FORESIGHT

Cyber Trust and Crime Prevention project

Executive Summary

OFFICE OF SCIENCE AND TECHNOLOGY

FORESIGHT

CYBER TRUST AND CRIME PREVENTION

EXECUTIVE SUMMARY

OFFICE OF SCIENCE AND TECHNOLOGY

This report is intended for all those with an interest in the potential future opportunities created by information and communication technologies, including decision-makers in government and business. It will also be of interest to professionals engaged in research in a wide range of related academic disciplines. The report provides an entry point to more detailed reports on various aspects of the underlying science and technology, also published by Foresight, which have informed the project's work summarised here.

This report has been produced by the Cyber Trust and Crime Prevention project of the Foresight programme. Foresight is run by the Office of Science and Technology under the direction of the Chief Scientific Adviser to the British Government. Foresight creates challenging visions of the future to ensure effective strategies now. Like other Foresight reports it has actively involved other government departments, in this case especially the Home Office.

Scene understanding
Cognitive modelling
Smart surveillance
connectivity
Contention management
Dynamic applications
Pattern recognition
Grid computing
Broadband access
Ubiquitous computing
Data compression
Behaviour prediction
Processing power
Wearables and embeddables
Information security
Technologies
Applications
Issues
Tagging things and people
Location-based services
biometrics
Open Source Software
mobility
cryptography
Fault tolerance
Web services
Trusted platforms
Agency, proxies, avatars
Fault prevention
Rigorous development methods
Quantum encryption
Dependable systems
Knowledge management
Nanoscale computing
identity

Foreword by Sir David King

Chief Scientific Adviser to UK Government and Head of the Office of Science and Technology.

The importance of Information and Communications Technologies (ICT's) to the people of the United Kingdom and to the UK's economic well-being is widely accepted. The majority of people use mobile phones and increasing numbers are using the Internet to obtain information, make purchases and access public services. ICT's enhance the quality of life, and are a key part of the knowledge economy.

The pace of technological change remains fast: smart objects, intelligent agent software, new forms of pervasive computing and other developments will continue to give us new possibilities. It is rarely clear precisely what form these possibilities will take, or how people will want to use them. At the same time some aspects of information technology, such as the structure of the Internet, are essentially well established, but their profound effects are changing as they work their way through the economy.

The project's aim was to explore how we can do our best to ensure that the UK is well placed to develop and to benefit from information technology. We will need to build systems that are trustworthy and also enable people to know when and how to place their trust. We must ensure that systems, and systems of systems, are as robust as possible, and that they are designed to reduce new opportunities for crime. We must continue to use ICT as one of the ways to reduce existing crime rates.

This project, like other Foresight projects, started by bringing together researchers from diverse disciplines in order to exploit our world-class academic strengths, from philosophy to systems design and encryption to economics. These experts identified the areas of science and the humanities that they felt would be important in creating the cyberworld, and in understanding it. They then stepped forward to 2018 to create visions of the future that would help to bring the implications of today's decisions to life.

The project has produced reviews of the science, scenarios and other material that will help inform discussion and actions across a wide range of areas. It has also built up extensive networks across science,

business and government. I am delighted that so many of the participants are now carrying forward the project's work, and the stakeholder group, chaired by Hazel Blears, has agreed to meet again in a year's time to track progress.

Preface, by Hazel Blears, Home Office Minister for Crime Reduction, Policing, Community Safety and Counter-Terrorism

I have found the role of chair of the stakeholder group a fascinating and illuminating experience. I say fascinating because the project has brought together a wide range of stakeholders, end users and specialists to investigate these important, and complex, matters. The investigations spanned the technical and social issues related to the use of networked systems and were informed by leading experts in the fields under consideration. The analysis of the issues was well informed and often thought-provoking.

I also noted that it was an illuminating experience. As a non-scientist I have never before had the opportunity to work with such an eminent group of scientists to discuss these issues. It has added to my capability as a Minister by giving me direct insight into how science needs to be central to strategic policy matters.

The issues raised by the project are both challenging and of great importance to our society. The use of the Internet, and other networked systems, has increased dramatically over recent years. It is difficult to imagine an environment without the computer and network facilities that are common today. This has brought many benefits to society. Unfortunately, like all advances, these have also been abused for criminal purposes and by those with malicious or anti-social intent. We have, and will continue to, tackle these abuses. Current examples include new legislation to tackle the on-line grooming of children and the development, by the Home Office, of a strategy to combat e-crime.

The report sets our a number of challenges for the future and I am particularly interested in how we can all work together to ensure the UK obtains the maximum benefit from this new technology whilst minimising its misuse.

The project has provided:

- valuable reviews of the current state of the art in relevant fields, including such areas as identity and authenticity, trust and the development of trust, and the issue of reliance on software that learns your behaviour

- views of possible developments in software and hardware

- scenarious highlighting how the future may develop both risks and opportunities and how we might respond to positively influence that development.

It has also brought into focus a range of issues that are key to the shape of the future in this area. Examples include:

- identity and authenticity and how the physical and virtual world relate

- privacy – how do we strike the balance between individual privacy and the general public's good

- how we build a legal and regulatory framework that is beneficial and effective

- the spread of technology increases in its complexity and the resultant effect on robustness and security.

These will be valuable in both informing and driving the policy in this area.

I would like to say how encouraging it is that so many people volunteered their time to work on the project. These have included representatives of a number of government departments, commercial organisations, learned and professional societies, law enforcement agencies and individuals. I would like to thank them for their participation and valuable contribution.

Contents

Key Supporting Documents*

Science Synthesis: "A Synthesis of the State-of-the-Art Science Reviews": Authors: Professor Brian Collins [Royal Military College of Science Shrivenham] and Professor Robin Mansell [London School of Economics and Political Science].

Technology Forward Look: "Technology Forward Look: User Guide": Authors Bill Sharpe [Appliance Studio] and Stefek Zaba [Hewlett Packard], edited by Martin Ince.

Scenario and Gaming Report: "Gaining Insight From Three Different Futures": Maarten Botterman, Jonathan Cave, James P Kahan, Rebecca Shoob, Robert Thomson and Lorenzo Valeri [RAND Europe]

* For a full set of project documents please see the project website at *www.foresight.gov.uk*

Summary

- Information and communication technology – ICT – has brought, and will continue to bring, massive benefits to all of us. However, as it reaches further into our public and private spaces, it raises complicated, uncertain and interdependent issues. How do you know whom you are dealing with when you send an email? How do you want to be able to vote or to receive benefits, health care and financial services in the future? How can we use these technologies to reduce crime and what should we do to limit the crime opportunities they may offer? What standards of protection should we apply?

