Cyber Security
Knowledge Transfer Network

E·S·R·C
ECONOMIC
& SOCIAL
RESEARCH
COUNCIL

ESRC

ESRC Seminar Series

Mapping the public policy landscape

The economics of information security

Foreword

Future historians may well describe ours as the age in which mankind harnessed the power of computers to store and provide fingertip access to vast and various quantities of data. Computer technology guides and controls the use and flow of information in Government Departments, organisations, businesses ranging from banking to music, and indeed the general public. It has offered dramatic enhancements in efficiency and user friendliness, and its influence for good is increasing day by day.

At the same time, however, the incentive for criminal intervention in each of these areas has grown at a corresponding rate. Moreover our increasing reliance on computerised systems to do business has introduced new vulnerabilities which challenge our expectations of resilience and dependability.

Consequently this seminar, organised by the Economic and Social Research Council (ESRC), the Cyber Security Knowledge Transfer Network (KTN) and Hewlett-Packard Laboratories (Bristol) could not have been more timely.

Adequate controls against cyber-crime and ensuring robust resilience against power failures, viruses and the like both require investment. If stakeholders are to strike an appropriate balance between finance, risk and security the economic basis for decision-making needs to be better developed and understood. In particular, practitioners need to know what constitutes value for investment in the safeguarding of information, and how standard business models can be modified to take account of the need for protection against cyber-fraud.

This seminar brought together leading researchers in the economics of information security and those concerned with its practical application. Participants examined the conceptual and theoretical bases on which decisions should be grounded, shared their experiences and laid the foundation for future exploration and collaboration by setting up a Special Interest Group on the economics of information security.

Professor Ian Diamond AcSS
Chief Executive
Economic and Social Research Council

Cyber Security KTN

The Cyber Security Knowledge Transfer Network (KTN) under the Directorship of Nigel A Jones provides a single focal point for UK Cyber Security expertise and it is free to join. It aims to achieve its mission by providing an environment in which:

- industry, academia and Government (at national and regional levels) can come together to explore key issues in developing secure systems
- views and information can be exchanged to provide integrated solutions, and exploit synergies between existing and nascent platforms
- strategies are formed and markets grown collaboratively
- cross-sector partnerships are built and maintained
- UK expertise in Cyber Security is promoted on a national and international basis.

For example, the Cyber Security KTN in its Special Interest Groups aims to:

- Help users of cyber security technologies and services make better informed decisions as to what they really require in order to protect themselves. Initially this would be done by developing practical metrics for assessing the effectiveness of cyber security solutions in providing protection against changing threats in dynamic business environments; facilitating cost-effective solutions and risk management.
- Help users of large-scale identity management schemes learn from those already experienced in deploying solutions. Initially focusing on the Financial Services sector by studying their previous experience in implementing global and cost effective solutions; seeking to transfer lessons learnt, best practice and identify identity capability and technology gaps.
- Help non-expert users behave more securely in the cyber domain by seeking to understand how to develop and create trust in humans, and how to make risks more tangible.
- Investigate why it is that we still develop code with potential security vulnerabilities when the theory on how to develop code without such coding errors has been available to the community for many years. Then to propose an approach to enabling the software industry to produce higher integrity software.
- Facilitate the benefits promised by Trusted Computing by considering the approach from a user's perspective. Particularly, by investigating the potential applications, benefits, business models and use cases for exploiting trusted computing; understanding the sociological, technological and business environmental barriers to uptake.

The Cyber Security KTN is funded by Government, Regional Development Agencies, Devolved Administrations and the Research Councils. It is managed by QinetiQ, an activity which involves delivering the energy and glue required to achieve critical mass and momentum in order for the KTN to succeed.

The Economics of Information Security

Speakers

The academic perspective

TYLER MOORE Doctoral Researcher, University of Cambridge, joined the Security Group in 2004 as a PhD student investigating social and economic mechanisms as tools for strengthening network security. Research interests include security economics, decentralised network security, and quantifying electronic crime. Prior to joining Cambridge, he studied at the University of Tulsa, identifying several vulnerabilities in the public telephone network's underlying signalling protocols and developing techniques for detecting attacks on the telecommunications infrastructure. Moore is a 2004 UK Marshall Scholar and a US National Science Foundation Graduate Research Fellow.

CHRISTOS IOANNIDIS Professor Ioannidis joined the School of Management of the University of Bath in September 2004 where he is convenor of the Accounting and Finance Section of the School. Previously he was the Head of the Department of Economics and Finance at Brunel University His teaching expertise covers Corporate Finance, Finance and Investment Analysis, International Finance and Financial Econometrics at both the undergraduate and postgraduate levels. Professor Ioannidis' main research themes are a) Asset Valuation Models, b) Financial Market Volatility and c) Financial Markets and the Macroeconomic Environment. He has published a number of papers in the Journal of Forecasting, the Journal of Political Economy, the Journal of Business Finance and Accounting, European Journal of Finance and the Journal of Futures Markets. He has been acting as a consultant to a number of public bodies and private firms (ONS, Defra, First Plus Bank etc) and he has a long term association with other universities and research institutions in the UK and France.

The industrial perspective

DAVID PYM Principal Scientist in the Systems Security Lab (SSL) at HP Labs, Bristol (HPLB) is also Professor of Logic & Computation at the University of Bath, where he has led the development of the Mathematical Foundations research group. Prior to joining HP Labs' permanent staff, he was a Royal Society Industry Fellow at HPLB. Prior to moving to Bath, he was Professor of Logic at the University of London, where he also held an EPSRC Advanced Fellowship. In SSL, he works on mathematical systems and security modelling, using algebraic, logical, stochastic techniques, and services sciences. He leads an HP Labs project – 'Trust Economics' – on systems and security modelling and the economics of information security. Degrees: MA in mathematics (King's College, Cambridge), PhD in mathematical theory of computation (University of Edinburgh), FBCS, CITP, FIMA, CMath, CSci.

BRUCE HALLAS has advised widely for nine years within the private and public sector upon information risk management, assurance, information and IT security management. His career is based in a foundation of legal, financial and marketing experience and qualifications rather than IT skills and training. This drew him early in his career to the conclusion that information security was a business opportunity with negative and positive risk at the heart of any strategy. Currently, through his information security practice Marmalade Box, he is exploring the relationship between economic and social prosperity and information security, techniques for embedding cultural awareness and the challenges faced by the UK's small to medium enterprises in adopting best practice.

Organisations

NIGEL JONES QinetiQ, Director, Cyber Security KTN. Since joining QinetiQ in 2004, he has led a team delivering a consultancy and research business in the domains of security, resilience and intelligence. He has a special interest in understanding and analysing risk environments, the use of intelligence systems to aid decision-making and in the integration of human factors into security systems. Nigel's experience is derived from a military career in Information Operations and the design and delivery of education and training prior to joining QinetiQ.

HP Laboratories Hewlett-Packard is a technology solutions provider to consumers, businesses and institutions globally. The company's offerings span IT infrastructure, global services, business and home computing, imaging and printing.

HP Labs is Hewlett-Packard's corporate long-term research organisation. Its European facility, based in Bristol, represents about 25 per cent of HP's research activity, and conducts basic and applied research in a wide range of areas, including many aspects of information security.

Marmalade Box takes a multi-disciplined approach to the design and delivery of information risk management solutions for small to medium sized enterprises. An independent and BSI approved supplier, they claim a track record of delivering and supplying information security best practice. This includes attention to employee and third party misuse and access through to technical and legal threats and vulnerabilities. Having assessed information security risk, they go on to design appropriate controls, audit and provide ongoing year-round support.

Executive Summary

Introduction

Russia launches cyber attacks on a neighbouring state. China is reported as training thousands in the art of computerised information sabotage. On 7 April 2008 Associated Press said the US Navy is seeking to boost the nation's cyberwarfare capabilities by looking beyond defending the Internet and are developing ways to launch virtual attacks on future enemies. On the home front public confidence in our collective ability to protect private and business information is at an all time low and the concern of businesses, organisations and Government regarding the security and privacy of computerised information is a hot topic.

