Internet Safety and Security Surveys – A Review

Edited by:
Robin Sharp
Informatics and Mathematical Modelling
Technical University of Denmark

November 2007

Kongens Lyngby 2007
IMM–Technical report–2007–21

Technical University of Denmark
Informatics and Mathematical Modelling
Building 321, DK-2800 Kgs. Lyngby, Denmark.
Phone +45 45253351, Fax +45 45882673
reception@imm.dtu.dk
www.imm.dtu.dk
IMM–TECHNICAL REPORT: ISSN 1601–2321

Abstract

This report gives a review of investigations into Internet safety and security over the last 10 years. The review covers a number of surveys of Internet usage, of Internet security in general, and of Internet users' awareness of issues related to safety and security. The focus and approach of the various surveys is considered, and is related to more general proposals for investigating the issues involved. A variety of proposals for how to improve levels of Internet safety and security are also described, and they are reviewed in the light of studies of motivational factors which affect the degree to which such proposals are successful. The report concludes with a summary of areas in which more research appears to be needed.

Contributors

This report has been produced by the ***CIT-AWARE*** consortium:

Robin Sharp (Technical University of Denmark)
Lisa Gjedde (School of Education, University of Aarhus)
Helle Meldgaard (DK-CERT/UNI-C)
Preben Andersen (DK-CERT/UNI-C)

and was prepared and edited by Robin Sharp.

Further details of the ***CIT-AWARE*** project can be found on the website:

`http://www.cit-aware.dk`

Acknowledgements

CIT-AWARE is a project within the research program on citizens' ICT-security, *"Borgernes IT-sikkerhed"*, supported by the Danish Strategic Research Council. The participants in the project express their gratitude for this support.

Contents

Chapter 1

Introduction

When the Internet was first developed, its users were predominantly a small community of technically educated people who had an experimental attitude to this new mode of communication, were willing to accept a certain amount of risk in exploiting it, and could evaluate the dangers inherent in various activities which relied on its use. The main focus in the original design of the Internet was to provide a convenient set of simple services which were relatively resilient to failures in the communication network. Safety and security were not considered especially important issues.

During the 1990s, the situation changed radically, due in particular to four developments:

1. **New services:** A long series of new, more complex services began to be offered to users of the Internet. Many of these services were intended to support applications such as banking, commerce or civil administration, or to support the establishment of social groups such as meeting fora. For such applications, security failures could have severe economic or personal consequences for the parties involved.
2. **Malware:** Malicious persons began to develop malware – software deliberately intended to breach security in computers in which it was installed. Such malware could easily be distributed via e-mail or offered via websites to which unsuspecting users could be attracted. In many cases the users might even be unaware that the security of their computer system had been compromised so that, say, their personal data could be read by outsiders or their system could be used to perform attacks on other computers.
3. **Exploitation of unsafe behaviour:** Criminal elements began directly to exploit Internet services such as e-mail and chatrooms in order to perform criminal activities which they would previously have performed off-line, such as making paedofile contacts to minors or obtaining personal information by social engineering. Such activities seldom rely on technical security breaches, but instead exploit users' poor understanding of what constitutes safe behaviour on the Internet, where it in many contexts is possible to hide one's true identity.

4. **Inexpert users:** As a consequence of the usefulness and ready availability of the new Internet services, large numbers of people with no technical background and no understanding of the risks involved began to use the Internet.

The obvious implication of these four developments is that safety and security issues have become more important, at the same time as the users of the Internet in general have become less competent at dealing with these issues. This is a very troubling implication, since it may lead to a general lack of confidence in the use of the Internet, as a result of incidents which expose ordinary citizens to financial fraud, impersonation, sexual harassment or other unpleasant experiences. Studies of risk perception [62] have shown that even a small number of (real or imagined) incidents may have profound effects on public perception of a technology, so the consequences of even small breaches of security should not be underestimated.

1.1 Investigations into Internet Safety and Security

A considerable number of investigations have been performed in an attempt to discover the extent to which this new state of affairs is – or is likely to become – a real rather than just a potential problem. Roughly speaking, these investigations fall into three groups:

1. Studies of the actual incidence of Internet security incidents and the extent to which counter-measures are deployed, indicating the general risk due to failures of Internet security.
2. Studies of the actual incidence of unpleasant user experiences, indicating the general risk due to unsafe behaviour.
3. Studies of user awareness of ICT safety and security issues and users' actual behaviour when using the Internet.

The term *risk* is here used in the technical sense, to mean *the chance, in the quantitative sense, that a hazard occurs* [67] and causes some harm. Note that this is an objective definition of risk, and must not be confused with *perceived risk*, which involves social factors such as public attitudes, credibility and personality.

Quantitative estimation of the (objective) risk can be approached in a very large number of ways [67], and the approach used in practice depends strongly on traditions within the domain being investigated. In the area of ICT security, the traditional view is that harm occurs when a *threat* is realised against some weakness in the system, known usually as a *vulnerability*. Such vulnerabilities can be of a technical nature (for example, a design error in the operating system makes it possible for code from a computer virus to be executed on a user's computer without the user's knowledge) or of a socio/psychological nature (for example, it is possible by sending a suitably worded e-mail to persuade the recipient to open an attachment which actually causes code from a virus to be executed).

How much harm occurs in practice depends on the level of threat in relation to the behavioural and/or technical measures deployed to counter the threat. The *level of threat* is in the context of ICT security generally defined as the product of the frequency of attempts to exploit the vulnerability and the consequences of a successful attempt. The relationship between these concepts is often visualised in terms of the matrices shown in Figure 1.1: A high threat level (red area, left) arises when the consequences of successful exploitation of a vulnerability are high, and the frequency of attempts to exploit the vulnerability is also high. A high risk (red area, right) arises when the threat level is high and the level of deployed counter-measures is low. The yellow areas indicate medium levels of respectively threat or risk, and the green areas low levels.

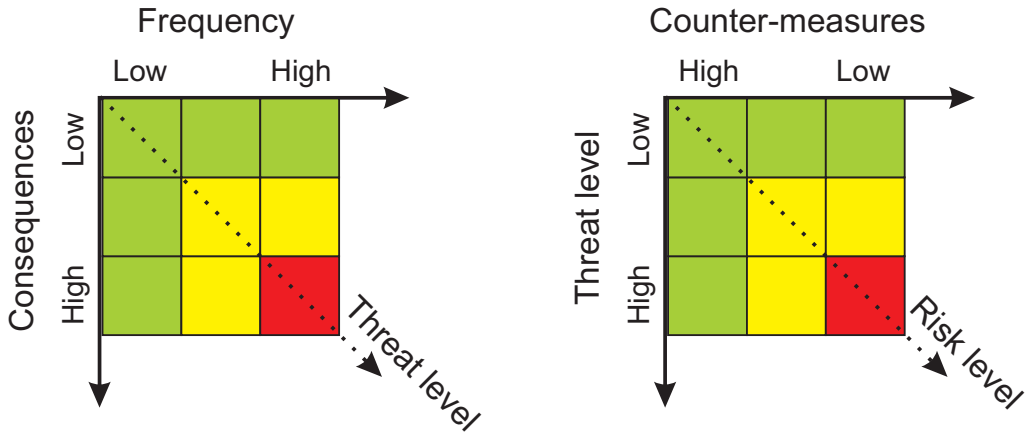

Figure 1.1: Matrix for evaluating level of threat (left) and level of risk (right) in the domain of ICT security

In principle, a high level of awareness should lead to a decreased risk, and thus to less harm occurring, because the users demonstrate more appropriate (i.e. safer or more secure) behaviour – in the terms used in the risk level matrix, they deploy more or better counter-measures. In reality, however, this is not necessarily the case, since the users may lack the technical competence to improve their level of security or may fail in practice to follow the principles which they know to be the right ones. Many studies therefore distinguish between three levels of safety and security:

1. **Knowledge:** The user knows of the existence of a potential problem with respect to safety or security – for example, she knows that a computer virus may be spread by e-mail.
2. **Understanding:** The user understands how to deal with a safety or security problem – for example, she knows that a virus scanner can be used to detect and remove vira from incoming e-mail, and knows how to install and set up such a scanner.
3. **Compliance:** The user acts correctly in order to avoid a safety or security problem – for example, she in fact installs and sets up a virus scanner to detect and remove vira from incoming e-mail.

Several of the studies have also, directly or indirectly, been associated with campaigns intended to increase users' knowledge of ICT safety and security issues, to disseminate information which

leads to better understanding, or to encourage more appropriate behaviour and thus a higher degree of compliance.

1.2 Structure of the Report

The purpose of this report is to review some of the most important national and international studies, and to comment briefly on relevant campaigns. Many of the studies and campaigns which we have included are elements in national programmes for increasing ICT security in general, and are therefore repeated at regular intervals. Where this is the case, we will in general only give a reference to the most recently available version in the open literature.

The overall structure of the report is as follows: In Chapter 2, we review a series of studies of Internet security in general, including surveys of actual security practices, actual vulnerabilities and security failures and actual concerns about security in various segments of society. In Chapter 3 we consider studies of Internet safety. These include not only a number of studies which have focussed on the extent to which users – especially children – engage in unsafe behaviour, and possibly experience unpleasant incidents as a result, but also studies of psychological phenomena associated with Internet use or misuse, including sexual abuse via the Internet and Internet addiction. In Chapter 4 we turn to the topic of safety and security awareness, where there have been a small number of surveys which have specifically aimed at determing the level of awareness in various segments of the population. In Chapter 5 we consider a number of proposals for improving safety and security, starting with general proposals and guides for how to conduct awareness campaigns, and then reviewing some existing campaigns. Since it is evident that human users do not always follow the good advice of such campaigns, we end this chapter with a summary of relevant research into the motivational and other psychological mechanisms which affect people's actual behaviour with respect to safety and security. The report concludes with some tentative conclusions and a summary of areas where there are unanswered questions which could generate new topics for research.

Chapter 2

Surveys of Internet Security

The studies considered in this chapter have been concerned with various aspects of Internet security in a general sense. This includes surveys of actual practice in companies or among the general public, surveys of technical vulnerabilities, and surveys of what various segments of society consider to be important requirements with respect to Internet security. All the studies have been traditional quantitative investigations, based on the use of questionnaires.

2.1 Actual Practice

In many Western countries, there is an established tradition for investigating the level of ICT security via surveys of the general public or of commercial or public institutions. The questions asked typically relate to one or both of the following areas:

- **Practice:** What have the respondents done in order to achieve an appropriate level of security, either by deploying technical counter-measures or by applying behavioural policies?
- **Failures:** What failures of security have been observed, in the form of successful hacker or malware attacks, Internet-based crime, failures to follow internal security procedures, unpleasant personal experiences or other similar indications of lack of security?

The successful execution and subsequent usefulness of surveys of this type seem to depend to a considerable extent on the existence of a formal organisation, involving the major stakeholders, for organising the surveys at regular intervals – and for subsequently disseminating the results. In such an organisation, the stakeholders feel they have some motivation to keep up to date with what is happening in the security world. When such an organisation is not present, the surveys tend to be less systematic and the "difficult questions", such as the number of successful attacks observed in the course of a year, tend to be avoided.

Three examples of countries which have published regular surveys of ICT security at a relatively high level of detail are:

1. **France**, where the surveys are currently organised by CLUSIF, (*Club de la Sécurité de l'Information Français*), an association with about 600 industrial enterprises and public institutions as members. CLUSIF's surveys extend a long tradition started in France by the FFSA in the 1980s.
2. **USA**, where the surveys are organised by CSI, (*Computer Security Institute*) in collaboration with the FBI Computer Crime Squad. The CSI is an association with more than 600 members, and has been performing annual surveys since 1996.
3. **Germany**, where the surveys are currently organised by the BSI (*Bundesamt für Sicherheit in der Informationstechnik*). This is a federal government organisation with a mandate to improve ICT security in Germany. Their surveys include data from several sources. The BSI itself carries out surveys of ordinary citizens, while data about enterprises and public institutions are largely taken from the surveys performed by the technical newletter *<kes> – Die Zeitschrift für Informations-Sicherheit*, which produces bi-annual surveys for its readers.

It should be noted that these surveys are not entirely comparable, due to their varying scope. In particular, there are two different viewpoints of what constitutes an ICT security failure. The narrow viewpoint is that only successful malicious attacks should be considered, while the broad viewpoint is that failures attributable to non-malicious occurrences such as mistakes by the respondents' own personnel, hardware failures, fire, flooding and so on, should also be included.

2.1.1 France

The French organisation CLUSIF customarily carry out separate surveys of security practice and cybercrime. The most recent published survey of security practice is from 2006 [10], and relates to the year 2005. It covers three major areas of French society in which IT plays an important role. The respondents were:

1. 400 companies of at least 200 employees. This represents about 7% of the total number of such companies in France.
2. Civil administrations in 50 areas of at least 30,000 inhabitants (about 15% of the administrations of this size).
3. 186 hospitals of various sizes (about 17% of the public hospitals in France).

The respondents were chosen at random from the relevant areas of society, and were not specifically members of CLUSIF (who might be assumed to have a level of security which would be higher than average).

75% of the companies and 68% of the civil administrations stated that they were strongly dependent on IT, in the sense that a breakdown of more than 24 hours would have serious consequences

for their activities, while 23% of companies and 28% of the civil administrations could stand a failure lasting up to 48 hours. For the hospitals, the level of dependency on IT depended on the size of the hospital, being significantly higher for large hospitals (> 500 beds) than for small ones (< 200 beds).

The CLUSIF survey is particularly interesting because it is specifically related to ISO Standard ISO/IEC 17799:2005[1] on best practice in the area of IT security. One of the main intentions was to discover the extent to which the respondents followed the principles of this standard. Accordingly, the questionnaire used in the survey was structured in a manner reflecting the structure of ISO/IEC 17799, and contained questions related to 10 of the main topics covered by the standard:

5. Security policies.
6. Security organisation.
7. Asset management and risk identification.
8. Personnel security.
10. Management of communications and operations.
11. Access control.
12. Acquisition, development and maintenance.
13. Security event management.
14. Continuity management.
15. Conformance.

Topic 9 (Physical security) was deliberately omitted.

For most of these topics, there was very little difference between the three groups of respondents taken as a whole. However, it was noticeable that large companies, administrations and hospitals were considerably better prepared in relation to ISO/IEC 17799 than their smaller companions. This means they were more likely to have a formal security organisation, a formalised security policy, an organisation for dealing with security incidents, plans for ensuring business continuity and so on.

The CLUSIF survey takes the broad view of what constitutes a security failure. Failures were observed to occur at almost the same rate as in the previous (2004) survey. Occurrences of the most common failures (those observed by at least 10% of the respondents in at least one group) are shown in Figure 2.1. Interestingly, only one of these is due to malicious attacks, namely infection by vira. Other forms of attack were observed by 5% or less of the respondents. This probably reflects the high percentage of respondents who had deployed anti-virus software, anti-spam software and firewalls. On the other hand, the large number of ordinary thefts and outages due to causes other than malware or hacker attacks indicate that awareness of more traditional forms of IT security needs to be maintained at a high level.

CLUSIF's latest report on cybercrime [11], published in January 2007, relates to events in 2006. It gives a review of some major cases of cybercrime, in France and elsewhere, which had been

[1] Subsequently renumbered to ISO/IEC 27002:2005.