- Cyber trust derives from perceptions of the purposes of ICT-based systems, and trust in how they are built and used in relation to their purpose. Much of trust in cyber systems is about system functions and roles in relation to ordinary life, and our perceptions of what it means to be citizens, customers, community members and individuals.

- Crime prevention – guarding against criminal exploitation – is only one aspect of creating trustworthy citizens. Just as reducing crime, whether it is physical crime or cyber crime, is only one of the many potential uses of ICT systems. This project addresses some of the broad issues in relation to trust, but gives special emphasis to those raised by crime prevention. If we do not start to define and tackle these issues now, we risk delaying or losing some of the further potential benefits that the technologies can clearly bring.

- The project explores the underlying scientific evidence, the technologists' views of what might be possible and, using socio-economic input, takes a leap into the future of 2018 to show some of the ways the UK might evolve.

- The issues are not well defined, and the empirical base in many areas is limited. The experts' overall message is that the complexity and pervasiveness of ICTs will require new ways of thinking, particularly about how to manage the threats to people and society. If we carry on as we are, in the long term we are likely to run into problems. These may be because system complexity reduces the system's dependability, and as software projects become more and more difficult to manage, their outcomes become harder to predict and test. Or they may be because increasing numbers of small failures and irritations cause some people to want to choose not to depend on large systems. Or they may be because of a smaller number of more widespread failures that disrupt life at home or

at work. Or it may be because current governance frameworks are not capable of dealing with the full range of implications of information technologies in the future.

- Just as the technologies are global in scope, so is the arena for action. Many of the decisions about what ICTs we will use are made in Europe, the US and the Far East. Whatever those decisions are, we need to consider how we can influence manufacturers to design out crime and design in usability as a fundamental principle. At the same time we will have to consider how to tackle the fact that online crime is not constrained by national boundaries and when things go wrong it is difficult to identify who should be liable. Addressing these issues will require collaboration between governments and business, and with users.

- Because ICT is such a powerful driver for change, the issues it raises do not have single or simple answers. People will want to use it differently in different areas of life – they will apply different standards to, say, the need to identify someone who votes as compared to someone from whom they buy a second-hand book. People will also make different judgements based on their experience, education, the reported experience of others around them, and the way in which risks and benefits are reported in the media.

- Framing the choices in an accurate and realistic way is the key to getting the best for the UK. The project has therefore been built around using extensive science and technology analysis. Expert views from a wide range of sources provided input to create a series of scenarios that illuminate the essential challenges and dilemmas of cyber trust and crime prevention, in a way that will be accessible to a broad range of interested parties including government, business and the public at large.

- Behind these findings is a range of complex arguments that shows that the issues raised by ICTs do not create a coherent set of challenges capable of being addressed by a single approach. There are, however, common themes, frameworks and languages for beginning to tackle the full range of challenges. The most important next step is to get these tools into the hands of people tackling specific policy and strategy decisions. The project's plan of action is therefore geared to engagement with a range of stakeholders and to using the scenarios and underpinning work on a sustained basis.

Chapter 1

Introduction

Trust can be defined as: a firm belief in the reliability or truth … of a person or thing … a confident expectation …

The aim of the project

- To use the best available science to explore the application and implications of next-generation technologies.
- An independent look: while the Office of Science and Technology commissioned the work, the findings are independent of Government and do not constitute Government policy.
- To provide a review of the science and visions of the future, and to establish the actions which follow and the networks needed to support them.

Why the project was needed

Information and communications technologies (ICTs) have a key role in the modern world, affecting how we work and play, how we deal with others, and the way we think about ourselves. Such technologies are increasingly pervasive, bringing both social and economic benefits. Already, the software industry alone accounts for around 3% of the UK's GDP, with over 1 million people working in ICT in the UK in over 130,000 companies. This sector is now growing strongly again (predicted 3.2% growth in 2004 in the UK), despite the global economic downturn.

The UK is in a strong position to exploit the advances being made in ICT. We have the world's second most productive science base in terms of volume and impact of scientific publications; 80% of the UK population can access broadband; the UK is the second largest software consumer in the world, the third largest producer of ICT

goods and is predicted to become the biggest market for ICT in Europe in 2004. Maintaining our status as a world leader in ICT will be a key driver for increasing prosperity in the UK in the 21st century.

ICT's importance will increase as existing technologies work their way through the economy and as new ones emerge. Taken together, the technologies that will have impact in the future are those that get locked in through the workings of market, regulation and choice. We will want to:

- ensure that new technologies can be used to create wealth and improve the quality of life as rapidly as possible
- enable technology to be used to reduce existing crime
- reduce the extent to which technology introduces new forms of crime, or extends the scope of existing crimes.

Getting the best out of ICT presents future challenges because:

- the technologies raise new issues, in terms of scale, complexity and intangibility
- rapid rates of technological and behavioural change may create new opportunities for crime and for new approaches to crime reduction and crime detection
- those rates of change are fast relative to the rate at which individuals gain experience, and to the rate of change in systems of education, governance and consensus-building. Each generation will grow up with a different and richer experience of ICT and how it can be exploited.

ICT-related crime already has a significant impact on businesses, governments and organisations around the world. IT security problems have now become a fact of business life in the UK, with over two-thirds of businesses experiencing at least one security breach in the last year*, the most common being viruses (68%), staff misuse of IT systems (64%), fraud or theft (49%) and unauthorised access by outsiders (39%). The average UK business now receives

* Information Security Breaches Survey 2004, DTI Survey

roughly 20 viruses a year (rising to 50 for large businesses) and has its web site scanned or probed many times. The average cost of an organisation's most serious security incident was about £10,000. For large companies, this was more like £120,000. Although the average seriousness of security breaches has fallen slightly since 2002, the number of incidents has increased, so the total cost to UK business continues to run into billions of pounds.

In response to this growing problem, *IT security has become an increased priority to UK businesses.* Three-quarters of companies rate security as a high or very high priority for their top management or board of directors. However, the treatment of this priority is patchy. For example, although 93% of companies have anti-virus software, half were infected by a virus in the last year, reflecting the increasing trend for viruses to exploit vulnerabilities in operating systems, which companies often do not keep up to date with the latest security patches. Although three-quarters of businesses with in-house websites have a firewall, for over half of these it is their sole defence. Contingency planning is not much better, with fewer than one in ten businesses having tested their disaster recovery plans. The main source of these problems is that many companies lack the expertise to address this complex issue, with only one in ten having staff with formal IT security qualifications, and continue to under invest, with the majority spending less than 1% of their IT budget on security. This report helps set the longer-term context for the Government's approach to these issues, which are currently being addressed in the information assurance and e-crime strategies.