This concern forms the context in which on Wednesday 9 April 2008 the ESRC, the Cyber Security KTN and HP Laboratories hosted a Public Policy Seminar 'The Economics of Information Security'.

Faced with the practicalities of designing and procuring security solutions, businesses and other organisations struggle to answer a range of questions including:

- How much investment in information security is enough?
- How can expenditure be justified?
- How can value be demonstrated?
- How can the performance of investments in information security be measured? And how can they be adapted in the light of evaluation?

This seminar aims to examine the conceptual, theoretical and practical bases on which such decisions can be grounded. Whilst the largely qualitative risk-based approach is well-developed and practiced by security specialists, the economic basis for decision-making is less well-developed and understood, certainly when security thinking is exposed to more financially driven stakeholders. More specifically, this seminar explores questions such as:

- What are the factors that inform investment decisions?
- Are economic models useful in aiding security planning and decision-making?
- Which models are applicable? For example, the many different approaches to return on investment, guardianship, or stewardship?
- Can economic models be integrated adequately with models of systems, the services delivered by systems, and the behaviours of the many different types of user?
- What are the incentives associated with the many different types of defenders and attackers?
- Is there an economic relationship between defender and attacker?
- What constitutes value in information security? And how can value be measured?
- Can economic models be operationalised sufficiently so that they can be deployed by practitioners?

Information security is now a mainstream political issue. An appropriate regulatory framework is now in process of being devised for the EU and not before time. The direct cost to Europe of protective measures and electronic fraud is measured in billions of Euros. Even greater indirect costs accrue from public concerns about information security that hinder the development of both markets and public services.

A question of trust

Naively, perhaps, we expect computer systems to be trustworthy. We expect them to be resilient and do what is required of them despite environmental disruption, the all too human mistakes of users and operators, even deliberate attacks by hostile interests. We do not expect them to do other things like feeding our personal and business information to unauthorised parties. This is the basic premise that has led companies, organisations and Government to entrust vast and ever-growing swathes of information handling and trafficking to computerised information technology (IT).

Today IT is essential to the day-to-day operations both of Government and business in general. In particular The Internet underpins a considerable amount of global economic activity, permitting huge changes in traditional business models. It has also radically changed the way in which individuals are able to access information, entertain themselves, and even the way in which they meet their partners. It has undoubtedly been, and continues to be, a powerful force for good.

In March 2007 the total number of Internet users world-wide was put at 1.114billion, or 16.9 per cent of the world's population. Internet penetration continent by continent varies from 3.6 per cent in Africa to 69.7 per cent in North America. In the United Kingdom Internet penetration is 62.3 per cent, among the highest in Europe, with growth from 2000–2007 put at 144.2 per cent. Some eastern European countries have seen growth over the same period, albeit from very low levels, of well over 1,000 per cent.

Our personal lives also involve IT in areas ranging from communication with family and friends to online banking and other household and financial management activities. Companies large and small are ever more reliant on IT to support diverse business processes ranging from payroll and accounting, to inventory tracking, sales, and support for research and development (R&D). In short, IT systems are increasingly needed for companies to be able to operate at all.

More fundamentally, critical national infrastructures and networks ranging from telecommunications to those associated with energy, banking and finance, defence, law enforcement, transportation, water systems, and Government also depend on IT-based systems.

In the near future, what has become known as 'pervasive computing' will see IT built into a whole range of everyday objects from cars to refrigerators to enhance their usefulness. We ourselves, already iris-scanned at airports may soon be expected to carry our personal IT-readable identity cards.

Cyber Security today

Many, perhaps most people would see the IT-enhanced future as a rosy one. It goes without saying, however, that the ability to fully realise the benefits of IT depends on these systems being secure. Yet even though a secure cyberspace is vitally important to the nation, cyberspace is far from secure today. We face real risks that adversaries will exploit vulnerabilities in our most critical information systems and indications of the size of the threat, whether associated with losses or damage, type of attack, or presence of vulnerability, indicate a continuously worsening problem. Moreover, reports may even understate the actual scope of the threat, since some successful attacks are not noticed and others noticed but not reported for fear that exposure would weaken the credibility and even the stock value of the victim concerned.

Economic considerations

This last point introduces the pivotal *raison d'être* of this seminar. It has been claimed elsewhere that the systems and technological know-how required to protect us against much of the projected cyber-onslaught already exist. However there may too often be far-reaching financial consequences accompanying their implementation. Any business mover and shaker faced with a request for investment in a new and probably expensive security protocol will first ask when or even whether it is going to pay for itself.

The stakes, however, are high. The potential consequences of a lack of security in cyberspace fall into three broad categories.

- First is the threat of catastrophe – a cyber-attack, especially in conjunction with a physical attack, could result in thousands of deaths and many billions of pounds of damage in a very short time.
- Second is what has been described as a frictional drag on important economic and security-related processes. Today, insecurities in cyberspace systems and networks allow adversaries (in particular, criminals) to extract billions of pounds in fraud and extortion – and this alone is often sufficient to twist the arm of reluctant businesses to expend additional resources to defend themselves against these threats. If cyberspace does not become more secure, the citizens, businesses, and Governments of tomorrow will continue to face similar pressures, and probably on a greater scale.
- Third, concerns about insecurity may inhibit the use of IT in the future and so lead to a self-denial of the benefits that IT brings, benefits that will be needed for the national competitiveness of the UK as well as for national security.

It has often been said that what can be measured can be controlled. Certainly what is thoroughly discussed and researched can produce a better understanding of why cyberspace is as vulnerable as it is. The ESRC/Cyber Security KTN/HP Labs Public Policy Seminar on the Economics of Information Security provided a valuable forum to explore how, given the necessary economic incentives, new technologies and policies can be implemented, making cyberspace safer and more secure.

About 8.3million American adults were victims of identity theft in 2005, according to the Federal Trade Commission. About 3.3million adults experienced misuse of non-credit card accounts, slightly edging out the hijacking of credit cards, which was suffered by about 3.2million Americans. Some 1.8million victims found that new accounts were opened or other frauds were committed using their personally identifying information. About ten per cent of people in the most recent survey said thieves got at least $6,000 worth of goods or services.

ID fraud in the UK increased by 70 per cent in the past year with 170,000 people reporting stolen identity.

The way forward

If we are to achieve anything more than laying speed bumps in the path of the cyber criminal's juggernaut we may need a different way of thinking about the means by which secure systems are designed, developed, procured, operated, and used. This new approach would entail new directions in education, training, development practice, operational practice, oversight, liability laws, and Government regulation.

As things stand we are a long way from meeting this goal even though the deployment of cyber-security measures that are quite unsophisticated can make a significant difference against casual attackers. If individuals and organisations collectively adopted current best practices and existing security technologies, individuals and the nation itself would experience a very significant heightening of cyber security.

It has to be said, however, that even assuming that everything known today was immediately put into practice, the resulting cyber-security posture would still be inadequate against today's threat, let alone tomorrow's. To close this gap, one of the key things we need is an extension and amplification of our approach to research.

> A good solution to a cybersecurity problem is one that is effective, resilient against a variety of attacks, inexpensive, cost effective and easy to deploy, is easy to use, and does not significantly interfere with the function of the system of which it interacts.

Traditional research tends to be problem-specific but problem-by-problem or even problem-class by problem-class solutions, are unlikely to be sufficient to close the gap by themselves. Unorthodox, clean-slate approaches will also be needed to develop new ideas and new points of view that revisit the basic foundations and implicit assumptions of security research.

Research is needed both to develop new knowledge and to make such knowledge more usable and transferable to the field. Cyber-security threats are evolving apace and continuous defensive research will always be needed. The corollary of this is that such research must be seen to have a status and underpinning support structure sufficient to attract the highest order of personnel.