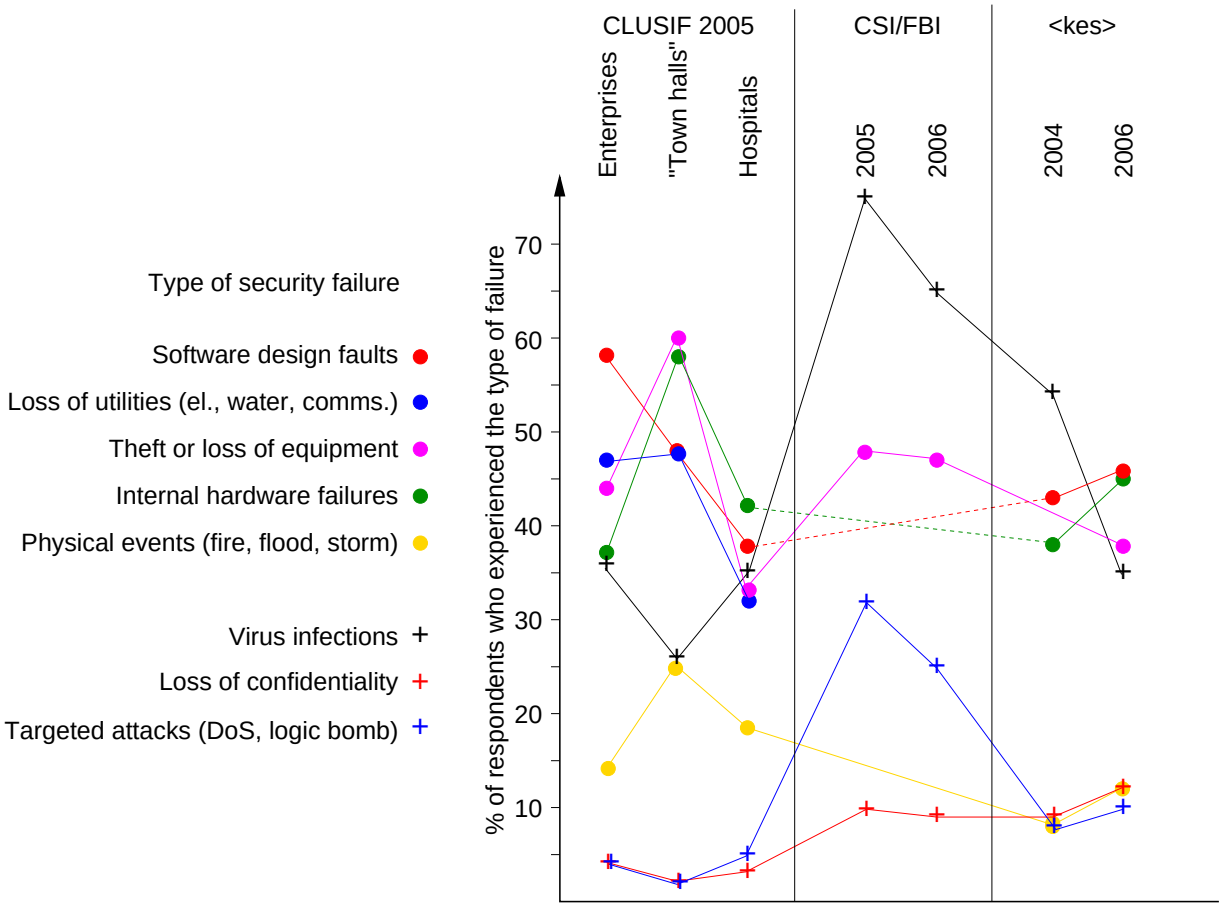

Figure 2.1: The most common security failures found by the CLUSIF, CSI/FBI and <kes> surveys, expressed as the percentage of respondents who had experienced at least one incident of the type indicated during the year of the survey.

made public in the course of the year, with a view to providing an assessment of emerging risks and trends in existing risks. The principal trends noted for 2006 were:

- **Use of "money mules"** to whitewash funds illegally acquired (via phishing, scamming, use of keyloggers etc). The mules are private individuals who receive the funds in small portions and transfer them electronically to "clients".
- **Identity theft**, for example using Trojan horses with keyloggers. A case from the UK involved information collected from 2300 compromised computers. The malware used to collect the identity information came via many different types of website. Some of the keyloggers could even handle several types of virtual keyboard.
- **SPam over Ip Telephony** (SPIT), with the possibility of sending vast numbers of calls in a short time at very low cost.
- **Manipulation of stock prices** by circulation of false information in spam mail, possibly sent via botnets. Several cases from USA involved sending spam including a stock management tool with a Trojan keylogger, so the spammer could steal the victim's online brokerage account details. The intruded account could then be used to manipulate the prices of chosen stocks by buying or selling.
- **Zero-day attacks**, exploiting newly discovered vulnerabilities before patches are available. This seems to be an increasing problem, as the number of vulnerabilities announced increases year by year. In 2006, a market developed for zero-day exploits for supposedly very secure systems, such as Windows Vista. Often the zero-day attack is only used once, and on a few carefully chosen targets. Ordinary mass attacks such as worms or vira, which cause a widespread alarm seem, on the other hand, to be on the decrease.
- **Phone taps and high-risk investigations** for industrial espionage or obtaining other confidential information by fraudulent means. Several cases, based on telephone taps, social engineering or similar techniques, became public in the course of the year.

2.1.2 USA

The annual CSI/FBI Computer Crime and Security Surveys consider both computer security trends, trends in cybercrime and the effects of new regulatory or legal initiatives. In contrast to the French surveys, however, they take the narrow view of what constitutes a security failure, i.e. only consider security failures due to malicious activity. The latest published survey is currently the 11th annual survey, published in 2006 and referring to the year 2005.

The 2006 survey [32] was based on questionnaire replies received from 615 respondents, drawn from among the members in the USA of the Computer Security Institute (CSI), an organisation for information security professionals. Respondents represented a large number of different branches of industry and public institutions. The industrial enterprises included both very large firms (34% of respondents came from firms with annual revenues exceeding $1 billion) and much smaller ones (25% from firms with revenues less than $10 million).

The results of the survey are in general similar to those of the CLUSIF 2005 survey. Despite widespread use of firewalls (98% of respondents), anti-virus software (97%) and anti-spyware software (79%), successful virus attacks were observed by 65% of all respondents, and misuse of computer systems by 52%. As in the French survey, a considerable number of thefts of equipment were observed, with 47% of respondents having experienced theft of mobile equipment such as PCs, PDAs and mobile phones. These results are summarised in Figure 2.1.

The CSI/FBI survey is not directly related to the use of IT security standards such as ISO/IEC 17799. Nor was the topic of cybercrime dealt with in terms of detailed case studies as in the CLUSIF cybercrime surveys. On the other hand, it contains information which makes it possible to consider security activities from a cost-benefit viewpoint. Values were put on the estimated losses due to various forms of attack or misuse, and on the security expenditure per employee. The respondents were also asked to give an evaluation of the level of investment in security operations, security equipment and security awareness training. The results of this evaluation varied from one branch of industry to another, with the general feeling in most branches that not enough investment was taking place, particularly in the area of security awareness. This evaluation is in general accord with a similar survey made by the Business Software Association (BSA) among 850 members of the Information Systems Security Association (ISSA) at the end of 2004 [60]. In the BSA/ISSA survey, the three most commonly named challenges for successful implementation of an Information Security program were:

1. Availability of budget (identifed by 52% of respondents).
2. Employee awareness (45% of respondents).
3. Security staffing (43% of respondents).

Finally, respondents in the CSI/FBI survey were requested to identify the most critical issues for the next two years. Perhaps surprisingly, in view of the fact that successful virus attacks were both the most common and the most expensive in terms of losses, only 52 out of 426 respondents identified vira and worms as a “most critical” issue. This put it in the 4th place in the “most critical” table, where the first three places were occupied by:

1. Data protection and application vulnerability security (identified by 73 respondents).
2. Policy and regulatory compliance (63 respondents).
3. Identity theft and leakage of private information (58 respondents).

The survey did not include questions which could explain why the respondents had this perception of the relative risks, but it can be surmised that the companies judged the three top-ranked issues as ones which (although very rare) could have extremely costly consequences.

2.1.3 Germany

In Germany, the federal organisation BSI (Bundesamt für Sicherheit in der Informationstechnik) has been responsible for carrying out and publishing the results of general surveys of IT security since 2005. More specific surveys of industrial enterprises and public institutions are published by the journal <*kes*>. The most recently available <kes> survey was published in 2006 [46], based on replies from 160 respondents, mainly from large or medium-sized enterprises and institutions. The general results of the <kes> surveys are publicly available, while the detailed data are only available to survey participants.

Like the CLUSIF and CSI/FBI surveys, the <kes> 2006 survey investigated security failures, the organisation of security functions, management attitudes, knowledge of security issues, techniques used to achieve security, and issues related to outsourcing. The survey is based on the broad view of security failures, and therefore includes statistics on traditional failures as well as malicious attacks. The most commonly observed types of security failure are shown in Figure 2.1. As in the French and US surveys, the most frequently observed malicious failures in enterprises were due to successful attacks via malware (vira, worms, Trojan horses or spyware), which were experienced by 54% of the respondent enterprises in 2004 [45] and by 35% in 2006 [46]. Virus and worm attacks were also the ones which were most expensive to deal with, both in time and money. The average time for which systems were out of operation due to virus/worm attacks was 47.8 hours (the maximum was 1000 hours), while the average cost of recovery was 18 324 Euro (maximum 500 000). Overall, 78% of all respondents had experienced at least one malware attack during the year.

The enterprises participating in the survey were also asked about which of 50 counter-measures they had deployed on three categories of system:

1. Servers and other central systems;
2. Clients and similar end systems;
3. Mobile units.

Table 2.1 summarises the situation with respect to those counter-measures which were installed on at least 75% of systems in at least one category. An interesting feature of this part of the survey is the observation that counter-measures based on “new technology”, such as the use of smart cards or biometric information, had only been deployed on a very small number of systems. All the highly popular measures listed in Table 2.1 are very well established ones.

Finally, the <kes> 2006 survey investigated what the respondents believed to be the biggest hindrance to improving Information System security in their enterprises. The four most common hindrances mentioned were:

1. Lack of funding (mentioned by 55% of respondents)
2. Lack of awareness among employees (52%).
3. Lack of awareness or support in the top management (45%).
4. Lack of awareness among the middle management (37%).

Counter-measure	Servers	Clients	Mobile units
Firewalls	89%	52%	42%
Anti-virus	94%	98%	79%
Backup	97%	50%	41%
Passwords for authentication	93%	92%	82%
Log of unauthorised access	76%	36%	21%
Anti-spam	79%	59%	47%
Physical access control	85%	54%	—
Fire alarm	81%	45%	—
Secure data storage rooms	80%	21%	—
No-break power supplies	90%	21%	10%
Mains surge protection	84%	39%	18%
Air conditioning	85%	14%	—

Table 2.1: Commonly deployed counter-measures noted in the <kes> 2006 survey [46].

This makes lack of security awareness somewhere in the organisation the biggest single factor affecting security improvements in a negative way.

The BSI surveys published in 2005 [6] (with information about 2004) and 2007 [7] (with information about 2006) achieve more generality by compiling data from many sources (including the <kes> surveys), some relating specifically to German IT systems, while others describe more general European or world-wide conditions. The BSI surveys also include information about ordinary citizens as well as enterprises and institutions. On the other hand, in contrast to the CLUSIF, CSI/FBI and <kes> surveys, they only deal with security failures and associated cybercrime, and do not consider investment levels, the cost of failures, installed counter-measures or organisational issues such as the use of standards like ISO/IEC 17799.

The BSI surveys also discuss levels of cybercrime, and trends in this area. In the 2005 survey [6], the most important increasing trends were said to be:

- **Industrial espionage,** either due to internal "moles" or external agents.
- **Attacks exploiting the IT infrastructure,** such as routers, DNS servers etc. A particular source of danger was considered to be attacks on process control (SCADA) systems, where security often plays a very inferior role.
- **Attacks on commercial enterprises,** including theft of credit card data, DDoS attacks on e-commerce sites and the like.
- **Criminal hackers,** instead of the previously dominant amateurs who only hacked IT systems for "sport".
- **Regional adaptations of malware,** for example in connection with large popular events in specific countries.

In rough terms, these trends coincide with those noted down in the CLUSIF cybercrime survey. In the 2007 survey, it was noted that these predicted trends had been observed in practice in the

intervening period. The 2007 survey does not contain a new assessment of cybercrime trends, but concentrates on a review of changes in technology which may affect ICT security, such as the introduction of Web 2.0, Unified Threat Management Appliances (UTMA), new cryptographic hash functions to replace the widely used but possibly compromised SHA-1, and the use of longer cryptographic keys, possibly embedded in crypto-chips. The effects of these changes will obviously not be seen for a number of years.

2.1.4 Other Surveys

All three of the major surveys discussed above have concentrated on security in enterprises and public institutions of various sizes. Much less effort seems to have been put into investigating the security situation for individual ordinary citizens. One of the few surveys of this type has been performed for IT og Telestyrelsen, the Danish telecommunications regulatory body, by Teknologisk Institut in Denmark [74]. Strictly speaking, this was a survey of the ICT literacy of Danish citizens, but this included some aspects of ICT security, such as the ability to use and update anti-virus programs, the ability to use a digital signature and the ability to install and set up a digital signature. A further survey on Danish citizens' *attitudes* to IT security [59] will be discussed in Chapter 4 below.

2.2 Vulnerabilities

Surveys of what people do and what security failures they observe do not in general attempt to find the reasons for such failures. A number of organisations have therefore attempted to systematise knowledge of technical vulnerabilities so that individuals and enterprises can adopt suitable counter-measures in order to reduce risk. Suppliers of technical counter-measures such as anti-virus software, or software for the detection of spyware or other malware, build up large databases of vulnerabilities within their area of expertise. Most of these databases can be freely accessed by the general public, whether or not they are licensed users of the detection software. However, we consider them to lie outside the scope of this report.

A more general collection of information about vulnerabilities has been built up by the SANS Institute, who regularly publish a list of the most commonly exploited Internet vulnerabilities observed within 20 different categories in current computer systems [69]. This "Top-20" list is a so-called *consensus list* based on information collected from government security agencies such as the Department of Homeland Security (DHS) in the USA and the National Infrastructure Security Coordination Centre (NISCC) in the UK, from various branches of CERT, and from about 50 specialists from leading security consultancy companies and suppliers of ICT security products.

The latest published version of the list is the 2006 version, which includes information on the

following 20 categories:

1. **W1.** Internet Explorer
2. **W2.** Windows Libraries
3. **W3.** Microsoft Office
4. **W4.** Windows Services
5. **W5.** Windows Configuration Weaknesses
6. **M1.** Mac OS X
7. **U1.** UNIX Configuration Weaknesses
8. **C1.** Web Applications
9. **C2.** Database Software
10. **C3.** P2P File Sharing Applications
11. **C4.** Instant Messaging
12. **C5.** Media Players
13. **C6.** DNS Servers
14. **C7.** Backup Software
15. **C8.** Security, Enterprise, and Directory Management Servers
16. **N1.** VoIP Servers and Phones
17. **N2.** Network and Other Devices Common Configuration Weaknesses
18. **H1.** Excessive User Rights and Unauthorized Devices
19. **H2.** Users (Phishing/Spear Phishing)
20. **Z1.** Zero Day Attacks and Prevention Strategies

The categories whose identification starts with W apply to Windows systems, M to Mac OS, U to Unix, C to cross-platform applications, N to network devices, H to security policies and personnel and Z to zero-day attacks. For each category, information is given on the principal vulnerabilities and counter-measures to prevent their exploitation, which enables the technically minded reader to understand what has to be done in order to improve Internet security. On the other hand, although it is based on some kind of quantitative assessment from the respondents, the published list does not include actual quantitative data on the frequency of (successful or unsuccessful) attempts to exploit the vulnerabilities, so it cannot be used for quantitative risk assessment. (It should perhaps also be pointed out that, since the list pre-supposes considerable knowledge of technical terms and procedures, it is unsuitable for non-technical readers.)

2.3 Concerns

In addition to the surveys whose main focus is Internet security *per se*, there have in recent years also been a considerable number of more general investigations of the way in which people use the Internet. Such surveys are in general motivated by a desire to pinpoint current or potential developments in society as a consequence of the new possibilities for communication which the Internet offers. However, as a component of some of these surveys, respondents have also been

asked to voice any concerns which they have about the Internet – for example, to explain why they avoid using the Internet for certain purposes, or to say what would be needed in order to convince them to use the Internet. Responses to such questions typically include an element of evaluation of the security of the Internet. It should, however, be noted that this generally reflects the *perceived risk* of using the Internet. This may be substantially different from the *objective* risk or threat level which the previously discussed surveys of Internet security aim to measure.

2.3.1 The Oxford Internet Surveys

Two comprehensive surveys of the use of the Internet by ordinary citizens in Britain have been carried out by the Oxford Internet Institute, in 2005 [21] (with 2185 respondents) and 2007 [22] (with 2350 respondents) as part of the World Internet Project (WIP). These surveys cover a very large number of issues, including access to the Internet, the most frequent uses of the Internet, changes in habits due to the availability of the Internet, time used on the Internet and differences between Internet users and non-users ("the digital divide"). Three sections of these reports are of particular interest in the context of this review:

- Attitudes towards the Internet and privacy.
- Attitudes towards regulation and parental control.
- Unpleasant experiences on the Internet.

