.C. has embraced cloud computing to provide their email and other productivity tools, citing lower development costs and ease of use as its key advantages. [17]

### **Legal jurisdiction**

Cloud computing has raised certain political and legal issues. Many of these have arisen because cloud computing requires the user to expose their data to a third party for storage and handling. Such data may potentially be stored within a different legal jurisdiction to the originator of the data. Differences in freedom of information and anti-terrorist laws can mean that this data may be accessed with fewer legal challenges than would otherwise have been the case. Other technologies can help mitigate this risk, for example encryption, though this does not guarantee the data will be safe, as the passwords to unlock encrypted files can be found through malicious attacks, phishing or espionage. Information transmitted from one country to another may also go through a third, or indeed many countries, where it may be intercepted, copied, modified or corrupted.

### **Data recovery and faults**

The user may rely upon the cloud computing application providers to recover their data in the event of the loss of data. If the provider goes out of business or terminates their application or service the user may not be able to get their data back.

Cloud computing not only allows access to remotely stored data over the internet, but can also provide applications that process or analyse data. Providers of such applications and analysis, like their counterparts who provide traditional 'installed' programs, may be a target for litigation if their application was found to be at fault and directly caused a loss to the user.

### **Centralisation**

Increased use of cloud computing may lead to greater centralisation of data storage, provision of services and data analysis. This could in turn lead to aggregate losses across many companies if services or data is lost or damaged. Traditionally, when bugs are found in software, users have to download a correction (or 'patch') and apply it themselves; cloud applications can apply patches seamlessly without users needing to be involved – this allows weaknesses in programmes to be fixed quickly and arguably reduces risk. However, as is so often the case, a higher probability local risk may be replaced by a lower probability, systemic risk of software failure.

## WEB 2.0

Web 2.0 represents a new way in which users and programmers use the internet. Social networking websites, blogs and wikis are good examples of the Web 2.0 approach and all have one main theme in common: content is provided by the users of the website and not just the owners. Networking websites, such as Facebook, MySpace and Twitter, allow groups of people to share information: either general information such as what they may be doing in their day-to-day lives; or they can be focused around specific information such as political issues or climate change for example. Web logs, or blogs, are often limited in scope to articles published by a single person or group of people with a common connection. Lloyd's itself publishes risk blogs at <http://blogs.lloyds.com/>. Wikis also share information but allow users to construct web pages, the most common example being Wikipedia which is an encyclopaedia created by its users.

**ALL THESE TECHNOLOGIES  
MEAN THAT ANY PERSON  
WITH ACCESS TO THE  
INTERNET CAN NOW  
BECOME A PUBLISHER**

The amount of free information that is now easily obtainable is vast. By analysing or tracking this information people can identify key issues that are of concern to groups of people. This may be of interest to governments who wish to gauge public opinion. Lawyers who wish to identify a good candidate for mass tort might be able to use this information to identify trends. Interest groups in litigious issues can also easily form and reach a large, potentially global, audience. The risk of litigation may therefore increase; though conversely issues may be brought to light earlier which could help risk managers within companies avoid latent class actions. Insurers may be able to use this information for claims management as a way to anticipate potential claims.

All these technologies mean that any person with access to the internet can now become a publisher, but, unlike traditional publishers, they are unlikely to have had training on how to avoid libel issues. Some wikis and blogs have their content moderated, but for many individuals the content they publish consists of their raw unexpurgated thoughts.

It may be possible to systematically scan blogs or similar fora to provide an early warning for emerging risks. For example google have developed an application [18] that flags up an increase in searches for terms such as 'flu'; the hope being to spot an epidemic in the early stages.

Web 2.0 also provides a new source of leaking information from organisations and companies. A concern is that published information on the internet can affect reputation, merger/acquisition negotiations and share price. While this risk is largely recognised, it is hard to mitigate or control a disgruntled or naïve employee who is intent on publishing information. Accidental release of information can be controlled to some extent by publishing clear guidelines on what information related to the organisation employees can publish.