The intellectual rewards can be high. Professor Ross Anderson of the Computer Laboratories, University of Cambridge has spoken elsewhere of the delightful insights provided by convergence between disciplines as diverse as war games, micro-economic theory and the topology of complex networks and its use in the analysis of information security. His colleague Tyler Moore spoke at the seminar of security failure being caused at least as often by bad incentives as by bad design. People who connect insecure machines to the Internet do not bear the full consequences of their actions. Professor Christos Ioannidis of the University of Bath highlighted the powerful tools that economic theory could bring to the security problem. Professor David Pym of the Security Lab at Hewlett-Packard Laboratories analysed how information systems are embedded in their economic environment and Bruce Hallas of Marmalade Box introduced us to the practicalities involved in persuading small and medium enterprises to adopt good information security practice.

Laurie John, TVSF Consultants

The Economics of Information Security

This keynote presentation was given by Tyler Moore on behalf of Professor Ross Anderson, both of the Computer Laboratory, University of Cambridge. Tyler Moore emphasises that security failure is caused at least as often by bad incentives as by bad design.

Over the past few years the economics of information security has become a thriving and fast-moving discipline. The motivation for this is that technical explanations for security failure are often insufficient. Economics can explain many of the failures and challenges in a new way. As companies are beginning to realise the value of good information security practice so security measures are being used not only to manage the evils of the attackers but also to support the business models of companies. However we need to increase the amount and value of information available to consumers in making decisions about security of one product or service versus another.

Information security (IS) is now a mainstream political issue, and can no longer be considered the province of technologists alone. People used to think that the internet was not secure because there was not enough of the right technology, not enough sophisticated cryptographic mechanisms, authentication or filtering etc so advanced encryption, public key infrastructure and firewalls were added but the internet did not get any safer. About 1999 it became clear that even the latest and greatest technology will not solve all our problems. There is a different explanation at work: incentives.

Misaligned incentives

As well as collecting data on what fails and how, security economists have discovered that systems often fail not for some technical reason, but because the people who guard them, or who could fix them are insufficiently motivated.

> In the USA, when a customer disputes a card transaction, the bank must either show that the customer is trying to cheat or offer a refund. In the UK, banks tended to claim that their ATM system was secure so the customer must be mistaken. Yet UK banks spent more on security but suffered more fraud. Economists call this a 'moral hazard effect'. UK bank staff knew that customer complaints would not be taken seriously so they became careless. This led to an avalanche of fraud.

Often they are not the ones who suffer when things go wrong. Again, legal theorists have long known that liability should be assigned to the party that can best manage the risk. But what do we find?

- Distributed denial service attacks where viruses infect machines. The users of the machines often do not know about it, but their machines are used remotely to target other people.
- Health records: Patients suffer when hospital system initiators put the simplicity of the IT system and its access to researchers above the value of patient privacy.
- Bank customers suffer when poorly designed systems enable phishing to happen and make fraud easier.
- Casino websites suffer whenever they are hit by denial of service website attacks and extorted for ransom.

Insecurity is often what economists call an 'externality' where an individual's actions can have harmful side effects on others rather than on the first party who takes a decision about security. An example of an externality in the wider world is environmental pollution. "Externality is a nasty market failure that may in some cases require Government intervention and regulation," Tyler Moore says, " but the problem with this is that Governments may not know what to do any better than business so you have to be very careful when you are treading through regulation."

Security as a business strategy

IS security regulations are starting to be used for new purposes. For example printer manufacturers like Hewlett Packard have a business model where they sell printers at a loss and try to regain the profit by selling printer cartridges. Price sensitive consumers appreciate not paying a lot for the printer initially but they do not appreciate having to shell out £30 a month or so for a new ink cartridge so third party companies started providing cheaper replacements. This necessitated the development of a security mechanism to authenticate the printer cartridge to the printer. "I'm not saying this is wrong," Tyler Moore says, "but this is reality. Businesses are starting to use security mechanisms in order to further their own strategy."

In digital rights management there is an unintended consequence of imposing a security rights mechanism. The record companies were pushing for using digital rights management to restrict access to digital music. Apple developed their own digital rights management tool format and iTunes has now become the most popular store. Too late the record companies found they were getting a raw deal because Apple had become the dominant player in the music industry and they could dictate prices.

The digital rights mechanism favoured Apple because it stifled competition. If you have 1,000 melodies on your iPod when that iPod needs replacing you will buy a new iPod so you can seamlessly transfer your music collection. It would be difficult to switch to a competing product like, say, the Windows coded media player. So we have to be careful how we look at security mechanisms and how they play out in the market.

The economics of IT

What is it about the economics of IT that differs from traditional industries?

- Network effects. The value of a network depends upon the number of users it has and its value increases superlinearly whenever you add more users.
- High fixed and low marginal costs. You have to pay a lot of money to develop the first copy of that new operating system. You have to pay the programmers. But once you have developed the product it costs you next to nothing to develop the next one. So the marginal costs are near zero. In a competitive industry that will drive prices down making it hard to regain capital investment so you have to have legal protection: patents to protect the recuperation of capital investments.
- Switching costs. A big point is that switching costs determine the value. (Shapiro-Varian theorem: The net present value of a software company equals the total switching costs.) Suppose you are running a company that uses Office or some software product and you are trying to decide whether you should upgrade to the next version or switch over to some competing product. You have to estimate the cost of switching to this new system including retraining every user to adapt to it. This consideration determines what price Microsoft can charge you for upgrading to the next version. If it is going to cost you more to switch to the competing product then you've just got to stick to who you've already got. That sets the price point. A similar argument, as we have seen, applies to digital rights management.

What does this mean for security? All these factors: high fixed and low marginal costs, network effects and switching costs can lead to dominant-firm markets with big first-mover advantage. Time to market is critical. The first company to offer a new service to the market and get people to adopt it gets dominant market share. Because they are dominant it becomes hard to switch to someone else. This means the market rewards fast movers. So Microsoft's initial policy of shipping out products before they were completely security verified was quite rational because at that point they were still building up market share. It is easy to blame Microsoft but whichever company was faced with this predicament they would have done the same.

> "The Microsoft philosophy of 'We'll ship it Tuesday and get it right by version 3' is not perverse behaviour by Bill Gates; it is quite rational."
>
> *Ross Anderson*

If you are trying to build a dominant firm in the IT industry you also have to appeal to the vendors of complementary products. Microsoft had to appeal to the application developers. That means making the programming interfaces as easy and uncomplicated as possible. Security mechanisms and security Application Program Interfaces are very onerous and this explains why you didn't see very extensive security APIs for early versions of Windows but you do see it now because Microsoft has gained the entrenched position.

Information asymmetry

Adverse selection and information asymmetries are technical terms in economics and indicate why security problems are far from straightforward.

George Akerlof won the 2001 Nobel Prize for Economics for analysing markets with asymmetric information

Nobel Prizewinner George Akerlof is best known for his article, "The Market for Lemons: Quality Uncertainty and the Market Mechanism", (*Quarterly Journal of Economics* 1970) in which he identified certain severe problems that afflict markets characterised by asymmetrical information. He used as a metaphor the used car market:

I have a high quality used car worth $2,000.

He is offering a low quality car of the same model for $1,000.

Buyers cannot tell one from the other so they refuse to pay $2,000.

I will not sell for $1,000. He will.

Result: the market gets flooded with low quality goods.

Ross Anderson has argued that the software market is like this. There is a similar asymmetry of information about the security of products. Vendors may say that their software is very secure, but it is often difficult for consumers to tell whether or not this is so. So because they cannot believe the claims they refuse to pay a premium for high security claims so the market will not spend money on providing it. This forms a vicious circle leading to insecure software in the market.

How can we reduce this asymmetry of information? You could have the software claims evaluated and adopt certification. Another more controversial approach is to establish a vulnerability market. (Schechter 2002.) You establish an open price for an undiscovered vulnerability and reward software testers (hackers) for identifying it. You increase this offer over time and as the price rises discovering vulnerabilities becomes more attractive. If you have a very insecure product where new vulnerabilities are released every day then the market price is going to be very low. If you have a secure product the price gets high enough to where it will attract investment and you can use the resulting market price as a signal as to the security of the software.