We need the best possible information and languages for framing debate and decisions. Foresight's emphasis on sound science and on imaginative futures work can help to achieve this:

- the overall future environment will be the result of many decisions, large and small, taken in the light of evolving trends and events. Different actors will take their own decisions for their own reasons, such as the introduction of wholly new types of goods and services, higher productivity, faster growth, greater efficiency in public service delivery, enhanced security, effective frameworks for privacy protection and reduced crime

- we have an incomplete but growing knowledge of the social context of ICT. Using this learning will help us to frame the choices better.

Framing the choices in an accurate and realistic way is the key to getting the best for the UK and this project has aimed to provide a basis for the continuing debates.

Chapter 2

The Project's Approach

Like others in the Foresight programme, the Cyber Trust and Crime Prevention (CTCP) project was led by a senior Stakeholder Group, chaired by a Minister, and was supported throughout by an expert Advisory Group. Over 45 scientists, and 260 experts overall, were involved over the lifetime of the project and in various ways, from authoring or reviewing papers to taking part in workshops.

Science Synthesis

The project began by commissioning scientific reviews of the current state of knowledge in relevant areas. Following discussion in expert workshops and at the Advisory Group, ten themes were picked covering a range of disciplines from philosophy and economics to psychology and the study of information systems. Each review paper was subjected to peer review. A full list of the papers and authors is given in Appendix A.

The project's two key experts, Professor Robin Mansell of the London School of Economics and Political Science and Professor Brian Collins of the Royal Military College of Science, Shrivenham, co-authored a synthesis paper drawing on the individual scientific reviews. The source material for this paper is available on *www.foresight.gov.uk*, and will be published in book format in due course.

Technology Forward Look

It is, of course, not possible to predict the future. However, we all make assumptions about what the world will be like when we make decisions today that will have impacts for us and for others over many years ahead.

As a first step towards looking forward, the project commissioned two technology experts to 'turn confusion into well-structured uncertainty', by attempting to reduce the unmanageable range of technology futures into a more tractable number of representative topics. This *Technology Forward Look,* which will be available on the web and in hard copy, gave an overview of the emerging world of

pervasive computing, and detailed discussion of six dominant organising themes in areas from web services and software liability to critical infrastructure and e-cash.

The analysis used a model that, in a very simplified way, was able to show how the different actors in society (consumer, business and government) interact through a range of means (market choice, standards and regulation). Their motivations and interactions can result in a self-reinforcing system of value creation, such as the personal computer (PC) based computer market, which may become stable for a lengthy period of time. See the *Technology Forward Look* for further discussion.

Scenario and Gaming Report

Using the *Technology Forward Look,* the scientific reviews and the expert workshops as inputs, a team from RAND Europe worked to produce three broad scenarios for the year 2018. These provided a narrative backdrop and gave pointers as to how the future might be unfolding as we live it.

The scenarios are summarised in Figure 2.1. They are built around three main dimensions of response to the challenges created by new technologies in their social context:

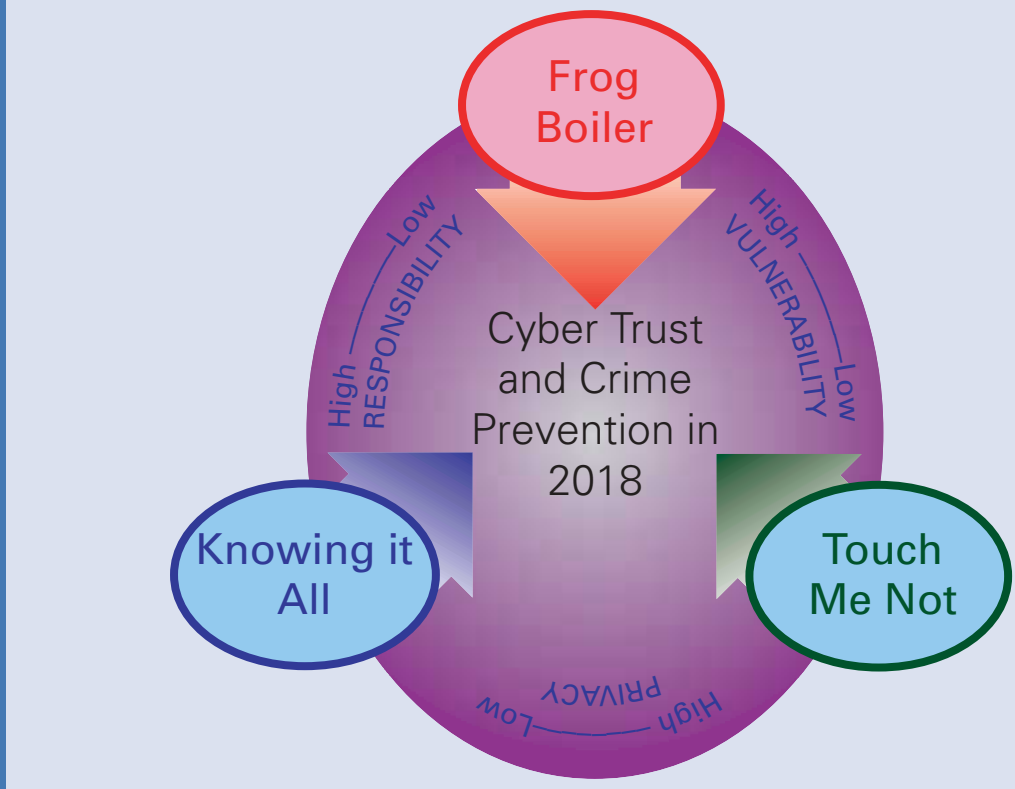
- vulnerability: the degree of planned resilience and trustworthiness inherent in the systems
- privacy: the degree of individual personal control over data
- order: the degree to which developments are planned collectively

The scenarios are deliberately positioned to span a future 'possibility space'. Within each scenario, government, business and society more broadly develop interlinked responses to any particular issue. The scenarios then allow for exploration of the benefits and challenges of the responses.

The RAND Europe team used its Virtual Future Hindsight© process to test the scenarios in a series of seminar gaming events – a method of systematically exploiting the expertise of a wide range of people to understand a problem that contains substantial uncertainties.

The purpose of the scenarios, the gaming and the modelling that underpinned them was to provide tools for people making decisions to help them think through potential long-term consequences and test for robustness against a range of possible futures – knowing that none of the individual scenarios is in any way intended to be a predicted or preferred future.

