Technology Strategy Board
Driving Innovation

Revolution or evolution?

Information Security 2020

Prepared by

PricewaterhouseCoopers

Contents

About the Technology Strategy Board

The Technology Strategy Board is a business-led executive non-departmental public body, established by the Government. Its role is to promote and support research into, and development and exploitation of, technology and innovation for the benefit of UK business, in order to increase economic growth and improve quality of life.

About PricewaterhouseCoopers LLP

PricewaterhouseCoopers LLP provides industry-focused assurance, tax and advisory services to build public trust and enhance value for our clients and their stakeholders. More than 163,000 people in 151 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

About this roadmap

This roadmap was commissioned by the Technology Strategy Board and jointly prepared with PricewaterhouseCoopers LLP (UK).

The purpose of this roadmap is to set out the drivers that will shape the future Information Security environment to 2020 and beyond. This roadmap is to inform business leaders and security professionals alike, and sets out potential future scenarios and issues around information security, allowing the reader to draw implications and conclusions that apply to them.

In preparing this roadmap we interviewed over 35 leading Information Security experts and business leaders across the private sector, academia and government to determine the key trends that are likely to impact Information Security to 2020.

We subsequently held a workshop with over 40 experts to validate the trends and explore them in further detail.

The research focuses on the commercial aspects of Information Security, but remains cognisant of trends in cyber security and warfare for military and intelligence applications. Our research primarily illustrates trends in the UK Information Security market, but the implications are relevant globally.

We would like to thank the following organisations for their participation in the research: **AstraZeneca, BBC, Birmingham University, British Business Federation Authority, BT, Chatham House, Cisco, Credit Suisse, Cyveillance, De Montfort University, Digital Systems Knowledge Transfer Network, European Information Society Group, Garlik, Hewlett Packard, IBM, IdenTrust, Information Commissioner's Office, Information Security Forum, Kaspersky Lab, Lloyd's of London, McAfee, Methods Consulting, National Grid, Ministry of Defence, Nokia, Office of Cyber Security, Oracle, PGP Encryption, QinetiQ, Queens University, Royal Holloway University, RSA, Security Innovation & Technology Consortium, Skype, Symantec, Technology Strategy Board, Travelex, Trend Micro,** as well as several others who would prefer to remain anonymous.

Executive summary

Information Security is a much broader concept than technology. It relates to protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. As the volume of information grows and continues to be increasingly stored and communicated in electronic form, Information Security is rapidly becoming intertwined with technology, and more specifically, the internet. This has given rise to the term Cyber Security and for it to be used interchangeably with Information Security.

This roadmap is for business leaders and security professionals alike, and sets out potential future scenarios and issues around Information Security, allowing the reader to draw implications and conclusions that apply to them.

Information Security, whilst being a very current and topical issue, is also an emerging sector that is undergoing significant change. The main suppliers shaping the Information Security industry are a converging group of technology vendors, system integrators, consultants and aerospace & defence companies. The available market research does not provide a consensus on the size of the IT security market, the best proxy for the Information Security market. The range of market research suggests that the IT security market is worth approximately £4-5bn per year in the UK and is growing strongly.

Over the next decade, Information Security requirements will be driven by various macro level factors, such as globalisation, climate change, regulation and evolving demographics. These will present opportunities and risks for organisations in dealing with Information Security issues, and also companies providing Information Security products and services. There is likely to be a greater degree of segmentation within the Information Security market in the future as suppliers specialise to meet the needs of specific groups. For example, the rising importance of Information Security in the healthcare sector as services are increasingly provided electronically is likely to drive specific regulatory and technology requirements.

Information Security is often considered to have three components; technology, processes and people. Technology has been a key aspect of Information Security in recent years, but increasingly, organisations are realising that processes and people are overlooked components when developing holistic approaches to Information Security. By 2020, there may be a reversion to technology being the key strand to Information Security, driven by significant increases in the volume of data, speed of processing and communication technology, and the emergence of more complex and automated threats.

The research identified seven interrelated key trends that are likely to drive change in Information Security through to 2020 and beyond – see diagram overleaf. The first three trends relate to changes in technology, whilst the following three trends reflect changing patterns in how people use technology and the internet. Finally, trust and identity are universal themes which are intertwined with many of the prior trends. These trends have implications for organisations of all sizes, individuals, governments and the Information Security industry.

The building blocks of modern communication technology are rapidly evolving and we see this change all around us. Televisions are blurring with computers, feature rich mobile devices are becoming more prevalent and fibre optic cables and wireless networks are enabling faster static and mobile broadband access. By 2020, ubiquitous devices will seamlessly and automatically interact with other devices around them, adapting functionality to their local environment and other objects in their proximity.

The volume of private information being shared has escalated significantly over the last decade, particularly driven by social networking, and this is likely to continue. Additionally, the volume and value of transactions through electronic channels is expected to continue to rise. These trends suggest that cyber criminals will increasingly be willing to invest further resources in developing more sophisticated attacks.

Regulation and standards will be important drivers of Information Security over the next decade, but will need to keep pace and evolve as technology and its uses develop. There is likely to be increasing pressure towards regulation in information security, with privacy and consent being a key driver.

Proving identity and establishing trust are two of the greatest challenges identified in the research. In 2020 as people spend an increasing proportion of their time online, identity becomes a greater challenge because fewer interactions will be face-to-face, a greater volume of private information may be available online and new technologies could make it easier to impersonate individuals.

Key longer term drivers

- Globalisation
- Increased focus on climate change
- Shifting global economic centres
- Changing demographics
- Increasing regulation / governance
- Increasing reliance on technology and information
- Changing attitudes towards privacy
- Evolving work / home balance

Key trends impacting Information Security to 2020

1 Infrastructure revolution

- Increase in penetration of high speed broadband and wireless networks
- Centralisation of computing resources and widespread adoption of cloud computing
- Proliferation of IP (internet protocol) connected devices and growth in functionality
- Improved global ICT (Information and Communications Technology) infrastructure enabling greater outsourcing
- Device convergence and increasing modularisation of software components
- Blurring work/personal life divide and 'Bring Your Own' approach to enterprise IT
- Evolution in user interfaces and emergence of potentially disruptive technologies

2 Data explosion

- Greater sharing of sensitive data between organisations and individuals
- A significant increase in visual data
- More people connected globally
- Greater automated traffic from devices
- A multiplication of devices and applications generating traffic
- A greater need for the classification of data

3 An always-on, always-connected world

- Greater connectivity between people driven by social networking and other platforms
- Increasingly seamless connectivity between devices
- Increasing information connectivity and data mining
- Increased Critical National Infrastructure and public services connectivity

4 Future finance

- Rising levels of electronic and mobile commerce and banking
- Development of new banking models
- Growth in new payment models
- Emergence of digital cash

5 Tougher regulation and standards

- Increasing regulation relating to privacy
- Increasing standards on Information Security
- Globalisation and net neutrality as opposing forces to regulation and standardisation

6 Multiple internets

- Greater censorship
- Political motivations driving new state/regional internets
- New and more secure internets
- Closed social networks
- Growth in paid content

7 New identity and trust models

- The effectiveness of current identity concepts continues to decline
- Identity becomes increasingly important in the move from perimeter to information based security
- New models of trust develop for people, infrastructure, including devices, and data

The research indicated that there is a need for a proactive approach to Information Security from all stakeholders given the rising complexity and volume of threats.

Organisations should ensure that approaches to Information Security are holistic and consider technology, processes and people. Approaches need to adapt to rapidly changing threats and technology, and also to changes in regulations and standards. However, it is important that organisations also focus on aspects of Information Security that are not necessarily driven by regulation and standards, for example, protecting commercially sensitive information or intellectual property.

Increasing focus on Information Security could also provide competitive advantage. Organisations that have effective Information Security in place could increasingly attract consumers to use their products/services. Information Security could also provide opportunities to sell products/services through new channels or interact with customers in new ways that are not possible today due to concerns about privacy and consent.

