Financial Services Authority

Countering Financial Crime Risks in Information Security

Financial Crime Sector Report

November 2004

Contents

1. Executive summary

Introduction

1.1 This report sets out the findings of our recent review of industry practices and standards in Information Security risk management relating to electronically-held data. The review covered internal and external threats to UK financial services firms. It also considered firms' interaction with the financial services industry and other stakeholders, including government bodies involved in fighting financial crime.

1.2 In line with the FSA's principle of senior management responsibility for risk management and controls, firms' directors and senior managers are responsible for countering the crimes Information Security risks can give rise to. And they are responsible for providing an effective lead within a firm to promote an anti-fraud culture. SYSC 3.2.6R states that a firm must take reasonable care to establish and maintain effective systems and controls to comply with applicable requirements and standards under the regulatory system. They must also counter the risk that the firm might be used to further financial crime.

1.3 This report does not constitute formal guidance from the FSA given under section 157 of the Financial Services and Markets Act. We hope that the findings of our review will help senior managers and staff involved in Information Security risk management in the financial services industry. It aims to help them compare the nature of their risks and risk management practices with those of their peers.

1.4 The FSA's Risk Review Department visited 18 firms, including retail and wholesale banks, investment firms and insurance companies. We undertook a systematic review following recurrent observations of Information Security weaknesses in both large and small financial services firms and in the light of a changing environment, for example the emergence of 'phishing' attacks.

1.5 We would like to thank the staff in firms that participated in the review for the information they supplied before and during our visits and for meeting us.

Main conclusions

1.6 Our overall conclusion is that while crystallised losses are low, Information Security issues pose a material risk to our objective to reduce financial crime. Firms could be more active in managing Information Security risks rather than being reactive to events, to protect better their own assets and those of their customers from the risk of fraudulent activity.

1.7 We observed a heightened awareness of the financial crime risks arising from poor Information Security. However, we also learned of a number of serious incidents such as failed firewalls and virus infections, as well as other near misses caused by inadequate Information Security. While some larger firms appear to have made progress, smaller and medium-size firms continue to carry more serious and substantial Information Security risks.

1.8 Many firms believe that their investment in Information Security is adequate, but they still experience Information Security breaches. Other firms appear to have increased spending on Information Security in response to a security breach, financial loss or a discovered vulnerability. We recognise that the level of Information Security investment should reflect the scale, nature and complexity of a firm. However, firms need to be alert to the Information Security risks they face and take risk-based, proportionate measures. Firms need to be aware of the ever-changing complexities of current Information Security threats and should review and prepare for them.

1.9 Most firms have had Information Security policies in place for many years, yet associated procedures and role responsibilities have not always been comprehensive. Firms' management have not always updated these policies to address the risks from new technologies, and control procedures may not be developed until firms' policies are updated.

1.10 The emergence of new threats to the industry has served to remind firms' management that they need to secure their assets and those of their customers from both internal and external threats.

- 'Phishing' attacks aimed at identity theft are an increasing financial crime risk. Firms cannot afford to be complacent in their defence strategy to protect themselves and their customers from the threat of such fraudsters. Firms' education of consumers plays a role in prevention; and well defined Incident Management procedures contribute to addressing attacks efficiently.
- 'Patch management' plays a significant role in addressing internet threats. Many smaller firms have yet to create an inventory of software versions; distribution of fixes was sometimes delayed through their inability to install patches automatically.
- The firms visited felt that outsourcing presented additional Information Security risks. The choice of function outsourced appeared to be critical – for example, outsourcing user administration made firms particularly vulnerable to financial crime risks. Although firms recognised the potential to save costs through outsourcing, their priority was to have direct control over critical processes.
- Few firms have created adequate reporting systems and automatic alerts on external threats using intrusion detection software because of a lack of technical expertise.

1.11 While new risks are emerging, we concluded that firms are still exposed to more traditional threats because information security frameworks, including risk management processes and practices, are not yet widely developed. Many firms have not invested sufficiently in controls – many 'old' risks, such as legacy systems with poor security design, remain.

- In our review, some firms were unable to articulate how they identify and assess Information Security risks. Where risks are recognised, there are weaknesses in monitoring. For example, firms' internal monitoring of events remains patchy with inconsistent, non-independent checks over the use of privileged accounts.
- Staff can play an important role in controlling or mitigating Information Security risks. However, staff training often misses opportunities to promote a culture of Information Security. This exposes the firm to unnecessary risks and costs. Some education material lacks impact – although for a minimum cost, enhanced security focus and awareness could effectively reduce exposure to viruses. For staff directly involved in Information Security controls, there are weaknesses in some cases. For example, firms lacking expertise to develop intrusion detection alerts and analytical reports, to deal with 'phishing' and to carry out technical IT internal audit reviews.
- Deficiencies in user administration continue to present risks to the effective segregation of duties for both users and technicians. Central account management appeared to be more robust than distributed maintenance. Some firms have carried out identity management projects to improve user administration.

1.12 Various industry bodies and government agencies are working to reduce financial crime. However, there appears to be a degree of overlap and duplication of effort in terms of Information Security advice. Many small-to-medium size firms are unaware of the many industry and law enforcement programmes and initiatives designed to fight financial crime. These include issuing guidance on best practice and publicising existing guidance. Few firms have fostered relations with the relevant bodies that are able to provide technical assistance and standards guidance to firms.