**IT IS CRITICAL WHEN  
MANAGING THE RISKS,  
THAT INNOVATION IS  
NOT STIFLED**

Social networks and other Web 2.0 applications can make users susceptible to malicious attacks [9] due to their inherent openness. Designers of social networking sites may have a conflict of interest between wanting their users to publish as much information about themselves as possible and reassuring them that their data is being kept safe and will not be disclosed to unintended third parties.

Despite the risks, Web 2.0 can enable innovation both within and outside organisations. It is critical when managing the risks, that innovation is not stifled. It is all too easy to adopt a policy that restricts access to information.

# GPS FAILURE

The Global Positioning System (GPS) is a US military satellite system that allows users on the ground to determine their position with a high degree of accuracy. While the system was originally a military project, it is now considered dual-use and plays an increasingly larger commercial role in wider society.

The system works using a network of ground stations and satellites, which transmit signals to handheld or ground GPS receivers. The signals sent by the satellites include their time and position, which allows a receiver to estimate the distance between it and the satellites. Once the receiver has estimated the position of four satellites it can work out its three dimensional position on the earth and correct for any inaccuracies in the handhelds own clock. The signals from the ground stations keep the satellites synchronised.

Originally, a policy of 'Selective Availability' for non-military use resulted in a deliberate reduction in accuracy for civilian use. However, in 2000 this was revoked prompting many new commercial and civilian applications including, but not limited to:

- surveying;
- navigation (sea, land, air, space);
- heavy equipment (construction, mining and agriculture);
- coordinating large communication systems, for example the signals are used by some mobile phone network base stations;
- geo-information for civilian use (walking, local information); and
- road pricing schemes.

**THE KEY EMERGING RISK IS THE IMPACT OF ONE OR MANY GPS RECEIVERS NO LONGER RECEIVE A SIGNAL, FOR WHATEVER REASON, AND THE RESULTING FAILURE OF SYSTEMS THAT RELY UPON GPS**

Other satellite systems are being developed by Russia, the EU, Japan and China. Global sales of GPS devices are now estimated at over \$20 billion a year with over 95% of units being sold for civilian use.

The key emerging risk is the impact, if one or many GPS receivers no longer receive a signal, for whatever reason, and the resulting failure of systems that rely upon GPS. The following sections explore some of the ways this could, in theory, occur.

## Severing of the signal

- **Satellite failure** – Satellite hardware and software can be damaged by accidental or wear-and-tear failure, by malicious intent or by space debris and solar storms. While satellites are constructed to high quality standards, they are susceptible to unanticipated breakdown like any other machine. This can be in the form of software bugs or hardware failure. Satellites can also be destroyed or rendered inoperable by solar flares or missile attacks. Solar flares are produced by the sun and their frequency follows an 11 year cycle so the level of risk varies over time. GPS is designed so that, at any point in time, a receiver can view many more than the required four satellites and so, to cause true disruption, many satellites would need to be destroyed, either at once or over several months, until they can be replaced.
- **Ground station failure** – GPS relies upon a number of ground monitoring and control stations that track and ensure the satellites maintain their correct orbits and update their onboard clocks. Damage to the ground stations or interference to communication with satellites could cause inaccuracies in determining positioning for end users.
- **GPS receiver failure** – Perhaps the most likely of events is the failure of the GPS unit held or used by the user. In 1995, the ship Royal

Majority grounded off the Nantucket coast resulting in \$7 million of damages and lost business. Their GPS receiver's antenna had worked loose and the system went into 'dead reckoning' mode which took the last known course and projected it forward - ultimately taking the ship off course. This event led to a change in GPS design, however it illustrates what can happen.