The extent to which respondents "agreed" or "strongly agreed" with various statements about privacy and the Internet is summarised in Table 2.2. The surveys revealed some differences

Statement	Extent of agreement	
	2005	2007
"People should be concerned about protection of credit cards"		88%
"People who go on the Internet put their privacy at risk"		70%
"People should be able to express their opinion anonymously"		60%
"Personal information is being kept somewhere without my knowing"	66%	84%
"The present use of computers is a threat to personal privacy"	49%	66%

Table 2.2: Concerns about the Internet and privacy. Source: [21, 22]

between users of the Internet and non-users (or ex-users). In general, a smaller proportion of non-/ex-users agreed with the statements given in the table; the only exception was the third statement, on freedom of speech, which users were much more likely to agree with (64%, versus 49% of non-/ex-users). These results indicate that there is a considerable degree of concern in the general population about privacy issues in connection with use of the Internet, in as much as well over half the respondents had these concerns. On the other hand, only 37% of users agreed that people could find their contact information too easily on the Internet (36% disagreed, and 27% were neutral).

Attitudes to regulation were in the Oxford Internet Survey mostly investigated in the framework of risks to children. A general question about whether or not governments should regulate the Internet gave no clear conclusions, with roughly 1/3 answering that they should, 1/3 that they should not and 1/3 being undecided ("it depends"). Non-users were slightly more in favour of government regulation than users. Roughly 85% of respondents thought that there should be some restrictions on online content for children, whereas 12% thought there should be very few restrictions and 3% thought there should be no restrictions at all. In practice, 60% of parents had rules about Internet use by their children at home, and 14% extended these rules to apply outside the home. The rules were most commonly ones intended to protect children against grooming (see Chapter 3 below), and therefore reflect concerns about Internet safety in relation to sexual harassment. Some families also had rules about time spent on the Internet, which reflects a concern about possible addiction.

Finally, the Oxford Internet Survey specifically asked respondents about unpleasant experiences which they might have had on the Internet. These included security failures such as virus infections as well as invasions of privacy or actual harassment. In line with the results noted in the ICT security surveys discussed in Section 2.1, virus infections were the most common unpleasant incidents (experienced by 34% of users in 2007), while:

- 18% had in 2007 been contacted over the Internet from some foreign country.
- 17% had been contacted by someone asking for bank details.
- 12% had received obscene or abusive e-mails from strangers.
- 9% had bought something which had been misrepresented on a Web site.
- 7% had received obscene or abusive e-mails from someone they knew.
- 2% had had credit card details stolen via use of the Internet.

Non-financial incidents seem in general to be on the decrease, whereas incidents related to finance (bank details, credit cards, e-commerce) are slightly increasing. Nevertheless, many users seemed concerned, particularly about bad experiences which they risk having via the use of e-mail. In 2007, 44% of the surveyed users had actively introduced counter-measures to prevent obscene or other unwanted e-mails, while a further 17% were concerned about the matter but had not (yet) taken action.

2.3.2 The Ofcom Media Literacy Survey

The Oxford Internet Surveys were directed at adult respondents in Britain and are concerned solely with Internet use. In the summer of 2005, the UK Office of Communications (Ofcom) conducted a more general survey of *media literacy*, which they defined as "the ability to access, understand and create communications in a variety of contexts". The results of the survey were disseminated in 2006 in a series of reports, in particular a report on adults [56] and one on children in the age group 8–15 [57]. As the report on adults covers many of the same issues as the Oxford Internet Surveys, we concentrate here on the report on media literacy amongst

Rules on...	8–11 year olds		12–15 year olds	
	Parent	Child	Parent	Child
Content	91%	70%	68%	53%
Length of time	23%	17%	10%	23%
Download/purchase	15%	15%	19%	18%
Computer location	24%	14%	12%	9%
Any rules at all	95%	79%	78%	67%

Table 2.3: Rules set by parents for children's Internet usage. Source: [57]

Reason	Age of child	
	8–11	12–15
Trust my child	48%	79%
Child always supervised	14%	1%
Don't know how to do it	13%	9%
Didn't know it was possible	9%	5%
Child too young to surf	12%	2%
They'd find a way round it	1%	6%

Table 2.4: Parents' reasons for not installing blocking controls for the Internet. Sources: [57] and [52]

children. The respondents were 1536 children plus a parent of each child, all of whom were interviewed in their own homes. Questions covered usage of a variety of media, including TV, radio, the Internet and mobile phones, and for the Internet included questions covering various possible concerns. Overall, 14% of all 8–11 year olds and 19% of all 12–15 year olds had at some time come across something on the Internet which they found "nasty, worrying or frightening". This observation was reflected in parents' attitudes, where 75% of parents of 8–11 year olds and 72% of parents of 12–15 year olds agreed that they were worried about their child seeing inappropriate things on the Internet. Parents also had worries of a rather different sort which might help to explain their attitudes: 48% of parents of 8–11 year olds and 66% of parents of 12–15 year olds agreed to the statement that their children knew more about the Internet than they (the parents) did!

Parents and children were also independently asked about whether the parents set rules for use of the Internet. Interestingly, there were some differences between the parents' and the children's answers to this (see Table 2.3). About half of all parents with Internet access had some sort of content blocking mechanism in place to prevent their children accessing certain types of website. Reasons given by parents who did not have content blockers are summarised in Table 2.4 (the ABA/NetAlert survey is discussed in Section 3.1.3 below). Although by far the most popular reason was "I trust my child", lack of technical competence is also a significant reason. We return to this issue in Chapter 5.

2.3.3 The Forrester/BSA International Consumer Survey

In November 2005, Forrester Custom Consumer Research performed a survey for the Business Software Alliance (BSA) [26], which specifically investigated consumers' attitudes to Internet security and how this affected their use of e-commerce. The survey involved 4711 respondents in four countries (Canada, USA, Germany and Great Britain), with at least 1000 respondents from each country. Overall, 71% of respondents replied that they were "Somewhat concerned", "Very concerned" or "Extremely concerned" about Internet security when taking part in online shopping activities, while 72% had these levels of concern about bidding or selling goods on online auction sites. There were small variations from country to country, with German consumers being least concerned, and Canadian consumers most concerned. Overall, 8% of respondents answered that their use of online shopping would be greatly affected because of Internet security concerns, while 21% (in Canada, as many as 40%) would not do any online shopping at all due to such concerns. The Forrester/BSA survey also covered some aspects of security awareness; we return to these in Chapter 4 below.

2.3.4 The Consumer Reports Webwatch Surveys

The US organisation Consumer Reports Webwatch has conducted two surveys [64, 65] which, like the Forrester/BSA survey, investigated consumers' attitudes to the use of the Internet, and to the security and safety problems associated with this use. Both the 2002 and the 2005 surveys involved about 1500 adult Internet users in USA. The surveys focussed mainly on four issues:

1. Concerns about trust in websites providing e-commerce or financial services.
2. Concerns about credit card fraud and identity theft.
3. Concerns about online dangers to children.
4. Concerns about whether information sites (such as news sites, blogs, and search engines) were trustworthy, or gave false or biased information.

Only the first three of these issues are relevant in the context of the current review.

In the most recent (2005) survey, 77% of respondents said that they trusted online stores "a lot" or "somewhat", while 15% only trusted them "a little" or "not at all". Trust in online auction sites was rather lower: 12% only trusted them "a little" and 11% "not at all". About 60% of respondents used one or more online financial services, the most popular being online banking (45%); the exact fraction depended somewhat on the age, income and education of the respondents. 68% of all respondents stated that they trusted online banking sites (as opposed to 23% who only trusted them "a little" or "not at all"). It is interesting to note that a further 23% of respondents, who in fact trusted banking sites to at least a moderate degree, in practice did not use online banking. The survey did not investigate why this was the case.

The risks of credit card fraud and identity theft were a major issue for many of the respondents. Two out of three respondents who used credit cards online were concerned (28% worried "a

Danger	Major problem	Minor problem	Not a problem
Adults seeking out children in chatrooms	86%	9%	2%
Ease of viewing sexually explicit material	82%	12%	4%
Large number of violent online video games	61%	25%	10%
“Educational” sites are just advertising	42%	42%	9%

Table 2.5: Perception of major dangers to young persons on the Internet. Source: [65]

lot” and 39% worried “somewhat”) about somebody stealing their card details during an online transaction. Similarly, 45% worried “a lot” and 35% worried “somewhat” about having personal information such as Social Security numbers stolen via the Internet. These concerns had led to noticeable changes in respondents’ behaviour on the Internet: 66% of those who worried “a lot” about identity theft had stopped giving out personal information on the Internet, 55% had started using just one credit card for all online purchases, 41% had reduced how often they shopped online, and 37% had even completely stopped buying things on the Internet.

Finally, like several other surveys worldwide, the Webwatch survey revealed considerable concern about dangers to young people who use the Internet. The respondents’ perception of the major dangers is summarised in Table 2.5. The Webwatch survey only contain very limited information about what respondents had done in view of these concerns: Parents tended to follow more closely what their children were up to on the Internet. Technical counter-measures such as filters, which could alleviate some of the concerns, were not considered.

Chapter 3

Surveys of Internet Safety

The studies considered in this chapter have been concerned with aspects of Internet safety, i.e. the extent to which users have unpleasant personal experiences when using the Internet. The studies fall into two groups: The first of these is a group of quantitative surveys based on questionnaires, mostly focussing on issues related to misuse of children. The second group contains a set of studies of various psychological phenomena associated with Internet use or misuse. These are mostly based on interviews or small experiments, and are therefore of a more qualitative nature.

3.1 Quantitative Studies

3.1.1 Online Victimization in USA

In the year 2000, a large survey of young Americans' experiences of what the survey report called "the seamier side" of the Internet was commissioned by the U.S. Department of Justice. The survey was carried out by the Crimes Against Children Research Center at the University of New Hampshire, and involved telephone interviews of 1501 demographically representative respondents of ages 10–17 who used the Internet regularly (i.e. at least once a month for the previous six months) [24]. The questions covered three types of incident:

1. Sexual solicitation and approaches.
2. Harassment, including threats, hate messages, "mobbing" and similar incidents.
3. Unwanted exposure to sexual material, such as images of naked people or people having sex.

The first two categories involve another person making a deliberate effort to contact the victim, typically via e-mail or by using a chat forum or instant messaging (IM) facility. 286 (19%) of the respondents had experienced sexual solicitation in some form; 2/3 of these were girls and 1/3

Way of resolving incident	Solicitation	Harassment
Logged off computer	28%	19%
Left site	24%	13%
Blocked perpetrator	14%	17%
Changed logon name/mail address	5%	3%
Told perpetrator to stop	13%	11%
Perpetrator just stopped	4%	10%
Contacted authorities	1%	2%
Other	20%	27%

Table 3.1: Resolution of cases of online solicitation and harassment. Source: [24]

boys. About a quarter of the victims characterised the approaches as “distressing”. 95 (6%) of the respondents had experienced harassment in some form; there were roughly equal numbers of girls and boys. About a third of the victims characterised the harassment as “distressing”. Ways in which incidents of solicitation or harassment were resolved are summarised in Table 3.1. Simple (essentially non-technical) expedients such as logging off, leaving the site or telling the perpetrator to stop seem to have been quite effective at ending such incidents, but it is not clear how good the long term effect was. Only about one in five of the victims used more technical (and probably more long-term) solutions such as changing their logon name, getting a new mail address or blocking the perpetrator. It was not clear from the survey whether this was due to lack of technical expertise or other reasons. The survey did not investigate the question of whether the victims had indulged in unsafe behaviour, for example by publicly exposing their e-mail addresses, telephone numbers or other personal details.

281 of the respondents had experienced incidents of unwanted sexual exposure via websites and 112 via e-mail; 93% of such e-mails came from senders who were unknown to the victims. Roughly a quarter of the victims said they were “very upset” or “extremely upset” by the experience. It is probably fair to assume that the offensive e-mails were sent as spam mail, and would largely have been removed by an efficient spam filter. Unwanted exposure via websites arose in three main ways:

- Through searches, often for apparently innocuous terms which in some contexts have a hidden, sexual meaning (47% of cases).
- Due to misspelling a web address (17%).
- Via links found on another, not sexually related, site (17%).

Escaping from this type of exposure requires a more pro-active strategy from Internet users, and a greater degree of awareness of where the pitfalls lie. Some of the exposure could probably have been removed by well-designed filtering or blocking software. However, at the time of the survey very few families in USA had installed such software, and those that had often had mixed experiences with respect to its effectiveness.

Reason given	Number of cases
Implied sexual threats	27
Strangers accessing personal details	23
Persistent attempts to make contact	14
Verbal abuse or intimidation	12
Hackers got into computer	9
Implied physical threats	8

Table 3.2: Reasons given for feeling unsafe or threatened while using the Internet. Source: [38]

3.1.2 Girls on the Net in New Zealand

In 2001, the New Zealand Internet Safety Group conducted a web-based survey [38] to investigate online victimisation of girls of age 11–19. There were 347 respondents, all resident in New Zealand at the time. 68.5% of them were using the Internet "most days" and 23% used it more than 10 hours a week. The respondents used the Internet in a variety of ways; for example, 47.5% used chat rooms, 56.5% used IM facilities and 86.5% used e-mail.

The survey focussed on approaches from persons met via the Internet and on harassment, corresponding roughly to the first two categories of questions in the US survey discussed above. When asked about contacts to persons first met via the Internet, 70.5% of respondents answered that they had sent e-mails to or received them from persons whom they had first met on the Internet, 29% had sent or received ordinary "snail mail" and 26% had phoned or been phoned. Only 23% had done none of these things. 85 respondents had been to a face-to-face meeting with someone whom they had met via the Internet, and about a third of these went to the meeting alone. Although a large proportion (53%) of the people whom they met were in the age group 15–17, roughly corresponding to the age of the respondents, a small proportion (18%) were rather older (more than 20 years old).

About 1 in 4 respondents said that they had felt unsafe or threatened while using the Internet. The most common reasons given for this are summarised in Table 3.2. This is a relatively larger number of cases than that seen in the US survey. However, it should be noted that the respondents in this survey did tend to indulge in what would normally be considered unsafe behaviour on the Internet, even though 91.5% of them had heard about Internet safety from one source or another. This can be seen both from the number of respondents who contacted people they had only met via the Internet, and from the fact that many of them exposed personal details via the Internet: 14,5% had posted a picture of themselves, while 35.5% had sent their address, telephone number or family name, and 26.5% had sent a picture of themselves to someone whom they had met on the Internet. There are no obvious technical ways of preventing such potentially dangerous behaviour. It can only be counteracted by activities which more effectively increase young persons' awareness of behavioural rules that maximise safety on the Internet.

Concern	Mentioned by		
	Parents	Boys	Girls
Exposure to pornography	63%	19%	17%
Communicating online with strangers	37%	15%	25%
Exposure to other inappropriate content	15%	9%	10%
Exposure to obscene language	10%	5%	
Exposure to violent content	10%	5%	
Malware or hacker attacks	5%	33%	18%
Inappropriate search results	5%	6%	
Pop-ups	4%	11%	10%

Table 3.3: The most common concerns about the Internet for Australian parents and children. Source: [52]

3.1.3 Internet use in Australian Homes

In 2005, the Australian Broadcasting Authority in collaboration with NetAlert Limited commissioned a survey of Internet use in Australian homes by children in the 8–13 year old age group [52, 50]. The investigation focussed on patterns of usage, experiences when online, and Internet safety issues. The survey was based on structured (questionnaire-based) telephone interviews of 502 children and their parents, supplemented with in-depth interviews of a small number of additional respondents. According to parents' estimates, 37% of the children used the Internet every day, and a further 34% used it 2–3 times a week. On average, the 8–13 year olds used the Internet for about 13 hours a month. (14–17 year olds in Australia use it about twice as much.) The most common uses of the Internet were for homework or study (89% of children), for playing games (about 80%), and for e-mail (71% of girls and 57% of boys). About 16% of children used chat rooms and about 50% used some kind of IM application.

A large majority of the respondents had a positive perception of the Internet. For example, 99% of the Australian parents thought that the Internet was beneficial for their child, the main reasons given for this being that it assisted their schoolwork, provided entertainment, improved general knowledge or allowed regular contact with friends or family. However, 92% of parents and 97% of the children had some concerns, of which the most common are summarised in Table 3.3. Very few parents or children mentioned risks such as arranging to meet someone in person, receiving unsolicited e-mails, fraud or loss of privacy/exposure of personal details.

These concerns reflect the *perceived risk* of using the Internet, and it became clear from some of the interviews that many of these perceptions were based on anecdotal evidence rather than actual experience. The actual level of risk can be gauged from Table 3.4, which summarises the extent to which children in fact had experiences related to the major concerns. Some of these experiences were strongly media-dependent: One in four children who used IM services reported that they had communicated online with people whom they didn't know, whereas fewer than one in twelve children who did not use IM had done this. The survey did not include questions on

Experience	Once only	More than once
Accidentally found website parents prefer you not to see	19%	21%
Searched for websites parents prefer you not to see	4%	3%
Contacted by or sent messages by people you don't know	7%	16%
Communicated with people you don't know in real life	4%	10%
Given out personal details to websites or unknown people	6%	8%
Arranged to meet someone first met on the Internet	1%	2%

Table 3.4: Childrens' actual experiences related to the major concerns. Source: [52]

Reason	Age
	8–13
Trust my child	50%
Other safeguards (e.g. supervision) OK	17%
Don't know how to do it	11%
Didn't know it was possible	4%
Too restrictive	4%
Don't believe it would be effective	5%

Table 3.5: Parents' reasons for not installing blocking controls for the Internet. Source: [52]

whether the children (or their parents) actually found these experiences frightening or unpleasant in other ways.