1.13 Our supervisory approach has considered Information Security under the IT risk element of our risk assessment framework. This may not have encouraged supervisors to consider the financial crime risks associated with it. We will use the fraud awareness training programme to give supervisors more tools to consider related risks.

1.14 We list the conclusions from each finding at the end of every topic.

Joy Alderton and Austin Dunn led the review and prepared this report.

The report is published for information but should you wish to provide us with comments please address them to:

Joy Alderton or Charlotte Gerken
The Financial Services Authority
25 The North Colonnade
London E14 5HS
Email: joy.alderton@fsa.gov.uk or charlotte.gerken@fsa.gov.uk
Telephone: 020 7066 0520 or 020 7066 1704

2. Introduction

Objectives

2.1 We aimed to investigate:

(i) how financial services firms manage their Information Security risks;

(ii) how these risks are evolving;

(iii) the risks they pose to our objectives; and

(iv) the role industry and government bodies play in assisting regulated firms to address these Information Security risks.

2.2 Financial Crime is nothing new; however, the ways in which financial crime is being committed are changing. Criminals are increasingly using Information Technology (IT) to commit crime. This is probably due to criminals' recognition that fraud, extortion and money laundering crimes can be committed just as easily in electronic form as they can physically. They realise poor Information Security offers a quick, cheap and easy way to commit financial crime against firms and their customers.

Scope

2.3 Our review covered industry practices and standards in Information Security relating to electronically-held data. It considered internal and external threats to UK financial services firms.

Why carry out this review?

2.4 The FSA has a statutory objective to reduce financial crime. Our scope is broad, requiring us to reduce the extent that regulated persons and unauthorised businesses can be used 'for a purpose concerned with financial crime'. Financial crime includes any offence involving fraud or dishonesty, market abuse and money laundering.

2.5 The Financial Services and Markets Act 2000 (FSMA) requires us to regard, in particular, the importance of regulated firms being aware of the risk of their businesses being used in connection with financial crime.

2.6 Information Security risks can contribute to financial crime risk. For example, someone gaining unauthorised access to information could use it to perpetrate fraud and market abuse. Our financial crime objective supports and is supported by our other statutory objectives of market confidence, customer protection and public awareness.

2.7 Trust in information is at the core of the financial services business. It is therefore imperative that firms provide controls to maintain the confidentiality and integrity of their information systems. This will minimise opportunities for financial crime.

2.8 Our visits to firms often revealed some issues with firms' management of their Information Security risks. With this in mind – and with the impact of issues such as the increasing use of outsourcing and the increase in 'phishing' identity thefts – we decided to carry out a structured review of Information Security risks.

2.9 We intend that this project:

- mitigates risks to our consumer protection and financial crime objectives by raising awareness of Information Security risks and the need for appropriate controls across firms, consumers and the FSA;
- improves the assessment of such risks by the FSA; and
- enhances the protection of customers' information.

This report does not constitute formal guidance from the FSA given under section 157 of the FSMA.

Methodology

2.10 We visited the following types of firm between May and July 2004, basing each visit on a standard questionnaire that enabled us to compare practices. We interviewed staff with similar roles in each organisation to gain a balanced appreciation of how Information Security was governed by those with varying interest in its management.

2.11 Where separate roles existed, we held standard sessions with the Heads of IT, Information Security, IT Operations, IT Internal Audit, Fraud and Human Resources. Where separate roles did not exist, for example in smaller firms, we aimed to cover those who had responsibility for these functions. We documented visits using a standard report framework enabling us to identify 'readily' differences between firms' operations.

2.12 Please note that the scope of the visit questionnaire was limited to the security of information held in electronic format and did not cover plastic card financial crime.

Type of firm	*Total Number*	*Small*	*Medium*	*Large*
Wholesale Banks	2	1		1
Retail Banks	5	2		3
Insurance (Life & General)	5		4	1
Broker (Securities)	2	2		
IFA	1	1		
Fund Management	2		2	
Fund Administrator	1		1	
Total	***18***	***6***	***7***	***5***

Categories were based upon number of UK-based employees: Small = under 100; Medium = between 100 and 10,000; and Large = over 10,000.

2.13 We also met representatives from the following government, industry and consultancy organisations to obtain their perspectives on emerging Information Security risks and to understand their interaction with regulated firms.

- Central Sponsor for Information Assurance (CSIA)
- National Hi-Tech Crime Unit (NHTCU)
- National Infrastructure Security Co-ordination Centre (NISCC)

2.14 In assessing firms' standards and practices, we used information about industry practice, as derived from the following sources:

- Association of Payment Clearing Services (APACS);
- British Bankers' Association (BBA);
- Department of Trade and Industry (DTI);
- Information Assurance Advisory Council (IAAC);
- Deloitte & Touche – Technology Assurance (Deloitte); and
- KPMG.