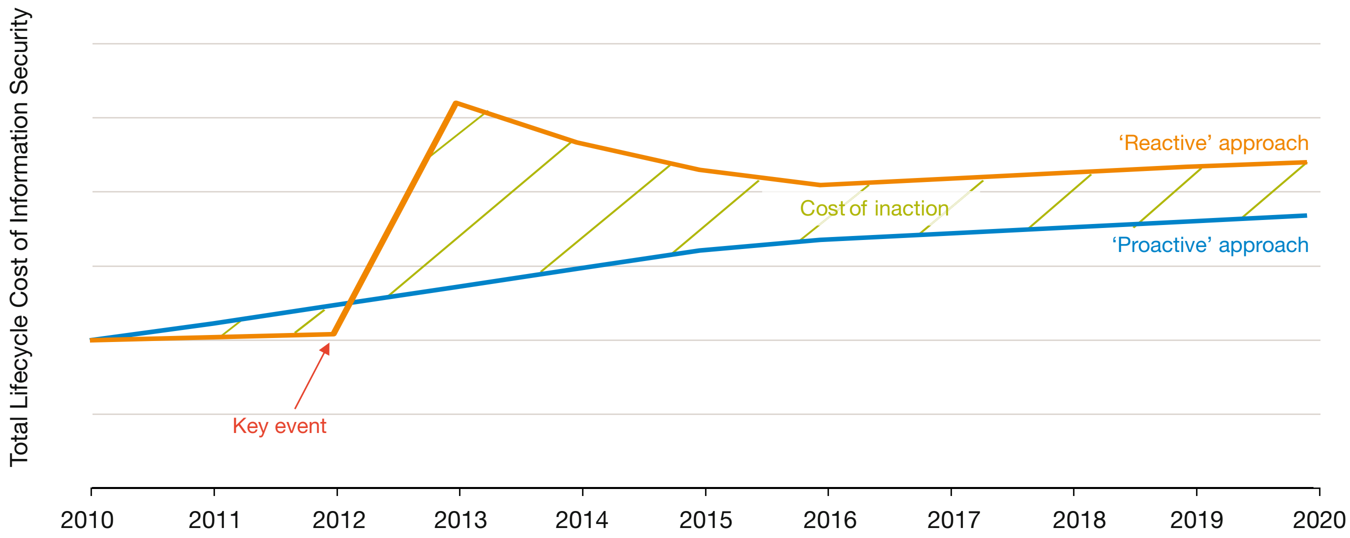
Organisations need to consider both the potential benefits and costs of their approach to Information Security with a holistic approach like the ‘Total Lifecycle Cost of Information Security’ model shown overleaf. This illustration demonstrates the potential long term impact of two different approaches to Information Security.

In the first scenario, the organisation does not have an appropriate approach to Information Security. It then suffers from an ‘event’ which causes cost to the organisation in the form of increased spending on Information Security solutions, loss of intellectual property, loss of market share and hence income, and damage to its brand.

In the second scenario, the organisation takes a more proactive approach to Information Security. It invests in Information Security solutions and benefits from greater trust from its customers and gains in market share, higher price points relative to its peers and agility in adapting its Information Security approach to market changes.

In this example, the organisation could be replaced with an industry, country or even a region.

Figure 1: The cost of inaction – two illustrative scenarios for an organisation's approach to Information Security



Definition										
	Total Lifecycle Cost of Information Security	=	Lifecycle costs of deploying and operating security solutions	+	Reputational value	+	Intellectual Property value	+	Operational effectiveness	+	Financial impact of incidents
			• Hardware / software solutions • Training • Consultancy costs • People costs		• Brand volume • Customer satisfaction/ confidence		• R&D information • Customer databases • Competitive information		• Productivity • Ability to service customers • Cost to serve customers		• Direct financial loss from attack

There are many uncertainties with respect to how Information Security will evolve over the next decade. However, it is certain that new Information Security requirements will require businesses to innovate to develop new products and services. This will provide opportunities both for businesses, to develop new business models and generate competitive advantage and for financial investors alike. It will also stimulate economic growth through consumption and exports, and make the UK a safer place to do business.

Are you up to the challenge?

one

Infrastructure revolution

The changing building blocks of electronic communication

The research identified that by 2020, communication infrastructure is likely to evolve in a number of ways:

- Increase in penetration of high speed broadband and wireless networks
- Centralisation of computing resources and widespread adoption of cloud computing
- Proliferation of IP (internet protocol) connected devices and growth in functionality
- Improved global ICT (Information and Communications Technology) infrastructure enabling greater outsourcing
- Device convergence and increasing modularisation of software components
- Blurring work/personal life divide and ‘Bring Your Own’ approach to enterprise IT
- Evolution in user interfaces and emergence of potentially disruptive technologies

The building blocks of modern communication technology are rapidly evolving and we see this change all around us. Televisions are blurring with computers, feature rich mobile devices are becoming more prevalent and fibre optic cables and wireless networks are enabling faster static and mobile broadband access. This evolved environment has significant implications for Information Security.

The centralisation of computing resources is expected to grow significantly over the next decade, driven by the requirements to reduce cost, reduce CO2 impact and improve service levels and functionality. Whilst our research suggested that cloud computing is overhyped, and it is already here in Facebook, Amazon and Google for example, our interviews recognised that businesses have been slow to adopt the cloud due to security concerns. These concerns include availability and reliability of services, data privacy, data classification and access, and compliance with regulatory requirements.

> *"The driving force behind the cloud is economics. You simply get better economics from one size fits all. Security concerns, however, are the key blocker.*
>
> *Tony Dyhouse, Digital Systems Knowledge Transfer Network"*

The cloud computing concept is in effect, the provision of IT as a service such that storage, processing, software and even security are all provided as services. This has significant implications for organisations that adopt this model, but also for the IT and Information Security industries which may need to adapt to this new ecosystem with new business models.

The proliferation of IP connected devices, ubiquitous wireless high speed broadband and growth in automated connectivity between devices will increase the number of threat vectors and enable attacks from a greater range of devices. These devices include a diverse range of hardware, operating systems and applications, potentially further increasing the number of threats.

As global ICT infrastructure grows in scale and performance, greater off-shoring of back office ICT infrastructure may occur due to cost reduction requirements, moving energy intensive equipment to regions with cheaper electricity (e.g. Egypt) or lower cooling requirements (e.g. Iceland). This could potentially lead to greater threats.

Continued globalisation driven by an improved global ICT infrastructure will enable collaborative working and provision of remote services through video links. Virtual healthcare may be a reality by 2020 which would imply greater personal information being transmitted online. There are already examples of X-rays from western hospitals being analysed by Indian radiographers and it is even conceivable that by 2020, the medical practitioners providing virtual care might be based outside the UK.

The blurring of personal life and work has been a trend that has been growing in prominence. Already, a "bring your own" approach to ICT infrastructure is becoming more apparent in the workplace. Home working exemplifies the blurring work/personal life dynamic, but arguably has been superseded by mobile computing of which it is a subset. The Information Security challenges associated with mobile devices include loss or theft of the mobile device resulting in exposure of data; interception of data that passes over the WiFi or 3G network; capture of data via Bluetooth connections; and mobile viruses. Whilst these threats exist today, the proliferation of mobile devices and how they are used will undoubtedly be a key security consideration over the next decade.