- **Signal jamming and spoofing** – According to the Ministry of Defence, GPS signals are weak and can be easily jammed or suffer accidental interference. Typically, jamming works by introducing noise to the GPS signal making it unreadable by a receiver. This has been highlighted as a potential terrorist threat as it is relatively easy to do. Accidental jamming can also occur by interference with a local telecommunication system. For example, two Navy ships inadvertently jammed the Port of San Diego for two hours affecting telephone switches, mobile phone networks and even a hospital paging system. Another technique, called spoofing, is where the original signal is overwhelmed by a larger signal that is issuing false information. This could potentially be used to veer ships off course or cause systems that use the timing signal to fail.
- **Pulling the plug** – The most widespread GPS system is owned and run by the US government and they can turn it off for civilian use if they deem it necessary. While they have given assurances that they will do their utmost to ensure its continued operation, a large scale war or terrorist intervention could reverse this decision.

## Impacts

- **Navigation** – Whether by sea, land, air or space, GPS is rapidly becoming a standard tool for navigation by commercial and civilian vehicles. Media regularly run stories of small villages becoming gridlocked by lorry drivers or drivers getting stuck on small roads while using their GPS. The technology is improving, but in the meantime there could be liability issues (relating to the misuse of GPS) to local residents and businesses. Perhaps the more material issues relate to the loss of the GPS service and how this would affect the marine, aviation and space industry. Insurers may want to consider whether ships, air and space craft are susceptible to GPS failure and to what extent it could result in damage to the vehicle and any potential for widespread losses. The classes of business that could be affected by physical damage include motor, aviation, marine and property including business interruption. In addition, casualty classes could be affected if a captain of a ship or aircraft relied solely on a GPS system and ignored other available methods. GPS is also being used by roadside recovery and road delivery services, and, if it were to fail, could potentially lead to a large number of relatively small claims with respect to spoilage of transported goods or loss from delays in delivery.
- **Heavy equipment, surveying and monitoring** – The mining, construction, agriculture and other industries increasingly rely upon GPS as an essential tool for machine control, surveying and measurement. It is used by cranes in container yards to operate safely and efficiently; risk monitoring of dams, bridges, skyscrapers and other large structures; precision agriculture to improve yields; warn mining vehicles of nearby obstacles; and construction of buildings. In a worst case scenario, property insurance could be affected if risk monitoring was to fail or if machinery were to act incorrectly, for example shipping cranes could damage containers by placing them incorrectly. Business interruption insurance may trigger from the inability of machines to operate as they are no longer "aware" of where they are. Professional

**INSURERS MAY WANT TO  
CONSIDER WHETHER SHIPS,  
AIR AND SPACE CRAFT ARE  
SUSCEPTIBLE TO GPS  
FAILURE**

indemnity could be an issue for surveyors if their equipment gave false readings which were not noticed but should reasonably have been picked up with appropriate cross checks.

- **Failure of large communication systems** – GPS is used for timing as the satellite signals, based on atomic clocks, provide a highly accurate source of time. This is utilised by mobile networks in areas such as handing over the control of a mobile phone when a user travels from one cell to another and in the encoding of mobile signals. The temporary loss of GPS signal would be inconvenient but a longer term outage could result in a massive loss in revenue for many types of business. The secondary effects could also be widespread given the modern world's reliance on digital communication. Casualty classes may be exposed to this if the physical mobile network operators became targets for litigation as individuals and business lost revenue.

GPS has developed into a very useful technology for many applications, although there are events that could cause it to fail that may not yet have been experienced during its relatively short operational history. There are proposed backup systems, such as developing the ground based radar LORAN system and newer navigational satellite systems. However, it would be prudent to examine the potential impacts of the failure of this technology and to ensure knowledge and practice of traditional positioning methodologies is retained.

# NATURAL AND MAN-MADE DISASTERS

We live in a physical world which has its own immediate perils including earthquakes, hurricanes, flooding and more exotic examples such as solar flares. These natural events can be devastating and result in consequences that are hard to predict. Natural catastrophes can cause damage to occur to buildings, utilities, transport networks and communication infrastructures. In addition, large and small scale accidents or malicious acts can result in similar damage to physical infrastructure.