Figure 2.1 **The three scenarios are set on the outer edge of the future 'possibility space' and are used as a tool to investigate the key factors that may affect cyber trust and crime prevention**



Knowing It All. In the years prior to 2018, the UK's police and intelligence services gained substantial capabilities to access and analyse information on individuals who might pose a threat to national security or be engaged in criminal activities. These enhanced capabilities were achieved through a combination of the consolidation of existing public sector databases, new legislation that obliged the private sector to retain and make available personal and transactional information, and new technologies that allowed this information to be used effectively. Measurable advances were made in the fight against crime on several fronts, and citizens generally approved of the concessions they had to make in terms of privacy. While the benefits of government knowing it all are widely acknowledged, there remain concerns about certain aspects of the present situation. In 2018, trust among individuals is low, and many individuals and firms believe that responsibility for security lies primarily with the state rather than themselves. While it is clear that not all vulnerabilities have been eradicated, reliable information on the nature and scale of those that do exist is missing.

Touch Me Not. Citizens are intolerant of intrusions into their privacy by government and business. Consequently, individuals are taking responsibility for security both online and offline. Cajoled by demanding and discerning customers, businesses are also taking privacy-enhancing technologies and processes seriously. In accordance with the high political salience of privacy issues, large-scale monitoring and surveillance by public authorities is severely curtailed. Vigilance and action by individual citizens and businesses has been effective in fighting certain types of crime, and the increase in individuals' acknowledgement of their responsibilities is generally applauded. However, critics point out that the emphasis on individual responsibility has exacerbated a digital divide, leaving some people more vulnerable than others. Representatives of the police and security services believe that restrictions on their powers to collate and integrate information on individuals unduly inhibit them in combating crime and terrorism. Furthermore, the large amount of private sector surveillance by individuals gives rise to the concern that privacy has been eroded, while the potential gains that could have been made by co-ordinating this surveillance have not been realised.

Frog Boiler. Information and communication technology, including wireless technologies is now an integral part of the activities of individuals, companies and public institutions. After many years of investment, the government still remains unable to provide secure electronic services to its citizens. Today, in 2018, the many faults in these government electronic systems and the management of electronic IDs and digital signatures make citizens very frustrated with these services. Some citizens even called for the reintroduction of paper-based services. Meanwhile, criminals have been increasingly exploiting government ICT systems to commit fraud and cybercrime. Industry has become totally dependent on ICT including wireless technologies. Investments in information security technology and management processes, however, are still limited to 2.3% of the overall ICT budget. These funds are not regarded as sufficient to counter the constant streams of viruses and other malicious software, as well as intrusions carried out by hackers and organised crime. It is now generally acknowledged that the police in the UK are unable to counter criminal activities involving the use of new ICT including mobile technologies. In general, while people see the benefits of electronic services, they also see the associated risks.

Chapter 3 The Evidence Base

Chapter 3

The Evidence Base

This section summarises some of the key findings from the scientific reviews. Unless indicated otherwise, the primary source is the *Science Synthesis.*

Q1 Why and how do people place trust?

Trust (trustworthiness and trusting behaviour) appears to reduce the need for costly control structures and make social systems more adaptable. One traditional view is that trust is the *effect* of good behaviour, and therefore ensuring trust requires that incentives for good behaviour are provided. Another view is that trust is the *cause* of good behaviour and that the best strategy to ensure that people behave well is to trust them, and make clear to them what behaviour is considered acceptable.

From an economic point of view, it may not be the level of trust that matters so much as its distribution. The distribution of trust supports the setting of priorities for establishing trusting relationships and a structure for negotiating the distribution of liabilities arising from interactions. It also does not follow that more trusting behaviour is always better, as higher trust may create more possibilities for crime.

Some research in the fields of human computer interaction and computer-mediated communication has focused on increasing people's trust perceptions, rather than on enabling people to make reasonable decisions about what or whom they may trust in cyberspace. However, there is some empirical evidence about the factors that determine trust (Table 3.1). There are also beginning to be frameworks for thinking about the different bases or tactics to support trust (Table 3.2).

Table 3.1 Factors in allocating trust

Whether users are prepared to trust, and engage in an exchange, depends on a number of factors that characterise the interaction. Factors that have been identified include:

1. The number of actors involved in the exchange (ranging from pairs to potentially millions).
2. The actor type (individuals, organisations, technology, such as an e-commerce website).
3. Whether the trust exchange happens at the same time for all pairs (staggered exchanges create higher strategic insecurity).
4. Whether the user can identify trust-warranting properties.
5. The types of signals employed to communicate trustworthiness (symbols and symptoms of trustworthiness, identity and property signals).
6. The person potentially placing trust, including propensity to trust, knowledge of the situation, prior experience, potential benefits they expect, and the risks they face (enacted as "trusting action") (Riegelsberger et al. 2003)

Derived from Sasse 'Usability & Trust in information systems.*

There is some evidence that people's level of trust in the Internet corresponds to a standard 'certainty trough' model. Those with little experience of the technology have low levels of trust in it or no opinion. Greater experience is linked to a higher level of trust, while those who have most experience tend to have greater awareness of potential risks.

* The source material for this paper is published in full on the Foresight website, *www.foresight.gov.uk*, and will be published in book format in due course.

Table 3.2 Tactics for creating or sustaining trust

Tactic	Description	Costs
Transparency	Allow principal access to hitherto closed processes, black boxes.	Potentially open to creating mistrust, if expectations are too high.
Transfers of ownership	Allow stakeholders decision rights and responsibilities.	Stakeholders may be more reluctant to put in effort than an agent.
Exploiting transitivity of trust	Where a trust network already exists, extend it via transitive (or, on occasion, distributive) extensions.	Neither transitivity nor distributivity are perfect models of trust. Plus this strategy cannot address any bootstrapping problem.[1]
Certification	Create some institutional support for digital signatures, thereby securing provenance.	Institutional structures are contrary to the anarchistic value ethos of the net, and thereby might work to reduce trust. Does not address bootstrapping, as the principal still has to trust the certification system and authorities.
Restriction	Increase trust by policies designed to avoid interaction with the non-trusting.	May be arbitrary. May be over-limiting. Hard to evaluate the efficacy of the tactic.
Formal methods	Use formal methods to avoid dealing with the scruffier parts of the web.	High modelling overhead. Plus the whole development of the web, with its heterogeneous users, has encouraged scruffiness. Many of the richer parts of the web are scruffy.
Calculi of trust	Use formal characterisations of trust relationships to govern when an agent should trust.	Trust, being a second-order phenomenon, is hard to model successfully. Such a system is likely to lack the flexibility inherent in trust.
Interrogation	Submit documents, webpages, etc, to interrogation and scrutiny.	Technology in the early stages.
Knowledge management	Use tools for knowledge management to maintain knowledge bases and keep them accurate, up to date and trustworthy.	High maintenance overheads.