2.15 We would like to thank the firms and interested parties who have helped in this review.

3. How big is the problem?

3.1 The exact value and frequency of financial crime committed in the UK is difficult to measure, with many surveys reporting across different industry sectors. While a firm can often assess the cost of detected financial fraud, it is harder to calculate the cost of crimes such as systems hacking, virus infection or of reputation damage caused by website violation. In this paper, we use the term 'financial crime' to mean both traditional financial fraud, as well as crime committed in new ways using IT, such as extorting money from firms to prevent Denial of Service (DoS) attacks.

3.2 The prevalence of hi-tech financial crime reported varies, but for the year 2003, 83% (NHTCU) and 94% (DTI) of firms in financial crime surveys said they had been attacked. In the NHTCU survey, of the 201 responding firms, 77% had experienced virus attacks, 20% DoS attacks, 17% financial fraud and 11% system penetration. In terms of the monetary cost, hi-tech crime accounted for £74m of the £195m financial crime total in the 201 surveyed firms, 44 of which were financial service firms. However, given firms' reluctance to report financial crime, the actual costs may be greater than reported.

3.3 The average 'cost per incident' is reported to range from £10,000 for a small firm to £120,000 for larger firms, with systems down-time being the biggest contributor to cost (DTI). When incident cost is considered against the frequency of attacks, with some large firms being attacked daily, it is easy to see how the cost escalates. Indeed, as Len Hynds, Head of the NHTCU, put it in February 2003: 'It is too early to put an accurate figure on the total financial impact for UK business, but all the indicators suggest that we are talking about billions rather than millions'.

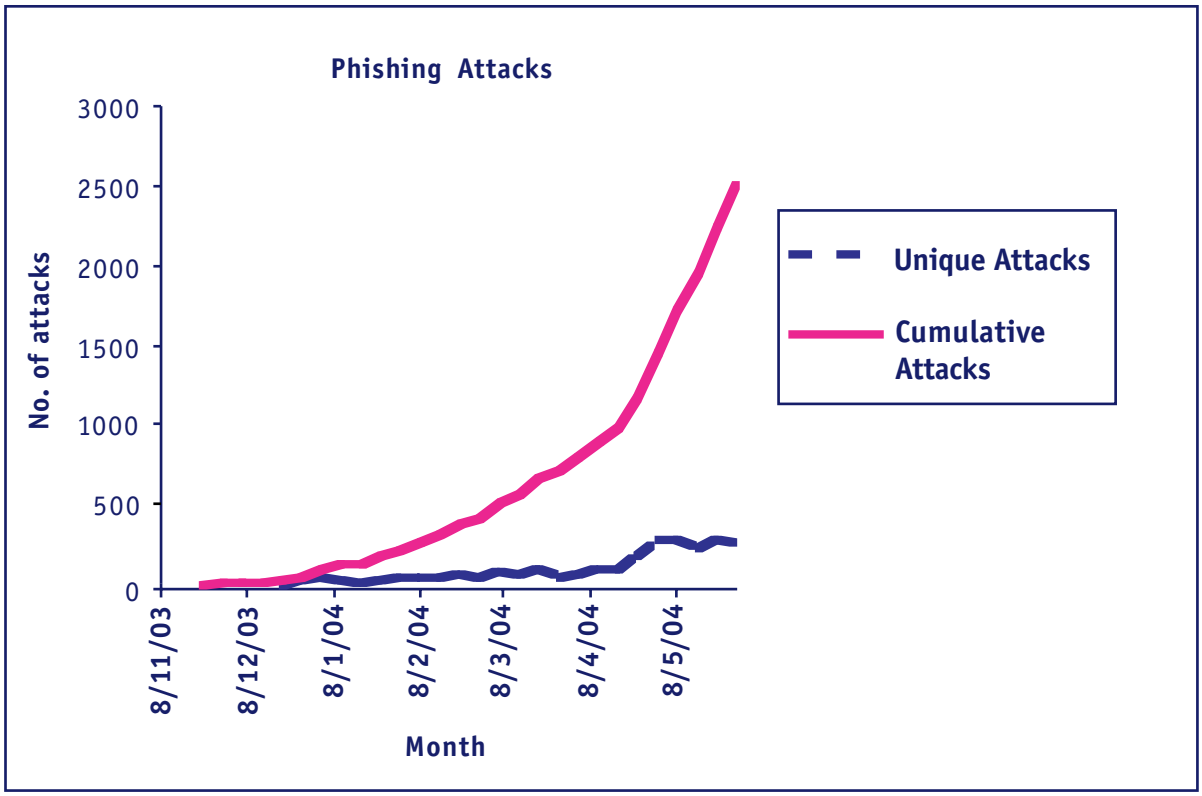
3.4 While the amount of UK losses is currently relatively low, we have looked at the experience in the US to gain an indicator of the potential threat, albeit across a larger population. Gartner Research reported in May that 'phishing' attacks cost US banks and credit card companies US$1.2 billion in 2003 and estimated that about 57 million Americans received a 'phishing' email last year.

3.5 Defences against hackers necessarily take time to devise, develop and implement. It often takes firms a significant period to develop technical infrastructure projects; an off-the-shelf solution also may not be straightforward to install. Firms will need to work not only on protection against current threats, but also have adequate systems to identify risks that emerge increasingly quickly.

3.6 In line with our principles of good regulation, we should take account of innovation and competition. Information security risks may affect the balance of us pursuing our financial crime objective while avoiding creating unreasonable barriers to entry or

restricting the launch of new products and services. Negative publicity about e-commerce may damage consumer confidence in this delivery channel.