> *"Smart phones are basically small PC's now, so all the current threats on a PC are simply transferred to the phone.*
>
> *Cyber Security Expert"*

Disruptive technologies may radically change Information Security over the next decade. Some of the areas identified include quantum computing, wireless electricity, new man-machine interfaces and the development of new communication protocols. The wide scale adoption of new collaborative productivity tools may also introduce new threats.

two

Data explosion

Not only is the volume of electronic data at rest and in transit expected to grow rapidly, the nature of data itself will evolve. Over the next decade, there is likely to be:

- Greater sharing of sensitive data between organisations and individuals
- A significant increase in visual data
- More people connected globally
- Greater automated traffic from devices
- A multiplication of devices and applications generating traffic
- A greater need for the classification of data

Sharing of appropriate information with appropriate people or organisations provides opportunities for new methods of social engagement, greater connectivity with customers and facilitates collaborative working. However, through social networking sites, the volume of private information being shared has escalated significantly over the last decade and this is set to continue without a shock or government intervention through education and/or awareness campaigns.

> *People are generally relatively guarded when they meet a new person face-to-face. But they seem to suspend this caution when online.*
>
> Dean Turner, Symantec

It is unclear how social networking and people's attitude towards privacy will evolve to 2020. In our research, two potential future scenarios were identified.

In the first scenario, current trends continue and sharing information becomes the norm, to the extent that those with low online social presence are perceived with suspicion. Alternatively, there may be a mass realisation about the threat associated with sharing information which would drive a more cautious attitude to sharing information. It is likely that if the future follows the first scenario, social networks will become an even greater target for fraudsters.

> *In the future we might see more automated attacks. If you have a machine that can data mine from social networking sites, making highly customised, realistic looking threats. There is also likely to be more targeting of high value individuals or high value groups.*
>
> *Cyber Security Expert*

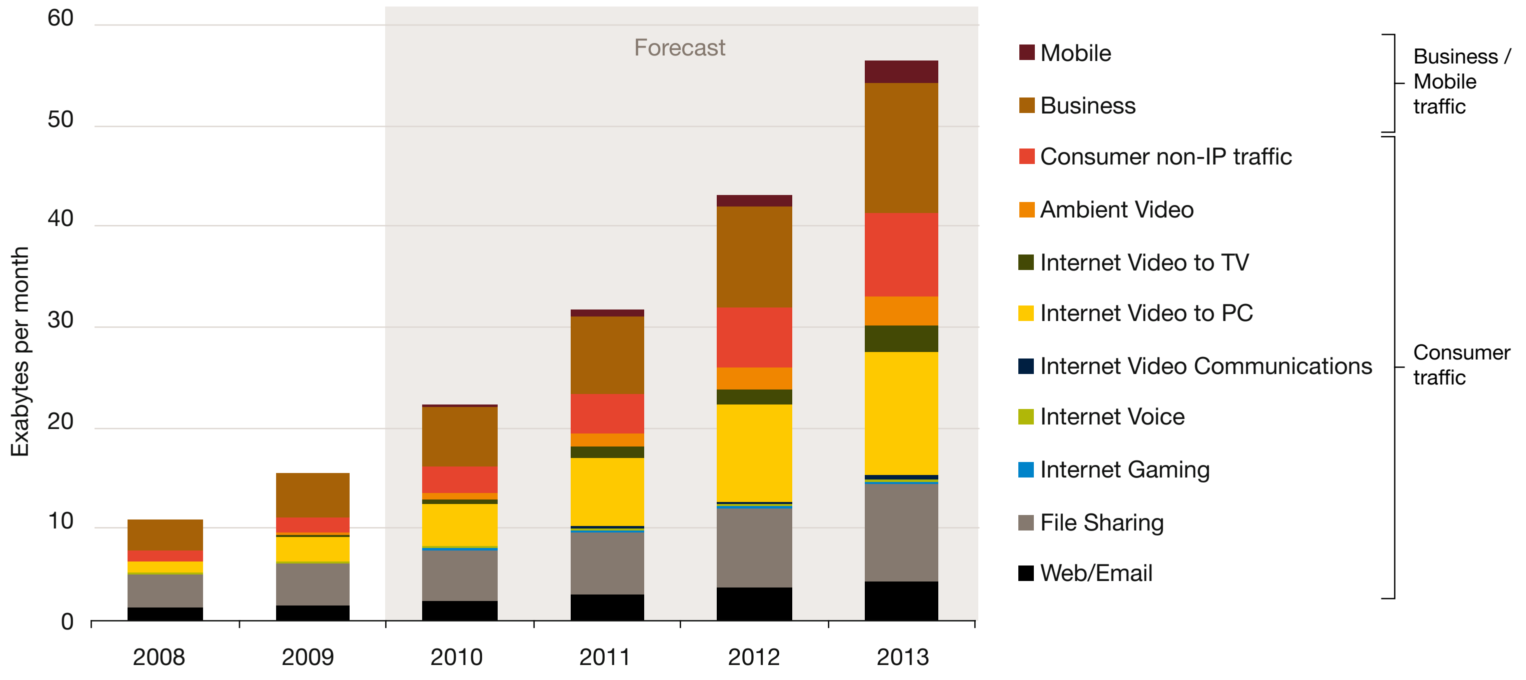
Social networking itself is also likely to evolve over the next decade. The user bases of Facebook and MSN are still growing, but many people, particularly younger people, are increasingly using Twitter and other emerging social networking platforms. For example, geolocation based social networks are already gaining traction and may present new threats and opportunities.

As businesses increasingly work collaboratively, there will be a greater need to share information electronically. This will drive requirements to classify information in order to define what can and cannot be shared in order to protect commercially sensitive information and to comply with regulations.

Internet traffic and the volume of data stored has grown exponentially over the last decade, and a recent report by Cisco suggests global IP traffic will quintuple from 2008 to 2013, representing 667 exabytes of traffic per year in 2013 (see figure 2). This trend is likely to continue to 2020, driven by strong growth in visual traffic, data exchanged between sensor networks and the increasing penetration of high speed internet globally. Streaming visual media is expected to be the primary driver of internet traffic growth over the next decade, through TV, video on demand, and visual communications.

In parallel, increasing autonomous connectivity between IP connected devices, in combination with growth in the volume of applications generating traffic is likely to drive strong growth in machine to machine (M2M) traffic to 2020.