Approaches to the problem of avoiding risk fell into two categories:

1. Technical approaches, such as use of filtering software.
2. Behavioural rules within the household.

About 35% of respondents used filtering software to block inappropriate websites. Reasons for not using such software can be seen in Table 3.5, which can be compared with the results from the Ofcom media literacy survey given in Table 2.4 on page 17. As in the case of the Ofcom survey, the most common reason given was "I trust my child", although once again lack of technical competence was a significant factor.

About 80% of the respondent parents used rules on what activities their children were allowed to take part in on the Internet, and about 73% had rules about what websites the children could visit. The most common specific rules are shown in Table 3.6, which can be compared with Table 2.3 on page 17 from the Ofcom survey. Once again, there were some quite large discrepancies between the parents' and the children's view of whether a rule was in force or not! It is clear from the survey that the use of trust and behavioural rules is much more common than the use of technical approaches (such as filtering) for reducing risk. This corresponds to the so-called "informed choice-making" paradigm of ICT safety, often preferred in societies where filtering is regarded as an authoritarian way of resolving the problem.

Rule	Parents	Children
Ask before visiting websites	38%	19%
Amount of time spent on Internet	30%	32%
Set time when Internet can be used	20%	14%
Only allowed to access specific websites	21%	17%
Not allowed to access adult content	16%	14%
Not allowed to use chat rooms	15%	10%
Restrictions on how chat rooms/IM are used	13%	6%
Not allowed to give out personal details	8%	9%

Table 3.6: Rules for regulating Internet use, according to (a) parents and (b) children. Source: [52]

3.2 Qualitative Studies

A considerable number of qualitative studies of Internet safety issues have focussed on adverse psychological effects on children. The issues considered include not only sexual solicitation, predation, threats, hate messages and exposure to pornographic material, as considered by the quantitative surveys discussed in Section 3.1 above, but also issues such as poor social development, social isolation and associated depressive symptoms. A general review of relevant studies has been given by Varnhagen [80] in her contribution to the 2007 edition of the book "Psychology and the Internet", edited by Jayne Gackenbach [30]. With respect to social interactions, the current consensus among psychologists appears to be that the Internet often provides a positive environment for social development through inter-personal communication. Major reasons for this seem to be that children can try out various personas, discuss personal problems and obtain personal information on embarassing topics without disclosure.

Walker [82, 81] conducted a number of studies in Europe, asking young people what they themselves consider as the dangers in using the Internet. A common attitude amongst the young interviewees was that adults' worries were largely misplaced: Pornography is just "a laugh", chatrooms are fun, and they do not believe that they themselves will ever become compulsive on-line gamblers. They see a big attraction in being able to experiment with different personalities, names, genders, ages and so on. This observation is in general accord with the reports of other authors, such as Valkenburg [79]. The conclusion drawn from this by Walker is that increasing Internet safety requires a long-term effort to change attitudes, similar to that needed to reduce drug abuse.

O'Connell [54] discussed commonly accepted safety guidelines for children, focussing on the issue of on-line solicitation in chatrooms, and the interplay between identity, trust and deception in this environment. O'Connell points out that children are at most risk when they fail to interpret cues which should signal danger, and that they cannot interpret these cues without understanding the situation in which they are operating. As pointed out above, many children engage in high levels of identity deception on the Internet, and enjoy chatrooms exactly because they permit this

type of explorative behaviour. So detecting danger is not just a question of detecting identity deception – the child also has to be able to detect other clues which indicate that something might be wrong. This usually has to be done in the context of an ambiguous discourse, where the predator does not say directly what he or she means. Current safety guidelines, such as "Report anything which makes you feel uncomfortable" or "Don't give out personal details" are not very helpful in this respect, since they do not assist the children to disambiguate the discourse. O'Connell suggests that teaching programmes should be based on the use of realistic scenarios, from which they can build up rules for themselves in a "Piagetian" process of self-directed learning. Some examples of scenarios can be found in [55].

The question of how easy it is to perform identity deception on the Internet has been treated by a number of authors. In a survey of 200 London school children, aimed at exploring the online behaviour of sex offenders, Davidson and Martellozzo [15] found that about 13% of the children had at some time believed themselves (or a close friend) to be talking to an adult posing as a child. About 70% of children claimed that they could easily tell the difference by looking at the language used; Davidson and Martellezzo did not, however, attempt to check this claim. A small experimental study by Hills [34] revealed similarly that it was relatively easy to tell the gender of the "opposite party" in computer-mediated communication (CMC) by exploiting linguistic clues, even in the absence of context clues such as (true) names or other gender-specific information. For example, it is known from a body of other research that males use more justifiers and references to quantity and place than females do, and are more likely to express their opinions, use judgmental phrases, action verbs, grammatical errors, contradictions and rhetorical questions, while females are more likely to use relative clauses, hedges, intensive adverbs, subordinating conjunctions, references to emotion, personal pronouns, self-derogatory comments, questions, compliments, apologies and tag questions. In situations where participants were trying to portray a false gender identity, Hills found that they exaggerated the traits which they believed characterised the opposite gender. Nevertheless, 69% of females and 91% of males could still be accurately classified by their communication partners, even when they tried to act like persons of the opposite gender, apparently because they could not manipulate all the gender-related features in their communication in an appropriate manner.

A rather different type of deception which is often discussed in the media is *social engineering*, where the intent is typically to obtain some secret information by fraudulently pretending to be someone else who has a rightful need for this information. In the context of the Internet, this type of deception often appears in the form of *phishing*, where false mails or websites are used to persuade people to reveal personal secrets such as social security numbers, bank details, passwords, PIN codes and so on. The total extent of phishing activity is very hard to estimate, but data collected in 2005 indicated that at that time there were over 16 000 websites implicated in phishing attacks. In order to understand why phishing works, Dhamija, Tygar and Hearst [14] performed some experiments with a group of 22 university students and staff, all of whom were familiar with the use of mail and the web. The respondents were presented with 20 websites, of which 7 were legitimate and the remainder were either genuine phishing sites or phishing sites constructed by the experimenters. Even though the respondents knew that they were expected

to look for phishing sites, the most convincing sites were able to deceive over 90% of the respondents, who in most cases plainly overlooked (or were unaware of the significance of) the indicators which show whether a website is legitimate or not. The ease with which phishing sites deceived respondents was independent of the respondent's age, sex and educational level. Dhamija, Tygar and Hearst concluded that this is essentially a technical problem in the human-computer interface, where users have to combine evaluations of a number of indicators (such as use of HTTPS, appearance of a padlock in the address bar, use of the expected graphic design for the site, etc.) in order correctly to evaluate the legitimacy of a website. The only effective cures seem to be good, persistent training or a radical re-design of browser interfaces.

A final area of focus for Internet safety studies has been the area of Internet addiction, defined as obsessive or compulsive use of the Internet in one way or another. Young [91] has identified 5 specific subtypes:

- **Cybersexual addiction:** Compulsive use of adult websites for cybersex or cyberporn.
- **Cyber-relationship addiction:** Over-involvement in online relationships.
- **Net compulsion:** Obsessive online gambling, shopping etc.
- **Information overload:** Compulsive web surfing or information seeking.
- **Computer addiction:** Obsessive playing of online computer games.

Widyanto and Griffiths [85] have reviewed a number of studies of such addictive behaviour. There is no real consensus among psychologists about whether it is an independent psychological disorder, or even whether it is technically speaking an addiction (i.e. a form of behaviour exhibiting properties such as tolerance and withdrawal symptoms). However, there is plenty of evidence from case studies that uncontrollable excessive Internet use exists and can have serious social and personal consequences for afflicted persons. Various possible explanations have been mooted for the magnetic attraction of the Internet, including:

- It provides a feeling of intense intimacy in communication.
- It promotes disinhibition, i.e. behaviour which is not inhibited by social convention or a desire to present oneself from one's best side. This may include activities such as self-disclosure, swearing, insulting, flirting, searching for sexually explicit content etc. [43].
- Users lose all sense of time and location.

At the same time, it appears that certain personality traits or psychological factors such as loneliness may promote addictive behaviour, implying that certain groups of people are especially at risk. As we shall see in Chapter 5, current approaches to improving ICT safety awareness are not designed to deal with this type of situation.

Chapter 4

Surveys of ICT Safety and Security Awareness

In this chapter we review a small group of surveys which focussed more directly on the question of ICT safety or security awareness than the previously discussed studies of ICT safety and security levels. The border line between the two types of survey is, of course, a fine one, and is best illustrated by an example: A survey of ICT security levels within a company might investigate the length of people's passwords. However, the use of a long password is not necessarily a sign of a high individual level of awareness – it might just be the case that the company has installed password software which makes it technically impossible to choose passwords of less than a certain minimum length and complexity. Investigations of awareness therefore need to discover not only whether people do the right thing, but also whether people know and understand what is the right thing to do. So the focus of such studies is on attitudes rather than the technical issues involved.

A major attempt to map out the level of IT security awareness in Denmark was performed in 2006 for IT og Telestyrelsen, the Danish telecommunications regulatory body [59]. The survey involved telephone interviews with 1000 respondents from all parts of Denmark, including specially selected groups from segments of the population which previous surveys had revealed to be "weak" with respect to IT security:

1. Women. (No information was provided about the proportion of women among the respondents.)
2. Elderly people, defined as over-60's, who made up 17% of the respondents.
3. Young people, defined as 18–29 year olds, who made up 12% of the respondents.
4. People with only a basic education, defined as those who left school at the 9th grade or below. 22% of respondents fell into this group.
5. People with no daily contact to IT via work or studies. 31% of respondents fell into this group.

It should be noted that some of these categories overlap; for example, it is obviously possible to have a female respondent who is also a young person with very little schooling and no daily contact to IT via work or studies.

The survey was designed to measure the the respondents' levels of respectively *Knowledge*, *Understanding* and *Compliance* in relation to accepted IT-security rules. The levels were evaluated for each of four specific areas (use of mail, use of the web, use of passwords and wireless networks), and also to obtain an "overall" level of IT security awareness. The general picture obtained was that there were high levels of knowledge, understanding and compliance relating to the use of passwords, independent of age, sex or geographical area, whereas the levels relating to use of mail, the web and wireless networks were significantly lower.

Unfortunately, from a scientific point of view the published report on the survey is not at all satisfactory. In contrast to most large international surveys, there is no description of the survey methodology, there are no demographic details, and the actual questions asked have not been made public. Moreover, the survey report does not describe how the index values for Knowledge, Understanding and Compliance were in fact evaluated from the responses to the questions, nor how the results in the four specific areas were combined to obtain the overall result. It is therefore very difficult to judge the validity of the results or to relate them to those found in other surveys.

In Germany, Dimler carried out a small survey of about 100 students from three faculties (law, education and business informatics) at the University of Regensburg [20] to investigate their level of IT security awareness. The survey was based on a questionnaire [19] which covered a wide range of issues, including the students' attitudes to:

- Making personal information public;
- Security in online transactions;
- Password protection;
- Security of ISPs;
- Use of online fora and chatrooms;
- The need to keep computers updated;
- Use of firewalls and virus scanners;
- Protection against loss or theft of data.

The answers to these questions were used to judge the overall level of awareness about IT security and data protection. Roughly 48% of students gave responses indicating that their attitude to data protection was that it was "very important", and about 36% that it was "important". There were only small differences between the faculties. With respect to IT security, roughly 70% gave answers indicating that it was "very important" and 20% that it was "important". Interestingly, the informatics students showed a higher degree of IT security awareness (more of them gave responses showing that it was "very important") than the students of education, who again showed higher awareness than the law students.

A small investigation of the IT security culture among 79 Swedish social workers from the Stockholm area was reported by Frisk and Törnberg [28]. Among social workers, it is particularly

important to maintain a high degree of data protection and to preserve the confidentiality of data related to the individual social clients. A high degree of IT security awareness should therefore be reflected in a high degree of attention to these issues. In Sweden, IT security activities in this area must follow a code of practice known as FA22, and the area is regulated by a complex of laws on the handling of personal data, the duty of secrecy among public employees, and the handling of personal information in the social sector.

The main part of the survey fell into two sections:

1. **Knowledge:** How much did the respondents know about laws, regulations and the security organisation, how well did they feel they had they been trained, and how experienced were they at using IT.
2. **Motivation:** What were the respondents' attitudes to taking risks with IT security, what was their perception of the IT-security environment in their workplace, and what was their attitude to issues like the use of passwords and the reporting of failures.

It is the issues in the Motivation section which correspond most closely to what we have previously discussed under the heading of security awareness. An interesting aspect of this survey is that it investigated the respondents' degree of "fatalism" with respect to IT security. For example, they were asked whether they agreed with the statements *"If I though about IT security all the time, I would not have time to perform my tasks at work"* (about 10% agreed, while about 50% said this was "not at all" the case), and *"accidents in the handling of information occur whatever you do"* (about 1% agreed completely or largely with this, while about 68% said it was "slightly" or "not at all" the case). This type of question reflects the fact that the survey was primarily a survey of *security culture*, which is very much a question of people's desire to maintain and improve the level of security, analogous to the concept of *safety culture* for conventional workplace safety. There was only a single question related to the respondents' technical practice. This concerned how many passwords they used when logging in to the network and the journalisation system; about 78% used two quite different passwords, 24% used the same password, and a very few used two similar passwords or only needed to give a single password as a result of the way in which their system was set up.

As a final example, we return to the international Forrester/BSA survey of consumers' needs for IT security [26], which we have partly discussed in Section 2.3. This survey also dealt with some aspects of IT security awareness:

- How confident were respondents that they could protect themselves against various forms of security failure? This type of question relates to their degree of *Understanding*. 79% of respondents felt "not confident" or only "somewhat confident" that they could protect themselves against theft of personal information, 74% against identity theft, 68% against spam, 62% against credit card fraud and 58% against computer vira.
- What types of software had respondents installed to protect themselves from online risks? This type of question relates to their degree of *Compliance*. They were asked about antivirus software, anti-spyware, email filters/spam blockers, firewall software and web content filters/blockers. Results varied somewhat from country to country, but overall 9% of

Term	Completely understand	Reasonable understanding	Aware of the term	Never heard of the term
Pharming	5%	9%	20%	66%
Malware	15%	16%	17%	52%
Phishing	21%	20%	19%	40%
Spyware	39%	41%	13%	7%
Hackers	60%	34%	4%	2%

Table 4.1: Understanding of popular IT security terms. Source: [26]

respondents had no such software installed, 25% had one or two of the listed items, 47% had three or four and 19% had all five. The worst group were US consumers, of which 13% had no products of this type installed (or at least didn't know they were there).

Unlike in most surveys, respondents were also asked about their level of understanding of common terms used when discussing IT security issues. The results of these enquiries are summarised in Table 4.1, and cast an interesting light over some of the other surveys, since it is evident that respondents often simply do not understand the technical terms being used. The implications of this are that much attention needs to be paid to the design of the questions and the style of survey, if credible results are to be achieved.

Chapter 5

Proposals for Improving Safety and Security

In this chapter we look at a number of published proposals for improving ICT safety and security. First we consider a number of general approaches to improving awareness which have been suggested. We then look at some specific proposals for raising awareness, firstly in the form of general guides for what to do to increase awareness via campaigns and secondly in the form of specific campaigns which have actually been run or are currently running via the Internet. Most such campaigns just give good advice, but since it is evident that not everyone takes the advice, we also summarise the results of a number of studies of why this might be the case. Finally we comment on the campaigns and other initiatives in relation to the general problem of how to increase the level of ICT safety and security.

5.1 Approaches to Improving Awareness

Although a considerable number of approaches to improving awareness have been suggested in the literature, most proposals fall into one of three categories:

1. **Campaigns,** where the intention is to draw users' attention to appropriate ways of behaving.
2. **Regulation,** which obliges users to behave in certain ways, with penalties for failure to comply.
3. **Demonstration,** or learning-by-doing, where users are exposed to situations where they are shown the consequences of their (possibly unsafe or insecure) actions.

