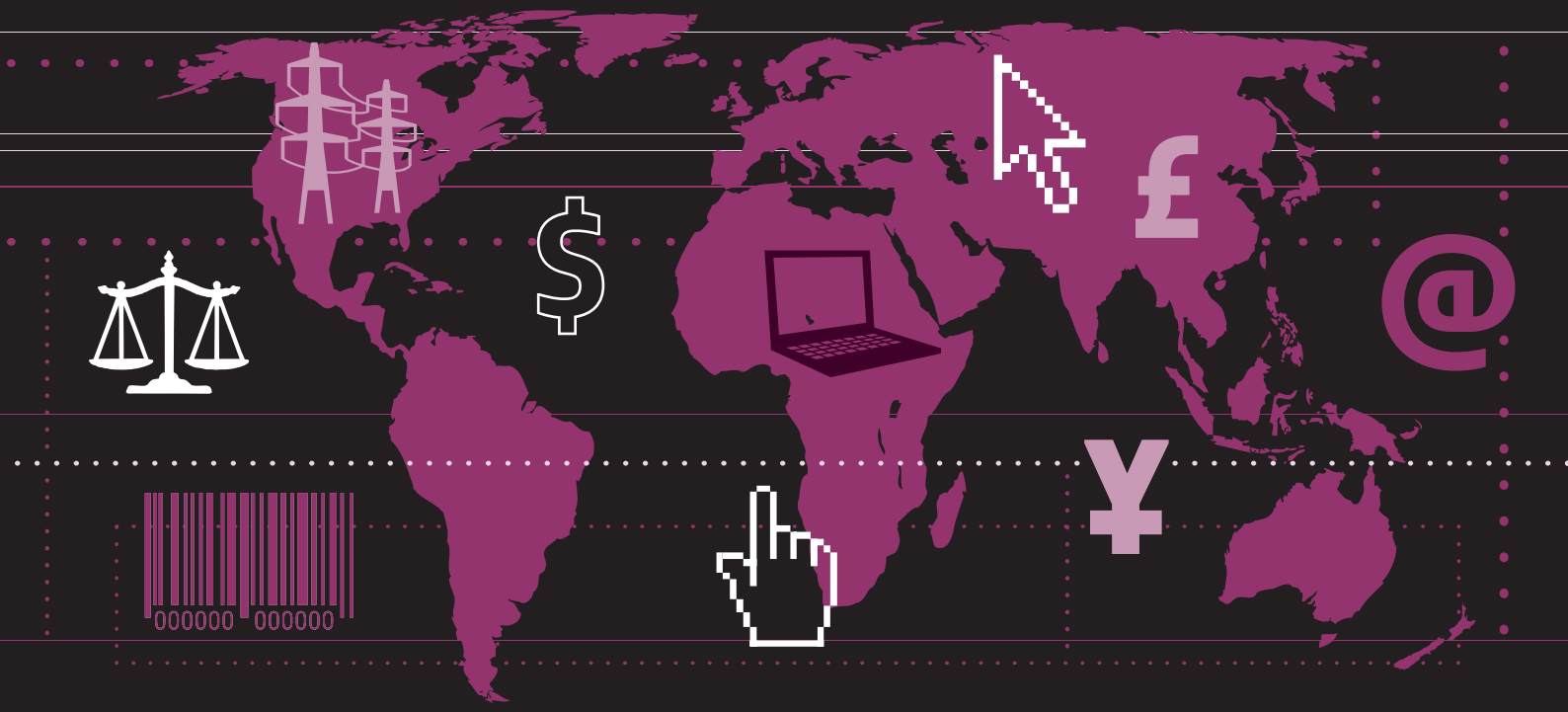
LLOYD'S

LLOYD'S 360° RISK INSIGHT

IN DEPTH REPORT

MANAGING DIGITAL RISK

Trends, issues and implications for business



ABOUT LLOYD'S

Lloyd's is the world's leading specialist insurance market, conducting business in over 200 countries and territories worldwide – and is often the first to insure new, unusual or complex risks. We bring together an outstanding concentration of specialist underwriting expertise and talent, backed by excellent financial ratings which cover the whole market.

ABOUT 360 RISK INSIGHT

Global risks change rapidly. Companies need to anticipate tomorrow's risks today. At Lloyd's, we've been helping businesses do just that for over 300 years. From climate change to terrorism, energy security to liability, boards must anticipate and understand emerging risks to successfully lead their companies into the future.

Lloyd's 360 Risk Insight brings together some of the views of the world's leading business, academic and insurance experts. We analyse the latest material on emerging risk to provide business with critical information. Through research, reports, events, news and online content, Lloyd's 360 Risk Insight drives the global risk agenda as it takes shape. We provide practical advice that businesses need to turn risk into opportunity.

Get the latest reports and analysis on emerging risk at www.lloyds.com/360

ABOUT HP LABS

HP Labs, HP's central research team, is chartered with enabling new opportunities for HP through technical innovation and scientific breakthroughs. HP Labs operates in seven locations around the world, including: Palo Alto, CA, USA; Bangalore, India; Beijing, China; Bristol, UK; Haifa, Israel; St. Petersburg, Russia; and Singapore.

ABOUT THE AUTHORS

Adrian Baldwin (PhD) is a Senior Researcher at HP Labs specialising in security. He has a particular interest in security analytics to understand risk and cybercrime.

Simon Shiu (M.Inst.ISP, PhD) is a Senior Research Manager at HP Labs. He has worked in security for the last ten years and published a number of papers in the area. He is also a visiting professor at Newcastle University.

Other contributing authors were **Martin Sadler**, Director of HP's Cloud and Security Lab, **Bill Horne**, Senior Research Manager at HP Labs and **Chris Dalton**, Principal Researcher at HP Labs.

ACKNOWLEDGEMENTS

We would like to thank the following people who reviewed, commented on and contributed to the report:
Iain Ainslie, Technology and Cyber Liability Underwriter, Ace European Group
Paul Bantick, Underwriter (Tech, Media & Business Services), Beazley
Dr Robert Coles, Chief Information Security Officer, National Grid
Prof Paul Dorey, Chairman, The Institute of Information Security Professionals
Luke Foord-Kelcey, Partner, Head of UK CommTech & Media Practice, Jardine Lloyd Thompson Ltd
Paul Howard, Head of Insurance & Risk Management, Sainsbury's Supermarkets Ltd
Simon Milner, Partner, Jardine Lloyd Thompson Ltd
Dan Trueman, Underwriter, Kiln
Aad van Moorsel, Professor of Computer Science, Director of the Centre for Cybercrime and Computer Security, Newcastle University, UK

LLOYD'S 360° RISK INSIGHT

IN DEPTH REPORT

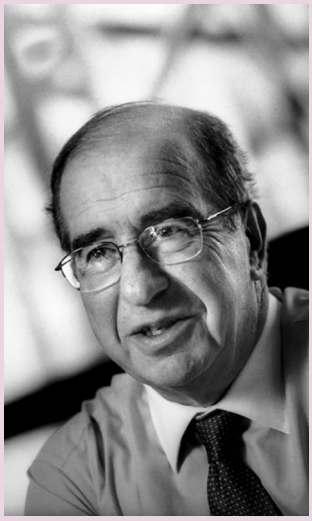
MANAGING DIGITAL RISK

Trends, issues and implications for business

Illustrations

Boxes

FOREWORD
FROM THE CHAIRMAN OF LLOYD'S



If we want to share an important document with a colleague on the other side of the world, we can do so in an instant, at the simple press of a button, and for free. Technology has made business truly global.

However, this also means that the business world has become dependent on computer systems. For example, entire supply chains are run by computer systems which track and trace goods as they travel around the world.

So whilst the benefits of the cyber revolution are undisputable, we need to look at the implications of our dependency on IT. Namely, we need to carry out proper assessments of the risks we face and put in place mechanisms to protect our digital data and processes.

Lloyd's has long offered policies to companies who want to protect their businesses against fire or flood. Companies now need to think about how they can protect their IT systems against an ever-growing number of threats.

Whether it's Smartphones or iPads opening up new entry points for hackers; data being compromised by the loss of USB sticks and laptops; or system failures; the risks are complex.

This report examines today's cyber risks, the threats they pose and what action can be taken to manage them.

It is clear that this is an issue which is high on the agenda of governments. The UK Government's National Security Council recently announced that attacks on computer networks are among the biggest emerging threats to the UK, ranking them alongside terrorism and a flu pandemic as the key dangers to UK security.

Law-enforcement agencies across the world are working to tackle the criminal aspects of cyber risk. A great deal of good work is being done. This is crucial because cyber crime is an international business.

Attacks on companies in one country can emanate from the other side of the world, while some countries are effectively "cyber sanctuaries", where criminals can operate free from cyber-crime legislation.

What is required is increased communication, co-operation and collaboration between governments, and a move towards uniform global regulation around cyber crime.

This report however, is aimed at the business community and what we should do to help identify emerging threats and deal with them.

Cyber risks are evolving all the time. Only by taking a truly joined-up approach, between countries and between the business community and governments, can we manage this truly global issue.

Lord Levene
Chairman
Lloyd's

EXECUTIVE SUMMARY

1. DIGITAL RISK NEEDS TO BECOME A BOARD-LEVEL CONCERN

Risk managers need to establish ways of regularly monitoring digital risks and providing an informed view to their companies. In particular, boards need to be made aware of digital risks and regularly updated on new developments and trends. Digital risk assessments will require input from technology experts and other stakeholders across the business; it may be sensible to set up a working group that meets regularly. Risk managers need to get closer to IT decision-making and forge strong links with their information security colleagues.

2. AS BUSINESS BECOMES INCREASINGLY RELIANT ON TECHNOLOGY AND THE RATE OF TECHNOLOGICAL CHANGE CONTINUES APACE, THE DIGITAL RISKS FACING COMPANIES ARE LIKELY TO GROW AND BECOME INCREASINGLY COMPLEX

Businesses are becoming increasingly reliant on technology to run their operations and services and while this brings obvious benefits, it also means companies are increasingly vulnerable to system failures, data losses and cyber attacks. As the amount of digital information grows exponentially, devices become smarter and connectivity increases, the digital environment is likely to become even more complex. Trends towards more social networking, the growth of cloud computing and varying (and often lagging) national regulations will only add to this complexity.

3. THE RANGE, FREQUENCY AND SCALE OF DIGITAL ATTACKS ON BUSINESS WILL GROW, WITH INCREASINGLY SOPHISTICATED ATTACKERS QUICKLY ADAPTING TO THE RAPIDLY CHANGING DIGITAL ENVIRONMENT

Organised criminals and state-sponsored attackers are well-funded and patient enough to run attacks over a long time or await opportunities. Underground forums on the internet make software and services available that simplify the task of attackers. This allows a wide range of attackers with different motivations and different methods to steal from, disrupt and spy on businesses. Cyber crime also funds the development of more malware, which enables more digital attacks.

4. RISK MANAGERS NEED TO DEVELOP COMPREHENSIVE DIGITAL RISK MANAGEMENT STRATEGIES THAT INVOLVE A RANGE OF MITIGATIONS, AS WELL AS RISK TRANSFER SOLUTIONS

Risk managers need to prioritise which of the many IT security options available will best mitigate risk for their company. They also need to consider how to best use technology standards, guidelines and research into digital risks to help manage cyber threats. In order to effectively manage digital risk, businesses should consider transferring some of these risks to third parties through insurance solutions. While many traditional insurance policies do not cover digital risk, there are a growing number of cyber-risk products and solutions becoming available.

5. THERE IS A NEED FOR INCREASED COMMUNICATION, CO-OPERATION AND COLLABORATION TO TACKLE DIGITAL RISK

Governments, industries and companies all need to work closer together to tackle increasing cyber attacks. While recent government cyber-initiatives in the US and UK are welcome, there needs to better coordination between governments and moves towards more consistent and uniform global regulation if cyber attackers are to be caught and punished. Similarly, there needs to be greater co-operation and sharing of information between (and within) industries and among companies to combat cyber risk effectively.

INTRODUCTION

We are all familiar with Hollywood images of *hackers**: bright individuals, masters of technology, and frighteningly knowledgeable about what is required to break through an organisation's defences. These pictures are reinforced when security professionals are interviewed by the media and we are led to believe we are under severe *threat* from sophisticated and determined adversaries. Yet businesses' IT systems keep working and clients and consumers continue to communicate, share information and shop online. Therefore, individuals are confused, and often sceptical as to how real the risks are in our online world.

To make sense of what is happening, and to make good judgements about the likelihood of future threats and their impact, those responsible for assessing and managing digital risk need to have a firm grasp of both the nature of today's 'attacks' and how these threats are likely to evolve as the technology landscape changes. They also need to understand how digital risks might affect their organisations and what they should do to mitigate them. This knowledge is particularly important if organisations are to make informed decisions on the adoption of new technologies.

Digital risk includes the following: the impact of natural disasters on our data centres and communications infrastructures; system failures; the actions of criminals intent on stealing online banking details or carrying out extortion (cyber crime); and corporate and nation state sponsored espionage aimed at stealing intellectual property. It also includes penetration or disruption of a nation's computing infrastructure (cyber warfare), online terrorist activity (cyber terrorism) and activist groups using the internet to further their goals (cyber activism).

These cyber threats can lead to a variety of wider risks for business, which include:

- Operational risks – the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Most digital risks will fall into this category; this leads to loss of service to customers, loss of data, loss of the internal network, or interruption to supply chains.

- Financial risks – financial losses may result from the inability to operate business processes (such as taking and fulfilling orders or running the manufacturing processes) as well as from fraud and theft.

- Intellectual property risks – the loss of product plans, marketing plans or critical intellectual property to competitors can seriously damage a company's ability to compete.

- Legal and regulatory risks – If the organisation is shown to be in breach of its regulatory requirements, which are becoming increasingly arduous, it could ultimately face sanctions or a fine.

- Reputation risks – public visibility of incidents can cause harm to the company's image, brand and reputation. This harm can arise from even small incidents, such as a loss of service or a breach of just a few records. In extreme cases, security incidents may cause shareholders to lose confidence in a company and will potentially affect its share price.

One thing we can be certain of is that many cyber criminals, and those nation states engaging in cyber espionage, will seek to be early exploiters of new technology. Technological advances mean we are collecting data at a phenomenal rate and aggregating that information in ways never thought of before: connecting it with individuals, and connecting individuals with each other. All of this gives rise to new forms of attack and therefore new risks.

This report highlights that:
- The *threat environment* is rich and evolving.
- Organisations are increasingly exposed to both cyber attacks and non-malicious threats to technology.

** For definitions of italicised words see appendix 1 (page 37) or the glossary (page 43).*

- Technology, and the way organisations use it, is evolving quickly, placing more strain on those responsible for assessing and securing its uses.
- Risk managers need to pay attention to both future *threats* and future uses of technology, moving beyond today's largely reactive approaches.

We begin by examining the evolving *threat environment*: who the actors are, their motivations, how they operate and how a typical attack might unfold. We then consider technology trends and their implications, and in particular the emerging uses of social networking and *cloud computing*. The final section provides guidance for risk managers on how to manage digital risks as the threat and technology trends evolve.

We are increasingly reliant on the computer systems that support the way we communicate; run our businesses; manage the delivery of our food, power and water; and control our cars. We need to take a systemic approach to understanding how digital risks could impact our businesses and develop appropriate risk management strategies and systems to reduce these risks without stifling the innovation and growth that new technology can foster. If our risk managers do their jobs well, our future online world will be safe and those Hollywood images will be just that.