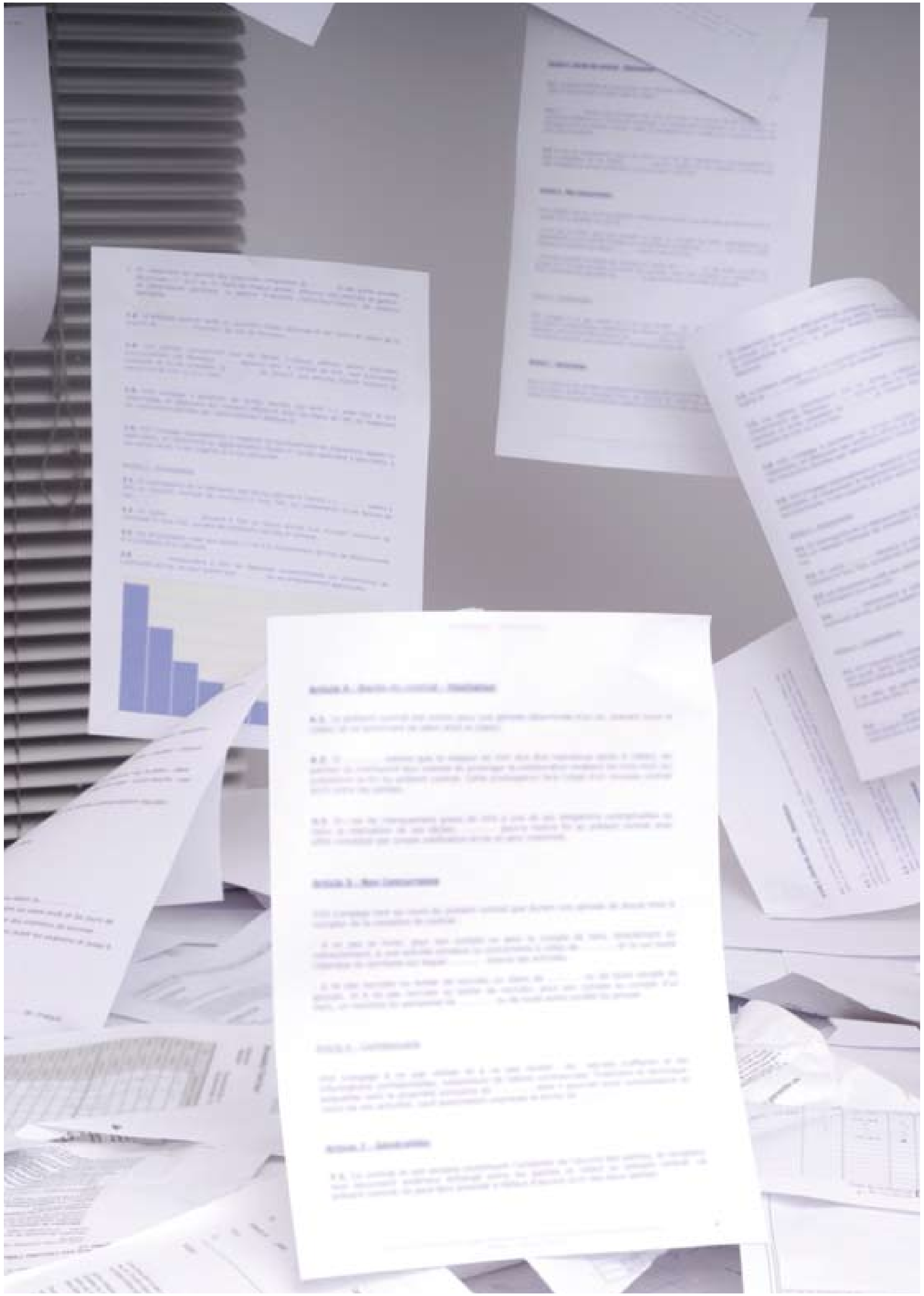
Figure 2: Dawn of the Zettabyte - IP Traffic forecast 2008-2013



Source: Cisco, 2009

The semantic associations required to transform data into information, and information into knowledge creates additional data in itself, and therefore greater IP traffic. Towards 2020, significant growth in the volume of data may drive requirements for automatic classification or intelligent tagging.

There are approximately 1.7 billion users connected through the internet in 2010, from a global population of 6.7 billion. The National Science Foundation (a US agency) has forecast that there will be almost 5 billion users online by 2020, a penetration of nearly 70%. Growth will primarily be driven by developing regions such as Asia, South Africa and South America moving online. This trend coupled with a shift of the global economic centres to the East presents significant Information Security challenges.



three

An always-on, always-connected world

Connectivity is set to increase significantly over the next decade in a number of ways:

- Greater connectivity between people driven by social networking and other platforms
- Increasingly seamless connectivity between devices
- Increasing information connectivity and data mining
- Increased Critical National Infrastructure and public services connectivity

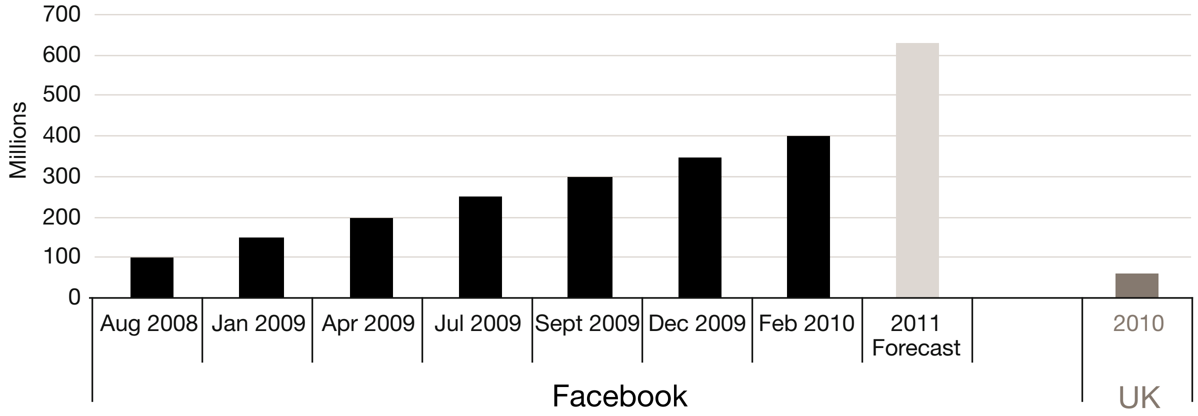
The internet has enabled people to connect in ways never seen before and social networking has emerged as one of the defining trends of the current decade (see Figure 3).

The internet has given users the means to interact with like-minded individuals, while the combination of always connected mobile devices and innovative communication platforms like Twitter have given individuals the ability to communicate, share views and canvass opinion in real-time.

Social networks have created new threat vectors including business reputation / brand damage and social engineering.

Real time, viral communication channels have made it possible for attackers to stage high impact attacks against organisations and individuals, or draw traffic or media attention through relatively simple attacks, for example creating malicious hype around a brand.

Figure 3: Socially Networking – Growth in Facebook user base versus population of the UK in 2010

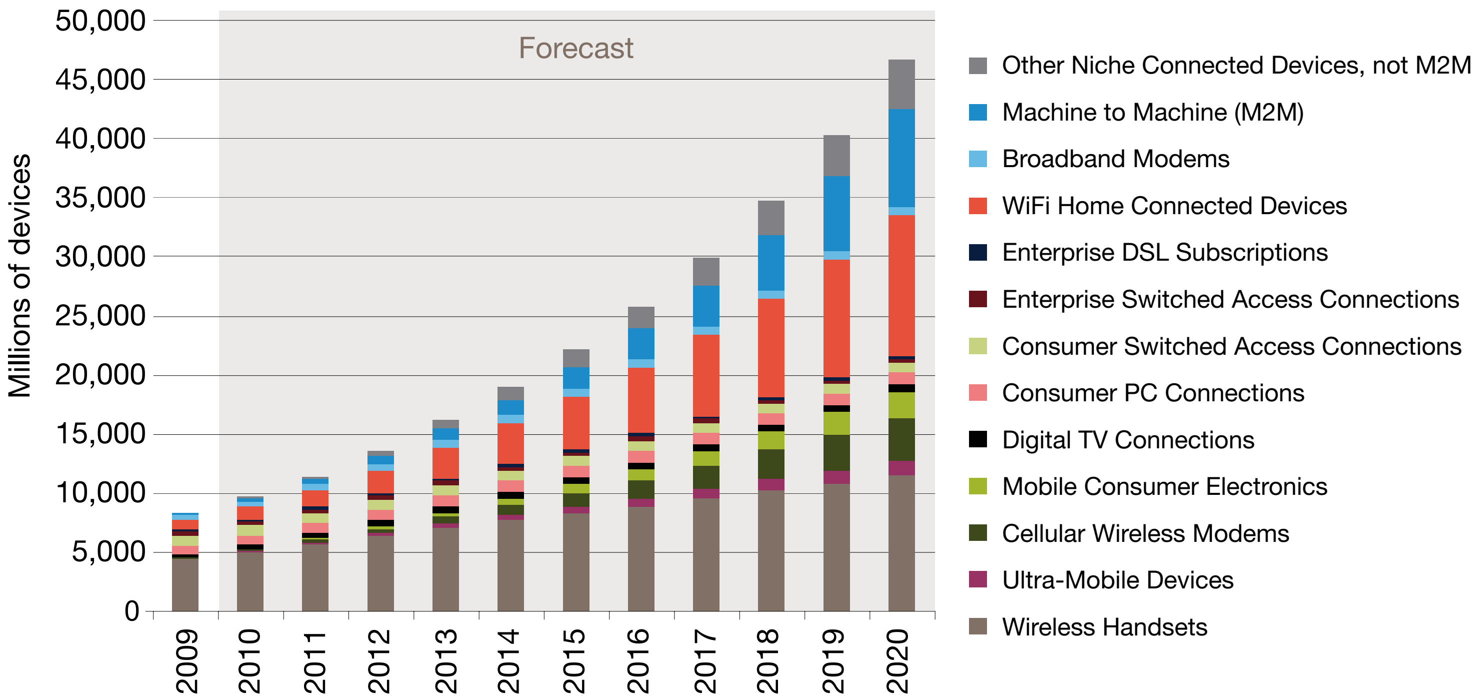


Source: Pingdom (2010)
Note: The chart is illustrative of the growth of social networking platforms. It is possible that a new form of social networking may have emerged by 2020.