In practice, these approaches are often combined, so that for example a campaign can draw users' attention to new regulatory policies, or may give users the possibility of testing whether they have understood the campaign. Whether a particular combination is relevant or not depends

on the target group for the activity (for example, whether it is aimed at managers, company employees or ordinary citizens) and whether the aim is to improve *Knowledge*, *Understanding* or *Compliance*.

A discussion of the main issues involved in the campaigning approach appeared in the 2002 edition of the Computer Security Handbook [68]. This publication is targeted at organisations and their staff, and proposes the use of "media campaigns" and "events" within the organisation to draw attention to important aspects of IT security which the staff should be aware of, and to motivate the staff to pay attention to security risks. This approach is described in more detail in the US National Institute of Standards and Technology (NIST) Special Publication "Building an Information Technology Security Awareness and Training Program" [88] from 2003. Significantly, the NIST report carefully distinguishes attempts to improve security awareness from attempts to perform security *training*. Awareness relates to the ability to recognise and deal with general security issues, whereas training is regarded as an effort to impart specific skills needed for carrying out a particular job in the organisation. A consequence of this viewpoint is that everyone needs to be taught about awareness, but only some personnel need to undergo training, which is regarded as lying at a higher level. We return in Section 5.2 below to the content of the type of campaigns proposed in the Computer Security Handbook and by NIST. An explicit example of such a campaign is described by Fox and Kaun [27], who emphasise that it is the combination of measures which characterises proper campaigns, as opposed to clamp-downs on individual issues which the management have caught sight of.

Within companies, IT security will always involve decisions by management, and Garrett [31] discusses how to raise managers' IT security awareness in such a way that they make appropriate and effective decisions. This involves attempting to:

- Modify their *perceptions of risk*, which may be affected by the way in which a situation is framed [77].
- Reduce bias due to faulty *judgmental heuristics* [44], in particular:
  - **Availability heuristic:** The frequency of an event is judged from whether one can easily recall a recent memory of it occurring.
  - **Representativeness heuristic:** The frequency of an event is judged from available descriptive or anecdotal evidence, rather than from correct use of statistics.
  - **Anchoring heuristic:** Decisions are made based on an existing mindset, even if the actual situation is not covered by that mindset.
- Counter *overconfidence*. It is known that people tend to be most overconfident in situations of moderate to severe difficulty [47], such as often arise in the area of IT security, and that they tend not to reduce their level of confidence as their knowledge of a situation decreases [63]. One result of this is that organisations often have an exaggerated view of their ability to deal with security incidents, seen in the light of the actual number of security incidents which they experience.

Managers, and others in a position of leadership, therefore have to be made aware of these behavioural tendencies and the campaign should focus on achieving this.

Approaches based on regulation reflect a completely different attitude to improving Internet security, in which an authority decides on what Internet service providers (ISPs) and users are allowed to do. Awareness in a regulatory framework is therefore a question of being aware of the current rules governing the regulated activities – and also of knowing which activities are not regulated. For these latter, the usual approaches to improving awareness will need to be followed. In the context of ICT security and safety, the focus of regulatory efforts is currently on *content regulation*, i.e. the setting up of rules for what is permissible content, and *protection of personal data*, in order to protect citizens' private lives. Both these areas of focus correspond to common concerns which citizens have about the use of the Internet.

Impermissible content falls into two classes:

1. **Illegal content:** Content which by law has been declared illegal. In Europe, for example, it is illegal to possess child pornography and (therefore) also illegal to transmit it via the Internet.
2. **Harmful content:** Content which may be considered harmful by certain segments of the population. Examples include pornography in general, depictions of extreme violence, material inciting to racial or other forms of hatred, etc.

This is a political minefield, since content regulation by the state can easily become a form of censorship. The European attitude is therefore that definitions of illegal content should be as narrow as possible, and that harmful content should be dealt with via a system of self-regulation known as the Safer Internet Action Plan (IAP), which amongst other things involves the adoption of codes of conduct for ISPs and content providers, the development of a filtering and rating system, and promotion of awareness-raising actions. Descriptions of the European regulatory framework for harmful content, and its relation to other legal principles such as freedom of speech and privacy, can be found in [9] and [48].

The third major approach to improving ICT security by increasing awareness relies on training Internet users to perform more safely in commonly occurring contexts. This exploits a *"Learning by Doing"* paradigm to increase the user's knowledge, understanding or compliance, typically by getting the user to perform in a series of scenarios and then providing feedback on his or her performance. Baier and Straub [4] give some examples of such scenarios intended to improve awareness of:

- **Internet security,** including the dangers of false e-mails and web pages, and the use of digital signatures.
- **Password security,** particularly the use of complex passwords of a certain minimum length.
- **Malware,** giving an introduction to various types of malware and ways of dealing with them.
- **Chip or swipe card security,** including the danger of having card details stolen via false ATMs.
- **Dangers of physical access to computers,** including the danger of having data files stolen.

- **Wireless LAN security,** including problems of unauthorised access, eavesdropping and suitable counter-measures.
- **Hacking and forensics,** intended to ensure that computer administrators react appropriately to an incident.

Following a similar approach, Guenther suggests a series of role playing exercises intended to exercise people's reactions to potential breaches of security [33]. These focus largely on dealing with obvious failures to observe security rules, and with attempts to breach security by social engineering. For example:

> "You notice a distinguished man in a three-piece suit with a nice leather briefcase in your headquarters building. He's not wearing a badge, but you're positive he must be an executive, as no one but executives wears suits in this building. What should you do?"

Such role playing exercises are intended to be performed in groups in a workshop or seminar setting, and participants are expected actively to discuss their answers to the questions, so a form of "group awareness" is established.

5.2 Guides to Improving Awareness

Based on some of the ideas mentioned above, there have been attempts to collect up sets of principles which should be used in any initiative which seriously aims at increasing ICT security awareness. The typical product of this is a guide which instructs managers or public authorities in what steps to take in order to improve security awareness – and thus, hopefully, security. Four well-known guides are:

1. *"Security Awareness"*, published as chapter 29 of the Computer Security Handbook (CSH) [68].
2. *"Building an Information Technology Security Awareness and Training program"*, published by NIST as Special Publication 800-50 [88].
3. *"Raising Citizen Awareness of Information Security: A Practical Guide"*, published by the eAware consortium [90].
4. *"A Users' Guide: How to Raise Information Security Awareness"*, published by the European Network and Information Security Agency, ENISA [23].

The CSH and NIST guides focus on IT security awareness in organisations, while the eAware guide focuses on awareness among ordinary citizens and the ENISA guide covers both classes of IT user. Despite these differences, there is broad agreement on what an awareness-raising programme involves. Some important keywords describing the steps in the awareness-raising process are:

Figure 5.1: A humorous approach to improving IT security awareness. Source: US Army Space & Missile Defence Command, `http://www.smdc.army.mil/g2/g2.html`

1. Perform a needs assessment to find out what needs to be improved. This may involve activities such as reviewing the current state of awareness and discussing with managers, policy-makers, regulators or stakeholders.
2. Define the target group(s), scope and objectives of the program. It is well known that different groups require different approaches, according to their interests and levels of knowledge, so it is important to find out whether the programme is directed at a group of IT system managers, of schoolchildren or of female pensioners.
3. Define a communication strategy (including a choice of appropriate communication media) for getting the message across to the chosen target group(s).
4. Produce material appropriate to these target group(s), scope and objectives.
5. Execute the programme.
6. Check the effect of the programme, typically by a new review of the state of awareness, and determine how the programme should be adjusted to get a better effect.

The guides typically also include suggestions for how to motivate people's interest in the topic, for example by using humour (cf. Figure 5.1), drama, attractive graphics or other inspiring presentation features, or by offering prizes or rewards for contributing actively to the programme. Characteristically, the guides do not in general go into detail about possible techniques which can be used to investigate and improve levels of IT security and safety awareness. So the question of whether the use of traditional oral presentations, questionnaires, games, e-learning, group seminars, media campaigns or other techniques is most effective in this context is not considered. Nor have we been able to find any published research which attempted to answer this question. The organisers of the programme therefore need to make their own decisions based on what they believe to be appropriate paedagogical and psychological principles. We return to this issue in Section 5.4 below.

5.3 Public Campaigns and Infosites

Most Western countries have set up some kind of campaign which is intended specifically to improve levels of security awareness among the general public. Such campaigns typically use media such as brochures, TV spots, electronic newletters and web sites in order to get their message across. In many cases the main campaign, which concentrates on informing the public about the issues involved and attempting to change people's attitudes, is associated with a separate so-called *infosite*, which provides concrete technical information on what to do to improve security in a home or enterprise. It would make no sense in the context of the current review to discuss all existing campaigns and infosites, so we have chosen some representative and easily accessible examples which also illustrate various communication strategies.

Denmark: The Danish campaign **netsikker nu!** uses a website [41] and a printed newspaper to draw attention to important issues and give good advice. This is a specific campaign within a general initiative, **IT-borger**, which publishes information [40] on a very large number of aspects of IT usage in the broadest sense, including the Internet, radio/TV and telephones. The information is highly verbally oriented, and appears as a collection of small articles on the different topics. Quizzes intended to improve IT security awareness are included in the material, all based on the "multiple choice" verbal questionnaire paradigm. Quiz participants get told how many questions they answered correctly, but do not receive detailed explanation as in a learning program.

Germany: The German Bürger-CERT service, organised by the BSI, runs the campaign **Sicher Informiert** [5] aimed at individual citizens and small businesses. The campaign uses a website and a fortnightly newletter to draw attention to important aspects of IT security and to issue warnings of current dangers. The corresponding infosite, organised as part of the **BSI für Bürger** initiative and entitled *Ins Internet – mit Sicherheit* [8], provides information on a large number of aspects of IT security and safety. The information is largely verbally oriented, but also uses cartoon figures to illustrate important ideas.

Norway: The Norwegian web-based campaign **nettopp** [53], organised by Norsk Senter for Informasjonssikring (NorSIS), uses a website to provide information on IT safety and security, particularly intended for small and medium-sized businesses and public authorities. Most of the information is verbally oriented advice, but as part of this campaign, a collection of entertaining short *video films* have been prepared, targeted at young people, under the general title of **PushPopBaluba**, illustrating various IT security situations.

UK: The UK web-based **Get Safe Online** campaign [36] uses a website to provide information on IT security and safety to the general public and to small businesses. The approach is intended to draw attention to the issues involved and to modify people's behaviour rather than to describe technology. Reflecting this approach, the website also includes pages telling stories about victims of various security failures. The material also includes some small quizzes based on the "multiple choice" verbal questionnaire paradigm, with feedback telling how many questions were correctly answered. For the slightly more technically minded, the infosite **ITsafe** [35] provides detailed warnings about current security

problems.

The UK Information Warfare Site, which provides information on Information Assurance (IA) in a broad sense, includes a Security Awareness Toolbox [37], an infosite which describes various ways of improving awareness. Most of these are aimed at enterprises.

Australia: The Australian **Netalert** initiative, set up by the Australian government to improve online safety for families, especially children, involves a number of awareness programs aimed at slightly different age groups and covering different aspects of IT safety and security [51]. These differ substantially from the large majority of the other campaigns which we discuss in the current report, as they (like the Norwegian PushPopBaluba films) are based on *video clips*, often in the form of cartoon films, which can be activated from the NetAlert website. The material also includes guides for teachers and guides for parents.

New Zealand: The New Zealand **Netsafe** campaign [39] is run by New Zealand's Internet Safety Group, a collaboration between the police, judiciary, ministries and other stakeholders. The aim of the campaign is to provide "cybersafety education for ... children, parents, schools, community organisations and businesses". The main website includes links to material intended for various age groups and segments of the population, and information about various aspects of IT safety and security, including legal aspects and topics such as privacy and anonymity. The material for children is designed to promote *interactive discussion*, where the children are immersed in a scenario and can discuss what they think is the right course of action before going on to the next step. The web pages for adults mainly contain more verbally oriented advice and instruction. There are no quizzes or other material providing feedback.

USA: US-CERT, whose main function is to disseminate information about current patterns of cyberattack, runs a website with **Cyber Security Tips** [78], which "describe and offer advice about common security issues for non-technical computer users". It is possible to subscribe to receiving these tips via e-mail or an RSS feed. Links on the website lead to further information on a broad variety of aspects of IT safety and security. The presentation is entirely verbal and there are no quizzes or other material providing feedback.

The Computer Security Institute (CSI) has developed a set of humorous online videos [12] intended principally for training personnel in enterprises. The videos illustrate the principles of safe and secure behaviour in six areas: Passwords, e-mail security, laptop security, internet security, social engineering and workspace security. The form of the videos imitates a sporting competition between two employees who are trying to win *"The World Security Challenge"*. People who are being trained watch the videos and participate in interactive exercises with feedback on their performance. This approach is quite different from any of the other awareness campaigns discussed here.

An overview of these various initiatives is given in Table 5.1 on the next page. Although quite a wide range of approaches is used in these campaigns, there seem to have been no recent attempts to determine the effectiveness of any of them by longitudinal studies of the target population. This is unfortunate, since investigations in the early 1990s indicated that, of the promotional media available at that time, only videos were effective in changing the level of security awareness; brochures and newsletters were in general ineffective.

Campaign/infosite			Media	Style	Quiz	Feedback
Netsikker nu!	C	DK	W, N	Verbal	Yes	Partial
IT-borger	I	DK	W	Verbal	No	—
Sicher Informiert	C	DE	W, L	Verbal	No	—
Ins Internet – mit Sicherheit	I	DE	W	Verbal	No	—
Nettopp	I	NO	W, V	Verbal, film	No	—
Get Safe Online	C	UK	W	Verbal	Yes	Partial
ITsafe	I	UK	W	Verbal	No	—
Netalert	C	AU	W, V	Verbal, film	No	—
Netsafe	C	NZ	W	Verbal	No	—
Cyber security tips	C	USA	W, J	Verbal	No	—
World Security Challenge	C	USA	W	Game	No	Yes

Table 5.1: Campaigns and infosites

The abbreviations used for the media types are: J: Journal; L: Newsletter; P: Newspaper; V: Video clip; W: Website.

5.4 Motivation and Commitment

The question of what to do to ensure that peoples' behaviour is actually improved by awareness initiatives has attracted a lot of attention. Obviously there are many similarities to the situations faced by teachers of all kinds, and many of the same psychological and paedagogical theories have been applied in attempts to answer the question of what it is that motivates users to do the right thing. The basic issues involved are, of course, by no means confined to the area of ICT security, and studies in this area often build on the large body of knowledge accumulated in more conventional areas of industrial safety. In our review of this area, we concentrate on two aspects:

1. Organisational issues which may affect people's willingness to think about (and act on) security issues.
2. Psychological issues.

5.4.1 Organisational Issues Affecting Motivation

A study performed in 1990 by Straub [73], well before the explosive expansion in the popular use of the Internet, attempted to answer the question of whether a decision to invest in Information System security within companies actually resulted in lower rates of wilful computer abuse by authorised users of the company's computers. Straub looked at the effects of three factors on the incidence and cost of computer abuse within 1211 organisations:

1. **Deterrents:** The number of security staff, number of hours of work put into security per week, severity of penalties etc.

2. **Preventives:** The number of security software packages in use.
3. **Motivational/environmental factors:** The employment status of offending users, the level of offenders' system privileges, the offenders' motivation for abuse, the number of opportunities for collusion etc.

Straub found that only deterrents had much effect on wilful abuse, a result in accordance with the criminological *theory of general deterrence*, which predicts that antisocial behaviour is inhibited by the prospect of heavy penalties and a high probability of detection.

With the expanding use of the Internet, other types of security failures than wilful abuse have come into focus. One of the first attempts to discuss motivational factors for attaining a high level of IT safety and security in relation to such failures was made by McLean [49], who approached motivation from a marketing point of view. McLean pointed out various consumer marketing techniques which would be suitable for use in awareness campaigns:

- **Conditioning:** Attempts to change the attitudes, perceptions or beliefs of consumers, without necessarily expecting any immediate active response in the form of changed purchasing patterns.
- **Behavioural change:** Attempts to persuade consumers to change their behaviour.
- **Point of delivery messages:** Attempts to pass on a message at the instant when the product is purchased or used.
- **Branding:** Use of easily recognised slogans, images or symbols to represent the whole product.

From marketing it is known that new products and technologies are accepted by consumers at different rates, a process known as *diffusion*. In marketing studies the segment of the population which will eventually accept and use a new product or technology is traditionally divided into five groups according to the speed at which they will adopt the new idea:

1. **Innovators:** The most venturesome, who are always eager to try out new things.
2. **Early adopters:** Opinion leaders who respond quickly to the successes achieved by the innovators by adopting the idea.
3. **Early majority:** A large group who are responsive to change and willing to conform when the benefits are clear.
4. **Late majority:** A large group who tend to be sceptical about new ideas and are somewhat resistant to change.
5. **Laggards:** Traditionalists who are definitely suspicious of new ideas and are often difficult to reach via a campaign.