3.7 From a consumer perspective, fraudsters have increased their 'phishing' activities dramatically; with financial services the most commonly attacked industry. In April 2004, the Anti-Phishing Working Group (an industry association) identified 1,197 unique 'phishing' incidents in April 2004. This was a 180% increase over the number of attacks reported in March 2004 and a 647% increase on the number reported in January 2004. Each 'phishing' attempt can result in thousands of people receiving a 'phishing' email asking them for bank account details, irrespective of whether they have an online bank account. Because 'phishing' scams are sent to thousands of people, even a small success rate in obtaining a person's online account and personal details encourages more 'phishing' attacks.



Anti-Phishing Working Group, Phishing Attack Trends Report, April 2004.

4. Main findings

4.1 The main findings from our review are presented below. Firstly, they cover threats to Information Security from 'phishing' and then the part that various industry and law enforcement agencies play to counter these and other types of Information Security-related financial crime. We then cover the establishment of an Information Security framework and some fundamental issues relating to firms' management of Information Security risks – employee education, user administration, patch management, monitoring and outsourcing.

4.2 A second section of findings describes the main Information Security risks and controls under the headings of organisation, people, processes and systems. We also consider external events and emerging risks observed in – or by – the firms in our review. This document is not intended to provide Information Security guidance as it focuses only on the Information Security risks that impact on our statutory objectives.

4.3 Some anonymised examples of Information Security incidents at firms illustrate our findings and are presented in boxed text. Conclusions from each finding are shown in bold italics at the end of each topic. We have included in our findings some of firms' commonly observed 'industry practices'. We have also incorporated material from publicly available Information Security guidance, although this is deliberately not comprehensive. For links to websites containing detailed Information Security standards and guidance, see this report's 'References & Useful Links' section.

Phishing and identity theft

4.4 Identity theft and fraud are important problems – and they are on the increase. They affect consumers and firms alike and are often one of the ways organised criminals raise money to fund more serious criminal operations such as people trafficking and drug smuggling.

4.5 'Phishing' attacks are where criminals send spoof emails misrepresenting corporate identity to trick individuals to disclose personal financial data such as account numbers and PINs. They create websites that mimic the trusted brands of well-known financial firms.

4.6 Fraudsters rely on the mass distribution of random spam emails using email addresses either purchased online, or harvested from websites and newsgroups using software. They hope to reach individuals who will fall for the scam and divulge their banking details resulting in credit card fraud, identity theft, and financial loss.

4.7 Initial 'phishing' attacks used emails that were poorly worded and contained numerous grammatical errors. However, recent fraudsters have downloaded web pages making the email and linked site appear indistinguishable from the genuine site.

4.8 The number of 'phishing' attacks is increasing as it represents a low-effort, low-risk strategy for the criminal and has potentially lucrative rewards. The Anti-Phishing Working Group recently reported in its 'Phishing Attack Trends Report' that there were 1,422 new, unique 'phishing' attacks in June 2004, representing a 19% increase over the previous month. It noted that a quarter of websites were hosted on compromised web servers, mostly in the US, remotely controlled by hackers. The sites had a global average lifespan of 21/4 days.

4.9 A limited number of firms we visited as part of this review had suffered 'phishing' attacks. All claimed their losses from UK 'phishing' attacks only amounted to the low hundreds of thousands of pounds. One firm, subject to weekly and sometimes daily attacks, gained the experience to respond systematically when their customers alerted them.

4.10 Firms state that such a low exposure from the UK has been because consumers are aware of the problem as a result of media exposure, as well as website messages and leaflets sent with bank statements advising consumers of the 'phishing' threat.

4.11 However, irrespective of the financial loss, the potential impact of consumers losing confidence in the internet as a service delivery channel is more important, considering the growing number of customers using online banking.

4.12 In terms of tackling 'phishing' attacks, firms have adapted and tailored incident response plans so that 'phishing' websites can sometimes be taken down the same or next day. This is an improvement – previously, it often took several weeks. However, the same 'phishing' site can re-appear the same or next day – hosted at a different Internet Service Provider (ISP). This makes the scale of the problem and the effort required to fight it clear.

4.13 Industry experience of 'phishing' has led APACS[1] to recommend the following practices for firms:

- Pursue policies that make the firm a difficult target, such as raising consumer awareness with warning messages on the firm's public website.
- In anticipation of an attack, prepare a response plan that may be activated as soon as an alert is raised, with identified people who have the correct skills to respond.
- Prepare scripts for all contact points through which a consumer or non-consumer can report a 'phishing' incident.

1 E-Banking Fraud Liaison Group: Phishing – Guidance, Best Practice & Lessons Learnt.

- Adopt a consistent practice for the use of email for customer communications across the firm. Furthermore, ensure central co-ordination of email marketing campaigns to enable customers to identify firms' genuine marketing emails.
- Review procedures for detecting an increase in emails bounced back from a spoof site (with a similar address) to the mail gateway following a customer's use of a spoof firm email address.
- Obtain contact lists for industry bodies, domestic and international law enforcement agencies before any incident occurs to allow prompt reporting and requests for assistance if 'phishing' websites hosted overseas need to be closed.
- Conduct active consumer education to raise awareness of potential scams, including advice on the website and information in statements. Provide a central email address that customers should send suspect emails to with an automatically generated response containing top anti-'phishing' tips.
- Liaise with other organisations to exchange information and obtain guidance on best practice.
- Use third party monitoring services to scan emails, the web and domain name registrations for mentions of the firm's name.