In 2020, ubiquitous devices will seamlessly and automatically interact with other devices around them, adapting functionality to their local environment and other objects in their proximity. This has been driven by consumer pull to use technology as an enabler to make everyday tasks easier.

> *Technology is becoming more pervasive and by 2020, we will have body area networks, and sensor networks in the house and people will be monitored for health reasons. Everything is connecting in a more automated manner and in the future you may have a house that detects a pacemaker in the vicinity, which doesn't allow the microwave to be activated!*
>
> *Tim Watson, De Montfort University*

Figure 4: Proliferation of devices – growth of global IP connected devices, 2009-2020



Source: Ericsson, ABI, Yankee Group, Strategy Analytics, Berg Insight

The seamless nature of communication is likely to be founded on open principles to reduce user involvement in managing connections. It is also likely that innovation in artificial intelligence will enable devices to make autonomous decisions on trust when connecting and exchanging data with devices and applications. This creates an opportunity for attackers to infiltrate a device by exploiting the device’s trust mechanisms without the user being aware.

Information is increasingly being used in a more connected manner. In the business environment, collaborative working tools are increasingly prevalent, while data mining algorithms have been developed which correlate data from a growing range of sources to identify patterns and trends, or to develop detailed profiles on individuals and groups.

> “ *Security will become the enabler. It will allow individuals living in tomorrow’s collaborative world to use any device they want for all personal or business uses. Virtual business applications will run on these devices, using federated security services provided through the cloud.*
>
> *JasonC reasey,*
> *Information Security Forum* ”

The emergence of geolocation data presents new marketing opportunities for businesses, but also raises privacy issues. This capability is already currently being used in fields as diverse as national security and marketing, and the number of application areas is likely to expand by 2020.

As ICT permeates into new domains, including Critical National Infrastructure (vital infrastructure assets including communications, energy, finance, etc), there is greater potential that ‘Consumer Off-The-Shelf’ (COTS) devices will interact with bespoke mission critical systems developed specifically for controlling power plants, cooling systems and other industrial equipment.

> “ *Common IT devices with their associated risks will increasingly come into contact (both directly or indirectly) with critical control systems found in national infrastructures, with a greater range of communications protocols over more readily accessible networks both wired and wireless. This is a necessary reality in order to increase the capabilities and efficiency of all of our smart infrastructures to have sustainable economic development for our societies. We must continue to evolve security technologies that can address these realities more effectively as well as ensure increased investment in private and trusted networks for our most critical systems.*
>
> *Daniel Thanos* ”

The networked nature of ‘Smart Grids’ makes it potentially possible to attack the grid itself without the need to target power stations, for example.

In 2020 it is likely that people’s ability to withdraw from the connected world will be reduced and being connected will become increasingly necessary to maintain an active role in society.

four

Future finance

A significant proportion of cyber crime is financially motivated and key developments in e-finance over the next decade could include:

- Rising levels of electronic and mobile commerce and banking
- Development of new banking models
- Growth in new payment models
- Emergence of digital cash

E-commerce and m-commerce (mobile commerce) have continued to grow despite the impact of the economic downturn as consumers have been drawn to the lower prices and the convenience of shopping online. In fact, recessions can accelerate this trend as we saw media companies like Zavvi go into administration during 2008.

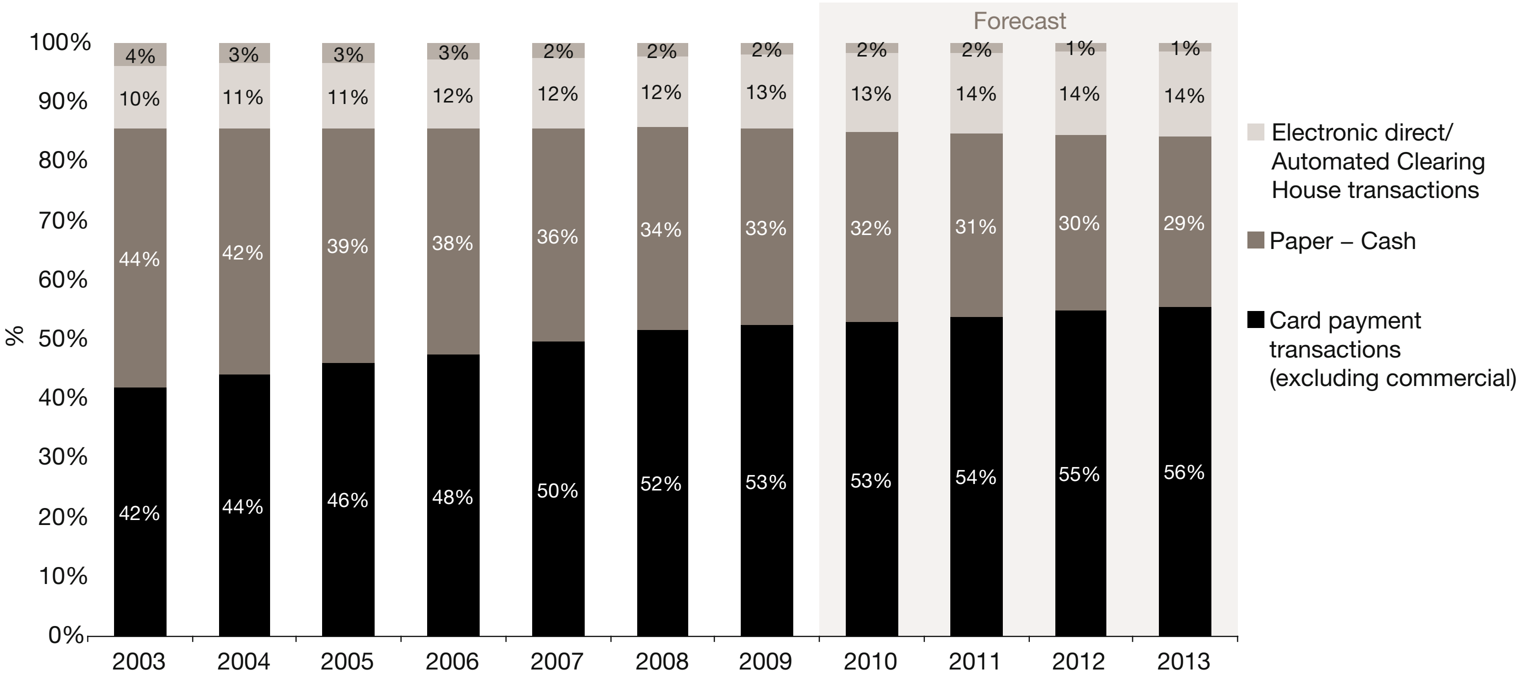
As the volume and value of transactions through these channels continues to rise, it is likely that cyber criminals will be willing to invest further resources in developing increasingly sophisticated attacks.

By 2020, the degree of physical interaction between banks and their customers may have declined significantly and new banks may emerge without any customer facing physical presence, building on the success of companies like Egg and First Direct. Increased e-banking and m-banking will enhance the need for strong identity management and authentication.