RECOMMENDATIONS FOR RISK MANAGERS

As technology is developing so rapidly and cyber attacks are becoming more sophisticated, the challenge facing risk managers is how to manage this increasingly complex digital risk environment. Within the report we provide some suggestions as to how business can respond to this growing digital *threat*, including some practical recommendations that risk managers can consider and implement straight away. The key recommendations are highlighted below, but please refer to part 2 'Business response and recommendations' for more information.

Recommendation 1: Risk managers should set up a working group to monitor and review the exposure of their business to digital threats and keep their boards regularly informed.

The working group should be made up of technology experts and key stakeholders across the business and should review the appropriateness of current risk management strategies.

Recommendation 2: Risk managers should become more involved in IT governance and strategy, and major technology transformations.

Most digital risk mitigation is managed through IT governance and many significant changes in business technology are driven by the IT department. This means risk managers should work closely with IT stakeholders and decision makers within the company and get more involved in helping shape IT governance and strategy.

Recommendation 3: Risk managers should ensure that recommended and applicable standards and frameworks are used to help manage digital risks.

There are many standard and best practice approaches to assessing digital risks and risk managers should ensure business and IT stakeholders are aware of and using these approaches when digital risk decisions are taken. They should look for any new best practice guidance for more unusual problems.

Recommendation 4: Risk managers should consider risk transfer solutions as part of their overall digital risk management strategy.

Risk managers should be aware that most traditional insurance policies will not cover digital risks. However, there are a growing number of cyber risk insurance products becoming available for risk managers to consider.

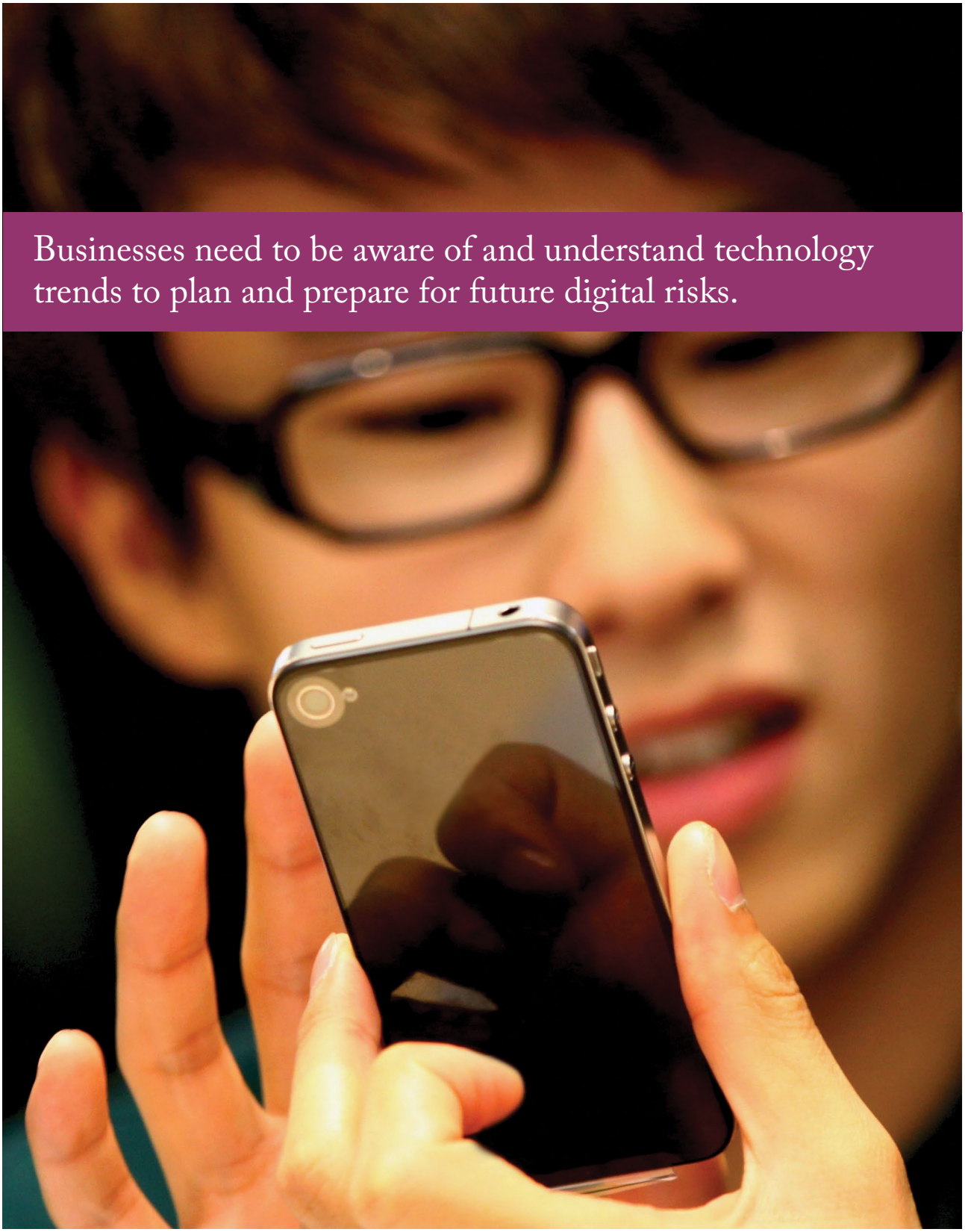
Recommendation 5: Risk managers need to play a role in shaping research around digital risks; helping researchers to understand the challenges in making effective and practical decisions around cyber risk.

As business technology becomes more complex it will be increasingly difficult to make good digital risk decisions. Researchers are developing better techniques but they need expert input and encouragement from risk managers.

PART 1

FUTURE TRENDS

AND RISK IMPLICATIONS FOR BUSINESS



Businesses need to be aware of and understand technology trends to plan and prepare for future digital risks.

1. Digital threats - crime and terrorism

It is increasingly common to open a newspaper or view a website and read about a new cyber attack or a company that has lost people's personal data.

Whether it's the FBI disrupting a large-scale, organised cyber-crime operation that saw thieves take $70m from victims' bank accounts[1], or the head of the UK's Government Communications Headquarters (GCHQ) saying the UK's infrastructure faces a credible *threat* of cyber attack[2], these stories will raise concerns. Risk managers need to ask whether their company could be the next victim. This is a complex question to answer and requires an understanding of business reliance on IT, the approach to threat mitigation and an understanding of the evolving digital *threat environment*.

Ten years ago, we faced the threat of a teenage *hacker* in their bedroom acting alone for kicks. We suffered from fast-spreading destructive *viruses* such as the ILOVEYOU *worm*, which flooded email systems in 2000, resulting in several companies switching off their email systems to prevent it spreading[3]. Figure 1 shows how viruses have progressed.

Today we face the much larger threat of *malware* (malicious software), which can spread through many different mechanisms, hide on our computers to allow an attacker to monitor our actions, and take control of our systems. Malware enables criminals to control our computers in order to steal money and information. The engineering behind some of the more sophisticated attacks requires a combination of skills and organisation that implies significant funding. As these attacks make money, this funds new developments and attracts organised crime.

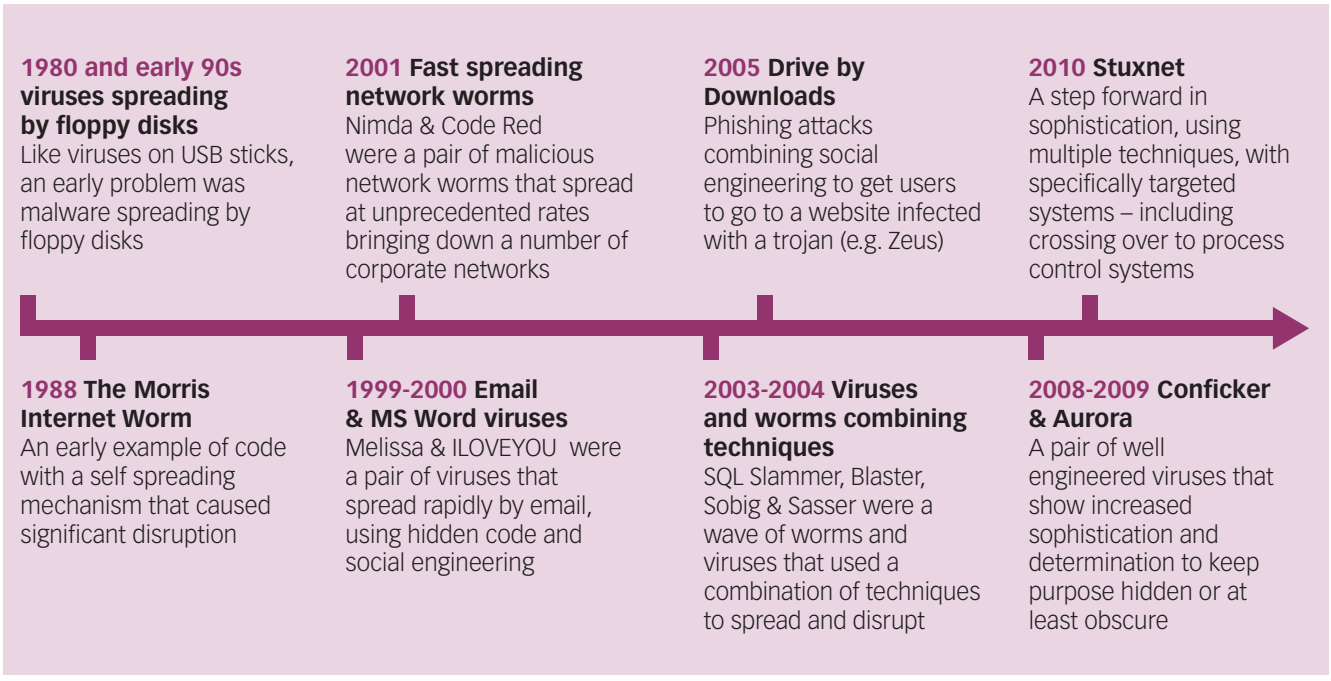
Many different attackers, with different motivations, are pooling their skills. We need to think about how attackers will adapt to take advantage of any potential vulnerabilities in our IT systems.

The complex interdependence of IT systems and business processes means even simple failures can have catastrophic effects and cause systemic failure.

1.1 The attackers and their motivations

Like the offline world, the digital space has a criminal underworld. However, instead of planning crimes during

Figure 1: **Changes in the nature of threats over time**



meetings and phone calls, these criminals use online forums and discussion groups to communicate. This underworld is diverse and brings together people with different skill sets; including highly technical ***hackers***, those who package and sell technology and those who specialise in stealing money from people's bank accounts.

Easy-to-use cyber-crime tools (***crimeware***) and services are traded through underground forums as are the results of cyber crime. The resulting marketplace makes complex criminal attacks possible for almost anyone with a grudge, as well as for well-funded organised crime gangs and even nation states.

The international nature of cyber crime makes catching criminals challenging. Many cyber criminals operate in countries that do not prioritise these crimes or where there is no cyber-crime legislation. Richard Clarke, the former White House advisor, has described these as "cyber sanctuaries"[4]. International co-operation is now critical to fighting cyber crime, as shown in one recent FBI case (see box 1). There are efforts to encourage further co-operation, including plans for a European Union Cyber Security Exercise in November 2010, to help build trust between member states[5].

The following list of roles, motivations and methods illustrate the range of digital ***threats*** facing business today.

Cyber theft and cyber fraud - Many cyber criminals are involved in '***carding***' and online bank fraud. This involves stealing people's credit cards and using online or stealing money from their bank accounts. Consumers are the traditional target for this group, but recently - as banks have improved their online security - these criminals have been increasingly targeting companies. As companies standardise financial processes, and criminals better understand how to compromise them, corporate fraud will be more likely.

Box 1: Zeus and thefts from small businesses

Organised cyber criminals stole $70m from a range of victims (mainly in the US): small and medium enterprises, municipalities, churches and individuals[6]. The gang had infected their victims' computers with a 'zeus ***bot***' enabling them to steal banking log-in ***credentials*** (see box 10 for a more detailed description) by monitoring their web browsing from afar. Using these banking details, they attempted to transfer $220m and successfully obtained $70m.

The FBI started an investigation that lasted more than a year after being alerted to a series of fraudulent automated clearing house payments. The scope and international nature of the crimes required them to collaborate with local, state and federal partners in the US, as well as police agencies in the Netherlands, UK and the Ukraine. On 30 September 2010, five people were arrested in the Ukraine, 11 in the UK and 37 in the US.

Industrial Espionage - There will always be unscrupulous individuals and companies who want to view their competitors' product plans and technologies. As more of this information is now stored on IT systems, it is more exposed. McAfee surveyed the top 1,000 senior IT decision makers, and reported that their companies lost an aggregate total of $4.6bn worth of intellectual property in 2008[7].

Insider trading based on internal knowledge (around issues such as possible mergers and acquisitions activity) can also provide a driver for those seeking private information about a company. A survey by the Financial Times suggests that 49% of all North American mergers and acquisition deals have abnormal trading patterns, suggesting information may be leaking[8]. Mergers and acquisitions teams obviously use computers and networks when preparing bids, and these present potential targets for hackers. Incidents are difficult to prove, and businesses should ensure information is properly protected.

The intelligence community suggests that some nation states are actively using industrial espionage to further the prospects of their private sector business interests[9]. Cyber attacks are clearly a way to achieve this.

Box 2: Espionage for share trading

The US Security and Exchange Commission (SEC)[10] filed an emergency action against Estonian traders who they believe had made at least $7.8m trading shares based on stolen information in 2005[11]. The traders were accused of stealing 360 press releases from the website of Business Wire, prior to publication. The commission suggested that this allowed the traders to strategically time their trades around the press releases.

Insider Attacks - Insiders provide two main *threats*. First, a disgruntled employee may want to take revenge on the company or individuals within the company, and IT systems can provide an easy way to cause disruption. Secondly, there are insiders that attempt to steal money, typically by manipulating corporate processes or the underlying IT systems. The theft of IP by employees is also a huge issue, particularly where employees leave and take customer or partner lists with them. For example, in 2008 CW-Agencies in Vancouver accused their IT director of stealing a backup tape containing 3.2 million customer records worth more than $10m[12]. The US National White-Collar Crime Center suggests that employee theft ranges from $20bn to $90bn a year and upwards of $240bn when accounting for losses from intellectual property theft[13].

Box 3: Attacks by disgruntled employees

Fannie Mae narrowly prevented a disaster that could have caused millions of dollars worth of damage when they discovered a time bomb in their computer systems. Shortly before having his contract terminated, an *IT administrator* reportedly added malicious instructions to a *script* that ran daily on a number of computer systems.

The **script** was set to delete all data on the servers as well as blocking reporting systems and administrator log-ins on the 31 January 2009. Fortunately, a different IT administrator discovered the script prior to its activation. This led to criminal charges for cyber intrusion[14].

After having his employment at GEXA Energy in Houston terminated, a database administrator caused damage by logging into the company's computer systems from his home. He also copied a database containing details of 150,000 customers. In court, GEXA said this resulted in a loss of $100,000[15]. The administrator pleaded guilty on 16 November 2009, which led to a 12-month sentence and an order to pay $100,000 in restitution.

Extortion - Extortionists generally use threats, such as the leaking of stolen data or a *denial of service* (*DoS*) attack on companies' IT systems, for financial gain[16]. They provide links to a website where they hold the data they have stolen, or demonstrate their ability to cause IT or service disruptions, and demand money not to release the data or repeat the disruption process.

Cyber Terrorism - Cyber terrorists use the internet to cause disruption and financial damage. Our critical physical infrastructures - such as power, water and transport systems - could be at risk of future cyber attacks as they become increasingly digitally connected. Such attacks could have a much greater impact than the denial of service attack against Estonia (see box 4).