'Phishing' Trojans

4.14 'Phishing' Trojans are often auto-downloaded from bogus web pages and secretly log keystrokes when a consumer visits an online banking site. 'Phishing' Trojans hide in system directories and monitor when consumers open an 'https' encrypted connection (Hypertext Transfer Protocol over Secure Sockets Layer) to particular banking websites.

4.15 Once an 'https' connection has been made, the 'phishing' Trojan logs keystrokes and take screen shots of the login process to obtain consumer information. The Trojan captures account details and emails them to the criminals.

4.16 Currently, there are no published good practices for firms or consumers to follow to combat 'phishing' Trojans. However, firms can take good first steps on anti-virus precautions by maintaining up-to-date anti-virus software and by encouraging their customers to do this.

4.17 ***'Phishing' attacks are increasing and will probably grow to include the smaller banks as well as the major ones. Although losses to date are low, effective customer education and good corporate communication is needed to minimise loss. Development and testing of 'phishing' incident response plans appears to be beneficial with sites being shut quicker, preventing customers disclosing their bank account and personal details and becoming fraud victims.***

Specific role of industry and law enforcement agencies

4.18 We asked firms about their relationship with UK industry bodies and law enforcement agencies concerning financial crime reporting, passing intelligence and providing Information Security advice. We also met the agencies concerned in order to understand what initiatives were in place to help firms reduce their financial crime risk.

4.19 Our review indicates that smaller- to medium-size firms have little or no appreciation of the different agencies' respective contributions to the reduction of financial crime or of the type of assistance on offer. Indeed, although all the firms visited stated that they would tell the police about an incident, few were able to give the name of the appropriate organisation they should contact.

4.20 Our findings confirm the 2002 NHTCU report looking at 105 firms, which noted that even though almost all the firms surveyed had experienced at least one serious computer-enabled crime, only 56% had actually involved the police.

4.21 In marked contrast, larger firms had numerous contacts among the various agencies such as APACS, BBA, NHTCU and the Metropolitan Police. They also had effective formal and informal communication networks through various forums and peer group discussion meetings.

4.22 An area of concern many firms raised was the apparent duplication of effort and lack of a single voice of authority on fighting financial crime. Many firms cited the recent rise in the number of 'phishing' attacks, but referred to the lack of a government or financial services 'front door' for businesses and consumers to knock on for advice.

A small UK firm was advised of a fake copy of its corporate website bearing its name and was unaware how to remove it or which agency to contact. It took ten days for the firm to find the solution; in this case to ask the United States Secret Service to contact the US-based Internet Service Provider to remove it.

[When a UK firm does not have the expertise to trace an ISP itself, it can contact one of the agencies below – in paragraphs 4.23 and 4.24 or in Section 6]

4.23 The financial services industry clearly recognises the need for a strategic and co-ordinated approach but does not appear to recognise the work being done by the Home Office through the Central Sponsor for Information Assurance (CSIA). The CSIA works with partners across government and the private sector, as well as its international counterparts, to help maintain a reliable, secure and resilient national information infrastructure.

4.24 There are a number of government departments and agencies involved, including the Home Office, the NISCC (National Infrastructure Security Co-ordination Centre), the DTI (Department of Trade and Industry), the NHTCU (National Hi-Tech Crime Unit)

and the CESG (Communications & Electronics Security Group – the national technical authority for information assurance). These are described in section 6 of this report.

4.25 ***In general we noted from our visits that few firms were aware of the assistance they could obtain to fight financial crime from organisations such as the DTI and NISCC. Few firms had made contact with these agencies – if only to set up a relationship. We understand that both the DTI and the NISCC would welcome approaches by firms and would be pleased to assist them. We have listed useful links and references in section 7 of this report and will provide a list on the financial crime sector page of our website.***

Information Security framework

4.26 Establishing an Information Security framework is critical for an effective, comprehensive, robust Information Security function. The concept of an overall Information Security framework was only apparent at large firms, although some of the parts were in place at smaller firms. While the framework needs to be appropriate for the scale, nature and complexity of the firm, common attributes included:

- Having Information Security governance mechanisms in place e.g. defined roles and responsibilities for both business and IT in terms of committees, steering groups and management;
- Forming high-level Information Security strategies and policies, as well as detailed underlying procedures, standards and guidelines covering e.g. network, operating systems, databases etc;
- Deploying policies and procedures into actions e.g. user administration, network and operating system management and education;
- Managing monitoring of events through methods such as audit reports, or managing information to determine how well Information Security policies are implemented and procedures followed to provide assurance over the process; and
- Risk management over Information Security risks to include risk identification, assessment, mitigation and monitoring.

At one firm, there was no Information Security Officer, so responsibility for Information Security was shared between senior management. This resulted in incomplete policies and procedures and a breakdown in the segregation of duties between development and production environments. It allowed developers access to the production environment where sensitive data was held.