Businesses, public organisations and individuals are increasingly reliant upon electronic systems that store and transmit information. These electronic systems rely upon infrastructure that may be damaged by a natural disaster or secondary impacts, such as fire, flood and landslides. Key components that are required for modern electronic/communication systems to operate that could be affected by a natural disaster include:

- Power stations that power electronic systems;
- Transport infrastructure to deliver fuel to power stations;
- Electricity supply infrastructure;
- Data centres; and
- Infrastructure to support networks (telephone, mobiles, wireless etc).

**A NATURAL DISASTER IN  
ONE PART OF THE WORLD  
COULD AFFECT  
BUSINESSES LOCATED  
ANYWHERE ON THE  
GLOBE**

Due to the increasingly global nature of electronic, information and communication systems, a natural disaster in one part of the world could affect businesses located anywhere on the globe if they relied upon critical information services, such as data centres or hosted web sites, that were located in the disaster zone. This occurred following the Taiwanese earthquake in 2006 that damaged undersea telecommunications cables resulting in reduced internet services in several other Asian countries. An example of a near miss occurred at Walham electricity-substation during the 2007 floods in the UK, which was saved from flooding and shutdown by the fire service and military. Had the substation flooded it would have affected hundreds of thousands of people nearby.

# CONCLUSION

The digital world is changing the risk landscape for information security as well as the use and storage of information and the control of physical assets and systems.

Trends in digital threats such as viruses and worms appear to be on the decrease, while malicious 'crime ware' programs that silently collect data is on the increase. Vulnerability management is an important technique and aims to identify, prioritise and patch vulnerabilities that malicious software typically takes targets. Mobile devices, due to their ability to connect with other devices and sources of information, are increasingly a target for criminals. Physical assets that are computer controlled may also be under threat from terrorists or disaffected employees who may be able to assume control or disable important systems.

While it is difficult to fully model the complexity of security systems in order to assess the probability or impact of attacks, it is possible to manage vulnerabilities to those attacks provided appropriate scenarios are considered.

The ISO/IEC 27001 standard can be used by insurers and risk managers to gain insight into what a good information security management system should take into account. Insureds can be asked if they work to the standard or if they are certified.

Cloud computing is increasingly popular and often delivers cost savings and efficiencies for storing and using information. However, there are concerns that a number of legal jurisdictions may apply to data as it is transferred around the globe; some more onerous than others. Greater centralisation of data may decrease risk of local data loss but might introduce a risk of systemic failure which is very hard to model.

The new way in which the web is being used through Web 2.0 applications allows anyone with access to the internet to become a publisher. Legal firms and insurers may be able to use the plethora of data and opinions in blogs, wikis and networking sites to identify emerging and potential claims.

The emerging technology of GPS is now used for critical processes in a number of industries. GPS signals can be disrupted by satellite failure, ground station failure, receiver failure, deliberate or accidental signal interference or imitation. Failure of GPS signals either maliciously (by criminals or terrorists for example) or through natural causes may affect navigation, the construction industry and those using GPS-guided heavy machinery. Overall GPS has decreased risk; but over-reliance may lead to risks of systemic failure.

The digital world is still susceptible to physical disasters such as flooding, earthquakes and hurricanes. Insurers who have exposure to digital risks may want to consider geographical aggregations of those risks. Investigations may also be warranted to determine whether the digital supply chain has any geographical concentration.

Inevitably, the risks relating to society's increasing use of digital technology are changing rapidly. Insurers should periodically consider whether such developments have changed the risk landscape leaving them more exposed than intended or providing them with the opportunity to develop new products.