Box 4: Cyber attacks on Estonia

A series of attacks brought down much of the internet in Estonia in an apparent retaliation to the removal of a Soviet war memorial[17]. This hit Estonia particularly hard as it had deeply embraced the internet revolution[18]. The attack started on April 2008 with a series of distributed denial of service attacks. These attacks targeted various government institutions as well as the main bank and newspapers and lasted about three weeks.

The attacks started with '*script* kiddies' (unskilled hackers) running programmes to flood servers at various targets. As the attack progressed, it was intensified using ***botnets***. Other hackers broke into websites deleting content and adding their own messages. There has been a lot of speculation about who initiated and ran the attack. The attack is an early example of a large-scale coordinated and targeted disruption.

In addition, terrorists are using cyber crime as a funding and money-laundering mechanism, as well as using the internet to radicalise and recruit people.

Cyber warfare - For nation states, cyberspace has become the fifth domain of warfare; they are increasingly investing in defences and preparing for attempts to penetrate their computers or networks[19].

Box 5: Attacks on SCADA systems

There is much speculation that the recent Stuxnet ***Trojan*** was designed to target nuclear facilities in Iran. The initial infections were largely in Iran and, as of 29 September 2010, around 58% of the 100,000 infected machines were located there.

SCADA Systems (Supervisory Control and Data Acquisition Systems) control manufacturing plants as well as power and water infrastructures. These systems have typically placed less emphasis on IT security and hence present alternative, potentially weaker, targets for criminals or terrorists. Stuxnet targeted a specific Siemens SCADA system via the windows machines hosting the industrial control systems[20].

Cyber activism - Cyber activists use the internet to make a political point and to launch campaigns. As part of these political campaigns, companies can become the target of boycotts and demonstrations, with the internet providing a way to organise and communicate such action.

Some campaigns spill out into more direct action. Political activists can try to damage and disrupt companies; for example, by defacing their websites or running ***denial of service*** attacks. Activists may also seek to obtain information that they can use to discredit a company.

The internet also provides a means for activists or disgruntled customers to spread information (or misinformation) about a company or its products and services.

Hacking - ***Hackers*** search for flaws (vulnerabilities) in computer systems and then develop ways of breaking in by exploiting the flaws (***exploits***). It is inevitable that this will continue and, as new technologies emerge, hackers will continue to look at how they can break them. Often hackers do not see themselves as criminals. Instead they see attacks as a way of demonstrating their technical skills and expertise. The initial motivation may even be more one of thrill-seeking by breaking into systems or vandalising websites. However, as their skills become recognised and they interact on underground forums they can sometimes get dragged further into the criminal world.

It is also worth noting the role that ***service providers*** play in enabling the ecosystem to operate. Hosting and ***anonymisation*** services have legitimate and worthy uses, but they also provide a convenient way for criminals to cover their tracks. Arguably, there are even a few service providers that operate directly in the interests of this community. For example, there are confidential anti-virus testing services that help hackers avoid their ***malware*** being detected.

1.2 Non-malicious events

As well as thinking about attackers, businesses also need to consider digital risks relating to non-malicious events. These range from natural disasters, such as fire, flood and earthquakes, through to human error, such as the misconfiguration of complex IT systems. For example, a simple error in a system configuration can leave a company vulnerable to attack. Simple hardware failures, along with power and communication failures, can also bring significant risks.

Box 6: Consequential damage at a supermarket
The knock-on effect of a *disk crash* at a supermarket caused empty shelves, lost sales and a bad customer experience.

In the summer of 2009, an overseas supermarket had a disk crash that they initially thought they had recovered from. Later in the month they had problems with their point of sale devices. An investigation uncovered a small configuration error due to the disk crash. As the point of sale devices failed, the supermarket returned to using the older manual card swipe devices to take payment. Real problems then occurred because their processes had been optimised to order short shelf-life goods according to information provided from their point-of-sale terminals. This resulted in empty shelves, lost sales and a bad customer experience. However, this particular supermarket had insurance, which covered the IT recovery costs and the loss of revenue.

Case study courtesy of Iain Ainslie, Technology and Cyber Liability Underwriter, Ace European Group

Natural disasters can have severe effects on a company's IT systems, as well as other aspects of the business. This is not just due to damage to a data centre or servers; it also includes damage to the power grid or communications infrastructure. Most companies have business continuity or disaster recovery plans to deal with these events, and it is important that these are regularly tested.

Probably the biggest source of non-malicious events is due to the actions or inactions of employees. Given the complexity of modern enterprise IT systems, even slight errors made by IT staff can have knock-on effects for other systems and business processes. Similarly, users sharing passwords can lead to inappropriate access, which can increase the chance of an internal attack or that an attacker may gain a sufficiently powerful user log-in.

Accidents caused by human error have had much recent press coverage; for example, laptops being left on trains or USB sticks containing *confidential* data being lost (see box 7).

Box 7: Examples of security breaches through USB sticks

There have been many security incidents relating to USB sticks resulting in data loss and computers being infected with *malware*. Some recent examples include:

A USB stick belonging to the Greater Manchester Police Training Unit was found on the road outside a police station in 2010. On it was information about how the police should cope with riots, violent suspects and terrorist incidents.

Youngsters from West Berkshire in the UK had details about their mental and physical wellbeing exposed because of an unencrypted USB stick being lost. This was the local council's second serious data loss incident during 2010[21]. This loss happened because the council was still using older *non-encrypted* USB devices, despite having moved to encrypted devices four years earlier.

NHS Lothian had to run an employee data security information campaign and purchase a technology solution to ensure only *encrypted* data could be written to devices[22]. This was triggered by the loss of a USB stick in 2008 that contained letters to Edinburgh GPs.

The US department of defence admitted in 2010 that it suffered its most significant breach of US military computers ever because of malware spreading via a USB stick[23].

Most companies rely on the internet to provide connectivity between various sites, external IT services and mobile staff. Events beyond a company's control can affect this infrastructure. For example, there were fears that the 2002 bankruptcy of WorldCom (a major telecommunications company) would severely disrupt the internet[24]. At the time, much of the internet traffic travelled through WorldCom's network and its failure could have had a knock-on effect for many companies. More recently, *denial of service* attacks in Korea, the US and Estonia (see box 4) have caused wide spread disruption[25,26].

1.3 Evolution of the attack environment

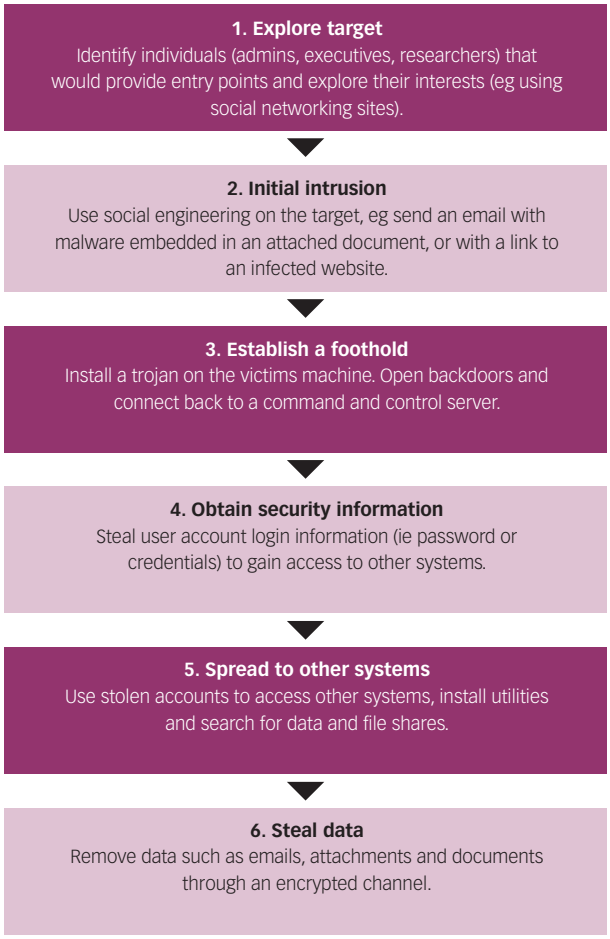
Only a few years ago, malware would spread by simple mechanisms such as email or by finding similarly vulnerable software over the network. In this way *viruses* overloaded the network, causing unplanned service disruption. The problem today is that malware spreads using multiple mechanisms and actively hides from security systems. An example of this is the 2008 Conficker *worm*. Stuxnet is a very recent and even more sophisticated worm that has the objective of reaching and controlling process control systems such as those in power stations (see box 8).

Box 8: Conficker and Stuxnet

Conficker is an example of a sophisticated worm that spreads using a number of mechanisms; including, flaws in Windows software, USB sticks and using a dictionary of common passwords to infect nearby systems. Conficker itself hides on a computer and subverts many of the local security tools. It has a communication mechanism allowing it to pick up new instructions, distribute any information found and forward instructions to other nearby computers also infected with Conficker. The Conficker writers demonstrated a huge amount of skill and knowledge of many aspects of IT in creating such a sophisticated and well-engineered piece of computer software. Despite much effort being applied to understanding Conficker, its purpose still remains unknown.

The Stuxnet *trojan* used to attack SCADA systems is unusually sophisticated, both in the tasks it is seeking to perform and in the way it spreads and communicates. It spreads through a wide variety of mechanisms using a number of Microsoft vulnerabilities, as well as through removable hard drives (including USB sticks), which help it cross from the internet to control networks. In their analysis Symantec suggest that there must have been a large development team behind Stuxnet, with knowledge of control systems and even of specific target systems[27]. They make the point that significant investment must have gone into this attack, although there was no obvious financial payoff.

Figure 2: **A typical schematic of a multi-stage attack**



The way attackers work has also evolved, with *malware* now being used to extract data over many months. Attacks often involve a mix of *social engineering* and malware to achieve an objective. Figure 2 shows the typical steps in a multistage attack: the attacker gains a foothold, spreads into other IT systems and finally removes valuable data. The most sophisticated attack, often known as an *advanced persistent threat* (*APT*), takes this general form. Here attackers target particular individuals and information; new attacks are often used to gain entry and spread, and attackers are careful to cover their tracks. The attackers play the long game, with repeated attempts to successfully complete their objective. Governments and the defence industry are the traditional targets for these attacks; however, more recently, attacks have been aimed at corporate IT (see box 9).

Box 9: Aurora attacks on Google

Operation Aurora, first reported in January 2010, was a highly sophisticated attack on Google and at least 34 other defence, finance and IT companies. Dmitri Alperovitch, the Vice President of Threat Research at McAfee said: "We have never ever, outside of the defence industry, seen commercial industrial companies come under that level of sophisticated attack."

The attack started using a previously unknown flaw in Internet Explorer, as well as through emails containing malicious PDF attachments (again, using previously unknown flaws in Adobe's Acrobat Reader). The attacker used these flaws to install *trojans* on computers connected to the company networks. These trojans then hid and gradually spread to other systems within the company network. The Trojans gathered information, sending it to a subverted server in Taiwan for collection by the perpetrators.

Cyber-criminal attacks have also grown in sophistication. Online bank fraud started as *phishing*: where the criminals would try to replicate a bank's website and persuade victims to enter their *credentials*. Now it uses trojan*s* on the victim's computer to record log-in details and even to enter transactions.

Box 10: Cyber-crime techniques

Criminals often start by setting up websites that infect visitors' computers and install Trojans. *Exploit* packs, such as Eleonore, are for sale on underground forums to help. Criminals then need to get visitors to their website either by using emails or by making their website appear high up in popular web searches.

A trojan is a programme that hides on victims' computer, monitors their activities and communicates information back to the attacker. Zeus has been a popular kit for producing and controlling trojans; however, SpyEye has recently become more popular. Trojan kits sell on underground forums: for example, the latest versions of

Zeus sell for $3,000 to $4,000. Older versions trade for less and are sometimes even downloadable.

A *trojan* or *bot* monitors people's web browsing to steal log-in details. A trojan is usually given a list of popular banking sites and logs all the web traffic to these sites, sending it back to the command and control server. This includes victims' bank log-in and transaction details. Additional 'injects' can be bought with the Trojan kit that ask extra bank verification questions or add additional transactions as the victim is banking.

Attackers then use the passwords to transfer money out of the company's bank account. Typically these transfers are made to a "*mule*'s" account: someone that they have recruited to receive money. Again, there are services available on underground forums to help recruit mules. The mules then wire money to the attacker in another country. Once a bank detects fraudulent transactions it will try to block, reverse or claim back the money, but it can often be too late.

1.4 Threat summary

Four major points emerge from our discussion of the *threat environment*:

- There is an increasing variety in the methods and motivations of attackers.
- Attacks are increasingly sophisticated. Attackers are now well-funded and are patient enough to run attacks over a long period of time.
- Cyber crime funds the development of more *malware*, which enables more cyber attacks.
- Many risks to digital security remain from more traditional sources such as accidents and environmental *threats*, including fires and floods.

Risk managers need to have an understanding of the threat environment and its effects on their business. The way a business uses and relies on IT systems will change over time and risk managers need to reflect on the following issues:

- Do changes in the threat environment necessitate changes in the company's response?
- Does this mean increased IT security investment or tightening policies that may cause business disruption?
- As we adopt new ways of using IT, we need to be aware that cyber criminals will take advantage of new weaknesses and find new opportunities for making money.
- With our increased reliance on IT, are our contingency plans sufficient to keep the company running?

The attack environment is agile and so will adapt to new opportunities. The next section describes future technology trends. We will show that these trends will bring more complexity, faster change and more business dependency. This will mean new opportunities for attackers, so we can expect the threat environment to continue to thrive.

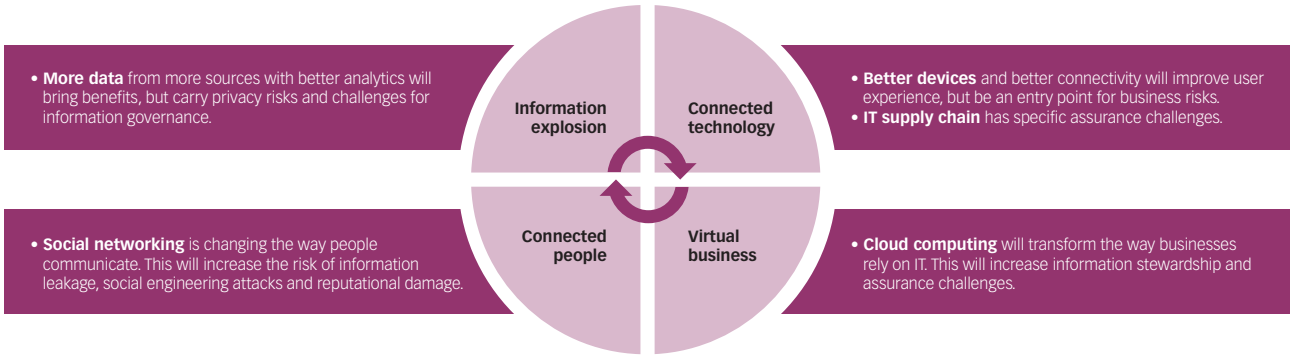
2. Current and future technology trends

In order to plan and prepare for future digital risks, businesses need to be aware of and understand technology trends. We examine four major trends (see figure 3) that will transform the digital risk landscape:

- The explosive growth in digital information
- Advancements in connected technology
- Changes in how people connect
- The trend towards virtual online business.

Recent advances in IT have brought huge changes to how we use and manage information: processors are smaller and faster; broadband and wi-fi have improved connectivity; screens have better resolution; touchscreens have become input devices; storage devices are smaller and hold more data; and power consumption and batteries have improved. This has allowed us to develop smartphones (such as the iPhone, Palm, or BlackBerry) that have more computing power and storage than desktop PCs had ten years ago.