WabiSabiLabi is an organisation aiming to bring the world closer to zero risk by providing better rewards for security researchers and organising an efficient and transparent marketplace. Its laboratory and senior security professionals, Switzerland-based, are nation independent and will begin by replicating and validating researchers' findings. It promises to provide a solid set of services, professional and editorial, to customise the distribution of the newly created intellectual knowledge to individually fit the different client's (institutional, business, security companies, vendors) needs.

Quasi-markets have been created for vulnerabilities but the practitioners do not publish their prices so you cannot obtain a market signal. In any case their business models are sub-optimal from a societal perspective because they will only disclose vulnerabilities to people who pay them for this information. Moreover they have an incentive to disclose vulnerabilities in order to harm non-subscribers to pressure them into paying for this information. Nevertheless, perhaps organisations like WabiSabiLabi may one day help us move towards an actual market for vulnerabilities by encouraging the sharing of pricing information, Tyler Moore says.

Adverse selection

Many Internet users cannot tell whether the website they are visiting is safe or not. One of the ways in which some companies have tried to self-regulate this and overcome this asymmetry of information is to pay a company to do some checks (all they may actually do is check whether you have a privacy policy). If you pass you can put a certification seal on your website. This indicates to consumers that this is a reputable company.

The problem with this is that bad companies are more likely to pay for the certification. A Harvard study shows that bad companies distributing malware, for example, are twice as likely to have one particular seal as good companies. "So if you see this certification seal you run away because you can't trust it at all!" Tyler Moore says.

This is what economists call 'adverse selection'. Another example is the insurance market where sick people are more likely to buy health insurance.

Regulatory options have been suggested for overcoming adverse selection. These include:

- Require certification authorities and search engines to devote more resources to policing content.
- Assign liability to certification entities if certifications are granted without proper vetting.
- Alternatively, regulate enforcement by requiring complaints to be published.
- Search engines could be required to exercise 'reasonable diligence' before agreeing to advertise.

"Do not click on ads."
Ross Anderson

The Harvard study also finds searching for a product like a screen saver on Google by using the search bar is far safer than clicking on one of the ads that accompanied the search. The moral is, do not click on ads and be careful in balancing business models for advertising compared to what actually happens in the market.

What role does policy have in strengthening security?

The new EU level Government agency ENISA has commissioned a report 'Security Economics and the Internal Market' on the policy options regarding the economic problems in providing information security. The authors are: Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore.
http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm

ENISA is a body set up by the EU to carry out a very specific technical, scientific or management task within the 'Community domain' of the EU: a **'European Community Agency'**. These agencies are not provided for in the Treaties. Instead, each one is set up by an individual piece of legislation that specifies the task of that particular agency.

The Agency's **Mission** is essential to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union.

Before we can get to a point where we are able to say "this is a good investment for our telecoms company, say, we need to know what attacks are actually happening and what harm they are doing," Tyler Moore says. So our first recommendation is for the EU to issue a comprehensive breach notification law which exists in some American states. This is good for consumer rights because it notifies consumers when their details have been compromised so they can take appropriate protective action and also it helps align the incentives for the companies to protect their data because they know disclosure will happen. It also provides lots of good data on breaches and when they happen so we can say something intelligible about the likelihood of it happening in the future and perhaps even insure against it happening.

Similarly we need to collect better statistics on losses in the financial industry because electronic crime is hitting the financial industry most. We need better statistics so we can know for example how effective chip and pin has been and was this a worthwhile investment in terms of reducing fraud.

The final verdict on chip and Pins

By Experian
February 14 2008

This Valentine's Day sees the second anniversary of the switch from signing for our **credit card** payments to using chip and Pin cards – but has the new system prevented criminals from counterfeiting our details and using our hard-won credit?

The answer from APACS, the UK payments association, is yes – but that fraud is far from dead and we should not drop our guard.

"The main aim of chip and Pin was to reduce fraud in the shops and it has succeeded – the cost fell from £218million in 2004 to £72million in 2006," said Sandra Quinn, director of communications for APACS.

Fraud on lost and stolen cards has also fallen, dropping by 15 per cent in the first half of 2007, compared to the same period in 2005, as cards without Pins are difficult to use in the UK's high streets and shopping centres.

Spring cleaning the Internet

The final problem is how can we clean up the Internet? "The Internet has a lot of bad stuff going on right now," Tyler Moore says. There are lots of botnets and lots of consumer machines that are infected, web-servers are compromised and host phishing sites so how can we mount a defence? Some ISPs are a lot better at cleaning up their bit of the internet than others but the environment is uncoordinated. Each ISP has to respond individually to requests for clean-up of machines when they are notified so the overall security of the internet as a whole is down to the weakest link: the one ISP that doesn't respond to requests.

Where there are lax ISP practices, attackers move in and compromise machines. The first step to remedying this is to publish good data on the amount of bad traffic that is emanating from ISPs throughout Europe. This ISP is emitting this much spam from this many ISP addresses or this many bots and this is the response time from the ISP whenever they are notifying on average. This procedure would shine some light on the situation so we can identify which ISPs are performing better than others.

This in itself is not going to be enough. Internet security is also characterised by negative externalities. Malware affects machines but the machine is not necessarily the main victim. The victim is the machine's neighbour whenever it sends out spam or whenever he hosts a phishing site or has a denial of service attack through some botnet.

New Botnet. 7 April 2008 http://it.slashdot.org/article.pl?no_d2=1&sid=08/04/07/1421228

"Storm is no longer the world's largest botnet: Researchers at Damballa have discovered Kraken, a botnet of 400,000 zombies – twice the size of Storm. But even more disturbing is that it has infected machines at 50 of the Fortune 500, and is undetectable in over 80 per cent of machines running antivirus software. Kraken appears to be evading detection by a combination of clever obfuscation techniques that hinder its detection and analysis by researchers."

So the users have no incentive to clean up their machine because they may not even realise anything bad is happening. The ISP's best response is to quarantine the infected machines and clean them up remotely but this is very expensive and while some of the better ISPs do it, some don't. Furthermore the ISPs themselves are not necessarily harmed that much by the actions of their users; it affects other ISP customers. Which brings us back to incentives.

Conclusions:

Liability and responsibility to act should rest with the entity that is best positioned to take action and in this case it is the ISPs. ISPs are the gate-keepers to the internet and they are in a unique position to first of all detect that there is a problem with one of their consumers' machines and second to take action to quarantine and initiate practices to clean up the machine.

Incentives explain the behaviour of end users and this in turn explains all the problems we have with security. The key to going forward is measuring security incidents in a more calculated way and we need to take action to deal with the externalities. Only then will we be able to overcome all these information security problems.

Research Agenda in Information Security Economics

Christos Ioannidis, Professor of Finance at the School of Management, University of Bath points out that if security specialists like his colleague at Bath, Professor Pym (q.v.) seek to bring economics into the equation, they should be aware that they are entering the realm of a discipline that is highly analytical and has a powerful methodology which thrives on hard data.

Economics is an imperialist science, in that it tries to claim the territory of all sorts of other social sciences. Unlike other fields of research in social sciences and business schools, economists and finance researchers abide by the following fundamental principles:

- Optimising behaviour. People normally know what is best for them and will not deliberately give up a profitable opportunity.
- There is no free lunch. For everything you do you must give up something and you had better measure what you are giving up in order to support optimising behaviour.
- Scientists are always demanding better answers to the most sophisticated questions and here statistical methodology econometrics offers a very powerful tool. It can be used for forecasting, simulation and testing hypotheses regarding behaviour.

Each of these principles needs to be applied to any consideration about information security.

Information Security under the microscope

"As an outsider I don't know what information security is" Professor Ioannidis says. "It looks something that the experts know but they cannot really define. How do we measure information security? How do we say whether it is going up or down? How does it evolve over time? The only thing we know is that something did not work so we can say there was a security breach. We must begin to define it."