4.27 ***Establishing an Information Security framework is critical for a comprehensive, robust Information Security function and forms the basis for the effective management of Information Security risks.***

Employee education

4.28 Employee education is important because no matter how good the policies and procedures are, employees can be the weakest link. A survey in May 2004 by anti-virus firm McAfee found that 50% of senior managers in small businesses blamed staff for the damage done by viruses and other computer security problems. They said employees downloaded unsafe programs onto work computers and disabled the security systems designed to protect them. Our observations at firms are consistent with McAfee's report.

A firm was infected with a virus after a travelling employee used a laptop which he had installed an ISP's software on – against his employer's rules.

As the laptop was only infrequently connected to the firm's network, it did not have the latest anti-virus update. When the employee connected it to the firm's network the virus spread before the latest update could be applied.

The virus rapidly replicated, resulting in the firewall being bombarded and ultimately failing. This caused the firm to be exposed because of a single employee's action.

4.29 We observed a wide variation in the level of Information Security education given to employees. As a baseline, most employees receive staff handbooks and are required to sign acceptance of corporate policies and acceptable usage conditions. However, given the large size of some of the documents, their effectiveness in user education is questionable.

4.30 Examples of user education included:

- Compulsory Information Security training for new staff using mixed media such as Computer Based Training, Video and Powerpoint formats;
- Security awareness programmes to get staff to understand the importance of Information Security and their individual responsibilities;
- Supplying staff with security awareness materials such as intranet pages, mouse mats, brochures, posters and identity badge clips with security messages etc;
- Annual mandatory testing of Information Security awareness along the lines of training given on anti-money laundering; and
- Giving news bulletins to staff about the importance of Information Security, particularly when Information Security makes the news.

4.31 ***Employee action, deliberate or accidental, can potentially result in serious Information Security issues such as virus infections. Staff should be provided with education of the firm's Information Security policies and procedures on joining. And they should receive additional updates on emerging threats to minimise risk.***

User administration

4.32 The user administration function at a firm – which includes adding, maintaining and deleting user accounts and updating access privileges – is critical to maintaining Information Security. This is because correct user administration restricts access to functions, applications or networks and can enforce the proper separation of roles and responsibilities.

4.33 Firms frequently have temporary user accounts that have been created but not deleted or user accounts for staff who have long left the firm. These create the potential for unauthorised access to applications or data.

4.34 We observed a range of solutions across small and large firms – ranging from manual user administration to automated identity management solutions. The latter capture and maintain details of employees' access rights across the organisation, using either centralised or decentralised administration. However, irrespective of the solution firms deployed, a number of common issues arose:

- Failure to reconcile between employees listed on Human Resources systems and live user accounts on a timely basis to identify redundant accounts;
- Failure to delete access rights when a staff member changes responsibilities or departments;
- No review of user account access rights or application(s) privileges by the business or IT to determine if a user has excessive rights or incompatible privileges for their job role;
- No segregation of duties between IT staff administering user accounts and those who review the appropriateness of account privileges;
- No review of generic accounts often used by technicians;
- Use of personal accounts for conducting user administration through temporary assigning of administrator privileges rather than using a dedicated systems administrator account;
- Outsourcing user administration to a third party without reviewing the effectiveness of the arrangement.

In one firm, user administration tasks were devolved to a business unit. However, control was compromised. The manager delegated this responsibility to a junior clerk who, by virtue of the role, inherited the manager's privileges needed to perform this task.

4.35 ***Weak user administration is a common and long-standing failing. Firms need to ensure that only current employees have access to systems and that these employees have the correct account privileges. Unless user account reviews are regularly conducted there is a risk that staff will leave or move and that user accounts will be used for unauthorised activities.***

Patch management

4.36 Patch management is obtaining, testing and installing code changes (patches) to software. Patch management is important as it is used to fix system vulnerabilities. It requires the co-ordinated deployment of the patch across a firm's computer systems to mitigate the risk of the vulnerability being exploited. It is necessary for firms to identify and resolve promptly any such risks. This is because the time between it being reported by vendors and subsequently exploited by viruses or other harmful programs or files is often no more than a couple of days.

4.37 Firms have conflicting priorities in securing their information assets quickly in response to a publicised vulnerability. As well as being required to test patches properly before releasing them to the production environment, firms must also maintain an up-to-date inventory log listing the patch level of their information assets. Most firms with a large number of servers and client PCs find orchestrated patch management more difficult than firms with small-scale infrastructure. However, we did see some use of automated patch management software solutions in larger environments.

4.38 Most firms either visit public websites or receive subscription services alerting them when patches are available. Example websites that report vulnerabilities and provide hyperlinks to patch providers include:

- http://www.uniras.gov.uk/l1/l2/l3/latest.htm
- http://www.uniras.gov.uk/vuls/
- http://www.cert.org/nav/index_red.html

4.39 The majority of firms test patches before promoting them to the production environment unless they are deemed critical. But some firms apply patches without any testing at all, which is dangerous if they have no contingency 'roll back' plan.

A firm downloaded a patch, but did not test its impact on a business critical application. Once the patch was deployed the application failed, resulting in business downtime with no customer service possible until the patch could be removed.