Figure 3: **Future technology trends**



Box 11: The pace of technology change – the example of the telephone

The telephone provides a powerful example of the increasing pace of technological change. By most technical measures of storage and processing the iPhone 4 is ten times more powerful than the 1995 Pentium-Pro based PC, which in turn was considerably more powerful than the original Intel 8086 PC.

The iPhone 4 was released in 2010, and 1.7 million devices were sold in the first three days. This is twice as many phones as the Bell telephone company (formed in 1877) were supporting in 1900.

Unlike early telephones, and most significantly because of the convergence of technology and connectivity, these modern devices are immediately able to connect and share data across many systems. By year-end 2010, it is estimated that 1.2 billion people will be carrying handsets capable of rich mobile commerce; thus providing a rich environment for the convergence of mobility and the web[28].

Rather than knowing how much more powerful these devices will become, the real challenge in terms of managing digital risk is predicting how people will use them and the implications of this.

At the same time, the internet has transformed the way we communicate and consume media. This started with email communication and static websites. Search engines such as Google made this content more accessible. As networks and home connectivity improved, users started to spend more time online. This led to instant messaging, richer interactive web content, webcasts, and downloadable music, films and applications. More recently *blogging*, *tweeting* and social networking sites have become very popular.

Companies have been transformed by these changes. Most use IT to run their business processes and many use the internet to connect to their customers. New consumer devices and applications continuously find their way into the enterprise. Companies also store and analyse huge amounts of information about their processes and customers.

"Enterprises are seeing a sea change from risk being associated with physical resources, like property, to being increasingly concerned with intangible digital assets."
Dan Trueman, Underwriter, Kiln

2.1 The information explosion

The amount of digital information is growing exponentially: more videos are created and copied; sensors collect more information; and more business, scientific and personal information is generated and published online. In addition, there are more ways to store, combine and analyse this information. In general this is a good thing; businesses are using this information to innovate, become more efficient and create better services. However, there are privacy concerns over the ability to find and correlate information about individuals. Plus, the new developments will create complexity, making it more difficult for businesses to control their use of information.

Business intelligence.

Companies are storing increasing amounts of data and using it to develop and optimise their business processes and strategies. Many corporate applications (including those around managing customers, the supply chain and finance) feed information into vast *data warehouses*. Business intelligence applications analyse the data and look for trends and anomalies, which are used to produce regular reports on how the business is performing.

Over time the amount of data and the sophistication of the analysis has increased. Technological advances have allowed businesses to explore the data, relationships and trends in ever more detail. In the same way that improved search on the web has changed the way we casually look up and check information, businesses will soon expect to be able to get quick answers to ad hoc questions about how the business is performing.

Business intelligence applications bring obvious advantages, but they will require even better data governance to ensure risks are managed. Businesses generally have policies and procedures to ensure security of information. For example, there will be policies to restrict access to applications and to ensure the *integrity* of databases and the proper archiving of files. Business intelligence increases the size, accessibility and complexity of these databases and will make it difficult to enforce these policies. As digital information gets more easily combined, copied, edited, emailed and published, information management will be even harder.

Box 12: The challenge of data governance

Zurich Insurance lost the personal details of 46,000 customers in 2010[29]. The data was stored on a back-up tape that was lost while being transferred to a data storage centre in South Africa. The Financial Services Authority (FSA) criticised Zurich UK for failing to ensure it had effective systems and controls to protect customer data handled in the outsourcing arrangement, and to prevent the lost data from possibly being used for criminal purposes, the FSA fined Zurich £2.27m.

Box 13: Heartland Payment Systems lose credit card details

Heartland Payment Systems found malicious software inside their payment processing systems. This *malware* was collecting unencrypted payment card data. As a major credit and debit card processor, this placed as many as 100 million cards - issued by more than 650 financial service companies - at risk. As a result, by the end of 2009, Heartland had incurred expenses totalling $128.9m and their share price had dropped from $14 to $4[30].

Businesses face a trade-off in deciding policies for information management. Providing easier ways to analyse data and using that data to optimise processes clearly has its benefits, but there are also risks.

Data integrity/availability - *Threats* to the quality of data can come from failures in both the central *data warehouse* (where all the data is stored) and the systems supplying the data. As business processes become more intelligently automated, the business will be at more risk when the *availability* or *integrity* of information feeds is affected.

Data confidentiality - Leakage of data from business intelligence systems provides others with an insight into how the business processes are performing. The wider the access, the easier it will be for attackers to find entry points that they can use to derive and extract data for both extortion and espionage.

Regulation - Business intelligence systems holding personal information about employees or customers must comply with data protection legislation. For companies operating in an international environment this means complying with many different pieces of data protection legislation. The data breach notification laws within the US require companies to notify and help manage the risks of customers whose data is lost. This legislation therefore can lead to both reputational and financial risks.

Other regulations may become applicable, depending on the type of data and regulations in a particular industry segment. In the US, the Sarbanes-Oxley Act mandates good practice to protect the integrity of financial reports and hence financial data. Basel II (for the banking sector) and Solvency II (for the EU insurance sector) also have strong data integrity requirements. Non-compliance can have serious consequences.

Increasing collection of data

Today we have public and private CCTV; systems to track people's movement through shopping centres using their mobile phones; smart meters monitoring electricity usage in our homes; and *RFID* tags to monitor the movement of goods. The growing trend to collect data from physical devices will lead to privacy concerns for individuals, particularly when coupled with storage and analytic capabilities.

In the longer term we can expect huge growth in sensors measuring everything in our homes, workplaces, highways and cities. Challenges will centre around whose information it is, who gets to see it and its provenance. There is likely to be societal unease over even more surveillance, yet there will also be benefits; for example, easing traffic congestion and reduced energy consumption.

Many companies will store, process and share sensor data or aggregated results. Policies and regulation on

appropriate use and levels of security will be needed to ensure good data *stewardship*. As in other areas, it will be challenging to define policies that take account of privacy concerns and yet encourage innovation.

2.2 Connected technology

Advances that improve devices, connectivity and ways to display information are generally good things, but there are risks. Employees are likely to want to use (unsecured) consumer devices in the workplace, which will increase the risk of security breaches.

Personal and business use of USB sticks and social networking sites are two current examples of employees' potential to cause security risks within their companies. As usage patterns change many organisations have had to create and implement policies after the event.

Further issues related to these technology risks are:

• How global supply chains affect the IT industry. Both software development and hardware manufacturing have aspects that make *assurance* of technology products challenging.

• Trends to build better security properties into standard computer systems. Since standard machines are a weak point for security management, this has the potential to significantly improve digital risk management.

For more information on both these issues, please refer to appendices 3 and 4.

Personal devices

Corporate IT has transformed from a world where most devices were permanently connected to the corporate network to one where users have laptops, smartphones and portable storage devices. While people value the increased mobility and connectivity, it means that data moves around the world with them. Devices touch many different networks, such as employee's home networks and those provided by hotels, airports and coffee shops. This exposes them to less protected environments and an increased risk of attack.

Other risks to business relating to the use of personal devices will include:

Physical loss - Devices are becoming smaller and more mobile, which increases the chances of them getting lost or misplaced. At the same time, storage and connectivity increases. This leads to risks of data loss and unapproved access to corporate networks. USB sticks provide a current example as they hold large amounts of data and are often lost (for example, last year a total of 4,500 USB sticks were found by dry cleaners[31]). Laptop loss also regularly hits the headlines, particularly where personal records are lost. If these devices are not secured, companies risk others gaining access to corporate services such as email.

Box 14: Laptop stolen from US Department of Veterans Affairs

The US Department of Veterans Affairs has estimated that the loss of 26.5 million personal records has cost between $100m and $500m. The data included names, birth dates and social security numbers of veterans and their families, along with details of military personnel on active duty. This breach happened when a laptop containing the data was stolen from a staff member's residence in May 2006.

Malware Spread - As mobility increases, devices will connect to many different networks; some of which may have hostile users and make companies more vulnerable to attack. Movement between these networks allows *malware* to spread; for example, from the home into the company. Even a USB stick can bridge these systems and spread infections between computer systems; for example, the Stuxnet *Trojan* spreads in this way (see boxes 5 and 8).

Enterprises work hard to protect PCs against malware by running *antivirus* systems and patching processes to fix software errors: a basic and minimal level of protection. As *hackers*' explore and find ways to attack a greater variety of devices, including smartphones, the scope of these security processes must increase. Otherwise, we

risk these devices becoming the attackers' entry point into the company. However, running these processes is becoming increasingly difficult as more employees use their own personal devices for work.

Device Security Failures - Often we rely on features in our devices to prevent others gaining access. Where there is a large range of devices or they are closed to external examination it becomes hard to know whether these mechanisms are trustworthy. For example, ***hackers*** have shown that they can remove an iPhone passcode[32].

Connectivity and convergence

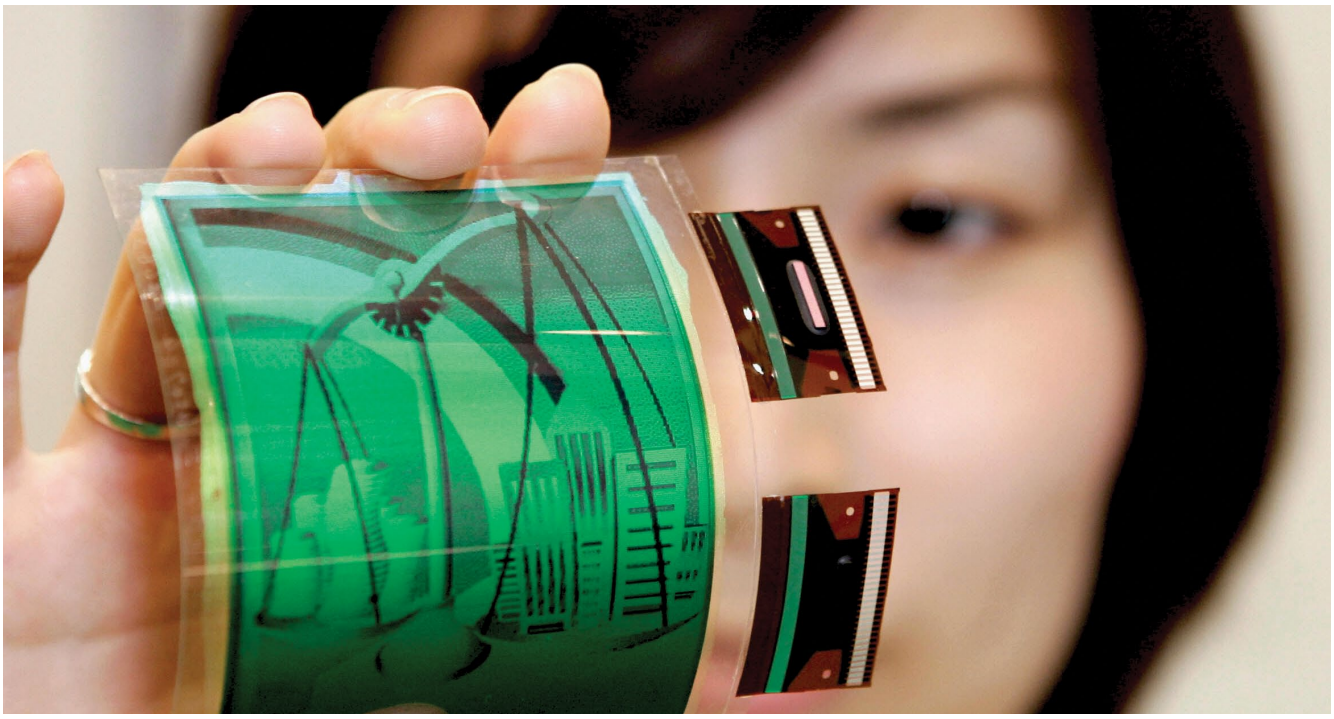
The digital world is not just about our computer systems. These days most physical devices, from the power and water grid to our cars, contain embedded computer systems. Traditionally, these systems operate on isolated networks, hence minimising many of the security ***threats***. However, more are now connecting to standard networks, and convergence to common software and ways to share data (eg USB sticks) will lead to further ways of being compromised. This was exploited by the Stuxnet ***Trojan***, as described earlier. In general, greater connectivity is exposing more systems to attacks that could affect basic infrastructure and, for example, stop factories functioning, disable cars or even cut power to regions.

Box 15: The hacked car

A security team have created software that can take control of cars[33]; for example, disabling the brakes or shutting off the engine[34]. Modern cars have a multimedia network that connects mobile phones, the dashboard, ***Bluetooth*** headsets and ***MP3*** players. These networks connect through a gateway to the engine control network, allowing the reporting of performance data. As the connectivity grows, there is an increased risk of an attack spreading to the engine control systems.

Transition to digital displays

Today, large flat-panel LCD displays are increasingly replacing posters. Research laboratories are investing in producing plastic flexible displays[35] (see ***figure 5***). These displays will be more like paper: much lighter and produced on rollers. Consumer devices will lose most of



their weight and, since these new displays only require power to change the image, battery life will increase.

As display technology advances, new usage models will be developed that improve the way we view information. These displays offer the potential to make vast amounts of information viewable at once. As businesses value new functionality and new ways to view information, growth in the use of large displays is bound to accelerate, despite the potential security risks.

As future devices take advantage of such displays, ***threats*** will develop to reflect the way they are used. Printed material is still one of the big sources of data loss. Devices and walls that retain displayed data will carry similar risks. As display sizes grow and are placed in public or semi-public environments, it will be harder to prevent unauthorised people from seeing ***confidential*** content. The risk is that most companies will find it too expensive to control routinely displayed information in the same way as they would control and vet press releases or marketing documents, for example.

2.3 Connected people

Internet ***Service Providers*** (ISPs) and broadband at home are enabling and encouraging people to:

- Use email and instant messaging to communicate.
- Use the web and ***web 2.0*** to publish and broadcast interactive information about themselves and others.
- Use social networking to create and maintain relationships.

These trends are affecting the workforce and working environment, often with positive business outcomes. However, there are many potential risks. Social networking, in particular, can be a source of information leaks; it can also inform ***social engineering*** attacks, spread ***malware*** or even be a cause of reputational damage.

Social networking

There is a growing range of online social networking methods and sites. Facebook is the most obvious and popular example. A key feature is that these sites allow people to maintain their existing physical social networks and grow them by finding people with common interests. Some social networking sites serve a particular niche; LinkedIn, for example, helps people develop their professional networks. Other sites encourage *blogging*, such as Twitter the popular micro-blogging site.

Social networking sites can be useful in promoting a company and its products and in communicating with different audiences. BT has even introduced an internal social networking site to encourage collaboration between its employees[36]. However, social networking also exposes companies to many new risks; these are discussed below.

Information leakage - Social networking provides ways for people to communicate and hence new ways for information to leak. The immediacy of blogs and ***tweets*** means that comments are sometimes not properly considered and reviewed, unlike carefully vetted reports and press releases. It is easy for pieces of confidential information to 'slip out'.

It is not just product plans that leak onto the social networking sites. General office gossip can spread out into public forums. If employees use such sites to vent their frustrations it can present risks to a company's reputation.

Box 16: Confidential information on LinkedIn

An employee working for Hays Specialist Recruitment left to set up a rival agency. However, while still at Hays the individual uploaded many of his business contacts into the LinkedIn social networking site; claiming that this was done with Hays consent. He also asserted that once the invitation to join his network was accepted "the information ceased to be confidential because it was accessible to a wider audience".

A judge rejected this argument in a court case in 2008 and required the disclosure of the LinkedIn records. This case raises issues around when information ceases to be ***confidential,*** particularly when posted on external personal sites. It also suggests that internet usage policies may need reviewing to mitigate potential risks.