Derived from O'Hara and Shadbolt 'Knowledge Technologies and the Semantic Web'[2]

[1] Transitivity = a relation between three elements such that if it holds between the first and second and between the second and third, it therefore holds between the first and third

Bootstrapping = where a system or process relies on feedback to operate, bootstrapping refers to the act of beginning its operations in the (possibly troubling) absence of feedback in the initial state (cf. 'pulling oneself up by one's bootstraps').

Distributivity = used here to mean in the case of trust, trust is distributive when my trusting each member of a group means I trust the group, and my trusting a group means I trust each member of it.

[2] The source material for this paper is published in full on the Foresight website, *www.foresight.gov.uk*, and will be published in book format in due course.

It is also important to distinguish between reported perceptions of trust and the way in which people actually conduct their lives. There is only a weak empirical foundation for assessing the basis upon which people are prepared to trust others in cyberspace or to trust in the trustworthiness of ICT systems. However, it is clear that they *are* prepared to trust, and in significant numbers – the total value being exchanged as gaming currency in cyberspace in 2001 was estimated as equivalent to the GDP of reasonably wealthy country.

Q2 How do people perceive risk?

There is extensive literature on risk, and perceptions of risk, and several frameworks or approaches (see e.g. Table 3.3). We are in the early stages of creating an evidence base to assess whether people act according to their perceptions of risk or their experience of actual incidents in cyberspace, and how those perceptions and that experience relate to the technical possibilities of risk.

A key insight for tackling issues of risk in the context of ICT, however, is that while technical experts tend to describe risks as chains of cause and event, others tend to see them in a social context of relationships. Their concerns about risk often express underlying values and attitudes to blame, morality, and the value placed on the outcome of an event. This means that disputes cannot necessarily be settled solely by refining understanding of the probability of particular outcomes.

Table 3.3 Perceptions of risk

Risks are generally more worrying (and less acceptable) if perceived:

- to be **involuntary**
- as **inequitably distributed**
- as **inescapable** by taking personal precautions
- to arise from an **unfamiliar or novel** source
- to result from **human**, rather than **non-human** sources
- to cause **hidden and irreversible damage**, e.g. through onset of illness many years after exposure
- to pose particular danger to **small children or pregnant women** or more generally to **future generations**
- to threaten a form of death/illness/injury **arousing particular dread**
- to damage **identifiable** rather than anonymous victims
- to be **poorly understood by science**
- as subject to **contradictory statements** from responsible sources

Based on Bennett. 'Understanding Responses to Risk: Some Basic Findings'. In, *Risk Communication and Public Health*. P. Bennett and K. Calman (eds.), New York, Oxford University Press, (1999), pp. 3-19.

Q3 How are identities established and how are notions of privacy constructed?

There are three classic ways for users to authenticate themselves to a system which may be a computer, network or another individual: something they *own* (usually a token), something they *know* (such as a password) and something they *are* (a personal characteristic, which may be a biometric such as a fingerprint). Combinations of at least two are common.

There are many mechanisms for authenticating identity in cyberspace, but single sign-on, where a user has a single user ID and password across all systems has been a target. There are now single sign-on mechanisms for usable authentication, but any breach means that unauthorised access to any system under that identity is possible. Much current interest is focused on the use of biometrics, and seven

general requirements that a biometric method must fulfil in order to be applicable for authentication have been defined (universality, uniqueness, permanence, collectability, performance, acceptability and circumvention). No currently available technology meets all the requirements to the fullest extent.

The choice of the most usable method depends instead on the characteristics of the user group, the task, and the physical and social context in which users and security mechanisms interact. In practice, the authentication system must be appropriate to the level of need: in particular, it must not be so complex that people don't use it – poor design can mean that users are left to make a choice between complying with security requirements and completing a task. Also, many users are not motivated to comply because they do not believe they are personally at risk or that they will be held accountable for failures.

Discussions about privacy generally presume that 'balance' is the main feature of policy responses to privacy protection. However, some approaches to privacy argue that the notion of balance itself stems from a set of assumptions about the ways in which people behave and society is constructed that is only one set among others that could be adopted. In particular, some argue that the individualistic approach gives insufficient weight to collective or community interests and to the notion of privacy as a social good alongside other social goods. Adopting this latter approach would require a greater focus on identifying the characteristics of the ways in which privacy is distributed, including the different ways in which it is surrendered and retained by different groups, and in the context of different transactions or systems.

The evidence of recent years is that many people are very ready to exchange personal information with a wide range of service providers in return for various price incentives, personalisation and other benefits.

Q4 What are the frameworks for understanding criminal opportunities and what kinds of new opportunities for crime does ICT currently provide?

A standard way of thinking systematically about the conditions necessary for a crime to occur and for ways to prevent it is the 'conjunction of criminal opportunity' model (*see box below and Table 3.4*)

Conjunction of criminal opportunity

Crime prevention can be defined as intervention in the causes of criminal events to reduce the risk of their occurrence and the potential seriousness of their consequences. Causes of crime can be complex and perhaps also remote and fairly weak, but immediate causes are reducible to just 11 generic precursors which act through common aspects of crime situations and of criminals – whether in the real world or cyberspace. This 'conjunction of criminal opportunity' occurs when a predisposed, motivated and equipped offender encounters, seeks or engineers a suitable crime situation involving human, material or informational targets, enclosures (such as a building or a firewall), a wider environment (such as a shopping centre or a financial system), and people (or intelligent software agents) acting in diverse ways as crime preventers or promoters (Table 3.4). Preventative interventions can act by interrupting, diverting or weakening any of these causes. Resources for offending determine what crime preventers are up against, as does the strength of the offender's predisposition and motivation (the casual opportunist versus the terrorist prepared to die for their ideology).

Trust fits into this framework in several ways, including in cyberspace. An Internet shopper who is too trusting may act as a (careless or negligent) crime promoter, as may a system designer. Conversely, to be an effective crime preventer means entertaining a healthy level of mistrust, and being equipped by applications and systems to apply it. Offenders exploit misplaced trust, sometimes to an expert degree, aided by software- and hardware-based resources (for example, fitting 'skimming' devices in cash machines to clone cash cards). In their turn they need to trust their own hardware, applications, and stolen or illegally bought passwords. And trust between offenders is a prerequisite for collaborating in a hostile environment of law enforcers, other predators and rivals for 'turf'. Whether such trust can be established purely in cyberspace or whether criminals have to meet up or get a reference from a trusted third party to learn to trust each other is an interesting point.