In general, the time at which people adopt a new idea after its inception follows a normal distribution, with a mean μ and a standard deviation σ, as illustrated in Figure 5.2. Groups 3 and 4 are by definition those that adopt the new idea within σ of the mean, which in a normal distribution means they contain about 34% of the population each. Similarly, group 2 adopts the idea between σ and 2σ before the mean and contains about 13.5% of the population, while group 1

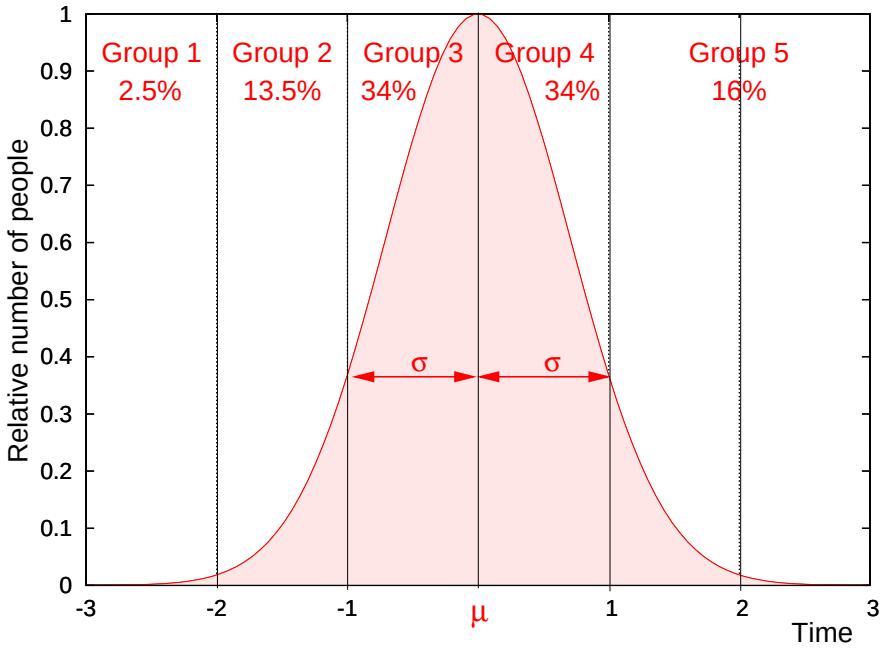

Figure 5.2: Acceptance of innovation over time. The scale on the time axis is in units of σ, the standard deviation of the distribution.

contains the earliest 2.5% of the population and group 5 the latest 16% (=13.5%+2.5%). McLean points out that, to achieve success in the adoption of an idea such as IT security, it is important to target the innovators and early adopters in the initial stages of the campaign; they will then help to bring the slower groups into line. Having a successful role model is in itself an important motivating factor for many people.

Spurling [72], in a 1995 case study from Alcoa Australia (whose principal product is aluminium, not an IT product), described some aspects of what the company had to do to ensure a higher level of IT security. Two major motivating factors were:

1. Commitment by the management;
2. Active involvement of all employees, so that they feel they are well-informed and their problems are listened to.

The actual awareness campaign at Alcoa appears to have been fairly traditional, involving oral presentations, security courses and awareness material based on several media, including booklets, cartoons, newsletters and screen savers. Despite this traditional approach, the awareness program was reported to be a success, so the motivating effect of knowing that “somebody cares” seems to have played a significant role.

Support for the idea that IT security in organisations is not just a question of writing a set of policy rules and buying some appropriate equipment, but also a matter which requires management to play a more active role, is provided by Wood [89]. His paper relies on empirical observation,

rather than statistical investigations, but his claims are widely accepted. Among Wood's main points are:

- Policies must be consistently and regularly enforced. (If there are exceptions to an item of policy under certain circumstances, they must be subjected to a risk analysis and fully documented.)
- Management must visibly support efforts to improve security.
- Management must allocate sufficient resources to achieve the level of security which they are aiming at.
- All users should go through regular security awareness reinforcement programmes.

In 1997, Williamson, Feyer, Cairns and Biancotti investigated what it is that motivates people to achieve a good climate for conventional industrial safety within an organisation [86]. They carried out a questionnaire-based study of 1560 workers (of whom 660 responded) in a wide range of jobs, and used factor analysis to reveal five important factors which affect safety (either positively or negatively):

- **Personal motivation:** Items which the respondent believes are necessary in order for him/her to behave more safely.
- **Positive safety practice:** Items which the respondent recognises as existing good practice with respect to safety.
- **Risk justification:** Excuses or reasons for not behaving safely.
- **Fatalism:** Expressions of the inevitability of failures of safety.
- **Optimism:** Expressions of the low probability of having an accident.

This corresponds in general terms to results from earlier studies, such as that of Cox and Cox [13]. To achieve better levels of safety, it is evidently important to counteract the demotivating beliefs associated with Risk Justification, Fatalism and Optimism, and to reinforce the motivating beliefs by providing personal motivators and ensuring that examples of good practice remain highly visible to everyone in the organisation. Although the Williamson study relates to conventional safety, the authors of the study point out that the beliefs observed were more or less invariable over a large range of workplaces and job types. Although this never seems to have been checked, there are therefore some grounds for believing that the results will also be valid for IT safety and security.

In the area of conventional safety, there have been a considerable number of studies of *safety culture* and its possible effect on the incidence of accidents in hazardous industries, such as the nuclear and chemical industries. There is no universally accepted definition of safety culture, but there is a general consensus that it describes the management and organisational factors which lead to safe operation. The corresponding concept in the area of ICT safety and security would be factors which lead to *Compliance*. Sorensen [71] gives a review of some studies of this topic in the area of nuclear power generation. Although it is widely believed that safety culture has an important effect on accident rates, Sorensen concludes that there is very little real statistical evidence for this belief – at least in the areas covered by Sorensen's review. More or less the

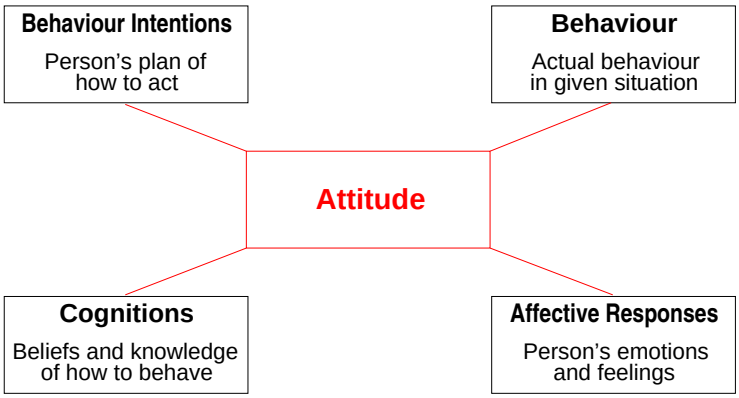

Figure 5.3: An attitude system

opposite point of view is, however, taken by Pidgeon [61], who claims that safety culture is "a concept uniquely capable of improving safety in complex systems". This seems to be an area where more research needs to be done.

5.4.2 Psychological Aspects of Motivation

Thomson and von Solms [75] analysed the task of improving information security awareness, using concepts from social psychology. Their analysis was based on an *attitude system*, as defined by Zimbardo and Leippe [92], which we show figuratively in Figure 5.3. Attitudes are affected by and interact with four factors, which also interact with one another:

- **Behaviour intentions:** The intentions of a person to behave in a certain way under certain conditions.
- **Behaviour:** The actual behaviour of a person under certain conditions.
- **Cognitions:** The knowledge and beliefs of a person regarding how one should behave under certain conditions.
- **Affective responses:** The emotional reactions shown by a person under certain conditions.

The challenge with respect to ICT safety and security is to change a person's *Behaviour* so that he/she behaves in a safe and secure manner. Following the general principles described by Zimbardo and Leippe, Thomson and von Solms considered three ways of doing this:

1. **Directly change** the person's **behaviour** (with no change of attitudes or knowledge). Well-known ways of achieving this include:
   - *Operant learning*, where "good" behaviour is rewarded and "bad" behaviour is punished.
   - *Shaping*, which encourages improvements in behaviour by making the rewards harder to get as time goes by.

- *Social learning*, where employees are encouraged to follow the example of their (well-behaved) peers.
- *Conformity*, where group pressure is exploited to improve standards.
- *Obedience*, where an authority sets the rules for what to do.
- *Reciprocity*, where the teacher treats the pupil nicely, in the expectation that the pupil will do the right thing "in return".
- *Commitment*, where the teacher gets the pupil to commit him/herself formally to a given course of action.

2. Change the person's **attitude via a change in behaviour**, thus (hopefully) ensuring a long-term change of behaviour. These changes can for example be based on:
   - *Attribution*, where the person concerned looks for rational reasons for his/her behaviour, and discovers that the only possible reason is a change in attitude.
   - *Self persuasion*, where the person (typically in a role play situation) is obliged to argue for a point of view which is contrary to his or her own.
   - *Dissonance*, where the person is obliged to deal with inconsistencies between his or her current attitudes and the behaviour exhibited.
3. Change the person's **attitude by persuasion**. This is generally believed to be the best long-term solution, but some well-known pedagogical requirements of Exposure, Comprehension, Acceptance and Retention of the message have to be fulfilled in order for it to work.

A more comprehensive treatment of motivation in relation to information security awareness was given by Siponen [70], who pointed out that most approaches to security awareness (such as [49, 87]) were *descriptive*, in the sense of just giving a set of guidelines without considering how to ensure that these guidelines would be followed. Like Thomsen and von Solms, Siponen proposed using behavioural theories as a basis for making the awareness program more *prescriptive*, so that users will internalise the guidelines as rules which they feel obliged to follow. The theories considered by Siponen were:

- Fishbein and Ajzen's **Theory of Reasoned Action (TRA)** [25]. This assumes that **behaviour** is determined by **intention**, which itself depends on:
  - I1. **Attitude**, which is determined by *behavioural beliefs* and *outcome evaluations*.
  - I2. **Subjective norms**, which are determined by *normative beliefs* and *motivation to comply*.
- Ajzen's **Theory of Planned Behaviour (TPB)** [1, 2]. This is a further development of TRA in which a third element contributes to intention:
  - I3. **Perceived behavioural control**, which is determined by *control beliefs* and *perceived facilitation*. According to Ajzen, these refer to people's perception of the ease of performing the behaviour of interest. Siponen took the point of view that this perception is most likely to be changed by technical training to increase skills. We discuss this point of view in more detail below.

  The relationships between the various quantities involved in the TPB (and TRA) are illustrated in Figure 5.4.

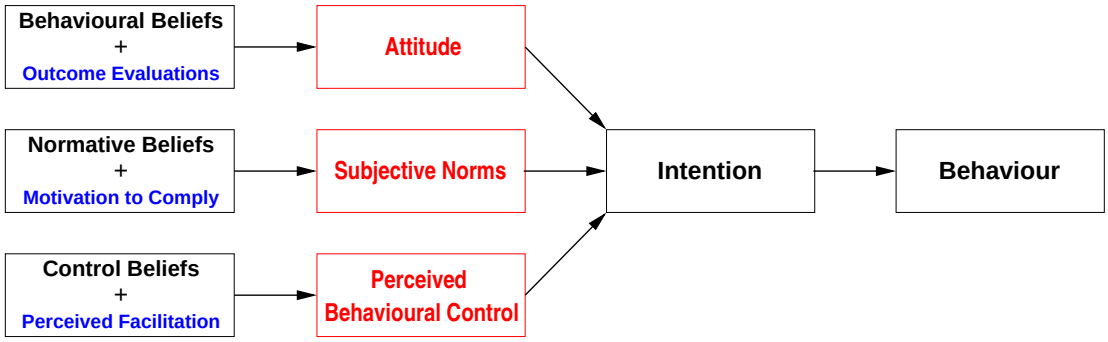

Figure 5.4: Relationships in the Theory of Planned Behaviour.

- Deci and Ryan's theory of **Intrinsic Motivation** [17]. Here the fundamental assumption is that people need to feel that they are free to make their own choices, and the question is how this can be ensured.
- Davis' **Technology Acceptance Model (TAM)** [16]. This model, often used to explain why people use or fail to use particular technologies, is based on the idea that actual use (i.e. behaviour) depends on **intention** to use, which in turn relies on a (positive) **attitude** to use, which in turn relies on two factors:

  A1. **Perceived usefulness**;
  A2. **Perceived ease of use**.

  In the context of information security, this means that security guidelines must appear to be useful to the user and simple to apply. Again, Siponen took the view that perceived ease of use is most likely to be changed by technical training to increase skills, a point of view which we consider in more detail below.

Siponen used these theories to explain why descriptive approaches to improving information security fail, and to indicate some strategies based on **persuasion** which are more effective. In order to achieve **intrinsic motivation**, the most useful strategies are those which are based on moral or ethical precepts, on inducing positive emotions, on persuading people that they can achieve a feeling of security, and on persuading people that security can prevent a loss of well-being. In order to achieve changes in **attitude**, as required according to TRA, TPB and TAM, strategies based on providing rational reasons for the desired behaviour or on the use of sanctions can also be used.

Another possible approach to motivation is to use *fear appeals* to change people's attitudes. This has been a common approach in public campaigns in several areas, particularly those related to health issues and road safety ("Smoking can damage your health", "Speed kills!", ...), and several psychological theories have been developed to explain how fear appeals work and should be applied. In the area of IT security, Weirich and Sasse investigated the use of fear appeals in a campaign to persuade users to use secure passwords [83]. Their approach was based on Rogers' *Protection Motivation Theory* [66], which in its most recent formulation postulates that an attitude change leading a person to (intend to) adopt a "good" response depends on that person's

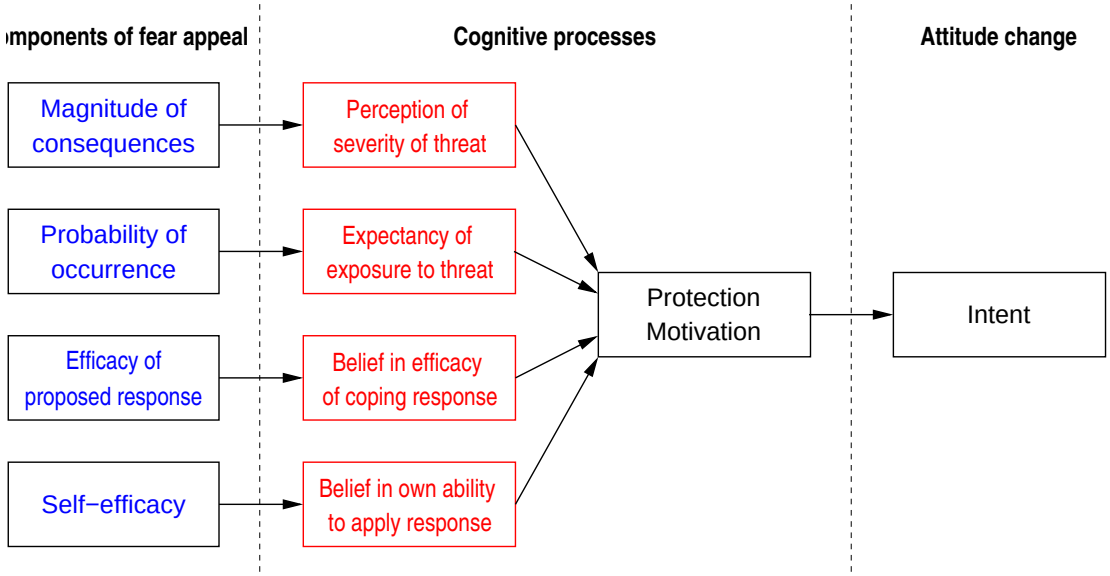

Figure 5.5: Rogers' Protection Motivation theory of fear appeals

motivation for protection, which in turn depends on the results of four cognitive processes:

1. Perception of the severity of the threat;
2. Perception of the probability of the threat materialising;
3. Perception of the efficacy of the response to cope with the threat;
4. Perception of the individual's own ability to produce this response (often known as *self-efficacy*).

This is illustrated in Figure 5.5. In the context of ICT safety and security, this means that a fear appeal to a user will be effective at getting the user to protect herself if the problem is serious, if it is likely to affect that user, if it can be avoided by taking suitable action and if the user is confident that she can in fact perform the action. By interviewing a group of users, Weirich and Sasse found that many of them initially could not see that poor use of passwords (lack of secrecy, use of weak passwords etc.) constituted a threat. It was therefore vital to provide a suitable fear appeal in order to rectify the situation. Interestingly, Weirich and Sasse suggested that if the users did not believe in any of the real existing threats, then the system managers could introduce a threat, such as making it difficult to get a new password if the old one got lost or compromised. Unfortunately, they did not report whether this approach actually had any effect. As the authors point out, it is well known that people often react negatively to fear appeals, so the efficacy of this approach is still unclear.