Information gathering - Social networking provides a window into people's lives that potential attackers can use to their advantage. When carrying out a targeted attack, such as ***spear phishing*** or industrial espionage, an attacker may spend considerable time gathering information about the company and employees using ***social engineering*** techniques. Social networking sites provide a great way to explore the background of a company and pick potential targets. This may involve identifying key individuals, perhaps a PA or ***System Administrator,*** researching their hobbies and interests, befriending them, questioning them, or directing them to websites that infect their computer.

Most social network sites do very little to check people's identities; all you need is a valid email address. Information on social networking sites has also been used to help impersonate people. For example, text has been taken and used in ***whaling*** emails to make them more believable.

Box 17: A fictitious identity experiment[37]

Thomas Ryan, a security consultant, created a fictitious security expert called Robin Sage as part of a 28-day experiment to show how easy it is to fabricate a credible identity, even in the security world. Ryan enrolled Robin on a number of social networking sites; her profile listed her job as a cyber-***threat*** analyst at the Naval Network Warfare Command and claimed she had a degree from MIT. Her profile also said she had 10 years experience, despite being only 25. Even this simple error did not prevent some security experts from trusting her.

In the course of the experiment Robin used these social networking sites to build a network of contacts within the defence and security industries and also within the alumni of MIT. Many of Robin's contacts treated her as part of the security community, asking her to review papers, speak at conferences and even contacting her about jobs.

Malware spread - Cyber criminals are starting to use social networking sites to spread malware. ***Spam*** and phishing attacks have become increasingly ineffective, but when messages come from people we know or feel connected to they become more believable. This provides a highly effective way of spreading infections.

Reputational attacks - Social networking and ***blogs*** can be a good way to promote a company and its products. However, it is also easy for others to publish stories that could damage a company's reputation. Companies should mitigate these reputational risks by keeping an eye on their online public profile and developing contingency plans to respond to any crisis.

2.4 Virtual business

Over the next few years, we expect a massive growth in ***cloud***, driven by investment by IT companies. For example, Steve Ballmer, Microsoft's CEO recently said: "About 70% of the folk who work for us today are either doing something that is exclusively for the cloud or cloud inspired… This is the bet for our company"[38].

This will lead to the emergence of a wide variety of new business services as well as the migration of current applications to the cloud. Ultimately, this could lead to the creation of truly virtual businesses where almost every aspect of a business is outsourced.

The cloud provides IT services on demand over the internet. This should be contrasted with a company running their own IT systems where they need to maintain sufficient capacity to meet their peak usage. By sharing the cloud providers systems, companies expect to achieve considerable cost savings[39]. Customers are able to rapidly increase or decrease the number of computer resources they are using, to fit with their business cycles. Cloud providers tend to offer standard services for many customers. This contrasts with IT outsourcing, where services and contracts tend to be negotiated to fit the customer's needs. The cost and agility gains mean that companies are likely to increasingly use cloud services. A recent survey of IT buyers by CIO magazine found that

companies expect to spend an average of 5% of their IT budget on *cloud* and expect this to double in the next five years. A more detailed explanation of cloud computing is given in appendix 5.

Box 18: Cost savings from cloud computing
A number of companies are already using cloud and achieving cost savings or business benefits. For example, the US Security and Exchange Commission (SEC) investor advocacy relations group migrated to a salesforce.com solution in the cloud. This provided them with better IT support for their processes and reduced the time it takes to close a case from over 30 days to less than seven. The cloud approach allowed the solution to be adopted with very little upfront investment. In another example, the state of Utah reduced the number of servers they use from 1,800 to just 400 virtual servers, saving $4m[40].

Despite the advantages, many are worried about the security implications of cloud. The CIO magazine survey placed this as the top concern for IT stakeholders41. It is not that cloud is necessarily less secure. In fact, when run by specialist IT providers, it may offer better security. However, for cloud to become a trusted platform for critical business services, it will need to provide much better *assurance* offerings, giving improved visibility on security levels that integrate into the overall digital risk management process.

There are a range of concerns relating to transparency and reliance on third-party cloud *service providers*. For example, legal and regulatory obligations will mean that companies will have to pay attention to:

Location - Where is data held in the cloud, what is the legal jurisdiction, and what are the implications and obligations?

Audit - Companies need to audit their IT systems; a generic audit by a cloud service provider will not normally suffice, and handling many different audit demands will undermine the cost model.

Governance - Many companies have integrated security and *identity management* approaches. Cloud services often have different security and access processes, which could undermine overall control and compliance.

Financial Resilience - If the service provider fails to make money, there is a risk it will collapse or withdraw the service. This can lead to operational risks and the *threat* that critical data is lost along with the loss of service. Even when data is recoverable, there may be costs in converting it to a usable form. Worse still, the data could potentially leak out if the cloud service provider's assets are sold.

Companies that have control over their IT systems can also make their own decisions about whether to vet IT staff, how much control or trust should be put in system administrators and whether to deploy new security technology. In the cloud they would need to rely on the choices of their providers.

Cloud platform and infrastructure providers operate on a very large scale and rely on sharing or reusing resources between customers. This will lead to particular security design choices. Customers should ask about the way processes, architecture and staff will ensure appropriate separation of their data: in terms of both *confidentiality* and *availability* of their information resources. Data can become concentrated among a few service providers and attackers may find it a worthwhile investment to break a cloud service to gain access to many companies' data.

The situation gets even more complex when software service providers run their offerings using cloud platforms or infrastructure. Some software service providers may use other third-party services as they construct their offerings. This increases the challenges around IT governance. It is no longer sufficient to know that one company is managing our risks appropriately. We need to look beyond the direct service provider and down the supply chain to look at the other service, platform and infrastructure providers. All stakeholders should be performing this due diligence and sharing appropriate assurance information.

Any transition to *cloud* is likely to be painful for mature companies. Existing IT departments will shrink and the skills required for the remaining staff may change. This transition process may well increase risks from internal *threats* if *IT administrators* become disgruntled. Having made the transition, it is then hard to go back and would be likely to require a new investment cycle. Moving to cloud may also reduce flexibility to respond to changes in regulation as it may be hard to force changes in the service contract.

3. Regulatory and legal risks

Concern that digital risks are not being adequately addressed is putting pressure on governments to fix the problem. This has led to many laws and regulations governing the way we use technology. New regulations can improve the situation but often prove costly.

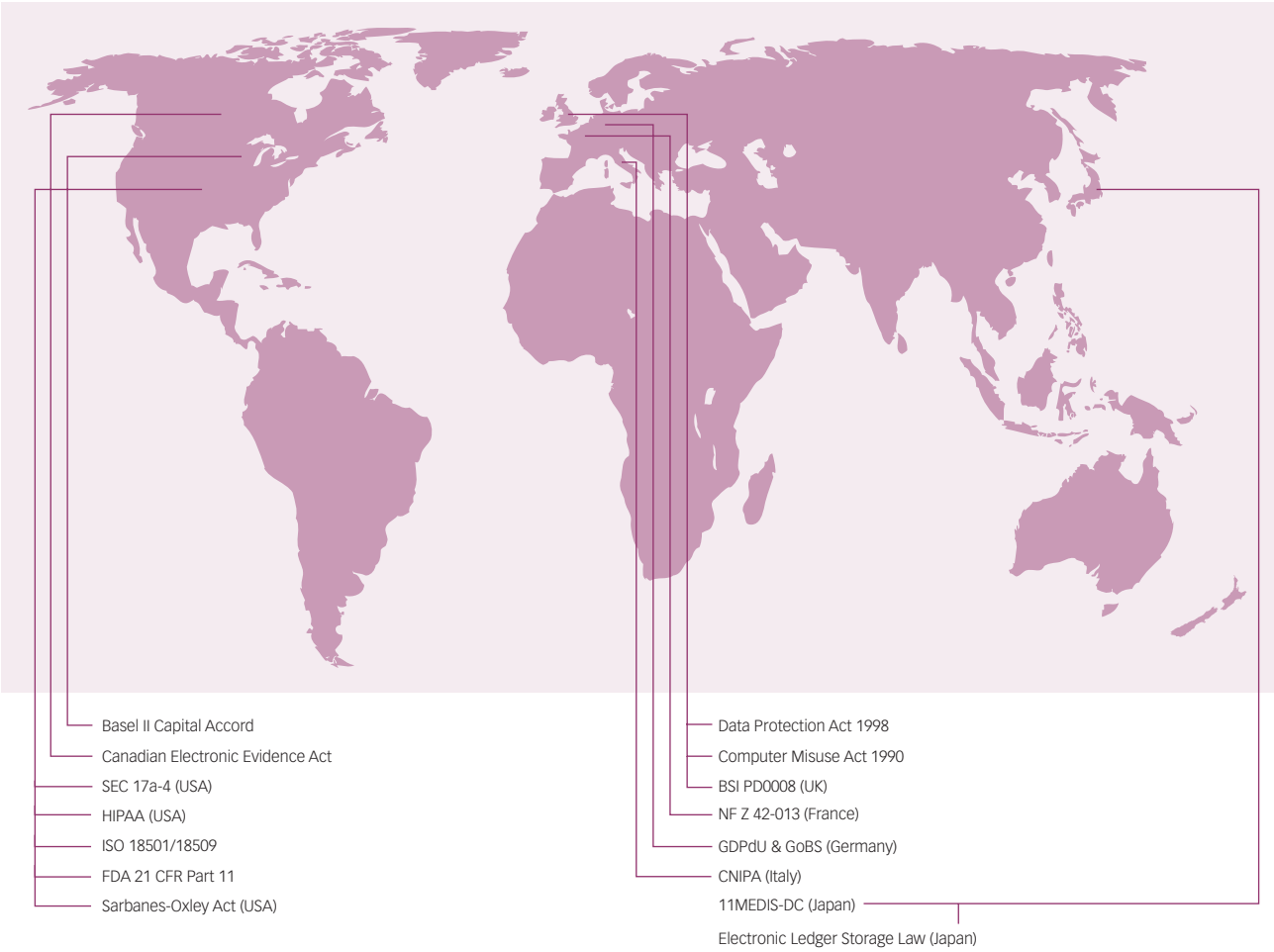
For example, the Sarbanes-Oxley Act of 2002 (SOX) was introduced to ensure the accuracy of a company's financial reports and therefore demanded checks on the *integrity* of the IT infrastructure and financial applications. SOX provided the business justification for improving security and *identity management*. However, this was costly: a survey by the US Chamber of Commerce in 2007 showed 69% of companies estimated their costs of complying with SOX at above $100,000[42].

3.1 Challenges of multi-jurisdiction

As technology advances new regulations often follow, but not necessarily consistently across the world. Keeping track of the different rules across multiple regions, countries and industries is becoming a major challenge for organisations, particularly multinationals (see Figure 4). Multinationals will have to deal with the different rules applied by each state as well as being aware of industry specific ones.

New regulations lag behind technological developments and vary across the world. For example, data breach and

Figure 4: **A sample of global regulations**



privacy legislation is still in its infancy, even though many companies have large customer databases retaining vast amounts of personal information. The EU has a regulatory approach to data protection that contrasts with the punitive post-incident data breach notification rules in the US. In May 2010, as news spread about how Google's streetcars were collecting wi-fi data, the US had a series of class actions. The UK responded through the information commissioner's office[43], while Australia treated it as a criminal matter for the police.

This developing legislation around privacy and data protection provides a good example of the challenge of multi-jurisdictions.

- In the US, most states have breach notification rules. These vary, but can be very expensive since failures can require the notification of many thousands of people.

- The US healthcare industry has the health insurance portability and accountability act (HIPAA) to protect patient health information.

- EU member states are required to implement the Data Protection Directive (95/46/EEC) which was introduced to harmonise national data protection laws throughout the EU. However, differences between national laws have arisen partly due to the fact that the Directive allows each member state to introduce or retain more stringent rules.

- The Gramm-Leach-Bliley Act in the US was introduced in 1999 to allow certain kinds of financial institutions to merge. This act includes a set of requirements for safeguarding the privacy of customers' personal financial information.

These different regulations are an indication of the challenges to come as communities increasingly find that they do not have shared views on what constitutes good *stewardship*.

Another current area of developing legislation is around government surveillance. Often the driver is national security, and so different countries have different rules for what businesses are obliged to share. Some examples of differing legislation include:

- The UK has had the Regulation of Investigatory Powers Act (RIPA) in place since 2000. In effect, this allows certain public bodies numerous rights to monitor or demand access to certain communications. Changes have occurred since its introduction: most significantly the change in 2009 requiring ISPs to log users' web and email activity.

- It is reported that the US is preparing a new bill to ensure ISPs are able to comply with orders to disclose the contents of communications[44].

- There has been controversy in Saudi Arabia surrounding the banning of BlackBerrys that are not enabled with government intercepts.

Regulations in different jurisdictions may even conflict. For example, the French Data Protection Agency (CNIL) has had to issue guidance to help companies manage apparent conflicts between data protection legislation and US discovery legislation (see box 19). The latter has required documents to be made available for court cases[45].

Box 19: e-Discovery challenges

The Office of Federal Housing Enterprise Oversight was forced to spend $6m (totalling 9% of its annual budget) to comply with a subpoena for electronic documents[46].

The US federal rules of civil procedure were amended to include electronically stored information in 2006. This means that both parties in litigation must supply a range of information from emails on social networking sites to system log files and surveillance tapes. Electronic data must also be preserved as soon as litigation is considered.

In the case of Harkabi v. Sandisk Corp, the judge ordered the defendants to pay $150,000 in monetary sanctions for the prolonged delay in producing details[47].

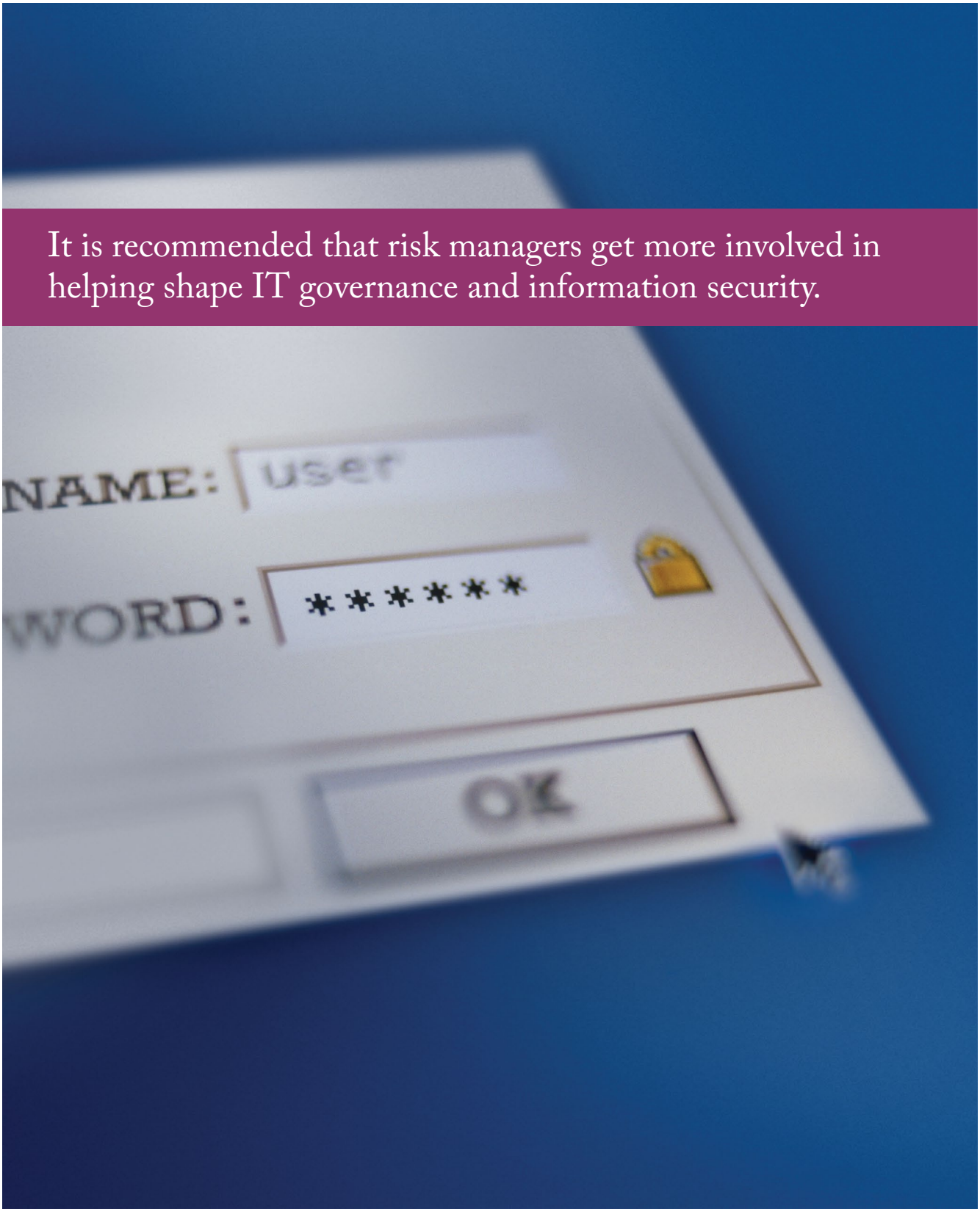
His ruling began: "Electronic discovery requires litigants to scour disparate data-storage mediums and formats for potentially relevant documents. That undertaking involves duelling considerations: thoroughness and cost. This motion illustrated the perils of failing to strike the proper balance."