Internet growth and social networking has enabled greater connectivity between individuals, which is bringing innovative new e-commerce and banking models. Peer-to-peer ‘social lending’ is one example, in which companies like Zopa are bringing together lenders and borrowers to transform the borrowing industry. If dominant social networking platforms like Facebook were to move into the financial services industry by leveraging their growing user base, it could revolutionise the industry because the traditional banking system has been shaped by the underlying need for trust, and the need for a third party to evaluate and price risk.

The concept of a cashless society has been discussed for some time and the emergence of contactless payment systems like the Visa Paywave and Mastercard Paypass may accelerate the trend, particularly given the phasing out of cheques by 2018 in the UK. Many experts believe that these technologies are merely the forerunner to mobile phone wallets with Near Field Communication capability. This could give rise to a range of new security risks as it becomes possible to steal money without the target even being aware of the attack.

Figure 5: Dash from Cash – Consumer payments by value, 2003-2013



Source: Euromonitor

Cash remains a popular choice for consumers (see figure 5) and by 2020, there is the possibility that ‘digital cash’ will have been developed, with the benefits of electronic payments, but with the privacy of cash.

> *“There is demand for anonymous electronic payments. There is no current equivalent to cash and even the new contactless payment cards leave a paper trail.*
>
> *Cyber Security Expert”*

Interestingly, the advantages associated with the non-traceability of digital cash also create new challenges. For example, by reducing the traceability of cash and making it more difficult to prove theft, it reduces the risk associated with an attack.

five

Tougher regulation and standards

Regulation and standards will be important drivers of Information Security over the next decade, but will need to keep pace and evolve as technology and its uses develop. There appear to be three key themes that could impact Information Security over the next decade:

- Increasing regulation relating to privacy
- Increasing standards on Information Security
- Globalisation and net neutrality as opposing forces to regulation and standardisation

Over the next decade, it is likely there will be increasing pressure towards regulation in Information Security, with privacy being a key driver. The European Commission highlighted the challenges succinctly in a recent statement:

“Our privacy faces new challenges: behavioural advertising can use your internet history to better market products; social networking sites used by 41.7 million Europeans allow personal information like photos to be seen by others; and the 6 billion smart chips used today can trace your movements.”

It also indicated that regulatory form would be required:

“With the Lisbon Treaty and the Charter of Fundamental Rights now in force, the Commission today said it wants to create a clear, modern set of rules for the whole EU guaranteeing a high level of personal data protection and privacy, starting with a reform of the 1995 EU Data Protection Directive.”

This trend is also apparent in the US where the State of Massachusetts recently enacted a new law on Data Breach Notification, mandating that local businesses be proactive in protecting residents’ personal information.

In terms of focus areas, the future challenges around privacy may well be defined by corporate organisations and increased marketing sophistication as well as developments in health information technology.

> “*Privacy will be profoundly shaped by companies’ desires to share information for business intelligence and derive revenue from direct and interactive marketing, the increasing inclusion of specific security controls in privacy laws, and the changes and investment in healthcare information used and the advent of electronic health records.*
>
> *Jim Koenig,*
> *PricewaterhouseCoopers LLP (US)*”

Regulation is likely to be a key driver for ensuring security of Critical National Infrastructure (CNI) given that in many countries, this is either part or entirely privately owned and operated.

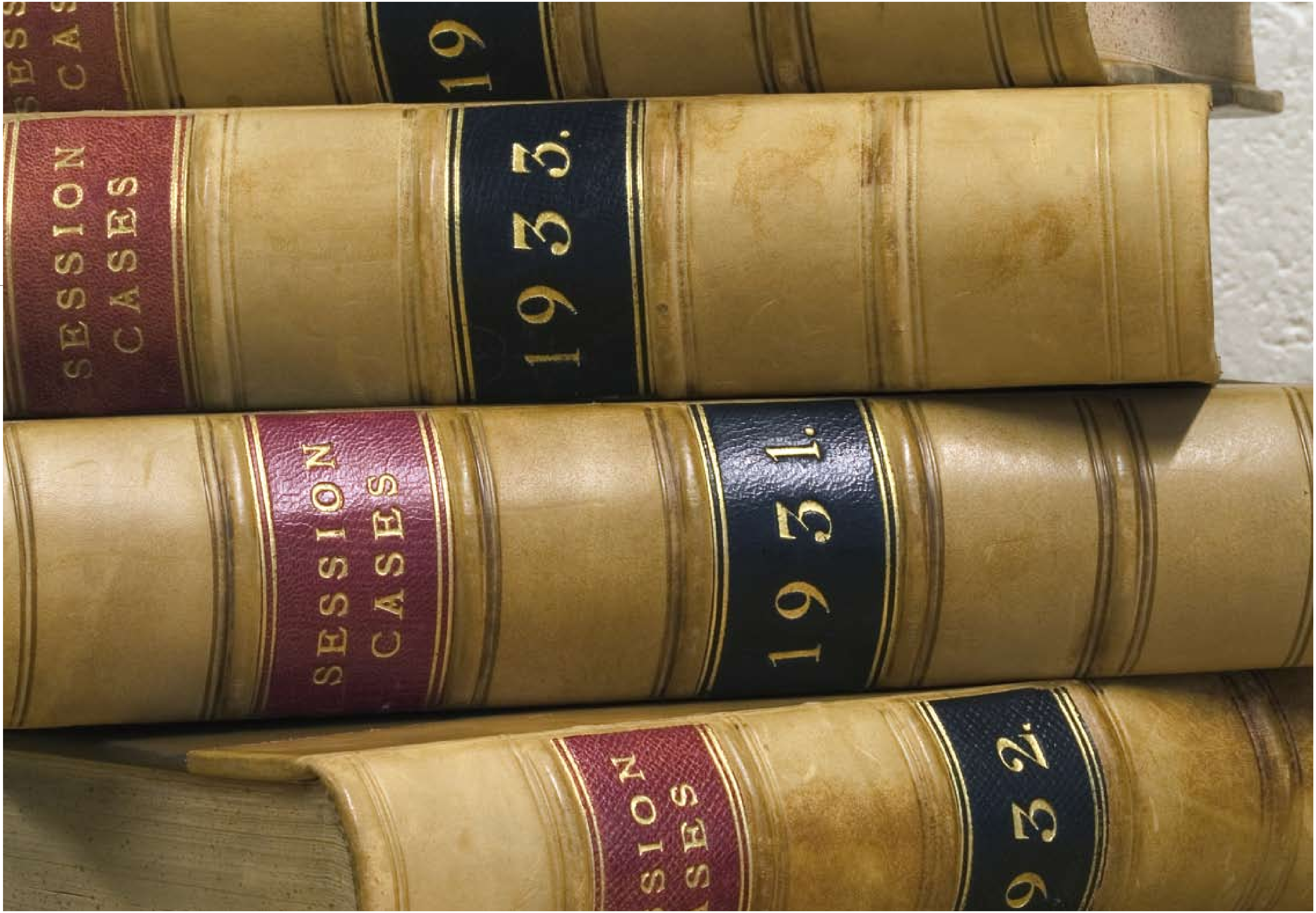
In addition to developments around privacy, there is also a parallel drive towards standardisation of Information Security in areas such as reporting of threats and threat levels, software patch management and software development processes and testing.

However, there are likely to be opposing forces to these mechanisms of adding control and structure to information and the internet. Globalisation will make it difficult for standards and regulation to be homogeneously applied across all jurisdictions. By 2020, the volume of internet users will be greater in Asia than any other region on Earth. It is not clear whether the West is going to be a leader or follower on Information Security and what the implications will be for Information Security in 2020.

A second adverse factor is the concept of net neutrality, the broad principle that all traffic must be treated equally by network carriers, without any restrictions or priorities being placed on content.