**INEVITABLY, THE RISKS  
RELATING TO SOCIETY'S  
INCREASING USE OF  
DIGITAL TECHNOLOGY ARE  
CHANGING RAPIDLY**

The fast, experimental and innovative nature of digital technology presents a challenge to risk managers and insurers. But we must not forget that cyber space provides considerable commercial benefits.

There is a danger that as industry seeks to manage the risk, innovation is stifled. Solutions must be developed that enable experimentation. IT departments are challenged with balancing the commercial needs of organisations with protecting them from attack.

# SOURCES OF INFORMATION

The following were useful sources of information used when drafting this report. Links are shown for ease of use and were valid at the time of publishing the report:

- [1] Introduction to NATO's policy on Cyber Defence, January 2008, [http://www.nato.int/cps/en/natolive/topics\\_49193.htm](http://www.nato.int/cps/en/natolive/topics_49193.htm)
- [2] US Cyberspace Policy Review, 2009, [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)
- [3] UK Cyber Security Strategy 2009, [http://www.cabinetoffice.gov.uk/reports/cyber\\_security.aspx](http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx)
- [4] "Unsecured Economies: Protecting Vital Information", a report by McAfee, <http://www.mcafee.com/>
- [5] "Symantec Global Internet Security Threat Report, Trends for 2008", April 2009, <http://www.symantec.com/>
- [6] "IBM Internet Security Systems X-Force® 2008 Trend & Risk Report", January 2009, <http://www.ibm.com/>
- [7] Nov. 3 order by U.S. District Court Judge William Young, civil action no. 07-10162-WGY, United States District Court For the District of Massachusetts , 584 F. Supp. 2d 395; 2008 U.S. Dist. LEXIS 94410
- [8] "Cisco 2009 Midyear Security Report", <http://www.cisco.com/>
- [9] "Ideas and Innovation", HM Government, August 2009 <http://security.homeoffice.gov.uk/news-publications/publication-search/general/Science-Tech-Booklet?view=Binary>
- [10] "Damage Control", CNET News, 6 February 2003, <http://news.cnet.com/2009-1001-983540.html>
- [11] "About information security", BSI Group, <http://www.bsigroup.com/en/Standards-and-Publications/Industry-Sectors/ICT/Information-Security/About-Information-Security/>
- [12] "Why is information security needed?", BSI Group, <http://www.bsigroup.com/en/Standards-and-Publications/Industry-Sectors/ICT/Information-Security/Why-is-Information-Security-needed/>
- [13] "Assessing information security risks", BSI Group, <http://www.bsigroup.com/en/Standards-and-Publications/Industry-Sectors/ICT/Information-Security/Assessing-security-risks/>
- [14] BSI summary of ISO/IEC 27001 standard, <http://www.bsigroup.co.uk/en/Assessment-and-Certification-services/Management-systems/Standards-and-Schemes/ISOIEC-27001/>
- [15] ISO/IEC 27001:2005 standard, [http://www.iso.org/iso/catalogue\\_detail?csnumber=42103](http://www.iso.org/iso/catalogue_detail?csnumber=42103)
- [16] Summary of Information Security Management Systems (ISMS), [http://www.iso.org/iso/iso\\_catalogue/management\\_standards/specific\\_applications/specific-applications\\_it-security.htm](http://www.iso.org/iso/iso_catalogue/management_standards/specific_applications/specific-applications_it-security.htm)
- [17] "Cloud Computing Is First Option for New Apps in Washington, D.C.", Government Technology, 10 August 2009, <http://www.govtech.com/gt/708898>
- [18] <http://blogs.lloyds.com/2009/01/22/floogle/>

Links to third party sites on this Website are provided solely for your convenience. Lloyd's makes no representations as to the security, quality or propriety of any site which may be accessed by following these links and accepts no liability for the content or for any loss or damage caused or alleged to have been caused by the use of or reliance on information contained in such sites or goods or services purchased from them. If you decide to access any of the third party sites linked from this report, you do so entirely at your own risk.