Key questions:

- Is IS fundamental? Does it have an existence of its own or is it an amalgam of particular intrinsic characteristics or attributes that link together to give some kind of an index? (The most important attributes would be confidentiality, integrity, and availability. CIA.)
- If it is not fundamental, it is an amalgam, a construct.
- If it is a construct, how do we construct it?

The relevant equations demand answers to the following questions:

- Do we simply add the characteristics up by some weight that will depend upon the organisation?
- Do we try to put in some kind of bench mark over and above which we consider each characteristic is desirable?
- Do we think the attributes have specific trade-offs which are measurable?
- If we believe that IS is a construct of fundamentals how are these fundamentals related?
- To what extent do these fundamentals differ across organisations, is there sufficient technical ability to combine them?
- We need to be able to write down an index, 1,2,3, -1–2 –3 etc. and work out whether increasing an attribute necessarily increases the index.
- What is the interaction of the attributes with the overall security index. This is where behaviour as well as technology comes in.

All this has to be taken into account in constructing a meaningful benchmark. Without a benchmark it is difficult to see whether you are winning.

Widening the picture

We need to identify the categories that the experts see as constituting information security, then use the technical expertise of engineers and risk managers to tell us how to construct the index. Then we can evaluate whether we are making progress or not. Otherwise, given that there may be an intrinsic tendency for under-investment in IS, there may seem insufficient incentive to invest.

The second item on the agenda is how do we as consumers, as individual users of IT understand information security and does this match the way the organisation views it? To what extent is information security a public good for the individual, but not for the organisation? Are there any incentive structures to bring these two points of view together in a mutually consistent way?

It is costly to the individual to invest in IS but the individual does receive a pay-off from the IS of the system. So do we optimise for the individual? Or do we construct an incentive structure that we optimise over the whole of the organisation? The maths show that total IS investment from open loop optimisation where everyone looks after himself is lower than if you have some kind of collusive optimisation. Economics can help devise a better incentive structure that co-ordinates individual and organisational needs.

Allocating the budget

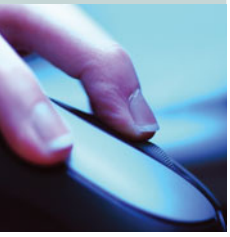
Both organisations and individuals spend money on preserving the integrity of their own system. How do we know whether the spending follows some rule or is a random reaction to a random event?

We can derive mathematically an explicit relationship between degradation and investment in IS. There are two factors: First the engineering of the system because different systems will have different vulnerabilities. Second, the system priorities. The nature of the organisation that ranks appropriately CIA will dictate which it values most. (If you are Amazon, availability is everything. Within these three fundamentals, confidentiality, integrity and availability, Amazon would probably value availability more than integrity).

Now we can begin to understand our own behaviour against threats given our own preferences. We can derive explicit causal relationships between IS and investment in IS given the system priorities, design, and the nature of the threat. We can determine how to spend our investment.

There are three outlets for investing: people and training people, processes and the associated technology. How do we allocate and optimise the budget between these three?

There will not be a unique solution. The answer will depend on the preferences and the state of the organisation: the network structure, management objectives and technical characteristics. Organisations will have to find their own optimal portfolio structure to invest in these three outlets. Meanwhile, can we offer them any advice?



Just give us the facts

In theory, yes, but to do so we need data. We can define the categories we think are important as suggested by the theory and use them to derive causal relationships and rules without which we cannot provide quantitative advice. But without adequate data the only thing you can do is to offer ad hoc solutions to problems as and when they occur and it is difficult to formulate a public and a private policy.

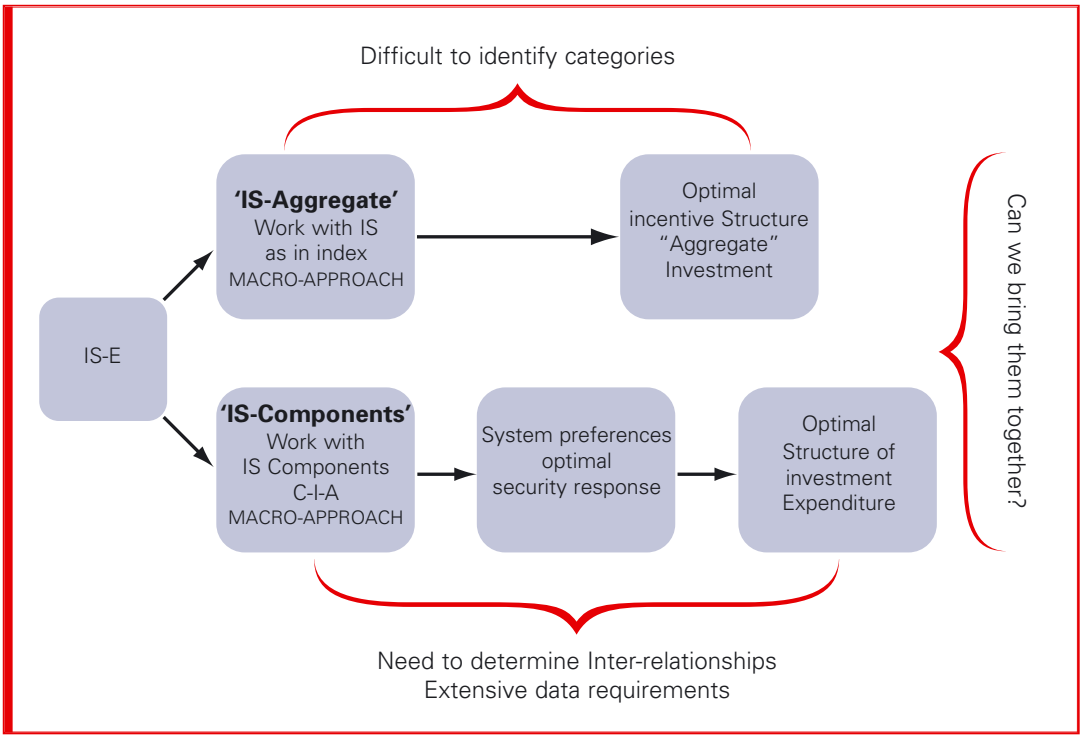
However, data collection has a lot of problems. Unlike economics and finance where all the data is available albeit at a price, this is not the case with IS. The data needed may be sensitive and the organisation concerned may not wish to reveal it.

To construct a repository of information one could, perhaps, set up a journal like Information Security Economics where all papers that are dealing with applied work must provide the data. (Any journal would have to provide pure data stripped from all identity to protect confidentiality.) That would slowly build a data bank that could be used by further research. Until then nothing is replicable so it is not proper science. However the process must not be too slow because the data might not be stationary, that means it might be driven by some technological process which changes, so the data might not have enough memory to be used.

The problem is difficult but it must be solved. Unless we can use data to make predictions and test the predictions out, we are left with pure conjecture.

Can we use existing experiences to anticipate information security needs? This would require some solid statistical work to see whether the data can provide description, whether the data is stationary, and other functions and only then would we get some serious predictions as to possible attacks. So again, we need to collect and analyse the data.

Figure 1: Research Paths



Research strategies

One can identify two broad strategies of research:

1. **The Macro approach.** IS used as a loosely defined index. This leads to an optimal incentive structure (a theoretical approach) and policy recommendations. It gives us broad suggestions about aggregate investment. The problem has been formalised but it is difficult to pin down exactly what we must do. If we need detailed quantitative information we need

2. **The Micro approach.** We look at the components of IS, ask if and how they are related and see how the system preferences and the stochastic attacks combine to define the optimal response of the system to a particular or expected threat. Given the possible evolution of security threats we can then say this is how you should share out the investment.

The micro approach requires some fairly tight theory to examine data relationships and it requires a lot of data, but this is provided by experiment. Psychologists and other social scientists observe the management of systems to define preferences rather than have economists theorising and putting parameters in simply to solve the problem. In understanding system preferences and the optimal security responses we need to refer to the people who actually work in the area.

Bringing all these factors together will not be easy, but it is worth striving for because in economics, all macro is based upon micro principles. So micro information can give us something big to say about security of information.