In a very recent high profile case, the U.S. Court of Appeals for the District of Columbia ruled that the FCC (Federal Communications Commission) lacked the authority to require broadband providers to give equal treatment to all Internet traffic flowing over their networks. This was considered a big victory for Comcast Corp., the US's largest cable company, although advocates of an open internet consider this to be a major setback.

One potential consequence of removing net neutrality would be that network carriers would be able to charge websites depending on traffic volumes and traffic priorities. However, there remains a large community that supports the concept of net neutrality and whilst it is not yet clear how this area will develop going forward, it is likely to have implications for Information Security.


SESS
CAS
19
SESSION
CASES
1933.
SESSION
CASES
1931.
SION
SES
932.

six

Multiple internets

Will one size fit all?

The internet may multiply over the next decade. There are a number of trends that could potentially lead to segmentation of the web:

- Greater censorship
- Political motivations driving new state/regional internets
- New more secure internets
- Closed social networks
- Growth in paid content

In some respects, the internet has already divided, with the global 'open' internet and then the censored internet in countries like China, Cuba, Iran, Saudi Arabia and North Korea. In Saudi Arabia for example, all international internet traffic is directed through a proxy farm which filters immoral and political content. Another example is the Golden Shield Project in China which blocks predefined IP addresses, thereby controlling viewable content.

The politically motivated development of parallel networks is an emerging challenge and there has been speculation recently about China and Russia developing alternate internet routes that bypass the ICANN (Internet Corporation for Assigned Names and Numbers) system – the web's global address book.

There is potential for a future divide around a secure and non-secure internet. The secure zone is likely to be established by enterprises as they become frustrated with the volume of extraneous data and threats online, particularly if it limits the ability to do business effectively with customers. Businesses may be willing to pay a premium for guaranteed availability and security.

> *“In the future, there may be a centralised agency overseeing the internet law enforcement function. There may even be two levels of the internet – the policed bit and the anarchic bit.*
>
> *Julia Harris, BBC”*

The secure web may require users to be running specific secure software, to have firewalls and other security in place, and to encrypt traffic to predetermined standards. This would primarily be driven by the need for secure financial transactions and to facilitate secure mobile working. In many ways this is an extension of the approach many businesses already adopt, which forces users to identify themselves to the enterprise network and apply security standards like encryption and multi-factor authentication.

However, this goes against the founding principles of openness for the internet and many of the benefits of the internet are derived from its ability to connect everyone, so there is a strong case against this divide.

> *I don't think the multi-zone internet will happen because most people don't care about privacy or secure networks, they want an omnipresent one. A secure web would also create a bigger target*
>
> *Tony Dyhouse, Digital Systems Knowledge Transfer Network*

Social networks are by definition exclusionary, and given the defining role social networks play in shaping the development of the internet, participation within social groups may increasingly define our lives and online experience, resulting in a societal divide. This has the potential to drive targeted attacks against specific social groups.

The internet provides individuals with access to a wealth of information of differing qualities through providers ranging from online broadsheet newspapers through to Wikipedia and Tweets. Trusted, quality providers typically have higher costs and although many have provided information for free to date, quality content is increasingly requiring premium access. This drives a divide between those who can afford to pay for trusted sources and those who revert to free, potentially non-trusted sources. Increased media hacking and social media hacking, if targeted at certain groups, could in effect be a disguised form of censorship.

seven

New identity and trust models

Identity and trust are key concepts to all aspects of Information Security and will be increasingly important over the next decade as:

- The effectiveness of current identity concepts continues to decline
- Identity becomes increasingly important in the move from perimeter to information based security
- New models of trust develop for people, infrastructure, including devices, and data

The concept of proving digital identity is one of the greatest challenges identified in our research. In 2020 as people spend an increasing proportion of their time online, identity becomes a greater challenge because fewer interactions will be face-to-face, a greater volume of private information may be available online and new technologies could make it easier to impersonate individuals.

Typical mechanisms for authenticating and verifying identity include passports, birth certificates, driving licences and biometrics (such as finger print and iris recognition). Electronic systems and personal accounts are generally accessed today using usernames and passwords, secret questions and personal information. However, personal information that has traditionally been used for identification purposes is no longer personal. Social networking websites abound with personal data and social engineering is increasingly being used to steal identities.

Systems likely to proliferate in the future will demand multi-factor authentication. These solutions may raise the security hurdle but are unlikely to solve the problem entirely and need to take account of the privacy and consent of the user in their design.

> *“You can’t just assume that an eye scan offers better protection than a username and password. The scan can still be manipulated by a hacker, who may try to switch out the master scan with their own. If you go to DNA identification, then people will get blood samples from hospitals. Every lock has a key.*
>
> *James Carnell, Cyveillance”*

The research suggests that over the next decade, the concept of identity and its usage will evolve. With the increasing adoption of cloud computing, security increasingly becomes data centric as opposed to perimeter based.

> *Historically the approach has been "outside in" with multiple layers of security. This model does not work in the virtualised environment and so a new "inside out" approach is emerging. The machine must be self-defending.*
>
> *Rik Ferguson, Trend Micro*

> *Cloud Computing as an enabler for business will live or die by identity management.*
>
> *Bruce Elton, Oracle*

So who will hold people's identities in the future? The OpenID concept is an example of how identity management may evolve over the next decade. The service is free and acts as an aggregator of information enabling a user to access multiple websites that support the service using a single username and password. The concept relies on the user trusting the provider of the OpenID service. Example providers of OpenID include Google, Yahoo, Orange and Myspace. A federated model of trust appears more likely to be the model of choice over the next decade as it avoids putting all the eggs in one basket, providing an attractive target to criminals. This model provides convenience, but does not address the issue of identity.

An interrelated concept to identity is trust. Various mechanisms have been developed to provide trust online including the eBay feedback model, the friend-of-a-friend concept and the VeriSign seals of approval. These models are primarily for human-to-human trust, but with increasing connectivity, there is an increasing need for humans to trust technology, technology to trust technology, and even technology to trust humans as devices increasingly act on behalf of individuals.

> *People are naturally very good at making judgements about trust from visual cues, voice, background information etc. But it's not easy to adapt these to make trust judgements when interacting with people over technology or about devices themselves.*
>
> *Cyber Security Expert*

New models of trust are needed. There are two likely approaches to this; either the system will need to present the user with a statement about the level of trust, or it will present the user with the cues to make the trust judgement themselves.

What does this mean for my organisation?

The developments in Information Security over the next decade are likely to have far reaching impact on organisations. There are some key questions to consider about how change in Information Security over the next decade could impact your organisation.

The world has changed and will continue to change. UK organisations depend upon reliable and accurate information provided by electronic systems to make critical decisions about almost every aspect of their business. The dependence upon these systems which deliver services to UK business and society is greater than it has ever been and is set to increase in the coming years. What we do to increase either Information Security and resilience of these systems is down to us.

The research indicated that there is a need for a proactive approach to Information Security from all stakeholders given the rising complexity and volume of threats.

Organisations should ensure that approaches to Information Security are holistic and consider technology, processes and people. Approaches need to adapt to rapidly changing threats and technology, and also to changes in regulations and standards. However, it is important that organisations also focus on aspects of Information Security that are not necessarily driven by regulation and standards, for example, protecting commercially sensitive information or intellectual property.

Increasing focus on Information Security could also provide competitive advantage. Organisations that have effective Information Security in place could increasingly attract consumers to use their products/services. Information Security could also provide opportunities to sell products/services through new channels or interact with customers in new ways that are not possible today due to concerns about privacy.