Table 3.4 Conjunction of criminal opportunity model

Potential offender:	**Crime situation:**
• presence (including virtual) in crime situation without leaving traces • perception of risk, effort, reward and conscience and consequent decisions • resources for crime (skills, weapons, knowledge, equipment, access to supporting network; Modus Operandi to maximise reward and minimise risk and effort, thereby creating crime opportunity) • readiness to offend (motivation, emotion, influenced by current life circumstances). • lack of skills to avoid committing crime (literacy, social skills) • predisposition to criminality (personality/ ideologically-based)	• target of crime (person, company, government; material goods, systems, information) that is vulnerable, attractive or provocative • enclosure (safe, building, firewall) that is vulnerable/contains targets • wider environment (town centre, airport, computerised financial system) that contains targets, generates conflict; and which favours concealment, ambush and escape over surveillance and pursuit • absence of preventers (people or intelligent software) that make crimes less likely to happen • presence of promoters (people or intelligent software) that make crime more likely to happen – including careless individuals, reckless designers/manufacturers, deliberate fences and criminal service providers

Based on Ekblom, P. (2001-2004) The Conjunction of Criminal Opportunity.
www.crimereduction.gov.uk/learningzone/cco.htm

The 'real' world and cyberspace may be different in profound ways, but research increasingly shows that many aspects of human behaviour remain constant. Most people are likely to find ways of translating conventionally understood norms and practices into cyberspace.

The main types of threat in a pervasive computing environment may be crudely categorised as faults, mischief, crime and terrorism (Table 3.5). The categories overlap but, for the project's purposes, the differences are largely connected with the motivation of the perpetrators, and therefore with the potential solutions or responses.

In terms of crime, ICT can create new criminal opportunities due, among other things, to the large numbers of potential users of the same services, its exploitable complexity and the geographical remoteness between actors.

Table 3.5 Types of threat associated with near-term technologies

Faults

- Generational problems that only emerge after innovation has occurred – such as Y2K
- Major outages from cascading failure
- Major negative emergent behaviours such as programmed trading by agents
- Simple but pervasive bugs in the infrastructure

Mischief

- Viruses, worms, DoS (denial of service) and Hacktivism. There is the inherent problem that the speed of transmission outpaces speed of response
- Script kiddies. Computing allows attacks to be automated, just like anything else
- But such attacks need to be visible to succeed in their own terms and confer peer bragging rights. Detection and response may be easier than when the motivation is fundamentally criminal

Crime

- Parasite/host ecology; tries to stay hidden (e.g. Trojan horse virus), needs the system to operate just well enough to exploit its vulnerabilities
- Always has the initiative in exploiting vulnerabilities
- Insiders have many ways to exploit systems. Outsourcing, and the nature of web services, mean that it is hard to have confidence in all the systems you are relying upon
- Automation makes it worthwhile to use large number of small transactions, and makes it feasible to prepare and launch huge simultaneous attacks
- Data mining can find key target information – criminals can do sophisticated market research
- Action at a distance changes the game

Terrorism

- Visible destruction is the goal
- No need for sophistication in the means
- Critical infrastructure or symbolic services are likely targets
- Exploit confusion – whole areas of societal infrastructure can be attacked to provide cover for the attack

Taken from *Technology Forward Look*

Chapter 4

Some Implications for Discussion

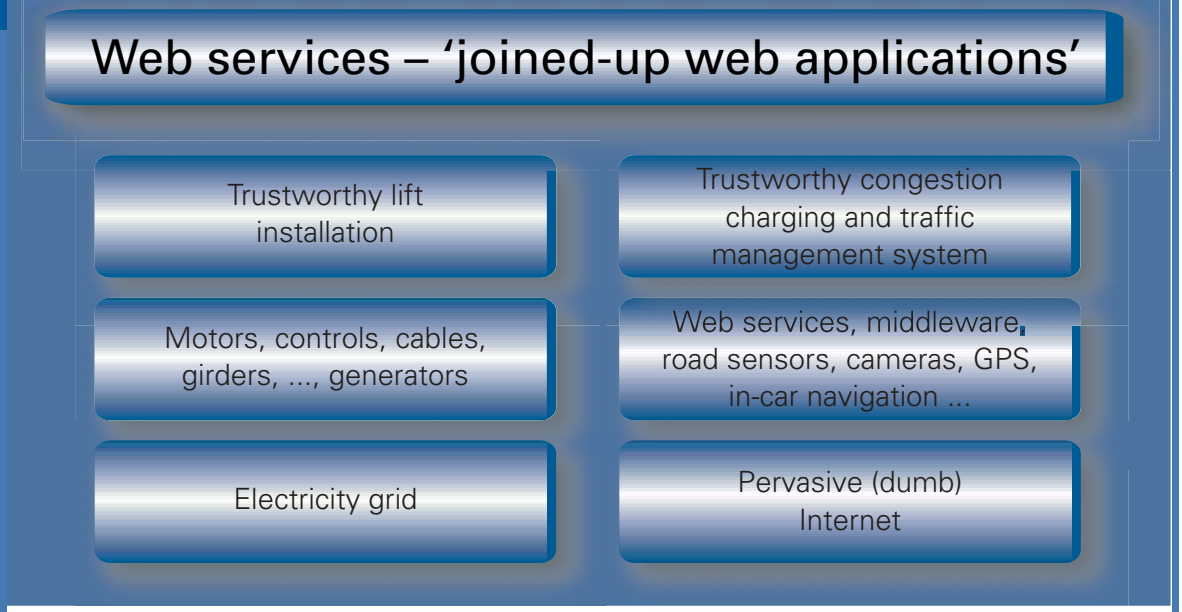
This chapter draws heavily on the seminar gaming process and scenarios reported in more depth in the *Scenario and Gaming Report*, on the *Technology Forward Look* and on the discussions at various expert workshops, as well as referring back to the *Science Synthesis.*

Q5 What will happen to the trustworthiness of complex ICT systems in the future?

The technologist participants in the project took the view that the trustworthiness of complex ICT systems would degrade over time, unless the market developed new mechanisms for enabling trustworthy system design and use. Otherwise the increasing complexity of individual systems and the increasing interdependence of separately designed systems would have unpredictable consequences for system behaviour.