Meanwhile, there is a lot of good academic literature to point the way.

Information Security Economics: A Systems Perspective

Professor David Pym approaches the economics of information security from the practical standpoint of the Systems Security Lab at Hewlett-Packard Laboratories, Bristol. His concern is with how systems are embedded in their environment and what sorts of environments we have to consider when dealing with IS and its investment issues.

"What is information security economics about for industry?" Professor Pym asks. "We need IS because bad stuff happens. But it's not just bad guys attacking us, it is things happening because of bad combinations of events compromising services. Typically people and organisations are paying for the provision of services and they get pretty fed up when those services fail to operate because of some security issue."

What is the point of departure for companies like HP to be interested in IS? Customers say "We don't know how much to invest in IS. Tell us how to assess our risk then we can work out how much to invest." This is a naïve posture. To discover why, we need to define our terms.

- Services are delivered by systems. People like Amazon ask us to deliver a big complex service with database etc. But a system is more than the computers and software. It has a variety of types of components.
- These systems are being delivered not in isolation but to make money for someone; for example the supplier who is delivering the software and the kit.
- What are systems? They have a technical core, but to deliver a service, systems have to have all sorts of interactions with people.
- Systems are embedded in an economic environment and are subject to threat.
- Threat implies the need for security.
- Security has been defined as making sure that just the right people have access to just the right information at just the right time. (Mike Wonham, HP.)

System interactions

The core of a baggage handling system is a conveyor belt with some software but it has a variety of interactions with all sorts of complicated things.

If you go to check-in at Terminal 5 you have to give your bag to someone who has to put the right piece of paper on the handle, put it on the right conveyor belt to go down to the right sorting area and it has to land up on the right flight.

The integrity of everything has to be maintained. You don't want bombs to appear magically between you and loading onto the plane and this all has to be done in the context of the airline trying to make some money.

Once we are clear about our system we can consider how it can be safely and securely embedded in its environment which includes its economic environment. We have to understand how to protect various properties we might care about such as confidentiality, integrity, and availability (CIA). Different organisations are going to have different priorities with respect to these concerns.

With the baggage handling system, availability means availability of the bag at the right place at the right time. You also have to ensure that the terrorist does not have access to it while it is on its way and that those who do have access will put it onto the right plane at the right time. You end up having access to it again at the end.

If you are an organisation like Amazon, you are very concerned about availability. Every hour your system is down is going to cost you an awful amount of money. You care a bit about confidentiality. One of the strengths of your brand if you are Amazon is that you have never had a report of a compromised credit card. Integrity of records is a lesser issue in situations like this provided promises are honoured with high probability.

Given this understanding, how does an organisation operating a system go about ensuring that its choices are realised by a security policy? Policies embrace investments in people, process, and technology. How do we decide what is the right balance of investment against these three in order to achieve the required profile of protection against the threat environment? That is the economics of security problem: how to balance those kinds of investments. It is by no means the only problem.

"It would be easy to think that all this was just about micro-economics. It is not." Pym says. "Lots of the concerns we have are about understanding the aggregate of consequences of the facts: how it is that different aspects of the problem aggregate to affect other aspects of the problem. It's entirely reasonable to believe that many of the techniques from macro-economics may be useful. The central bank's setting of interest rates may influence inflation and the unemployment profile and this can provide an analogy for how investments in information security will affect the trade-off between, say, the confidentiality and availability of information."

> "Security policies are intended to promote and enforce an organisation's priorities."
>
> *David Pym*

Major customers come to HP and say "You are providing us with all these systems and services. Tell us how much to invest in various kinds of security operations and how to do it. How much do I have to invest this year?" To understand how to answer, you have to understand the broader economic questions.

Risk assessment

How much to invest this year is a risk assessment. What kind of threat do I expect to be exposed to and with what probability will certain kinds of threats occur and therefore what kind of investment is appropriate against those kinds of risks.

We can use all kinds of accountancy based methods, NPV, RoI, ALE etc to come up with assessments of risk but they all depend on inventing some probabilities that certain events will occur. Invent is a good word because we just do not know what those probabilities are. "People talk about the lack of data and how good it would be to have more," Pym says. "We don't have the data and without the data it is very difficult to work out what the probabilities should be. This problem is not going to get solved in a hurry so we have to come up with another approach."

In order to understand the risk it is necessary to understand how that system or service relates to the economic and threat environment that it inhabits and to take on board the priorities assigned to CIA by the particular organisation. We need to understand the technology, the people, the economic environment and the threat environment.

The Trust Economics project

Fortunately mathematics provides tools for understanding these things. The critical thing is to integrate our understanding of the behaviour of users, the properties of the system and the driving economic rules. Then we can use modelling and simulation to enable us to understand how it is that a threat environment impacts upon a system in its economic context. We will understand how different stochastic representations of the threat environment for a particular system will behave.

"Note that this is not inventing probabilities for particular events," Pym says. "I am letting probability theory do the job for me and understanding the consequences of a particular system architecture in a particular threat environment and using that relationship to predict what will happen."

This endeavour, known as the 'Trust Economics' project is supported by the UK's Technology Strategy Board (about £1.7million over three years including industrial contributions). The Partners are: HP Labs, Merrill Lynch, University College London, University of Bath, and the University of Newcastle. The Project explicitly aims to integrate the understanding of systems, user's behaviour and economic environments in the context of security.

"This is pretty exciting but how are we going to make some money out of all this?" asks the ever-practical Professor Pym. "It is critical to move from a world in which security is added on as an afterthought to one in which it is a core part of system design. This will enable a more reliable delivery of service, strengthen the business process and so add value."

The value of security within the UK SME Sector

In his presentation, Bruce Hallas of Marmalade Box discusses the need for small and medium enterprises (SMEs) to embrace the economic benefits of improved SI practice.

While the corporate side of our economy is increasingly embracing the need for better information security, within the SME sector this need is poorly understood by business owners and managers. How important is this? The contribution of the SMEs is not just significant, it is absolutely critical to the economy moving forward.

According to the DTI:

- There are 4.5million businesses in the UK.
- 99.3 per cent employ 0-49 employees.
- They comprise 58.9 per cent of the total workforce of 24.4million.
- They account for 51.9 per cent of the £2,600billion UK turnover.

If we took the SME sector out of the equation a sizeable chunk of the UK's turnover would be non-existent.

What is the future contribution of the SMEs?

SME contributions:

- Driving force behind innovation
- Starting point for many entrepreneurs
- Corner stone of UK economic stability and growth especially in the knowledge based industries
- Much of the UK's R&D and university spin-outs comes from SMEs.

Oak trees start from small acorns but there are a lot of acorns that stay small. National policy for economic growth has a key focus on trying to promote small businesses in terms of start-up and development, and investment in support organisations has risen substantially in the last couple of years.

However, the Achilles heel of any business is cash flow. Income against expenditure. SMEs in general fail to understand how information security affects cash flow and how it affects profitability. This failure is partly due to the language we use. A lot of good messages are being transmitted but they are not in a language that the SME sector understands. Terms like risk management, compliance, information assurance, mean virtually nothing to the SME sector. So people lose interest straight away.

In theory, information ability, confidentiality and integrity (CIA) are critical. In practice there is often a gap between this theory and the practice within the SME sector. To bridge this gap we ourselves must be clear about the terms we use and their economic consequences.

Information Security Below Line Benefits

Key factors

- Operational loss
- Breach of contract
- Breach of statutory obligations
- Customer loss
- Damage to reputation

Operational loss:

The financial loss due to an information security incident leading to a breach in delivery of the operation of an organisation. This includes productivity loss: having a team of staff unable to access their system when the finance director is adding up the cost on a daily basis. It is a straight-forward argument. There is no science; it is in the books but many SME managers still need to be shown how to do it. Also opportunity costs arising from the amount of down-time in cleaning up the incident.

Breach of contract:

SMEs often outsource their risk management strategy although accountability still lies with them. For one SME, Marmalade Box developed a model for claiming back some of the cost of supplying security when the supplier was not actually managing the risk properly and, on applying this model, the SME was in a position to recoup.