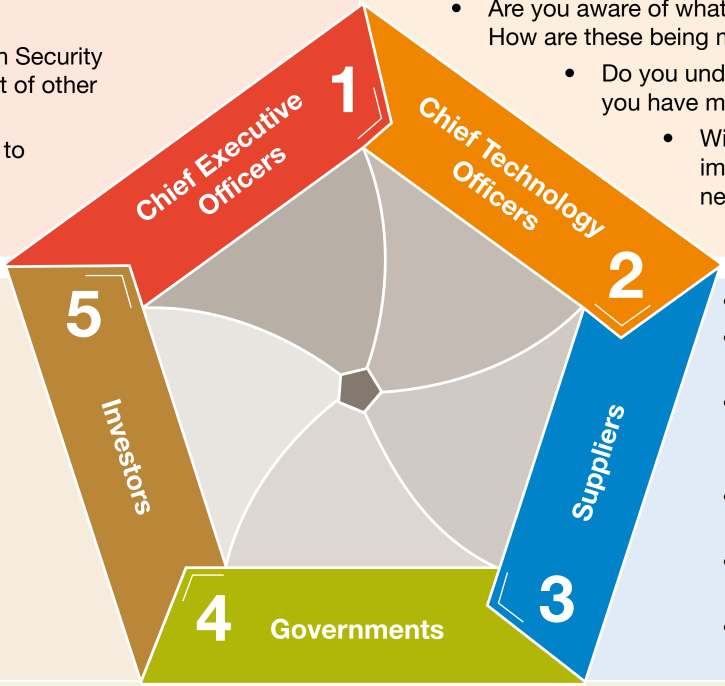
There are some key questions to consider about how changes in Information Security over the next decade could impact your organisation.

Key questions on how the trends in this roadmap could impact my organisation

Organisations dealing with Information Security issues

- How do you identify and measure Information Security related risks and compare them with other business risks?
- How will your organisation's business model evolve in the future, and what Information Security opportunities and risks will this present?
- How will you ensure compliance with Information Security regulations and standards, whilst not losing sight of other important Information Security issues?
- Does Information Security present opportunities to gain competitive advantage?

- Have you clearly identified what information is most valuable to your business and which information is most at risk?
- Have you effectively embedded good Information Security behaviours into your organisation's culture?
- Are you aware of what events may cause your business to lose its trusted status? How are these being mitigated?
- Do you understand the dependency you have on trading partners and do you have measures in place to ensure the security of information flows?
- Will any of the issues identified in this roadmap impact your immediate Information Security strategy, and your plans for the next 5-10 years?



Other key stakeholders

- Are there opportunities and risks relating to Information Security for the businesses in your current investment portfolio?
- How will the trends identified in this roadmap change the technology and Information Security industries' value chains?
- How will business models across all industries evolve due to the trends in this roadmap? What does this mean for future investments?
- What are the right technologies to invest in and when is the right time to invest?

- Where should R&D spending be prioritised?
- What is likely to be the greatest threat to customers over the next decade?
- How will your organisation's business model evolve in the future, and what Information Security opportunities and risks will this present?
- Where should the line be drawn between user education and automated security solutions?
- Are attitudes to security likely to change, placing a greater emphasis on secure development over speed to market?
- How will security solutions need to change over the next decade to respond to trends identified in this research?

- Is there a need for greater Information Security regulation? If so, what is the best approach and what is the right time for change?
- How can the Government ensure Information Security regulation is consistent with other countries?
- Is greater investment required in the Information Security industry or in Information Security skills?
- What are the medium term risks to the UK and the UK's wider interests of not taking a leading position in Information Security?
- Is regulation effective given the pace of change in technology and people's use of technology?

For further information about this roadmap contact:

Jan Schreuder
Partner
Sydney Information Security Services Lead
+61 (2) 82661059

jan.schreuder@au.pwc.com

Andrew Gordon
Partner
Melbourne Information Security Services Lead
+ 61 (3) 8603 6179

andrew.gordon@au.pwc.com

Kim Cheater
Partner
Adelaide Information Security Services
+ 61 (8) 8218 7407

kim.cheater@au.pwc.com

Cameron Jones
Partner
Perth Information Security Services
+61 (8) 9238 3375

cameron.jones@au.pwc.com

Joshua Chalmers
Partner
Brisbane Information Security Services
+61 (7) 3257 8391

joshua.chalmers@au.pwc.com

Patrick Kevin
Executive Director
Canberra Information Security Services
+ 61 (2) 6271 9267

patrick.kevin@au.pwc.com

We would also like to acknowledge the contribution of **Greg Bacon (PwC)**, **Jason Creasey (ISF)** and **Andrew Wilson (PwC)**.

This report has been prepared by the Technology Strategy Board together with PricewaterhouseCoopers LLP, UK (“PwC”) for Technology Strategy Board under the terms of the engagement contract with PwC dated 31st March 2010 (the “Engagement”). This report is for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this report without obtaining specific professional advice.

This report contains information obtained or derived from a variety of sources (as indicated within the report). PwC has not sought to establish the reliability of those sources or verified the information so provided. Accordingly no representation or warranty of any kind (whether express or implied) is given by PwC to any person (except to the Technology Strategy Board under the relevant terms of the Engagement) as to the accuracy or completeness of the information in this report.

PwC accepts no duty of care to any person (except to the Technology Strategy Board under the relevant terms of the Engagement) for the preparation of the report. Accordingly, regardless of the form of action, whether in contract, tort or otherwise, and to the extent permitted by applicable law, PwC accepts no liability of any kind and disclaims all responsibility for the consequences of any person (other than the Technology Strategy Board on the above basis) acting or refraining to act in reliance on the report or any information contained in the report or for any decisions made or not made which are based upon this report or information therein.

The quotes in this report reflect the views of the individuals and are not necessarily the views of their organisations.

We would like to thank the following people for their support with the research:

Name	Organisation
Paul Simmonds	AstraZeneca
Stephen Bonner	Barclays
Julia Harris	BBC
Mark Ryan	Birmingham University
Patrick Curry	British Business Federation Authority
Robert Nowill	BT
Dr Robert Ghanea-Hercock	BT Labs
David Livingstone	Chatham House
Dr Paul Cornish	Chatham House
Paul King	Cisco
Neil Todd	Credit Suisse
James Carnell	Cyveillance
Dr Tim Watson	De Montfort University
Roy Isbell	De Montfort University / PragmaticDefence
Tony Dyhouse	Digital Systems Knowledge Transfer Network
Philip Virgo	European Information Society Group (EURIM)
Steve Harris	Garlik
Daniel Thanos	GE Digital
David Pym	Hewlett Packard
Martin Borrett	IBM
Stephen McCartney	Information Commissioner’s Office
John Bullard	IdenTrust
Andy Jones	Information Security Forum
Jason Creasey	Information Security Forum
David Emm	Kaspersky Lab

Name	Organisation
Marcus Alldrick	Lloyd’s of London
William Cole	McAfee
Greg Day	McAfee
Luke Forsyth	McAfee
Julia George	Methods Consulting
David Ferbrache	MoD (Cyber & Influence Science & Technology Centre)
Mr Jessaji Dedra	MoD (Development Concepts and Doctrine Centre)
Dr Robert Coles	National Grid
Jussi Jaakonaho	Nokia
Steve Marsh	Office of Cyber Security, Cabinet Office
Bruce Elton	Oracle
Jamie Cowper	PGP Encryption
Jim Koenig	PricewaterhouseCoopers LLP (US)
Andy Hodgson	QinetiQ
Dr Godfrey Gaston	Queens University
Fred Piper	Royal Holloway, University of London
Andrew Moloney	RSA
Paul Osborne	Security Innovation and Technology Consortium
Adrian Asher	Skype
Dean Turner	Symantec
James Gay	Travelex
Paul Little	Trend Micro
Rik Ferguson	Trend Micro
Neil Morgan	Technology Strategy Board

And several others who prefer to remain anonymous.

Technology Strategy Board
Driving Innovation

For information on the Technology Strategy Board: www.innovateuk.org

For information on PricewaterhouseCoopers LLP: www.pwc.co.uk

© Technology Strategy Board, 2010. Publication: T10/037