There are also questions relating to the appropriate jurisdiction for an act committed within cyberspace, ie where will legal action be taken in the case of a dispute[48]? Some US states, such as Connecticut, claim jurisdiction where an offence impacts upon a computer located in the state[49]. Other countries, such as Malaysia[50], have a very wide definition of its jurisdiction. Therefore, an act that is legal in one country could lead to prosecution in others. Companies need to be aware of where legal action may occur.

Although each new regulation may lead to better security, it could also incur unforeseen legal ramifications. The pace of technology progress means that regulations will always lag changes brought about by technology. Moreover the regulations and ramifications will likely vary across jurisdictions. Dealing with the risks associated with multi-jurisdictional legislation and regulation is going to continue to increase in complexity and is a topic that organisations will have to pay close attention to.

PART 2

BUSINESS RESPONSE AND RECOMMENDATIONS



It is recommended that risk managers get more involved in helping shape IT governance and information security.

1.Risk governance

The primary governance question for digital risk is how serious is it for the business? We recommend that digital risk should increasingly be considered within a company's overall risk governance processes and structure and should become a major concern for boards. The question is how to do this?

This is still a hard question to answer, and will vary for every company. The future trends part of this report has painted a picture of an increasingly sophisticated and hostile *threat environment* that will adapt and develop in response to fast-changing technological advances. If anything, the digital *threat* is likely to get even more complex in the future.

This suggests that, in addition to any risk assessment and mitigation activities, risk managers need to make time to monitor developments in threats and technology and provide an informed view to the business about overall risks. They will not have all the skills and knowledge to do this themselves, and so they should look across the business to find the right stakeholders and expertise to help.

Recommendation 1: Risk managers should set up a working group to monitor and review the exposure of the business to digital threats and keep their boards regularly informed. More specifically:

- The working group should decide and review when the board should be actively involved or simply informed of digital risks to the business.
- The working group should include information technology experts and strategists, key business stakeholders and legal representatives.
- It is unlikely a single formula will work for regular analysis, but the structure of this report might provide an appropriate starting point.
- The working group should review the appropriateness of risk mitigation and transfer strategies currently used by the business.

More broadly, the trends show the need for more effective communication, co-operation and collaboration at multiple levels to deal with digital risks. Individual governments and regional bodies are beginning to do more, with a series of cyber security initiatives announced by the EU[51], US and UK. However, there is still very little sharing of information or coordinated response to attacks between stakeholders, ie between businesses, industries and governments. This makes it much harder to spot problems or to catch attackers. This is made worse by differing and lagging legislation and law enforcement between countries and sectors.

2.Risk mitigation

Mitigating digital risk is expensive for companies in terms of both investments and labour. Most of these costs fall within the IT department and it is the IT department's responsibility to keep responding to changing business needs while at the same time ensuring security is managed appropriately.

Continual technology change has led to many businesses having heterogeneous and complex IT. This makes security management hard. We will examine the range of security products available and the effort involved in putting good security in place later in this report. Risk managers need to work closely with the IT department to prioritise which of the many options available will best mitigate risk for their company while supporting the ongoing needs of the business.

We will also look at the standards and best practices that can be used to help manage digital risk.

2.1 Security and IT department

In the early days of IT, businesses custom-built systems to suit their needs. Gradually, standard software emerged for both infrastructure and applications. Making adjustments is often risky and expensive when old systems are still

being used. As new technology emerges most businesses find their IT is a complex mix of custom-built and commercial off-the-shelf applications and infrastructure. There are regular and ongoing attempts to consolidate and simplify IT services, but the pace of technology change makes this difficult.

This also makes security management hard in a number of ways. For example, it is difficult to enforce a centralised and uniform identity and access policy when every application has different *access control* mechanisms. Similarly, it can be difficult to determine how different components relate to each other, so it becomes difficult to determine where the business is at risk.

The IT security marketplace has responded, albeit in an unstructured manner, with hundreds of product categories (see Table 1) dealing with many of the different IT risk problems. This quickly leads to prioritisation challenges that require broad business, technical and security expertise.

As the quote below shows, there can be differences in culture and incentives between risk and IT functions. As such it is recommended that risk managers get more involved in understanding and helping shape IT governance and information security, particularly in promoting access to appropriate security skills and knowledge.

"As brokers we often see a certain tension between the insurance buyer and the IT Security team at the client. Essentially, the insurance buyer is tasked with identifying potential risk exposures, but the IT Security team is keen to demonstrate that they have fulfilled their task: to put in place and manage a robust IT Security system."
Luke Foord-Kelcey, Jardine Lloyd Thompson

Table 1: **A sample of major security product categories**

Data Protection & Privacy Management	Infrastructure Security	Governance, Risk, & Compliance Management	Identity & Access Management
Application Security	**Endpoint Security**	**Risk Management & Compliance**	**Identity Management**
• Application Penetration Testing • Application & Code Testing/Scanning • Web Application Firewalls • Service Oriented Architecture (SOA) Security	• Personal Firewall • Anti-virus, Anti-spyware, Anti-adware • Host intrusion Detection/Prevention Services • Mobile Devices Security	• Compliance Assessment • Vulnerability & Threat Management • eDiscovery & Archiving	• Directory Services • User Provisioning/ Deprovisioning
Content Security	**Network Security**	**Security Operations**	**Access Control**
• Email Security • Web Content Filtering • Other Channels (IM, P2P)	• Network Access Control • Network Intrusion Detection/Prevention Services • Firewalls • Virtual Private Networks • Unified Threat Management • Wireless Security	• Security Incident/Event Management • Forensics • Event Log Management • Security Configuration Management • Security Operations Centres	• Role Based Access Control
Data Security	**Data Centre Security**	**Business Continuity**	
• Enterprise Rights Management • Disk/File Encryption • Public Key Infrastructure • Data Loss Prevention • Storage Security • Database Security	• Cloud Computing Security • Virtualisation Security	• Disaster Recovery Services • Physical Security	

Recommendation 2: Risk managers should become more involved in IT governance and strategy and major technology transformations. More specifically, they should:

- Ensure awareness and understanding of the levels of reliance on technology across the business.
- Know the different roles within the business that are involved in managing digital risk, and ensure the appropriate experts and stakeholders own or input into digital risk decisions.
- Be aware when major transformations are due to occur and use these opportunities for active assessment of digital risk.

2.2 The cost of security

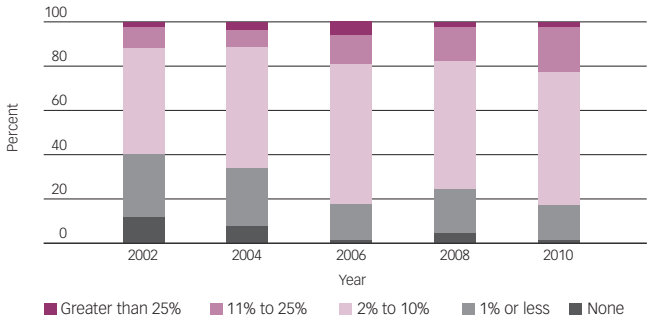
Obtaining accurate statistics on security spend and the cost of security incidents is difficult. Security spending within an IT department is often wrapped into the overall operational spend. In 2004, the congressional research service reported[52] that estimates of global economic losses from cyber attacks ranged from $13bn (*worms* and *viruses* only) to $226bn (for all forms of attacks). However, it also questioned the reliability of these estimates. Various IT security vendors have run surveys[53] with reports of average annual costs per business ranging from £1.2m to $3.8m and downtime for critical infrastructure companies costing an average of $6.3m per day.

Comparisons across surveys and over different years are hard to make, particularly as survey methodologies change. However, the Information Security Breach Survey (ISBS), produced by PwC and sponsored by the UK government, has run over a number of years with a consistent methodology[54].

The overall conclusions show that the approach of UK companies to security is maturing; for example, there is a steady increase in companies with documented information security policies: from 14% in 2000 to 55% in 2008, and this is forecast to continue increasing in 2010.

The changes in security spend as a percentage of IT spend (See graph 1) reflect this change.

Graph 1: **Security Spending as a % of IT spend**



At the same time, incidents are getting worse and more numerous. For example, the median number of incidents rose from 15 to 45 between 2008 and 2010. The perceived seriousness of incidents (see graph 2) is also increasing. There are more incidents in the serious, very serious or extremely serious percentage; increased incident costs also reflect this trend.

Graph 2: **Seriousness of the worst security incidents**

2.3 Standards, guidance and best practices

There are many national and international standards and good practice guides for managing information and digital risks (see Appendix 2). All these standards have slightly different approaches and purposes.

The British standard for security management, BS7799, was one of the early accessible guides that became

popular and trusted; this led to its adoption by the international standards organisation as the ISO27000 series. NIST also provide an important and influential set of standards for risk and *cloud computing*[55].

Several methodologies exist that aim to help organisations perform a systematic evaluation of their IT security risk[56]. These standards and methodologies help businesses to develop a systematic approach to prioritisation. For example, typical steps include:

- A scoping phase where the asset, system or service of concern is characterised.
- A *threat* analysis where the attacks, motivations, opportunities and *vulnerabilities* are considered.
- An analysis of the likelihood and impact of any of the threats occurring; this helps in prioritisation.
- An analysis of the risk mitigation options. Typically these would be security controls, but other risk management options are not ruled out.

Standards often point to known best practices for mitigating common risks. Regulatory initiatives such as Solvency II, SOX and Basel II have also stimulated more comprehensive enterprise risk management, which has improved risk mitigation.

The rapid pace of technology change means that there will always be new issues that require the development of new practices. For example, the Jericho Forum provided early guidance on the changing role of network boundaries (see box 20). In a similar way the Cloud Security Alliance and the European Network and Information Security Agency have both recently published guidance relating to risks associated with cloud computing[57].

Box 20: Jericho and early guidance for security

The Jericho forum is an association for security officers from multi-national companies, major security vendors, governments, and academics. Traditionally, IT security revolved around maintaining a strong network perimeter. However, over time organisations have found themselves needing to open up more and more of their internal applications and infrastructure. As a group, the Jericho forum was early to identify and discuss approaches to this problem, coining the phrase 'de-perimeterisation'. They developed a set of principles; including, the need for federated *identity management* and for components within the perimeter to be protected. This guidance is now available from the Open Group[58].

A common challenge is that technology experts understand and see digital risks from an IT perspective, but business units and managers are in a better position to view these in a wider business context. The Information Systems Audit and Control Association produce COBIT: a framework designed to help bridge the gap between control requirements, technical issues and business risks. However, very few individuals within a company have both the business oversight and the technical expertise. Moreover, these communities often use very different terminology and have different concerns. Although the COBIT framework can help, bridging the business-technology expertise gap remains an ongoing challenge.

Recommendation 3: Risk managers should ensure that best practice and applicable standards and frameworks are used to help manage digital risks. This means:

- Consider using standards for more common digital risk problems and looking for any new best practice guidance for more unusual problems.
- Selecting risk assessment teams containing the right mixture of business and technology stakeholders.

3. Risk transfer

In order to effectively manage digital risks, businesses can consider transferring some of these risks to a third party through the use of insurance. Many businesses may believe that their existing insurance policies will include digital risks, but most traditional insurance policies (property and commercial liability) tend to focus on tangible damage to physical property and do not cover the many new areas of digital risk. Similarly, traditional business interruption policies focus on damage caused by fire or flood and do not consider non-physical damage, such as *denial of service* attacks. However, companies may not be aware of the potential digital risk covers available to them.

Insurance for cyber risks has been available for some time, and the market has developed considerably over the last few years to help business manage the digital exposure they face. A lack of historical claims data and concern over the potential size of some digital losses has deterred some insurers, but there are a number of specialist underwriters now providing cover (including at Lloyd's). Although difficult to measure, the current market for cyber insurance is estimated to be around $600m: up from $450m - $500m in 2009[59].

Most coverage today is related to liability. First-party liability covers a company's own losses due to damage to *availability*, *integrity* and *confidentiality* of company data, intellectual property and other privacy infringement-related issues. Third-party liability covers related losses incurred by others. Insurance cover for third-party claims for breaches of rights of privacy are becoming increasingly popular, driven in part by the potential costs associated with the US privacy breach notification laws (see box 21).

There is also increasing coverage relating to business interruption. These policies cover a company's loss of revenue and additional expenses caused by denial of service attacks, *viruses* and fraud. They may also cover losses incurred as a result of disruption caused by the computer systems of suppliers. There are some policies that cover legal actions attributable to the failure of a product or service. Recently, insurance for cyber extortion has been emerging, which covers ransom for valuable information.

Box 21: Implications of US data breach legislation

US data breach legislation ensures that when personal data is lost there is an obligation to notify those affected. The costs involved can be very large, as an effective response could include:

- Forensic analysis to determine the what, who, when, where and how of the breach
- Legal advice on how to proceed
- Logistics of giving notification to large numbers of people
- Credit monitoring
- Setting up a call centre
- Handling of public relations
- Dealing with the losses of third parties

The potential scale of this impact means businesses should consider reviewing and revising their personal data protection practices and seeking advice on how they might mitigate the risk through insurance solutions.

Paul Bantick, Underwriter (Tech, Media and Business Services - Specialty Lines) Beazley

There are certainly several challenges facing the cyber-risks insurance market. One of the most difficult challenges is pricing, as there is limited data on security incidents; this is partly because there is a lack of incentives for organisations to report such attacks. In addition, new types of attacks are constantly evolving, which makes it difficult to gather reliable data.
It can also be difficult to estimate the likelihood that a particular kind of security event will happen. Equally, it is very difficult to quantify how the introduction of a new security technology or control may decrease the likelihood of an attack being successful. The impact of

a cyber-security event often involves intangibles, such as lost data, which are difficult to quantify and may only be relevant in the context of that particular organisation. Furthermore, many of the impacts of cyber-security attacks are secondary; for example, reputational damage, decrease in productivity and loss of consumer confidence.