However, complex systems can also display periods of stability. ICT itself is so various in its implications that, in designing solutions, it may be more helpful to think about specifics rather than about ICT as if it were a single issue. In practice, the trustworthiness of new services is likely to vary from case to case. Figure 4.1 compares the way in which the different vertical elements in delivering congestion charging over the web can be compared to the elements in providing a more familiar service, such as the lifts in a building. The trustworthiness of the service as seen by the user is based on assumptions, explicit or implicit, about the trustworthiness of many different sub-elements and operators.

Figure 4.1 Interdependence in familiar and novel applications



From the Technology Forward Look

In creating trustworthiness, as in reducing crime, workshop participants were adamant both that new technologies would continue to provide new solutions (for example, new forms of encryption, or intelligent agent software) and that they would not create 'silver bullets' that would enable perfect trustworthiness or zero crime. There are some fairly constant tensions that arise from basic human existence and these cannot be alleviated completely by any technological solutions.

End users will typically interact with new applications through public or private branded services, with little opportunity to form judgements about the nature of the underlying services and service providers. Where issues of public good are at stake, users are likely to rely on government regulation, as they do now in many aspects of life. One of the findings from the gaming seminars was a resistance among participants to being treated by government as if being a citizen and being a customer were equivalent in their implications for service delivery. Voting is more important than buying groceries; and the systems that enable it to be done online have to reflect this difference.

Q6 What might enhance the trustworthiness of complex ICT systems in the future?

One of the key findings from the scientific reviews was that greater trustworthiness in complex ICT systems requires better software project management (described in more detail in the full *Science Synthesis* paper). In addition, the development and introduction of new systems in a complex environment requires new ways of testing them, particularly more modular testing both of system parts and of system interdependencies.

Participants more generally took the view that for core services, multiple systems are likely to be essential for some time, in some cases, combined with low-technology back-ups. Similarly, for some, services robustness and, hence trustworthiness, might depend on having a diverse range of systems. At its core, getting trustworthy systems and trusting behaviour in the cyberworld depends on having the right levels of skills and information available to both developers and users, and incentives placed on those that have the ability to influence outcomes.

During the course of the project there was considerable discussion about the placement of liability, contractual arrangements for software, the use of privacy-enhancing technologies, regulation and the dynamics of innovation and the successful development and uptake of new services. Hardware and operating systems vendors, and users, have benefited from the existing market structures. Trustworthiness has not been a major issue in the development of new ICT over the last two decades, especially when compared with the importance of new functionality and time to market. Users generally welcomed new applications and, for individuals, the applications were not seen as penetrating far into areas of high personal concern such as financial, health and legal records.

However, some participants took the view that these current models of proprietary systems were at odds with modularity, stability, simplicity and open scrutiny. These requirements were likely to become increasingly important in the future. Some took the view that they were essential for the creation of highly trustworthy systems, especially as aspects of ICT become more commoditised and the balance of benefit moves towards greater emphasis on dependability and security. In that case, the UK and EU might create competitive

advantage by establishing effective standards in areas such as traceability and provenance, that could then be adopted elsewhere. Similarly, without more effective intervention or action to reduce the impact of new vulnerabilities, the risks created might be one of the biggest potential brakes on the deployment of new capabilities.

There was more general agreement that addressing trustworthiness in future generations of ITCs would require different technologies and behaviours from those in place today. In the particular case of the introduction of software agent-based systems and the 'semantic web', some scientific review authors emphasised the need to find protocols that ensured that the software and human agents could find no better option than telling the truth and interacting honestly with each other, acknowledging that each tactic for fostering trust (trust is different from truth) had costs.

Q7 What might enhance cyber trust?

The Internet is evolving. The common values on which it was largely established provided a basis for a certain degree of trust, but also made it vulnerable to those who wished to exploit it and who encouraged crime for the sake of peer recognition. Both of these factors are likely to become less influential as usage becomes more commoditised.

At several points during the project, participants found themselves facing a potential issue in which rapidly changing technologies and behaviours meant that there was little empirical evidence on which to base decisions. In most cases, this led them to the view that arguments should be presented in ways that make clear the ethical implications and positions of the key players, as the best way to enable decision-makers to take acceptable actions.

The emphasis on ethics was linked to an emphasis on process rather than on specific solutions, reflecting a belief that processes based on accepted principles and tools for thought could remain valid for longer than the resolution they generated which might be specific to an application or technology. There are no universal answers but there are universal languages for defining some of the choices and reasoning frameworks for use in critical debates, including those around the construction of crime opportunities, trust, perception of risk and notions of privacy (e.g. as a social good rather than as an absolute right).

The results of the gaming seminars pointed to several implications for those looking to enhance trust and the use of ICT-based services. Participants showed:

- desire for the access to information on self and the greatest possible individual control consistent with the full range of objectives and technological realities, negotiated differently for different services and applications. (These discussions acknowledged the difficulty of delimiting or assigning ownership to 'traffic' information such as that currently generated by mobile phone use, once there are many more such digital transactions for many more purposes, not all of which are likely to require explicit consent in each instance)

- desire for a clear governance structure to detect and react to abuses or failures. Different scenarios generated different governance structures in detail

- willingness to sacrifice some efficiency in core services for the sake either of having multiple systems providing different paths to the same end (i.e. redundancy to provide security) or decentralised systems

- acceptance both of the important role of multiple identities and anonymity (as happens now, for example, with married women who use different names in personal and professional lives, or in the anonymity of our daily cash transactions and of voting); and of the essential necessity of having a single identity linked to an individual for some purposes, especially where the public good is involved

- belief that the issues for the criminal justice system that are raised by the need to collect and use digital evidence are sufficiently difficult that they are not capable of satisfactory resolution by 2018.

See the *Scenario and Gaming Report* for more detail.

Q8 Can we reduce new types of criminal opportunities associated with ICT?

There will be a lot that is old about the new cyberworld. In particular, in discussions of risk and perception of risk, participants felt that there might be a tendency to set higher standards of protection against crimes related to cyberspace simply because the means of committing them are new. Insofar as fear of these crimes is higher because the crimes are new, it might be reasonable to set higher standards, but the trend underlying this approach should be presumed to decrease over time.

In addition to the specific measures to enhance trust discussed in Q5, participants identified two strong themes throughout the project. The first was the importance of making information available, making it easy for people to find it, and acting on its implications to reduce their own vulnerability to crime and preventing their systems being used to harm others. In particular, while the generations currently at school might emerge with a fairly sophisticated understanding of virtual transactions, many people who would be relying on them for decades are already in the marketplace.