The question of how users view compliance towards an Information System security policy was considered by Pahnila, Siponen and Mahmood [58], who pointed out that there is very little theoretical or empirical basis for methods which attempt to ensure compliance. Pahnila et al. therefore carried out an investigation of 245 users in a Finnish company, to see whether they

could find support for a model covering this issue. The model combined several theoretical approaches:

- Fishbein and Aijzen's Theory of Reasoned Action (TRA) [25], which, as discussed above, postulates that:
  - Behaviour depends on intention, which in turn depends on attitude.
  - Attitude depends on normative beliefs, which reflect the normative expectations of other people.
- General Deterrence Theory, which mandates the adoption of appropriate **sanctions** for failure to comply.
- Rogers' Protection Motivation Theory [66], which is here used to explain how the users' perception of **threats** and perception of their own **ability to cope** with these threats affects their attitude to complying with IS security policies.
- DeLone and McLean's concept of Information Systems Success [18], which leads to the idea that compliance will depend on the **quality of the information** available in the system.
- Triandis' Behavioural Framework [76]. This extends Aijzen's Theory of Planned Behaviour with the ideas that people's attitudes to a task are amongst other things affected by:
  - **Facilitating conditions**, i.e. factors which are perceived as making the task easy. In the context of IT security policy compliance, this could include factors such as easy access to the policy, good training, ease of use of technical counter-measures and so on.
  - **Habits**. In the context of security, this indicates the importance of building up good habits from the very start.

A schematic view of the postulated relationships in the combined theory is shown in Figure 5.6. The results of the reported survey gave no support to the ideas that:

- Perception of own ability to cope with a threat has an effect on attitudes towards compliance.
- Sanctions have an effect on intention to comply.
- Rewards have any effect on actual compliance.

These unconfirmed relationships are indicated by dashed lines in the figure. There was, however, statistically significant evidence that the remaining relationships shown in the figure were valid. These results need to be taken into consideration in the design of awareness campaigns.

5.5 Comments on the Proposals

The proposals reviewed above approach the topic of improving ICT safety and security from a large variety of different starting points. One of the main reasons for this is the belief that

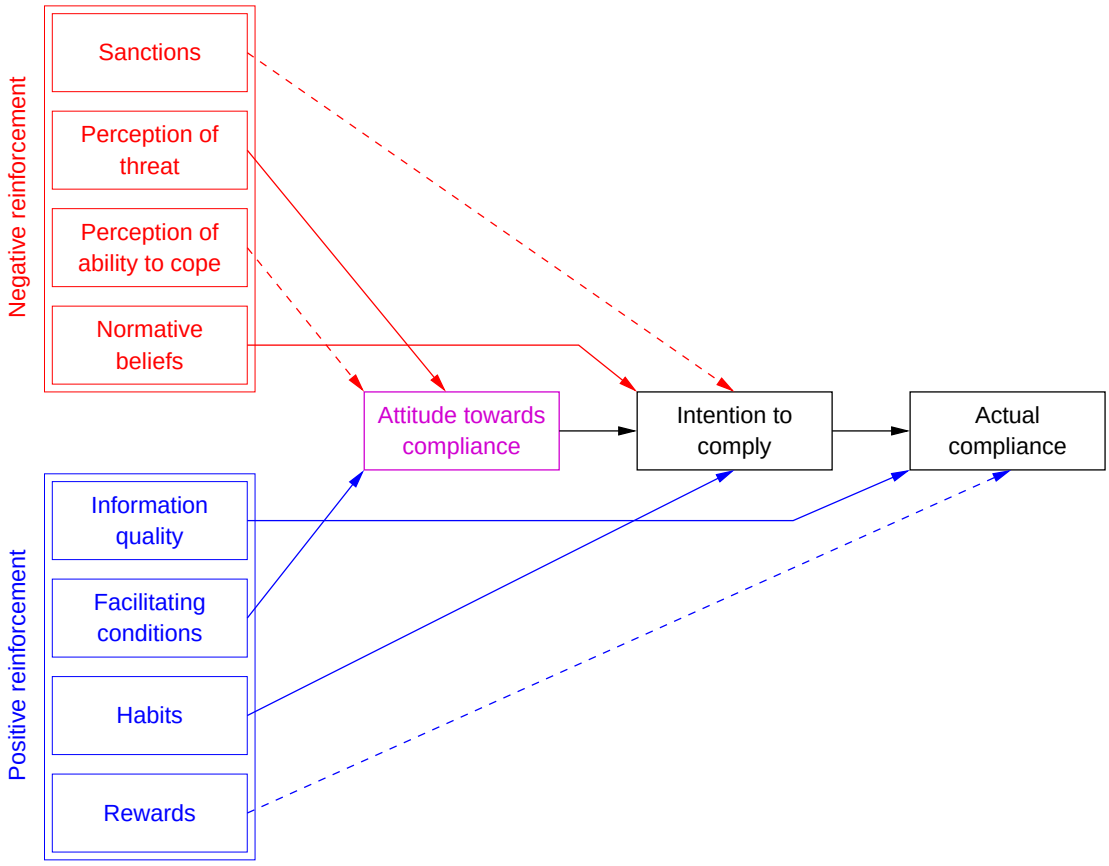

Figure 5.6: Pahnila, Siponen and Mahmood's model of factors affecting user compliance to IS security policies. Source: [58]

different segments of the population respond to awareness initiatives in different ways and have to be handled in a manner appropriate to their background and current needs. One particular dividing line separates the proposals for improving safety and security in enterprises from proposals aimed at the general public. Enterprises tend to follow a more regulatory approach based on company security policies, which in some branches of industry (such as banking) may lead to highly restrictive rules of behaviour and possibly severe sanctions for failure to comply. In most cultures, this approach is not acceptable to the general public, who also in general lack the technical ability and support which can make it feasible. Ordinary citizens therefore need an approach which is more based on persuasion and easily-digested information.

Another characteristic divide lies between those proposals whose effectiveness has actually been investigated and those proposals which describe purely theoretical models. Methodologies for running security awareness campaigns in enterprises, such as the widely used proposal from NIST [88], state clearly that the level of security awareness should be measured before and after the campaign. This would seem to be even more important if the campaign is run as part of a program of research into effective awareness improvement, since it is the only feasible way to evaluate whatever method is being used. Unfortunately the literature only contains very sparse material on such investigations. This is particularly noticeable in the case of campaigns aimed at the general public, where we have been unable to find *any* verifiable published reports of the effectiveness of a public campaign. Currently, it is therefore quite unclear how much of the theoretical work carried out on security campaigns in enterprises can be applied to the more general public.

Most proposals for improving safety and security are related to improving ICT safety or security *awareness* at the *knowledge* and, to a certain extent, the *compliance* level, where there have been a number of studies of what to do. At the level of *understanding*, the situation is less clear. As pointed out in Chapter 1 of this report, to improve the general level of safety and security it is necessary to ensure that users deploy appropriate technical and behavioural counter-measures against the existing threats. There are a number of issues to be dealt with here:

1. Users must know which technical measures to deploy (e.g. install a virus scanner).
2. Users must know how to deploy these measures (e.g. how to install and set up a virus scanner).
3. Users must know how to behave safely in relation to the activities in which they take part (e.g. don't open attachments in mails from senders whom you do not know).

The focus of current campaigns and websites is mostly on the first and last of these issues. Unfortunately, most of the sites which offer technical advice assume a considerable amount of pre-knowledge of the technical issues involved. Very little attention seems to have been paid to the question of how to improve *understanding* among non-technical users, so that they are better able to fend for themselves. Several previous investigations have demonstrated that it is notoriously difficult, even for relatively experienced IT users, to set up security mechanisms correctly on an ordinary home computer [84, 42, 29]. This is evidently an area which merits considerably more attention.

Chapter 6

Conclusion

In general terms, the studies of ICT safety and security which we have discussed in this report attempt to answer one or more of the following questions for a given segment of the population:

1. How do people use the Internet?
2. What issues and perceived risks occupy people's minds?
3. How common and how serious are incidents which cause actual damage to ICT assets or unpleasant personal experiences?
4. What do people do to reduce the risk of using the Internet?
5. What are people's attitudes to ICT safety and security?
6. How can the level of ICT safety and security be improved?

This is a very large area to cover, and general conclusions are therefore difficult to draw. However, some specific features of the studies are quite striking, and in this chapter we will comment briefly on these.

One noticeable feature is that the great majority of the studies which concern themselves with security and safety levels and counter-measures (i.e. questions 3 to 6) are concerned with ICT safety and security in *enterprises* rather than in the population as a whole. The reasons for this are never made explicit, but a qualified guess would be that both public and private enterprises are strongly affected by requirements for good IT governance, and therefore feel they have a *duty* to protect their information assets. This gives them a motivation for investigating their own situation, either alone or as part of a general initiative, and even makes them willing to pay substantial sums to obtain the necessary level of security. Citizens in general merely have a *desire* to protect their assets, and so do not have such a high degree of motivation. Investigations of ordinary citizens' ICT safety and security therefore only take place if a public or private funding organisation is willing to invest in an initiative to achieve better ICT security for the general population. This seems to happen relatively rarely. With the expanding use of the Internet for private banking, e-government, e-learning and similar activities, it would seem important to study the ICT security of the general population more closely.

Investigating (and hopefully improving) the level of ICT safety and security among the general population is difficult, not just because of the magnitude of the task, but also because the technical nature of the domain of ICT security makes it difficult to formulate questions which will actually be understood. Although this aspect of studies of the general population is often ignored, investigations such as the Forrester/BSA survey of consumers' needs [26] indicate very clearly that the general public's understanding of even quite common IT security terms is extremely limited. Worse still, it is a common observation among IT professionals that people without technical training often have a picture in their minds of how their computer works and what the Internet does which is very far from the technical reality. For example, it has been known since the time of Project MAC in the 1960s that people often think of the computer as a sentient being with a mind of its own ("It is thinking about it", "Oh, now it says…", or "It decided to…"). In more recent times, network technologies such as broadband networks, wireless networks and even the Internet itself have been the subjects of similarly imaginative "explanations", leading to observations such as "If I turn off the wireless network, then I can't hear the radio" or questions like "Have we reached the end of the Internet?". The models of the world which underly such statements can easily clash with explanations of safety and security. Use of the classic form of interview questionnaire generally relies on the assumption that the respondent can at least understand the questions. However, this assumption may well be ill-placed in the context of investigations into technical topics such as ICT security. It seems important to perform more serious investigations of people's understanding of basic ICT security concepts, so that subsequent investigations of people's *knowledge* and *understanding* can take place on a more solid foundation than they do today.

Another major challenge in relation to improving the level of ICT safety and security among the general public is to find methods which will motivate even non-technical persons to make their IT systems secure. In this respect, just asking people about their abilities and attitudes via questionnaire-based interviews or web sites is not very helpful. Cognitive studies, such as those we have considered in Section 5.4.2, indicate that, in order to be motivated, people must firstly recognise the seriousness of the problem to be dealt with, and secondly be convinced that they can solve the problem in a (relatively) simple way, preferably without being *forced* to do so. Traditional questionnaires do not offer either of these possibilities. If people are to improve their security level, there is a need for:

- Feedback to the respondent which directly illustrates how his or her behaviour can have serious consequences for his or her property or person.
- Explanations of steps which can be taken to improve this situation.
- Automatic re-evaluation of the respondent, so that better behaviour is praised or rewarded and poorer behaviour leads to opportunities for new suggestions of what to do.

These kinds of mechanism can be built into interactive training scenarios of various types, either based on interactive Web pages or embedded within computer or video games. This type of environment, essentially based on e-learning, can be set up in a way which appeals to large segments of the population.

As an example of this approach, some preliminary experiments have been carried out within the *CIT-AWARE* project, where *animated questionnaires* were presented on a Danish Web site [3]. Participants were exposed to simulated situations which might occur in their Web browser or mailer, where they had to make choices relevant to safety and security, and were given immediate feedback and advice based on their performance. The site attracted 230 respondents within a period of about 4 weeks, without any significant effort to advertise its existence. Respondents said that they found this combination of testing and learning very attractive. This approach, together with others based on e-learning, seems to merit further attention.

A large number of initiatives, such as campaigns and infosites, for improving the safety and security level of the general population have seen the light of day. It is, however, very noticeable that the actual effect of such initiatives is rarely (if ever) checked by repeated surveying or more extensive longitudinal studies. There are reports of a number of investigations in the early 1990s which attempted to find out how effective different promotional media were at changing the level of security awareness. The results of these investigations are, however, no longer publicly available, and we have been unable to find any more recent longitudinal studies of the general population. All the well-known guides to improving security awareness [68, 88, 90, 23] emphasise how important it is to measure the level of awareness both before and after a campaign or training initiative, and this advice is very commonly followed within enterprises. It would be very interesting to see a genuine longitudinal study of the effects of existing campaigns.

Finally, it seems appropriate to end this report with a word of caution: None of the surveys which were looked at could confirm the picture often presented in the media that the Internet is an extremely dangerous place to move around in, and that only by investing in expensive equipment and protective software can we protect ourselves against its perils. As in very many technical areas, the perceived risk greatly exceeds the objective risk, and in most cases quite simple technical precautions and rules of behaviour are enough to keep us safe. This is not an argument for complacency, but an argument for better education and information which will enable ordinary citizens to evaluate their security needs and take suitable precautions to protect their interests.

Bibliography

[1] I. Ajzen. From intentions to actions: A theory of planned behaviour. In J. Kuhl and J. Beckmann, editors, *Action Control: From Cognition to Behavior*, pages 11–39. Springer, New York, 1985.

[2] I. Ajzen. The theory of planned behaviour. *Organizational Behavior and Human Decision*, 50:179–211, 1991.

[3] Theo Andersen. Animerede spørgeskemaer for sikkerhedsbevidsthed. Msc thesis 2007-74, Informatics & Mathematical Modelling, Technical University of Denmark, July 2007. Available at URL: `http://www2.imm.dtu.dk/pubdb/views/edoc_download.php/5404/pdf/imm5404.pdf`.

[4] Harald Baier and Tobias Straub. *Awareness by Doing* – ein neues Koncept zur Sensibilisierung von IT-Anwendern. In *Beiträge des 9. Deutscher IT-Sicherheitskongress des BSI*. BSI, May 2005.

[5] Bürger-CERT. Sicher Informiert. Web publication, 2007. Homepage at `http://www.buerger-cert.de`.

[6] Bundesamt für Sicherheit in der Informationstechnik. Die Lage der IT-Sicherheit in Deutschland 2005. Report, BSI, July 2005. Available at URL: `http://www.bsi.bund.de/literat/lagebericht/lagebericht2005.pdf`.

[7] Bundesamt für Sicherheit in der Informationstechnik. Die Lage der IT-Sicherheit in Deutschland 2007. Report, BSI, July 2007. Available at URL: `http://www.bsi.bund.de/literat/lagebericht/lagebericht2007.pdf`.

[8] Bundesamt für Sicherheit in der Informationstechnik. Ins Internet – mit Sicherheit. Web publication, 2007. Homepage at `http://www.bsi-fuer-buerger.de/`.

[9] Federica Casarosa. A safer Internet for children: the European regulatory approach, with evidence from Italy and United Kingdom. In Victoria Nash, editor, *Safety and Security in a Networked World: Balancing Cyber-rights and Responsibilities*. Oxford Internet Institute, Web publication, September 2005. Available at URL: `http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/federica_casarosa.pdf`.

[10] CLUSIF. Politiques de sécurité des systèmes d'information et sinistralité en France. Bilan de l'année 2005. Report, Club de la Sécurité de l'information Francais, 30 Rue Pierre Sémard, Paris, 2006. Available at URL: `http://www.clusif.fr/fr/production/sinistralite/docs/etude2005.pdf`.

[11] CLUSIF. Cybercrime Overview 2006. Report, Club de la Sécurité de l'information Francais, 30 Rue Pierre Sémard, Paris, 2007. Available at URL: `http://www.clusif.fr/fr/production/ouvrages/pdf/CyberCrime2006.pdf`.

[12] Computer Security Institute. World Security Challenge. Web publication, 2007. Homepage at `http://www.gocsi.com/WSC/`.

[13] Sue Cox and Tom Cox. The structure of employee attitudes to safety: A European example. *Work and Stress*, 5(2):93–106, 1991.