A company has to balance investing in security technology, in order to minimise the likelihood of being the victim of a security attack, and investing in insurance to minimise the resulting impact on their organisation. Again, because of the limited information that is available, this is a difficult decision for risk managers.

Cyber insurance is likely to continue to develop, evolving as technologies change and new crimes or *threats* emerge. The data breach example shows how laws and regulations can drive the adoption of insurance, but this will depend on the legal jurisdiction where a company operates.

Some areas of cyber risk are likely to remain challenging in terms of developing insurance solutions. For example, where a company loses competitiveness and believes it is through the loss of their intellectual property, it may be hard to track down evidence of the events or quantify this. As such, although important, insurance will only ever form part of a company's overall digital risk management strategy.

Recommendation 4: Risk managers should consider risk transfer solutions as part of their overall digital risk management strategy. This means:

- Recognising that most traditional insurance policies will not cover digital risks.
- Being aware of the range of cyber-insurance products that are currently available and monitoring new product developments.
- Reporting on security incidents and pushing for industry-wide data to be made available.

4. Managing complexity

Managing digital risk will depend heavily on experienced staff and experts using their intuition to make good decisions. Moreover, the complexity of these decisions looks likely to increase because of changing legislation, human factors and evolving technology.

More research is certainly needed to deal with the complexity of digital risk and to help businesses respond to the increasingly aggressive *threat environment*. In this final section we provide a brief overview of some of the relevant research challenges and approaches. This research should help businesses find the right balance as IT security should not become so restrictive that it stifles innovation.

4.1 Research on economics and human factors

IT systems involve people (users, customers, suppliers, administrators, managers) and it has become vital to understand the way they affect security outcomes. Businesses need to make explicit decisions about where to put *assurance* mechanisms in place and where it makes sense to influence people's behaviour. For example, a good, mandatory training programme for all employees on IT security and privacy may be more cost effective than rolling out a complicated technology solution. Different choices may be appropriate for different regions and functions, but the security team needs to understand what is achievable with technology enforcement, which policies are workable, and what training is required.

Current research on the economics and human factors of security is beginning to provide useful accounts of the incentives of stakeholders and their effect on complex systems. Researchers from multiple academic fields are collaborating and discussing findings. One such example is the Workshop on the Economics of Information Security (WEIS). Although this work is in its infancy, its influence is likely to be felt in future generations of standards and best practices.

4.2 The future of digital risk management

This report has clearly shown how digital risk is constantly changing.

This means that we need better ways to understand and monitor the threat environment. This is not an easy task; it is a huge area and any formulaic approach is likely to be out of date in a short time. Therefore, risk managers should stay abreast of the current issues and trends, especially those that might impact their companies. An additional challenge for the risk and technology industries is how to improve risk analysis and decision-making.

All security decisions will involve trade-offs. These will typically be between:

- Lowering the risk of reputational, IP, or monetary losses
- Supporting priorities to grow the business or reduce costs

This is an important message. Although the risks here are potentially large, it is important that businesses innovate and seize the opportunities created by IT. The analytics for decision support must help risk managers deal appropriately with this trade-off.

Recommendation 5: Risk managers need to play a role in shaping research around digital risks, helping researchers to understand the challenges in making effective and practical decisions around cyber risk. More specifically they should:

- Promote awareness of the complex inter-dependency between business risks, human factors, legal issues and technology trends.
- Encourage more research on digital risks.

CONCLUSIONS

Businesses, people, society and government are more dependent on information technology than ever before. The future of our global society is inextricably linked to information technology and the internet. The trend is continuing; we will be even more dependent on IT in the future. It is true of the developed world and also the developing world, where the mobile phone is transforming businesses and lives. There is no going back; neither would anyone seriously argue that we should.

Most of the digital risks we have so far described share similarities with risks we have always faced. However, in our new cyber-society, the ways in which we are now exposed to these risks has fundamentally changed. Criminals have always stolen money, used extortion, stolen information, and used terrorism. Natural disasters and mistakes have always led to disruption and losses. Technology, by making information and processes more accessible, by cutting across geographies and jurisdictions, by changing people's behaviours and expectations and by connecting so many resources, has increased the speed at which these risks can occur as well as amplifying their impact on our economies and on our society.

Businesses are heavily reliant on IT and they are exposed to these risks. This report shows that the threat environment includes attackers with powerful capabilities and diverse motivations and that business operates in multiple jurisdictions with widely varying regulations. These factors alone make it difficult for businesses to manage digital risk. In addition, the growth of digital information, improved connectivity of people and devices, and the *virtualisation* of business are all set to drive change and increase complexity for businesses. Attackers will adapt and evolve to this new context, taking advantage where security lags the technology changes. It will be very hard for businesses to keep up.

Businesses are responding to these changes, and we have made a series of recommendations to risk managers. Today, most digital risk mitigation happens within the IT department. We advise that risk managers should be involved, to bring broader business perspectives to decisions. We also describe the growing cyber-insurance market and recommend that companies track and use this market to complement mitigations with risk transfer.

The real challenge for risk managers is to work out how to monitor digital risk in order to decide how seriously it should be treated. The trends suggest that digital risks are a board-level concern for many companies. We suggest there should be regular intelligent (rather than formulaic) review, based on a combination of the threat environment, current technology trends and the current risk management strategy.

The final conclusion is to remind readers of the need for a balanced approach to risk management. Businesses should strive to take advantage of technology; not doing so will stifle growth opportunities. The business community has a common interest in understanding digital risks, keeping it under wraps benefits only the cyber criminals. A willingness to share information about attacks and their consequences, the impact of failures and the risks that we face will strengthen the ability of business to operate successfully in cyber society; even in the face of significant and real digital risks.

APPENDICES

APPENDIX 1: WELL-KNOWN ATTACK TECHNIQUES AND TERMINOLOGY

Term	Definition
Advanced Persistent Threat (APT)	A long-term targeted attack to gain information on or from individuals or organisations. Attacks are characterised by the use of sophisticated hacking and social engineering techniques.
Backdoor	A backdoor is a vulnerability in software or hardware that bypasses any security mechanisms that are in place and allows an attacker access to the compromised system.
Bot/Botnet	A network of software agents or (ro)bots (hence the name botnet) that perform actions as determined by a control system. Typically each bot is a piece of malicious software that is installed unknowingly on a computer and controlled by a criminal known as a bot herder or bot master. They are usually used for mass emailing (spam) or to perform denial of service (DoS) attacks.
Carding	Carding is a word associated with the theft and fraudulent use of credit card information. It is often closely related with the use of stolen online bank account details.
Click Fraud	A kind of internet crime in which an attacker exploits pay-per-click advertisements. Typically, the attacker runs a website which hosts a pay-per-click advertisement. Accomplices or automated computer programmes are then used to click that advertisement multiple times in order to receive revenue from the advertiser for those clicks.
Crimeware	Software designed specifically to engage in illegal activity.
Denial of Service (DoS)	A type of attack that attempts to prevents a system from processing or responding to legitimate requests, typically by overloading the system with bogus requests. This means websites might not be able to handle customer requests and orders and will therefore lose business, suffer financial losses and risk reputational damage. It can also be used for extortion purposes.
Drive-by Downloads	A download of data or software that happens without knowledge or consent of the user. Drive-by downloads may happen, for example, when a user visits a website and clicks on a link resulting in malicious software being downloaded on to their PC.
Exploit	An exploit is a piece of computer code that allows an attacker to take advantage of a bug (or vulnerability) in a computer system. A hacker will typically use an exploit to gain remote access to a computer system.
Hacker	A person who breaks into computer systems or computer networks.
Malware	Malware (ie malicious software) is software designed to perform unauthorised operations on a computer.
Mule	A person who transfers stolen money, thus obscuring the identity of the attacker. The 'mule' may not be aware that they are being used in this way.

Pharming	A technique used to redirect traffic from a legitimate site to a malicious one. Pharming attacks may occur by compromising Domain Name Servers (DNS) or by compromising the user's machine.
Phishing	The use of emails to trick a user into performing an action. For example, a phishing email might tell a user to click on a link that takes them to a fake banking site where they then enter their username and password. The term phishing is derived from fishing; the criminals are 'fishing' for victims that they then reel in.
Social Engineering	Attempts to get a person to violate a security policy or reveal confidential information through interpersonal contact. For example, an attacker may impersonate a system administrator in order to get a user to reveal confidential information, such as a password.
Spam	Spam is used to refer to unsolicited electronic junk mail. It is often used to sell fake medicines but is also a term used by cyber criminals when they mail out emails for various scams or phishing.
Spear Phishing	A targeted version of phishing, where the phishing email is more specific to the user (see also whaling).
Spyware	Malware that attempts to compromise the confidentiality of end users by stealing information from their computers, such as usernames and passwords or other personal information.
Threat	The potential for an attacker to exploit a particular vulnerability and attack a system.
Threat Environment	The way in which many threats are created. Here we include the attackers, the ways they may attack and also the creation of new attacks.
Trojan	Malware that appears to perform a useful function but in fact compromises the security of the system.
Virus	Malware that can replicate itself through the sharing of code and data. Viruses generally attach themselves to data (such as emails or documents) that is shared between users.
Vulnerability	A flaw in a system that allows a potential breach of security.
Whaling	Phishing attacks targeted at specific people, normally high-net-worth individuals.
Worm	Malware that replicates itself and infects other computers on the network. Unlike viruses, worms can usually spread without human intervention using vulnerabilities in the target.
Zero Day Attack	An attack that exploits a vulnerability that is not widely known and for which there are no existing fixes. For many vulnerabilities there is a time or risk window from when it is publicly known until the vendor releases a fix or patch. The 'zero day' refers to this time window being zero or negative since the vulnerability is already being exploited.

APPENDIX 2: SOME WELL-KNOWN SECURITY STANDARDS

Standard	Description
ISO 27000	The ISO/IEC 27000 series is a set of information security standards published by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). The standards are best practices for information and risk management.
COBIT	The Control Objectives for Information and related Technology (COBIT) is a set of best practices for use by managers, auditors and IT users. COBIT defines a set of generally accepted measures, key indicators and processes for IT governance. COBIT helps define the level of security and controls necessary to protect an organisation's assets and meet certain regulatory compliance objectives.
Common Criteria	Common Criteria, also known as ISO/IEC 15408, are international standards for defining security requirements and evaluating compliance to those requirements.
COSO	The Committee of Sponsoring Organisations of the Treadway Commission (COSO) is a body that publishes a set of best practices for organisational governance, internal controls, risk management, fraud and financial reporting.
NERC CIP	The North American Electric Reliability Corporation (NERC) publishes a set of standards for Critical Infrastructure Protection (CIP) for the power systems industry.
NIST	The US National Institute of Standards and Technologies (NIST) publishes a series of best practices for a wide range of computer security issues.
PCI DSS	The Payment Card Industry (PCI) publishes a Data Security Standard (DSS) to help organisations that process credit card information to prevent fraud by having adequate security controls to protect the confidentiality and integrity of credit card information.

APPENDIX 3: SUPPLY CHAIN

Globalisation has introduced significant challenges around managing and assuring the supply chain of products and services[60]. The IT industry is not immune from these challenges, and some of the issues are amplified by the particular nature of IT products and services.

The IT industry is still largely in its infancy with regards to verifying the correctness of software components. Additionally, software development has few barriers to entry and, as such, it is possible that any given software component may be made up of components from a large number of sources from many different localities and operating under many different legislative domains. *Open-Source* software adds another particular complication. A software product or service based on *Open Source* may have dependencies on many thousands of developers, with perhaps no single organisation able to take responsibility for it.

On the other hand, core computer hardware manufacturing has extremely high barriers to entry (largely down to the complexity of the manufacturing process). In addition, the drive towards cost savings and efficiencies has led to a handful of manufacturers supplying much of the world demand for core IT components, such as laptops, servers and network switches.

These two aspects of the nature of IT products and services have important supply-chain consequences. Firstly, it is difficult to establish that a particular software based product is free from unwanted side effects, such as *malware*. Secondly, mitigating supply-chain risk by purchasing core IT components from multiple sources is becoming less effective because more and more core components are supplied from the same handful of manufacturers.

Governmental concern over the inability to assure the supply chain of IT products and services has surfaced in several major countries, including the US and UK. The fact that supply-chain *assurance* of the components that make up our IT systems is a difficult challenge for manufacturers and *service providers* to deal with means there is a genuine risk that governments will attempt to legislate, or at least regulate, in this space. This has the potential to lead to a range of effects: from increased costs through to even less choice as to where core IT components can be sourced from.

APPENDIX 4: SECURING THE INFRASTRUCTURE

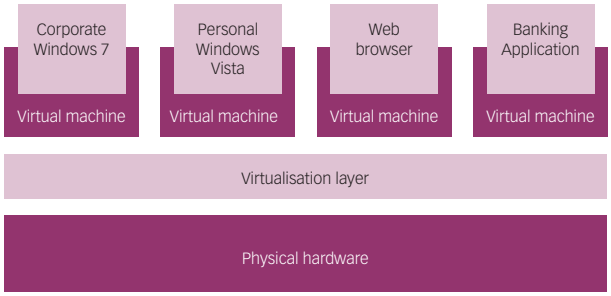
The ability to embed security support directly into the hardware of client and server computing platforms is being developed as a way of improving the trust we place in our underlying IT components.

This approach is motivated by the desire to provide components that are resistant to software-based attacks and to provide a base set of strong security properties that can be built on with confidence by higher level (software) components. Examples of this type of embedded hardware security include the Trusted Platform Module (TPM)[61].

At the very least, these hardware-based security mechanisms offer an organisation the ability to reliably and robustly identify their IT assets.

Along with this focus on embedded hardware security, we are also seeing an interest in machine *virtualisation* as a way to improve on the underlying security properties of our IT infrastructures. Modern operating systems are growing increasingly large and complicated. Microsoft Vista is estimated to have around 50 million lines of code compared to the 40 million of the earlier Windows XP and 11–12 million of the earlier NT 4.0. McConnell reports an industry average of about 15–50 errors per 1,000 lines of delivered code; although, not all errors will be sufficiently exploitable to allow security controls to be bypassed[62].

Figure 5: **Schematic of a virtualised personal computer**



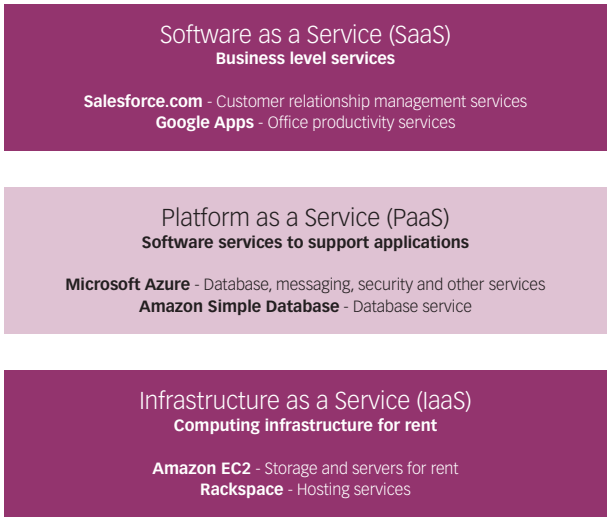
Virtualisation offers us the ability to carve up a single physical hardware platform, such as a client laptop or a server system, into what are known as Virtual Machines (VMs) (see Figure 5). Each Virtual Machine runs a standard operating system (eg Windows 7 or Linux) as though it was running directly on the machine hardware. However, the virtualisation layer gives us a point below the operating system, but above the real machine hardware where strong *security policy* controls can be enforced. From a security point of view, this is important. For example, we can use virtualisation to implement personal firewalling or *virus* checking in a way that we know will still be enforced even if the main operating system is compromised.