4.40 The industry noted the following as features of effective patch management:

- Quick identification of vulnerabilities by, for example, tracking alerts on advisory websites;
- Evaluation of patches to assess the impact on the firm's business systems;
- Proper testing of patches and their and timely application; and
- Maintenance of records in an inventory log of current software versions and location of patches' installation.

4.41 ***Firms need to ensure that they have a well-organised patch management process, whereby patches are identified, prioritised, assessed, tested and rolled out across the firm's infrastructure. Furthermore, firms should determine the need to maintain an inventory log of patches applied according the complexity of their infrastructure.***

Monitoring

Internal threats

4.42 The monitoring of sensitive or high risk events within a firm's systems is important to maintain accountability. For example, it is sometimes necessary for firms to make sensitive changes, such as amendments to unit prices, in a database run directly by a Database Administrator, rather than through an overlying application that maintains an audit log. Such a sensitive change should be logged by a database audit log, reviewed and reconciled to a unit price change request.

4.43 In a similar way, technicians may need temporary privileged access to a live application in production should a processing error be identified. To mitigate the associated risks, management may include formal authorisation to provide an audit trail demonstrating the controlled use of such a facility. The password associated with the account should be changed by the manager after the code correction is made and stored securely.

4.44 Irrespective of the size of the firm, such actions need to be independently checked to ensure that no unauthorised activities have occurred. In many instances, we found that firms carried out little or no monitoring of applications, databases, operating systems or networks – despite exception reports being available.

4.45 Industry good practice is that system activities are monitored and regularly reviewed to validate application, database, or operating system activities, particularly if they are sensitive to the firm. We noted that although exception reports from monitoring activities are generally available to management, they are rarely reviewed unless the firm requires an investigation.

In a positive development, a firm implemented an online application to automate the management of privileged user accounts and passwords for critical European systems. The system featured storage, release, and encryption of passwords designed to prevent and provide early warning of unauthorised usage.

4.46 ***Firms need to determine the sensitivity of the data they hold on their internal systems and ensure that they maintain an appropriate level of monitoring to provide assurance that all systems activities are accounted for and authorised.***

External threats

4.47 Intrusion Detection Software works by identifying patterns of network traffic that look suspicious and may represent an attempt to gain access to a firm's network. Intrusion Detection Software monitors for exceptions to a predefined set of rules and will issue an alert to the administrator when it identifies an unexpected pattern.

4.48 We noted that several firms, large and small, were not monitoring external events effectively – in some cases because they did not have Intrusion Detection Software. In others, Intrusion Detection Software was installed, but the firm was unable to analyse the alert logs meaningfully because of the large number of false positives. In some instances, it was apparent that the firm knew what should be done but lacked the expertise to develop the desired alert and reporting process.

4.49 Recognising that Intrusion Detection Software analysis may be unsatisfactory, two firms are investigating the use of Intrusion Protection Systems. This software scans a firm's network and highlights routes through which intruders could potentially enter, allowing firms to address security weaknesses.

4.50 There is an increasing need for firms to provide remote access facilities to accommodate staff who are working away from the office and for technicians providing remote IT support. Almost all of the firms we visited allowed some form of remote access to their systems – typically for email access, using token based authentication with encryption through a Virtual Private Network.

4.51 We noted that few of the smaller firms recorded remote connections or carried out any form of user tracking unless carrying out an investigation. Monitoring remote access to systems is important as it will help identify possibly security breaches.

Some firms recognised that while their in-house expertise was limited, it was essential to maintain the integrity of the firm's perimeter. Therefore, they outsourced the intrusion detection function to a specialist company that provided alerts and reports to the firm according to their defined parameters. This appeared to be a satisfactory solution to the lack of expertise – albeit more costly than in-house developed routines.

One firm recognised its failure to review exception reports that had been highlighted for some years by their Internal Audit Department. In an attempt to address this, the firm ran a project that created a central repository for all logs from databases, operating systems and intrusion detection software allowing review.

4.52 ***Firms need to consider the likely threats against them to determine the type of perimeter monitoring they need. However, for firms with an internet presence this is likely to be essential. Real-time alerts should be developed to warn of potential attacks supported by appropriate reporting functionality for senior management.***

Outsourcing

4.53 US market researcher Gartner predicted in 2003 that one in 20 IT jobs in US customer-facing organisations would move offshore by the end of 2004. This prediction looks as if it is being borne out in the UK as well as the US.

4.54 Firms face pressure to outsource to remain competitive with the cost base and head count migrating offshore. Outsourcing activities such as IT Development, Operations and Contact functions (e.g. call centres), allows firms to build operational efficiencies, react and be flexible to competitive pressures and to provide organisational resilience.

4.55 When outsourcing, a firm has to balance the cost savings realised with the operational risks taken in terms of the outsourced staff, processes and technology. A wide range of outsourcing practices was evident in the firms we visited – from no outsourcing to extensive outsourcing.

4.56 Experience of outsourcing and offshoring varied – with one firm inheriting a subsidiary's outsourced function and only assigning it low-risk work, while another firm was embracing outsourcing by expanding its offshore operations with a new call centre function. One firm stated that security considerations were a factor in its decision to return its outsourced IT Operations process back to an in-house function.