Breach of statutory obligations:

In the face of criminal activities against security vulnerabilities, criminal legislation enables investigations to take place, interviews with employees, removal of equipment for analysis – all will disrupt the operation of a business.

Customer loss:

When there is a breach of security a UK customer generally does not find out about it. But if they were to and, as has been suggested, we consider the adoption of disclosure laws similar to those in the States customers might decide not to do business with that organisation. Yet with TK Maxx, initially there was a backlash but then people still kept shopping at TK Maxx. This raises separate issues regarding the behaviour of consumers who still want to do business with an organisation whether or not have they have IS in place.

Damage to reputation:

The loss of 2million customer details would probably justify further investment in IS but the loss of a small number would not. Yet the principle of IS is the confidentiality of data whether it is regarding one person or one million. This raises an interesting social/economic question.

In the context of business to business transactions, then reputation could well be an issue.

Information Security Above Line Benefits

Key factors

- Market differentiation
- Increasing the existing value proposition
- Additional service/product offering
- Greater margins and retaining profitability

Specific markets are coming under increasing pressure regarding statutory compliance. Also there is social pressure from consumers who now expect security to be in place because they are adopting more leading edge technologies that have potentially more vulnerabilities. Now for the first time there is even political pressure since the HMRC event led to a swing in the polls, which led to IS gaining a raised political profile.

Market differentiation:

If you as a supplier can clearly show that you have good IS practices you can provide a level of assurance which is rare in the UK. But if an SME can make good IS practice demonstrable to people who don't understand the jargon, it can differentiate itself in the market.

Increasing existing value proposition:

If an SME has done a good IS job it should tell its customers, not just sign a confidentiality contract. If it does, it may be able to charge more and the value proposition between the two organisations could thereby be enhanced.

Additional service/product offering:

In the UK the best assurance you tend to get is something within the terms and conditions. "As a trained lawyer I can tell you one thing about terms and conditions. They are only of any value when something goes wrong," Hallas says. Customers appreciate the fact that nothing is completely secure. Mistakes will happen. But what they want to know is, do *you* know that they are happening; are you in control? Show them that you are by, for example, an audit report and that audit report can become a tool which you can sell as a product.

Bridging the gap

Speak to small and medium sized businesses and they would agree that the foregoing two sections provide full, unassailable justification for investment in IS, Hallas says, yet when you go and look at an operational level, it is not there. Why is there this gap? Obviously it is the fault of the management team.

The priority of most management teams is about earning money and keeping their operating costs low. They do not understand the impact on their business of an IS incident even though the average cost of a security incident has gone up by 25 per cent. Until they do understand they are not going to push IS up the agenda.

Unfortunately SMEs have limited resources. IS practitioners are neither abundant nor cheap. So given that they have been fed the idea that IS is a feature of IT SMEs go to IT as a much bigger and cheaper pool of resource.

> "In our reaction to initial security incidents we looked for a solution rather than understanding what the problem was. We're dealing with the hangover now. We continue to foster the misconception that it is about IT."
>
> *Hallas*

Having sidelined the problem to IT, management teams think they have dealt with the technical threats. Yet the biggest vulnerability lies with people. People who do things maliciously or by accident.

Meanwhile their competitors are demonstrating the implementation of IS best practice, and they are not, so they are losing the competitive edge and may not be able to secure that next contract. All this depends on the ability and experience of the management team.

> ISO 9000 is rapidly becoming the most important quality **standard**. Thousands of companies in over 100 countries have already adopted it, and many more are in the process of doing so. Why? Because it controls **quality**. It saves money. Customers expect it. And competitors use it.
>
> ISO 9000 applies to all types of organisations. It doesn't matter what size they are or what they do. It can help both product and service oriented organisations achieve standards of quality that are recognised and respected throughout the world.

> *ISO* is the *International Organization for Standardization*. It is located in Switzerland and was established in 1947 to develop common international standards in many areas. Its members come from over 150 national standards bodies.

"The SMEs are going to feel the squeeze," says Hallas. Within corporate UK the pressure will come through ISO 9000. This standard will also impact on the SME sector.

The other pressure will be the fact that at a political level there is an increasing recognition of the fact that protection of the consumer is weak. National Consumer Council's Ed Mayo wants increased protection. But passing new laws does not make protection any better because most companies cannot afford to take organisations to court. In any case the only reason we seem to need more legislation, according to the Chamber of Commerce, is that we have poor implementation of acknowledged IS best practice anyway.

What do we need most?

Data. Reliable and independent sources of information on threats, vulnerabilities and likelihood of occurrence. With enough data we could spot the trends and predict the onset and development of threats to the SME sector.

Means of reporting the cost savings. Clients lose substantial sums because of virus problems. Logs, can identify which viruses are critical to the business. By bringing the log information and the impact together one can assess what level of IS investment is appropriate.

Effective market and statutory pressure. However, you can have as much regulation as you want but if you are not enforcing it, it is not beneficial.

Business support organisations. "It is worrying to see that among the organisations that support the SME environment, the Chambers of Commerce etc the message continues to be IT," Hallas says. "Yet the people who advise those organisations know it is not about IT. Also they are not putting the arguments forward for the economics of IS and coming up with a business justification."

Education. SMEs need to know what IS means to their organisation in terms of £sd. "When they do, I can guarantee that you will see a shift in the philosophy of adoption of IS," Hallas says. They also need to be able to analyse and conduct risk assessment. ENISA is currently trialing a new risk assessment approach which takes risk assessment down from weeks on end to four days which in terms of the impact upon SMEs is significant. Above all, in the information and knowledge-based economy, SMEs will need to treat and manage information security like any other asset.

Meanwhile the Cyber Security KTN is doing valuable work on identifying what threats are out there. We need to go further and ask not only about the technology of the threats but why people do them in the first place.

Finally it is heartening to find that the emphasis of Government at the moment is that a lot of what is going to happen in the growth of the UK is not coming from big corporations so much as from the innovation, the bright ideas and the entrepreneurial flair of the SMEs turning small acorns into big oak trees.

Discussion

The discussion opened by questioning the value of Confidentiality, Integrity and Accessibility (CIA) as touchstones for information security best practice. First they were not independent but interacted with each other. Neither were they all-encompassing. The man in the street was likely to be predominantly interested in confidentiality but other factors such as reliability were also significant.

As far as the economics were concerned the leading question was "are you in the private or the public sector?" The private sector was concerned about the cost of IS. In the private sector it was "all drawn out of the revenue". Also a private company will be far less likely to divulge sensitive information. It may not even be wise to reveal that they had been successful in defending against a specific attack!

Categories of investment variables offered included people, process and technology but over and above this was choice of system architecture. Get this wrong and no amount of expenditure on firewalls, for example, would produce any benefit. Processes were generally seen as central especially if this category was broad enough to include authentication (of season tickets, for example).

When there is a breach of security, who is liable? The equipment or software provider or the user? A comprehensive and understandable legal framework needs to be drawn up. (The USA may be moving towards a consumer's bill of rights regarding security.)

Finally the need for more data was re-emphasised. Not only that, but there needed to be more cooperation between data holders and data analysts. In practice, in the rush to set up a project data collection is the last thing on people's minds. We need to set up a system where likely problems are formulated and analysed before even thinking about solutions and we need to establish a route for sharing information. This in itself would furnish data. There is no quick fix to the data problem but "Perhaps the KTN or the ESRC could be instrumental in this," a delegate said.

Key findings and conclusions

- **What are the factors that inform investment decisions?**

Theoretical factors include asymmetric information and adverse selection. Confidentiality, integrity and availability (CIA) are critical. This is increasingly being taken on board by large organisations but SMEs too often fail to understand how IS affects cash flow and profitability. Also they may not have the resources to pay for security specialists and mistakenly farm out the problem to IT.

- **Are economic models useful in aiding security planning and decision-making?**

Yes. Economics can explain many of the failures and challenges in a new way.