Aside from the ability to provide 'tamper-proof' security controls for a single operating system running on a virtualised platform, virtualisation also offers up a number of interesting possibilities from a security point of view. These range from the ability to strongly separate the business and personal use of a single platform through to app-store like provision of IT services, as well as more advanced scenarios where business-level information flow could be strictly controlled.

APPENDIX 5: CLOUD

The US National Institute of Standards and Technologies (NIST) have tried to standardise ***cloud*** service definitions into three service categories (see figure 6).[63]

Figure 6: **Cloud service types**



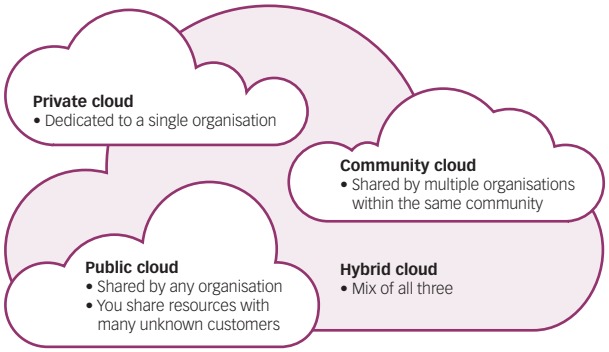
Cloud services charge according to usage. For example, Amazon charge for each machine-hour; higher-level platform or software ***service providers*** may charge on a per-transaction basis. This should be contrasted with a company running their own IT systems, where they need to maintain sufficient systems to meet their peak usage. By sharing cloud providers' systems, companies expect to make considerable cost savings.

In offering usage-based cost models, cloud service providers tend to have standardised contracts, and customers cannot negotiate on terms and conditions. This is a significant change from traditional IT outsourcing, where a company will carefully negotiate a contract that covers multiple years. These outsourcing contracts will incorporate the customer's security policies, helping them ensure their potential risks are managed.

Cloud service providers deliver the flexibility and cost savings by sharing resources between multiple customers (sometimes described as a multi-tenant model). This can involve allocating a resource to one customer for one hour and then to a different customer the next. Alternatively, some resources support multiple customers using them at once, often using ***virtualisation*** technologies.

Cloud services can also have different ownership models. Figure 7 shows NIST's definition of cloud ownership models.

Figure 7: **Cloud ownership models**



Much of today's discussion of cloud is around infrastructure or platform as a service. As cloud computing develops, it will provide a low investment route for innovation with high-level business and end-user services. This is likely to lead to the creation of an eco-system of services that build on each other and are potentially run by small start-up service companies.

GLOSSARY

Term	Description
Access Control	A mechanism by which users or devices are granted or denied access to data or other resources (see also authorisation).
Anonymisation	The process of removing data that can identify a person or compromise their privacy. Or, a service that hides a person's identity so that their actions cannot be traced.
AntiVirus Software	AntiVirus software is used to protect a computer system against malware, viruses and worms. It generally scans files on disk for known signatures associated with malware as well as monitoring web traffic and email.
Assurance	The degree of confidence that security needs are satisfied.
Availability	The assurance that authorised users are granted timely and uninterrupted access to objects.
Blog	A web based log that contains regular information about a person's activities and their thoughts on events. Blogs can include pictures and videos as well as text.
Bluetooth	A wireless based communication system that allows devices in close proximity to exchange information. It is commonly used to connect mobile phones to headphones.
Cloud and Cloud Computing	A paradigm of computing in which computing, network and storage resources are dynamically allocated to applications; these are often hosted by external third parties.
Confidentiality	A security property concerned with ensuring that information is not disclosed to unauthorised parties.
Credential	A credential is used within the computer system to control access to information and resources. This typically this takes the form of a username and password.
Cryptography	Mathematical algorithms applied to data that are designed to ensure confidentiality, integrity, authentication and/or other security properties.
Data Warehouse	A repository of an organisation's electronic data, used to enable decision support for a wide variety of business purposes.
Disk Crash	A failure of a hard disk drive, often resulting in permanent damage to the disk.
e-Discovery	The discovery of electronic information as evidence within the context of civil litigation.
Encryption/Decryption	Encryption hides data using a key and cryptography. Decryption allows those in possession of the key to recover the original data.

Identity management	The process of managing the identities of employees within a company along with the systems and applications to which they should have access.
Integrity	A security property concerned with ensuring sensitive information has not undergone an unauthorised modification.
IT/Systems administrator	A systems administrator is the person responsible for keeping a computer system (normally the servers in a data centre) running. The role requires the person to have the right to access most parts of the system and hence should only be given to a highly trusted individual.
MP3	MP3 is a format for digitally storing sound on a computer. It is more commonly used to refer to music stored on a computer.
Open Source	The open-source model of software development involves a number of independent software engineers collaborating to produce software products where the source code (blueprint) is made available along with the software product.
Radio Frequency Identification (RFID)	RFID is a technology for tracking and identifying an object remotely. A RFID tag is attached to the object and responds to radio frequency signals generated from an RFID reader.
Script	Scripts are computer programs typically used by computer administrators to automate routine tasks. They are text based, and the instructions are readable and directly run.
Security Policy	A set of rules and practices that define how a system or organisation provides security.
Service Providers	An entity that provides services to other entities. Internet service providers (ISPs) provide access to the internet, and there is a range of other types of internet based services.
Stewardship	Stewardship refers to the management or care of resources for which one has no ownership. Information or data stewardship will be of particular concern in cloud computing.
Tweet/Tweeting	A tweet is a short post or status update on Twitter, a microblogging service.
Virtualisation	A technique for partitioning a physical computer into multiple virtual computers, each with its own apparent Central Processing Unit (CPU), memory and storage.
Web 2.0	A term used to describe the changing trend on the internet from static websites to interactive web applications that encourage information sharing.

REFERENCES

[1] FBI press release 1 October 2010: www.fbi.gov/pressrel/pressrel10/tridentbreach100110.htm
[2] BBC report on GCHQ chiefs comments 13 Oct 2010: www.bbc.co.uk/news/uk-11528371
[3] www.zdnet.com/news/iloveyou-e-mail-worm-invades-pcs/107318
[4] Phil Muncaster, V3.co.uk, former White House advisor urges action on 'cyber sanctuaries'. Read more: www.v3.co.uk/v3/news/2271456/former-white-house-advisor#ixzz12igkyiOC
[5] Jeremy Kirk, CIO, European Union to hold cyber security exercise next month www.cio.co.uk/news/3244032/european-union-to-hold-cybersecurity-exercise-next-month/?olo=rss
[6] FBI press release 1 Oct 2010: www.fbi.gov/pressrel/pressrel10/tridentbreach100110.htm
[7] McAfee, Unsecured Economies Report: Protecting Vital Information (2009): http://resources.mcafee.com/content/NAUnsecuredEconomiesReport
[8] Victoria Kim, Financial Times, 2007 – Abnormal trading 'ahead of 49% of N American deals': www.ft.com/cms/s/0/45417ace-4387-11dc-a065-0000779fd2ac,dwp_uuid=aece9792-aa13-11da-96ea-0000779e2340.html
[9] MI5 – What kind of information do spies seek? Ref: www.mi5.gov.uk/output/what-kind-of-information-do-spies-seek.html
[10] The US Securities and Exchange Commission (SEC) acts to protect investors and maintain the integrity of securities markets: www.sec.gov/
[11] US Security and Exchange Commission – SEC files emergency action against Estonian traders: www.sec.gov/news/press/2005-155.htm
[12] Vancouver Sun – Data taken, company says (2008): www.canada.com/vancouversun/news/westcoastnews/story.html?id=055fa12a-2bca-4804-9bef-a44eee60de5f
[13] National White Collar Crime Center – Embezzlement/ Employee Theft (2009): www.nw3c.org/research/site_files.cfm?fileid=b3810dcd-c3b6-4a2a-86d5-d30db5366bd9&mode=w
[14] US District Court - District of Maryland, US vs Rajendrasinh Makwana: http://media.haymarketmedia.com/Documents/2/FannieComplaint_1217.pdf
[15] Department of Justice, Office of Public Affairs: www.justice.gov/criminal/cybercrime/kimSent.htm
[16] Sulkowski, Adam J, Cyber-Extortion: Duties and Liabilities Related to the Elephant in the Server Room (8 January 2007). Available at SSRN: http://ssrn.com/abstract=955962
[17] Guardian report on cyber attacks on Estonia: www.guardian.co.uk/world/2007/may/17/topstories3.russia
[18] Joshua Davis, Hackers Take Down the Most Wired Country in Europe. Wired (2007): www.wired.com/politics/security/magazine/15-09/ff_estonia
[19] 2010 Economist article on Cyberwar: www.economist.com/node/16481504?story_id=16481504&source=features_box1
[20] Symantec: Security Response W32.Stuxnet Dossier: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
[21] www.backup-technology.com/west-berkshire-council-suffers-second-data-loss/
[22] www.e-health-insider.com/news/4127/nhs_lothian_implements_usb_stick_lock-down
[23] www.computerweekly.com/Articles/2010/08/26/242526/Infected-USB-drive-39significantly-compromised39-Pentagon.htm
[24] BBC – Internet fears over WorldCom scandal: http://news.bbc.co.uk/2/hi/business/2072274.stm
[25] IBN Live – US suspects N Korea launched Internet attack on July 4 (2009): http://ibnlive.in.com/news/us-suspects-n-korea-launched-internet-attack-on-july-4/96715-2.html
[26] BBC – Estonia hit by 'Moscow cyber war' (2007): http://ibnlive.in.com/news/us-suspects-n-korea-launched-internet-attack-on-july-4/96715-2.html
[27] See the Symantec W32.Stuxnet Dossier: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
[28] See Gartner press release on the top ten strategic technologies for 2010: www.gartner.com/it/page.jsp?id=1210613

[29] See BBC report on the FSA fine for Zurich Insurance: www.bbc.co.uk/news/business-11070217

[30] Heartland Payment Systems SEC Filing Form 10-K, 10 March 2010.

[31] Credant, Data hung out to dry (2010): www.credant.com/news-a-events/press-releases/376-dry-cleaners.html

[32] www.youtube.com/watch?v=5wS3AMbXRLs

[33] Experimental Security Analysis of a Modern Automobile, Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage, Proceedings of the IEEE Symposium and Security and Privacy, Oakland, CA, May 2010

[34] BBC, Hacks mounted on car control systems: www.bbc.co.uk/news/10119492

[35] Technology Review – A flexible colour display: http://technologyreview.com/computing/25138/?a=f

[36] Personnel Today, BT to roll out Facebook-style social networking services to UK staff: www.personneltoday.com/articles/2010/06/02/55788/bt-to-roll-out-facebook-style-social-networking-services-to-uk.html

[37] Thomas Ryan: Getting In Bed With Robin Sage – Black Hat USA 2010: http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdfSage-v1.0.pdf

[38] Microsoft news centre: http://www.microsoft.com/presspass/presskits/cloud/videoGallery.aspx

[39] Although there are risks that a cloud provider fails to make provision for an aggregate peak in demand

[40] Vivek Kundra, Federal Chief Information Officer - Standards to Foster Innovation. NIST Cloud Computing forum and workshop 2010: http://csrc.nist.gov/groups/SNS/cloud-computing/documents/forumworkshop-may2010/nist_cloud_computing_forum-kundra.pdf

[41] CIO magazine, Cloud computing survey (2009) www.cio.com/documents/whitepapers/CIOCloudComputingSurveyJune2009V3.pdf

[42] US Chamber of Commerce Center for Capital Markets Competitiveness, Cost of SOX 404 Survey, 8 November 2007: www.uschamber.com/sites/default/files/reports/0711sox_survey_report.pdf

[43] BBC, Google in 'significant breach' of UK data laws: www.bbc.co.uk/news/technology-11684952

[44] Recent article by Charlie Savage in the New York Times, US tries to make it easier to wiretap the internet: www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1&scp=1&sq=US%20wiretap&st=cse

[45] Law.com EU Data Protection Meets US Discovery www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202436660249&EU_Data_Protection_Meets_US_Discovery

[46] www.cmswire.com/cms/enterprise-cms/taking-control-of-ediscovery-costs-are-archiving-costs-necessary-for-ediscovery-004014.php

[47] www.ediscoverylaw.com/2010/08/articles/case-summaries/in-davidandgoliathlike-struggle-for-electronic-discovery-court-orders-adverse-inference-monetary-sanctions-for-spoliation-and-delay/

[48] Susan W. Brenner and Burt-Jaap Koops, Approaches to Cybercrime Jurisdiction – Journal of High Technology Law Vol IV No 1.

[49] Approaches to Cyber Crime Jurisdiction www.thefreelibrary.com/Approaches+to+cybercrime+jurisdiction.(Report)-a0172599113

[50] Malaysia Computer Crimes Act (1997): http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025630.pdf

[51] ENISA announces EU boost to defenses against cyber attacks.

[52] Report by the congressional research service on the economic impact of cyber-attacks (2004): www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

[53] Daily Telegraph coverage of Symantec's survey: www.telegraph.co.uk/technology/news/7294810/Cyber-attacks-cost-businesses-an-average-of-1.2-million-a-year.html - McAfee report on high cost of cyber attacks: www.inc.com/news/articles/2010/01/reports-warns-of-growing-cyberattack-threat.html - Arcsight and Ponemon Institute first annual cost of cyber crime study: www.inc.com/news/articles/2010/01/reports-warns-of-growing-cyberattack-threat.html

[54] http://lfca.net/Reference%20Documents/2002%20ISBS%20UK%20Security%20Survey%20.pdf
www.pwc.co.uk/pdf/dti_technical_report_2004.pdf
www.infosec.co.uk/files/Survey_DTI_ISBS_2006.pdf
www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html
www.pwc.co.uk/eng/publications/isbs_survey_2010.html

[55] See the computer security division of the NIST website: http://csrc.nist.gov/

[56] C.J. Alberts and A. Dorofee, Managing Information Security Risks: The OCTAVE Approach. Addison-Wesley, 2002; J.A. Jones. An introduction to factor analysis of information risk (FAIR). www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf; T.R. Peltier. Information Security Risk Analysis. Auerbach Publications, 2nd edition, 2005; and G. Stonebumer, A. Grogen, and A. Fering. Risk Management Guide for Information Technology Systems. Technical Report Special Publication 800-30, National Institute for Standards and Technology, 2002

[57] See: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment and www.cloudsecurityalliance.org/

[58] See: http://www.opengroup.org/ and http://www.opengroup.org/jericho/

[59] Betterley, R.S., Cyber Risk and Privacy Market Survey 2010, June 2010. Available at: www.betterley.com

[60] Lloyd's, Globalisation and risks to business:
www.lloyds.com/News-and-Insight/360-Risk-Insight/Research-and-Reports/Globalisation/Globalisation

[61] Cyber Security - Knowledge Transfer Network - You mean you trust a computer?:
www.ktn.qinetiq-tim.net/content/files/groups/trustcom/TrustComputingWhitePaperfinal.pdf

[62] McConnell, Steve. 1993. Code Complete. Microsoft Press.

[63] NIST - The NIST Definition of cloud computing -- http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

Disclaimer

Since merchants first met to insure their ships at Edward Lloyd's coffee shop over 300 years ago, nearly every aspect of the way we do business has changed. But one constant is the bold confidence proclaimed by our motto, reflected in both our unique appetite for risk and our worldwide reputation for settling valid claims.

Lloyd's One Lime Street London EC3M 7HA Telephone +44 (0)20 7327 1000 Fax +44 (0)20 7626 2389 **www.lloyds.com**