[14] Rachna Dhamija, J.D. Tygar and Marti Hearst. Why phishing works. In *CHI2006: Proceedings of SIGCHI Conference on Human Factors in Computing Systems, Montréal, Canada*, pages 581–590. ACM, April 2006.

[15] Julia Davidson and Elena Martellozzo. Policing the Internet and protecting children from sex offenders online: When strangers become 'virtual friends'. In Victoria Nash, editor, *Safety and Security in a Networked World: Balancing Cyber-rights and Responsibilities*. Oxford Internet Institute, Web publication, September 2005. Available at URL: `http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/julia_davidson.pdf`.

[16] F.D. Davis. Perceived usefulness, perceived ease of use, and end user acceptance of information technology. *MIS Quarterly*, 13(3):319–40, September 1989.

[17] Edward L. Deci and Richard M. Ryan. *Intrinsic Motivation and Self-determination in Human Behaviour*. Plenum Press, New York, 1985. ISBN 1-85000-920-1.

[18] William H. DeLone and Ephraim R. McLean. Information systems success: The quest for the dependent variable. *Information Systems Research*, 3(1):60–95, 1992.

[19] Simone Dimler. Fragebogen zu IT-Sicherheit und Datenschutz. On-line publication, November 2005. Available at URL: `http://www-sec.uni-regensburg.de/awarenessstudie/fragebogen.pdf`.

[20] Simone Dimler, Hannes Federath, Thomas Nowey, and Klaus Plößl. Awareness für IT-Sicherheit und Datenschutz in der Hochschuleausbildung – Eine empirische Untersuchung. In *Sicherheit 2006. Beiträge der 3. Jahrestagung des GI-Fachbereichs Sicherheit*, number P-77 in Lecture Notes in Informatics, pages 18–21. Köllen-Verlag, 2006.

[21] William H. Dutton, Corinna di Gennaro, and Andrea Millwood Hargrave. The Oxford Internet Survey (OxIS) Report 2005: The Internet in Britain. Technical report, Oxford Internet Institute, University of Oxford, 1 St. Giles, Oxford, UK, May 2005. Available at URL: `http://www.oii.ox.ac.uk/research/oxis/oxis2005_report.pdf`.

[22] William H. Dutton and Ellen J. Helsper. The Internet in Britain: 2007. Technical report, Oxford Internet Institute, University of Oxford, 1 St. Giles, Oxford, UK, July 2007. Available at URL: `http://www.oii.ox.ac.uk/research/oxis/OxIS2007_Report.pdf`.

[23] European Network and Information Security Agency. A User's Guide: How to Raise Information Security Awareness. Report, ENISA, June 2006. Available at URL: `http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf`.

[24] David Finkelhor, Kimberly J. Mitchell, and Janis Wolak. Online Victimisation: A Report on the Nation's Youth. Report, Crimes against Children Research Center, University of

New Hampshire, Durham, New Hampshire, March 2000. Available at URL: http://www.missingkids.com/en_US/publications/NC62.pdf.

[25] Martin Fishbein and I. Ajzen. *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research*. Addison-Wesley, Reading, MA., June 1975. ISBN 0-20102-089-2.

[26] Forrester Custom Consumer Research. Understanding consumers' needs for Internet security. Report, Business Software Association, November 2005. Available via URL: http://www.bsa.org/usa/research/.

[27] Dirk Fox and Sven Kaun. Security Awareness-Kampagnen. In *Beiträge des 9. Deutscher IT-Sicherheitskongress des BSI*, pages 329–337. BSI, May 2005.

[28] Anna Frisk and Roger Törnberg. It-säkerhetskultur bland socialsekreterare. Master's thesis, Department of Computer and System Sciences, Stockholm University, October 2004.

[29] Steven Furnell. Why users cannot use security. *Computers & Security*, 24:274–279, 2005.

[30] Jayne Gackenbach, editor. *Psychology on the Internet: Intrapersonal, Interpersonal and Transpersonal Implications*. Elsevier, London, second edition, 2007.

[31] Chris Garrett. Developing a security-awareness culture – Improving security decision making. Whitepaper, SANS Institute, 2005. Available at URL: http://www.sans.org/reading_room/whitepapers/awareness/1526.php.

[32] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Robert Richardson. 2006 CSI/FBI Computer Crime and Security Survey. Technical report, Computer Security Institute, 2006. Available via URL: http://www.gocsi.com/.

[33] Melissa Guenther. Security awareness incident response scenarios: Experiential learning for meetings or to supplement presentations. Web publication, 2001. Available at URL: http://www.iwar.org.uk/comsec/resources/sa-tools/Scenario-Based-Exercises-for-Security-Awareness.pdf.

[34] Melanie Hills. You are what you type: Language and gender deception on the Internet. Bachelor's thesis, University of Otago, 2000. Available at URL: http://www.netsafe.org.nz/Doc_Library/Internet_language_dissertation.pdf.

[35] H.M. Government. ITsafe. Web publication, 2006. Homepage at http://www.itsafe.gov.uk/.

[36] H.M. Government. Get Safe Online. Web publication, 2007. Homepage at http://www.getsafeonline.org/.

[37] Information Warfare Site. Security awareness toolbox. Web publication, 2006. Homepage at URL: http://www.iwar.org.uk/comsec/resources/sa-tools/.

[38] Internet Safety Group. Girls on the net: The survey of adolescent girls' use of the Internet in New Zealand. Technical report, February 2001. Available at URL: http://www.netsafe.org.nz/Doc_Library/girlsonthenet.pdf.

[39] Internet Safety Group. Computer Security - the Net Basics and more. Web publication, 2007. Homepage at http://www.netsafe.org.nz/security/security_default.aspx.

[40] IT- og Telestyrelsen. IT-borger. Web publication, 2007. Homepage at http://www.it-borger.dk.

[41] IT- og Telestyrelsen. Netsikker nu! 2007. Web publication, 2007. Homepage at http://www.netsikkernu.dk.

[42] J. Johnston, J.H.P. Eloff, and L. Labuschagne. Security and human computer interfaces. *Computers & Security*, 22(8):675–684, 2003.

[43] Adam N. Joinson. Disinhibition and the Internet. In Jayne Gackenbach, editor, *Psychology on the Internet: Intrapersonal, Interpersonal and Transpersonal Implications*, chapter 4. Elsevier, London, second edition, 2007.

[44] Daniel Kahneman, Paul Slovic, and Amos Tversky, editors. *Judgment under Uncertainty: Heuristics and Biases*. Cambridge University Press, Cambridge, 1982. ISBN 0-521-28414-7.

[45] KES/Microsoft. Sicherheitsstudie 2004: Lagebericht zur Informations-Sicherheit. *kes*, (4–5), 2004. Online version available via URL: `http://www.kes.info/archiv/material/studie2004/ergebnis.htm`.

[46] KES/Microsoft. Sicherheitsstudie 2006: Lagebericht zur Informations-Sicherheit. *kes*, (4–6), 2006. Online version available via URL: `http://www.kes.info/archiv/material/studie2006/ergebnis.htm`.

[47] Sarah Lichtenstein, Baruch Fischoff, and Lawrence D. Phillips. Calibration of probabilities: State of the art to 1980. In Daniel Kahneman, Paul Slovic, and Amos Tversky, editors, *Judgment under Uncertainty: Heuristics and Biases*, chapter 22, pages 306–334. Cambridge University Press, New York, 1982.

[48] Eva Lievens, Peggy Valcke, and David Stevens. Protecting minors against harmful media content: Towards a regulatory checklist. In Victoria Nash, editor, *Safety and Security in a Networked World: Balancing Cyber-rights and Responsibilities*. Oxford Internet Institute, Web publication, September 2005. Available at URL: `http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/eva_lievens.pdf`.

[49] Kevin McLean. Information security awareness – selling the cause. In *Proceedings of the IFIP TC11 Eighth International Conference on Information Security, IFIP/Sec '92, Singapore*, pages 179–193. IFIP, May 1992.

[50] NetAlert Limited. Internet Safety Needs Highlighted as Cyber Survey Reveals Kids Online Younger and Longer. Online publication, April 2005. Synopsis of NetAlert/ABA report on Internet usage (Reference [52]).

[51] NetAlert Limited. Education programs. Web publication, 2007. Homepage at `http://www.netalert.gov.au/programs.html`.

[52] NetRatings Australia Pty Ltd. Internet use in Australian homes. Report, Australian Broadcasting Authority and NetAlert Limited, April 2005. Available at URL: `http://www.netalert.net.au/02010-kidsonline@home---Internet-use-in-Australia-homes---April-2005.pdf`.

[53] Norsk Senter for Informasjonssikring. Nettopp. Web publication, 2007. Homepage at `http://www.norsis.no`.

[54] Rachel O'Connell. Be somebody else but be yourself at all times: Degrees of identity deception in chatrooms. Web publication, 2001. Available at URL: `http://www.once.uclan.ac.uk/print/deception_print.htm`.

[55] Rachel O'Connell, Joanna Price, and Charlotte Barrow. Cyber stalking, abusive cyber sex and online grooming: A programme of education for teenagers. Technical report,

Cyberspace Research Unit, University of Central Lancashire, May 2004. Available at URL: http://www.uclan.ac.uk/host/cru/docs/NewCyberStalking.pdf.

[56] Ofcom. Media Literacy Audit: Report on adult media literacy. Technical report, Office of Communications, March 2006. Available at URL: http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/medialit_audit/medialit_audit.pdf.

[57] Ofcom. Media Literacy Audit: Report on media literacy amongst children. Technical report, Office of Communications, May 2006. Available at URL: http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/children/children.pdf.

[58] Seppo Pahnila, Mikko Siponen, and Adam Mahmood. Employees' behavior towards IS security policy compliance. In *HICSS'07: Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, page 156b. IEEE Computer Society, January 2007.

[59] Parkegaard og Kristensen Sikkerhed. Undersøgelse af den danske befolknings holdning til it-sikkerhed. Report, IT- og Telestyrelsen, 2006. Available via URL: http://itst.dk/static/Rapporter/befolkningsunders%F8gelse%20til%20offentligg%F8relse.pdf.

[60] Penn, Schoeland and Berland Associates, Inc. Key Findings from the BSA/ISSA Information Security Survey. Web publication, Business Software Association, February 2005. Available via URL: http://www.bsa.org/usa/research/.

[61] Nick Pidgeon. Safety culture: Key theoretical issues. *Work and Stress*, 12(3):202–216, 1998.

[62] Nick Pidgeon, Roger Kasperson, and Paul Slovic, editors. *The Social Amplification of Risk*. Cambridge University Press, Cambridge, July 2003. ISBN 0-521-52044-4.

[63] G.F. Pitz. Subjective probability distributions for imperfectly known quantities. In Lee W. Gregg, editor, *Knowledge and Cognition*, Carnegie Mellon Symposia on Cognition Series, chapter 3, pages 29–41. Lawrence Erlbaum Associates, Potomac, Maryland, 1974. ISBN 0-470-32657-3.

[64] Princeton Survey Research Associates. A matter of trust: What users want from web sites. Technical report, Consumer Webwatch, January 2002. Available at URL: http://www.consumerwebwatch.org/pdfs/a-matter-of-trust.pdf.

[65] Princeton Survey Research Associates International. Leap of faith: Using the Internet despite the dangers. Technical report, Consumer Reports Webwatch, 101 Trueman Avenue, Yonkers, N.Y., October 2005. Available at URL: http://www.consumerwebwatch.org/pdfs/princeton.pdf.

[66] Ronald W. Rogers. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In John Cacioppo and Richard Petty, editors, *Social Psychophysiology*, pages 153–176. Guilford Press, New York, 1983.

[67] Royal Society. Risk: Analysis, perception and management. Report of a Royal Society Working Group, Royal Society, London, 1992.

[68] K. Rudolph, Gale Warshawsky, and Louis Numkin. Security Awareness. In Seymour Bosworth and M.E. Kabay, editors, *Computer Security Handbook*, chapter 29. 4th. edition, 2002. Available at URL: http://www.nativeintelligence.com/ni-programs/cshch29kr.pdf.

[69] SANS Institute. SANS Top-20 Internet Security Attack Targets (2006 Annual Update). Web publication, November 2006. Available at URL: `http://www.sans.org/top20/`.

[70] Mikko T. Siponen. A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, 8(1):31–41, 2000.

[71] J. N. Sorensen. Safety culture: a survey of the state-of-the-art. *Reliability Engineering and System Safety*, 76:189–204, 2002.

[72] Phil Spurling. Promoting security awareness and commitment. *Information Management and Security*, 3(2):20–26, 1995.

[73] Detmar W. Straub, Jr. Effective IS security: An empirical study. *Information Systems Research*, 1(3):255–276, 1990.

[74] Teknologisk Institut. Borgernes IKT-færdigheder i Danmark. Report, IT- og Telestyrelsen, January 2007. Available at URL: `http://itst.dk/static/Rapporter/Rapport%20om%20borgerpolitik%20for%20IKT%20f%E6rdigheder%20endelig.pdf`.

[75] M.E. Thomson and R. von Solms. Information security awareness: Educating your users effectively. *Information Management and Computer Security*, 6(4):167–173, 1998.

[76] Harry C. Triandis. Values, attitudes and interpersonal behaviour. In Herbert E. Howe, Jr. and Monte M. Page, editors, *Beliefs, Attitudes and Values*, volume 27 of *Nebraska Symposium on Motivation Series*, pages 195–259. University of Nebraska-Lincoln, Department of Psychology, University of Nebraska Press, April 1979.

[77] Amos Tversky and Daniel Kahneman. The framing of decisions and the psychology of choice. *Science*, 211:453–458, January 1981.

[78] US-CERT. Cyber security tips. Web publication, September 2006. Homepage at `http://www.us-cert.gov/cas/tips/index.html`.

[79] Patti M. Valkenburg, Alexander P. Schouten, and Jochen Peter. Adolescents' identity experiments on the Internet. *New Media & Society*, 7(3):383–402, 2005.

[80] Connie K. Varnhagen. Children and the Internet. In Jayne Gackenbach, editor, *Psychology on the Internet: Intrapersonal, Interpersonal and Transpersonal Implications*, chapter 2. Elsevier, London, second edition, 2007.

[81] Rob Walker. Everyday stories of people using the Internet. In Victoria Nash, editor, *Safety and Security in a Networked World: Balancing Cyber-rights and Responsibilities*. Oxford Internet Institute, Web publication, September 2005. Available at URL: `http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/rob_walker.pdf`.

[82] Rob Walker and Babis Bakopoulos. Conversations in the dark: How young people manage chatroom relationships. *First Monday*, 10(4), April 2005. On-line publication, available at URL: `http://firstmonday.org/issues/issues10_4/walker/index.html`.

[83] Dirk Weirich and Martina Angela Sasse. Pretty Good Persuasion: A first step towards effective password security for the Real World. In *NSPW'01: Proceedings New Security Paradigms Workshop 2001, Cloudcroft, New Mexico*, pages 137–143. ACM Press, September 2001.

[84] Alma Whitten and J.D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th Usenix Security Symposium, Washington, D.C.*, pages 23–26. Usenix Association, August 1999.

[85] Laura Widyanto and Mark Griffiths. Internet addiction: Does it really exist? In Jayne Gackenbach, editor, *Psychology on the Internet: Intrapersonal, Interpersonal and Transpersonal Implications*, chapter 6. Elsevier, London, second edition, 2007.

[86] Ann M. Williamson, Anne-Marie Feyer, David Cairns, and Deborah Biancotti. The development of a measure of safety climate: The role of safety perceptions and attitudes. *Safety Science*, 25(1):15–27, 1997.

[87] Mark Wilson, Dorothea E. de Zafra, Sadie I. Pitcher, John D. Tressler, and John B. Ippolito. Information technology security training requirements: A role- and performance-based model. Special Publication 800–16, NIST, March 1998.

[88] Mark Wilson and Joan Hash. Building an information technology security awareness and training program. Special Publication 800–50, NIST, October 2003.

[89] Charles Cresson Wood. Policies alone do not constitute a sufficient awareness effort. *Computer Fraud & Security*, pages 14–19, December 1997.

[90] Steve Wooding, Aarti Anhal, and Lorenzo Valeri. Raising citizen awareness of information security: A practical guide. Report, eAware consortium, September 2003. Available at URL: `http://www.clusit.it/whitepapers/eaware_practical_guide.pdf`.

[91] Kimberly S. Young. The research and controversy surrounding Internet addiction. *CyberPsychology and Behaviour*, 2:381–383, 1999.

[92] Philip G. Zimbardo and Michael R. Leippe. *The Psychology of Attitude Change and Social Influence*. McGraw-Hill, New York, June 1991. ISBN 0-07072-877-1.