There were differing views as to whether growing user experience of faults and criminal opportunities would create sufficient demand for crime-prevention measures to generate an efficient market in them, or whether the existing market structure would have to change. Participants generally took the view that we would need new digital forensic systems for assigning clear provenances to some types of data object and to enable audit trails of users and changes. These factors could be explored more thoroughly in the context of specific decisions or issues using the scenarios.

The second strong theme was that crime prevention was a virtual 'arms race'. The rapid pace of change, innovation and uptake of many new services, and the implications of unintended dependencies, all mean that those trying to reduce crime are having to move more and more quickly to respond effectively. Many of the participants felt that the structures for dialogue between government and business would need to evolve in the future to allow quicker feedback on identifying and responding to potential criminal opportunities. Several of the project's extended group of stakeholders will use the project's findings to explore these issues in more detail as part of the post-project action plan.

Q9 What are the implications for research?

The *Science Synthesis* sets out several research frameworks. The key ones are: social amplification of risk, criminal opportunity models, assessment of impacts on privacy, dependable software engineering and digital forensics initiatives, all of which should be further developed and interconnected to increase our understanding of possible security measures and crime-prevention strategies.

Chapter 4 Some Implications for discussion

Chapter 5

Next Steps

The stakeholders are now committed to taking forward the work of the project.

Working with Foresight they will:

- engage with and reflect on the findings, including carrying out discussions with international audiences
- review key decisions and strategies in the light of the findings
- meet in one year's time to review progress against the commitments to action.

Post-project actions will include initiatives to:

- implement a programme of workshops to apply project material to specific challenges
- collaborate with the Royal Society, Institution of Electrical Engineers, British Computer Society, Information Assurance Advisory Council and other bodies to consider the project's implications
- develop toolkits to help stakeholders think about, communicate and act on cyber trust and crime prevention issues
- contribute to work being carried out by the Council for Science and Technology on the use of large datasets
- consider the implications for research with the Research Councils and other funders
- explore the implications for business and others, building on the extensive range of networks and contacts created during the project.

Chapter 5 Next Steps

Appendix A: List of Science Reviews and Authors

Science Reviews*

1. **Risk Management in Cyberspace** – James Backhouse, London School of Economics and Political Science (LSE), with Ayse Bener, Bosphorus University Turkey, Narisa Chauvidul, LSE, Frederick Wamala, LSE, & Robert Willison, Copenhagen Business School, Denmark.

2. **Usability and Trust in Information Systems** – M. Angela Sasse, University College London.

3. **Confidence and Risk on the Internet** – William H. Dutton, Oxford Internet Institute, University of Oxford & Adrian Shepherd, Oxford Internet Institute, University of Oxford.

4. **The Future of Privacy Protection** – Charles D Raab, University of Edinburgh.

5. **Perceptions of Risk in Cyberspace** – Jonathan Jackson, London School of Economics and Political Science (LSE), Nick Allum, University of Surrey & George Gaskell, LSE.

6. **The Economics of Cyber Trust between Cyber Partners** – Jonathan Cave, University of Warwick.

7. **Knowledge Technologies & the Semantic Web** – Kieron O'Hara – University of Southampton and Nigel Shadbolt, University of Southampton.

8. **Identities & Authentication** – Fred Piper, Royal Holloway, University of London, S Schwiderski-Grosche, Royal Holloway University of London and M.J.B.Robshaw, Royal Holloway University of London.

9. **Trust in Agent-Based Software** – Sarvapali D. Ramchurn, University of Southampton and Nicholas R. Jennings, University of Southampton.

Appendix A List of Science Reviews and Authors

10. **Dependable Pervasive Systems** – Cliff Jones, University of Newcastle upon Tyne and Brian Randell, University of Newcastle upon Tyne.

11. **A Synthesis of the State-of-the-Art Science Reviews** – Brian Collins, Royal Military College of Science Shrivenham, Cranfield University and Robin Mansell, London School of Economics and Political Science.

* The source material for this paper is published in full on the Foresight website, www.foresight.gov.uk and will be published in book format in due course.

Appendix B: Stakeholder and Advisory Group Membership

Stakeholder Group

Hazel Blears MP, Home Office Minister for Crime Reduction, Policing, Community Safety and Counter-Terrorism

Javaid Aziz, Chief Executive Officer, Aspective Ltd

Sir Christopher Bland, Chairman, British Telecommunications plc

Dr David Cleevely, Chairman, Analysys Ltd

Professor Ian Diamond, Chief Executive, Economic and Social Research Council

Sir Kieth O'Nions, formerly Chief Scientific Adviser, Ministry of Defence (MoD), now Director General of the Research Councils, replaced by Paul Hollinshead, Director, Science and Technology Policy and Management, MoD

Leigh Lewis, Permanent Secretary, Crime, Policing, Counter-Terrorism and Delivery, Home Office

Baroness Professor Onora O'Neill, University of Cambridge

Professor John O'Reilly, Chief Executive, Engineering and Physical Sciences Research Council (EPSRC)

Ed Richards, Senior Partner, Strategy and Market Developments, OFCOM, replaced by Peter Walker

Andrew Pinder, Government e-Envoy

Appendix B Stakeholder and Advisory Group Membership

Advisory Group

Dr Jeff Adams, Home Office *

Professor Anne Anderson, Glasgow

Dr James Backhouse, LSE

Professor Brian Collins, RMC Shrivenham.*

Dr Paul Ekblom, Home Office

John Edwards, Lawyer, Herbert Smith

Professor Tony Hey, e-Science

Bryn Hughes, dstl

Martin Ince, Journalist *

Professor Robin Mansell, LSE *

Graham Paterson, IEE

William Perrin, No. 10

Kevin Riordan, Cabinet Office

Andrea Simmons (replacing Andrew Rathmell), IAAC

Bill Sharpe, Appliance Studio

Martin Sadler, HP Labs

Professor Martyn Thomas, Consultant & EPSRC

* = Expert adviser to project

Appendix C: Cyber Trust and Crime Prevention Project Teams

RAND Europe Project Team

Maarten Botterman, Project Leader

Professor James Kahan

Dr Lorenzo Valeri

Dr Jonathan Cave

Dr Robert Thompson

Neil Robinson

Rebecca Shoob

Project Team

Sir David King, Chief Scientific Adviser to HM Government, Project Director

Dr Claire Craig, Director Foresight

John Flack, Project Coordinator

Dr Alex King, Foresight

Christine McDougall, Project Manager

Caroline Meehan, Project Support

Kathryn Waller, Foresight

Dr Miles Yarrington, Project Leader

Printed in the UK on recycled paper with a minimum HMSO score of 75

First published June 2004. Department of Trade and Industry. www.dti.gov.uk