- **Which models are applicable?**

The economics of IT differ from traditional industries, for example in having high fixed and low marginal costs. Nevertheless the science of econometrics offers powerful analytical tools to information security problems.

- **Can economic models be integrated adequately with models of systems, services and user behaviour?**

Work needs to be done on this. However, already as companies begin to realise the value of good information security practice so security measures are being used not only to defend against attacks but also to support their business models.

- **What are the incentives associated with the many types of defender and attacker?**

Security economists have discovered that systems often fail not for some technical reason, but because the people who should be concerned with their security are inappropriately and insufficiently motivated. Research is still needed on why attacks are instigated.

- **What constitutes value in information security and how can it be measured?**

Key factors include market differentiation, increasing the existing value proposition, additional service or product offering, greater margins and retaining profitability. Means of reporting the cost savings are under active development and have been successfully applied.

- **Can economic models be operationalised sufficiently to be used by practitioners?**

Strangely enough, industry seems hopeful whereas the economists themselves feel a lot of work has to be done. What is certain is that economic analysis of an IS problem can prevent basic mistakes being made.

In addition to these considerations, statutory policy has a major role in strengthening our security posture, provided it is given teeth.

The overarching requirement, however, is for the development of a procedure for gathering hard data on information security attacks and defence in such a way that it does no harm to the organisations that supply that data. The Cyber Security KTN expects to be active in this area.

Every journey needs a beginning and this seminar pointed the direction towards heightening the deployment of improved information security.

Sources and resources

- Workshop on the Economics of Information Security (WEIS), Dartmouth College, Hanover, NH, USA, June 25-27, 2008 http://weis2008.econinfosec.org/
- *Security Economics and the Internal Market* http://www.enisa.europa.eu/pages/analys barr incent for nis 20080306.htm
- Cambridge Security Group blog http://www.lightbluetouchpaper.org/

Tyler Moore's home page

- http://www.cl.cam.ac.uk/~twm29/

Christos Ioannidis' home page

- http://people.bath.ac.uk/ci200/

For an expert exposition of the technical issues in IS:

- Anderson R (2001) *Security Engineering* – J. Wiley

For an influential model in optimal investment in IS:

- Gordon L.A. Loeb M.P. (2005) *Managing Cyber-Resources: A Cost Benefit Analysis* McGraw-Hill
- Willemson J (2006) *On the Gordon and Loeb Model for Information Security Investment*

For a model of under-investment in IS:

- Garcia A, Horowitz B (2006) *Potential for Underinvestment in Internet Security: Implications for Regulatory Policy*

For the modelling of cyber risks

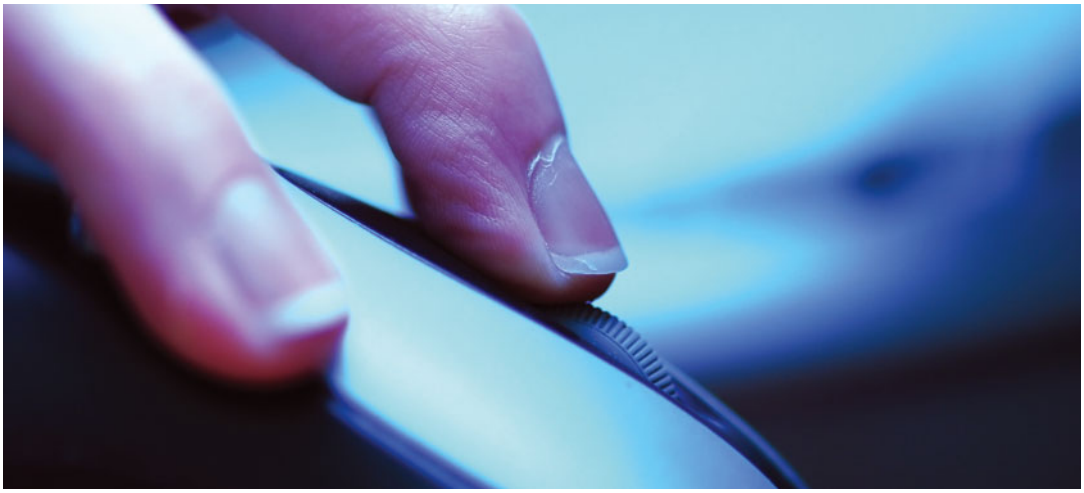
- Bohme R, Kataria G (2006): *Models and Measures in Cyber Insurance*

For the econometric application of the impact of IS breaches

- Arora A et al (2004): *Impact of Vulnerability Disclosure and Patch Availability – an Empirical Analysis*

For the incorporation of the IS components tradeoffs in IS modelling:

- Beautement et al (2008) *Modelling the Human and Technological Costs of USB Memory Stick Security*



Acronyms and abbreviations commonly used in Information Technology

AES Advanced Encryption Standard

APACS Association of Payment and Clearing Services (UK)

API An **application programming interface (API)** is a source code interface that an operating system, library or service provides to support requests made by computer programs

APWG Anti Phishing Working Group

ATM Automatic Teller Machine

Botnet **Internet bots**, also known as **web robots, WWW robots** or simply **bots**, are software applications that run automated tasks over the Internet. These tasks can often be criminal in intent

B2B Business-to-business

B2C Business-to-consumer

BSI Bundesamt f¨ur Sicherheit in der Informationstechnik (DE)

CERT/CC Computer Emergency Response Team (Co-ordination Center)

CGEA Community General Export Authorisation

CIWIN Critical Infrastructure Warning Information Network

CNI Critical National Infrastructure

DDoS Distributed Denial of Service

DES Data Encryption Standard

DG Directorate General

DRM Digital Rights Management

EAL Evaluation Assurance Level (of the Common Criteria standard)

EMV Europay, Mastercard and VISA (a standard for chip card payment systems)

ENISA European Network and Information Security Agency

EPCIP European Programme for Critical National Infrastructure Protection

EULA End-user License Agreement

GCHQ Government Communications Headquarters (UK)

GPS Global Positioning System

ICT Information and Communication Technology

IDABC Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens

IDS Intrusion Detection System

IP Internet Protocol

IRC Internet Relay Chat

IS Information Security

ISAC Information Sharing and Analysis Centre

ISP Internet Service Provider

ISTR Internet Security Threat Report

IT Information Technology

IXP Internet Exchange Point

LHS Left-hand scale

MLAT Mutual Legal Assistance Treaty

MLS Multilevel Secure

MSSP Managed Security Service Provider

NACE Nomenclature of Economic Activities (an industry classification)

NATO North Atlantic Treaty Organisation

NGO Non-governmental Organisation

NIS Network and Information Security

NSP Network Service Provider

ODF Open Document Format

OECD Organisation for Economic Co-operation and Development

OEM Original Equipment Manufacturer

OMA Open Mobile Alliance

OS Operating System

PDA Personal Digital Assistant

PIN Personal Identification Number

PISCE Partnership for ICT Security Incident and Consumer Confidence Information Exchange

PKI Public Key Infrastructure

PNG Portable Network Graphics

R&D Research and Development

RFID Radio Frequency Identification

RHS Right-hand scale

SCADA Supervisory Control and Data Acquisition

SIM Subscriber Identity Module

SME Small and Medium Enterprise

WGA Windows Genuine Advantage (an anti-piracy tool)

Further information

Cyber Security Knowledge Transfer Network
www.ktn.qinetiq-tim.net/

Hewlett Packard Laboratories Bristol
www.hpl.hp.com/bristol/

Marmalade Box
www.marmaladebox.com/

The Economic and Social Research Council is the UK's leading research and training agency addressing economic and social concerns. It aims to provide high-quality research on issues of importance to business, the public sector and Government. The issues considered include economic competitiveness, the effectiveness of public services and policy, and our quality of life.

The ESRC is an independent organisation, established by Royal Charter in 1965, and funded mainly by the Government.

Economic and Social Research Council
Polaris House
North Star Avenue
Swindon SN2 1UJ

Telephone: 01793 413000
Fax: 01793 413001
www.esrcsocietytoday.ac.uk