4.57 Where firms outsourced either in the UK or offshore we noted common practices in terms of:

- Assessing the level of risk associated with the function and only outsourcing those activities whose risk level was deemed acceptable;
- Controlling and monitoring third party access to critical or sensitive systems;
- Conducting service provider due diligence; and
- Vetting outsourcer's staff recruitment process.

In outsourcing its user administration, a large firm omitted to specify adequate controls. It subsequently found that the outsourced firm did not reconcile user maintenance records with the actual users.

4.58 ***Firms cannot outsource their responsibility for Information Security and therefore should take reasonable care to supervise the outsourced functions carried out by its contractors (SYSC 3.2.4G). They can do this through clearly defined Service Level Agreements that articulate responsibilities for maintaining Information Security.***

5. Other findings

Organisation

Organisation structure

5.1 The position of the Information Security function within an organisation may be critical in the implementation and budgetary support of security matters. It may indicate how senior management perceive the significance of secure controls within the firm's overall operations.

5.2 Information Security reporting lines can indicate how firms' senior management view the importance of the IS function. We saw a variety of structures, which could all operate effectively. Examples seen included:

- The Information Security function embedded (three levels down) within a large technology department. This did not sound optimal. However, this firm was committed to security controls and fully aware that Information Security needed to be involved in all development activities. So in practice the strength of the function was not diluted.
- Another firm placed a newly-created Information Security management position with a reporting line to the Board. This allowed the manager to influence the direction of IT development and instil an awareness and consciousness into the senior management, which had virtually ignored security for many years.
- Other organisations had the Information Security function within the IT function with the Information Security manager reporting to the IT manager. This arrangement appeared to work, as the IT manager could ensure that appropriate resources were allocated to the Information Security function.

5.3 The key to success appeared to be the commitment of senior management to funding the development and implementation of robust security features. We noted particular differences in management's appetite for addressing security-related audit issues. There were examples where significant deficiencies had been outstanding for several years. The specific monitoring weakness had not been fully understood and with competing business development projects, no efforts had been made to rectify the situation, even partially.

5.4 It appears to be somewhat irrelevant whether Information Security is 'located' within the IT department or positioned with a direct reporting line to the senior executive. This is because a senior manager's attitude to Information Security risks will affect whether investment is a priority in protecting the firm from internal and external threats.

5.5 Traditionally, management has not been keen to invest in Information Security as they have not been aware of the potential risks and have failed to see the return on security investment. The recent emergence of internet risks and hacking threats has begun to change this approach. The diverse organisation of the Information Security functions we saw indicated that there was no useful comparison to be made about a firm's investment in Information Security as costs were spread around differently in organisations.

5.6 However, we were pleased to learn that many firms were investing in infrastructure projects that addressed facets of the security framework. Management appear to have recognised omissions of the past and they are generally committed to current expenditure requirements.

Several large firms had commenced Identity Management projects – long term developments that aimed to capture and maintain global employees' details. Systematically, databases were being filled in with key information that would eventually incorporate access rights and user profiles for each application used.

5.7 ***Senior management are ultimately responsible for Information Security, but may delegate responsibility to appropriate managers. Senior management need to ensure that clear reporting lines exist and be confident that the responsible person is suitable to carry out the function and is appropriately segregated from other persons and departments.***

Management information

5.8 The nature of management information produced on Information Security incidents varied between the firms reviewed. Small firms produced little or no information reporting, while large firms had extensive management information reporting.

5.9 A medium-sized firm performed a weekly review of all security incidents giving details of the virus attacks and security-related topics of interest such as the latest vulnerabilities. This was supplemented with a monthly summary for all senior managers. The weekly focus ensured that Information Security remained high on the firm's priorities.

5.10 ***The FSA Systems and Controls Handbook states in 3.2.11G that: Senior management should be provided with the management information it needs to identify, measure and control risks of a regulatory concern such as the use of the firm's systems for the purposes of financial crime.***

Internal Audit

5.11 The NHTCU 2003 survey reported that of the firms surveyed, 21% conducted security audits that complied with the British Standard 7799, 12% audited to 'other' standards and 35% audited without reference to any standards. More worrying was the 23% who stated that they did not do regular security audits. The other 9% were in the 'don't know' category.

5.12 It is important for firms to determine how effectively their control environment is working. This is usually, although not exclusively, carried out by the firm's Internal Audit (IA) department.

5.13 We found that larger firms had IA functions, although there were variations in the number of IA staff considered necessary. Small firms often had little or no IT IA resource. In such cases, these firms place reliance upon external auditors or consultants to provide assistance either as one-off assignments or as part of the statutory year end audit process.

5.14 Among those firms who had IA departments, we noted that the majority of IT auditors had some form of professional qualification e.g. CISA (Certified Information Systems Auditor) or QiCA (Qualification in Computer Auditing). Firms also appeared to take continuing professional education seriously, with staff regularly being sent on appropriate Information Security courses.

5.15 In some smaller firms, we noticed that the scope of IT reviews undertaken was limited to the expertise of the auditor. This biased the type of reviews carried out. Furthermore, we noted a general lack of automated system audit tools, with some firms using dated audit tools. This lack of sophistication and/or auditor expertise may account for the non-technical and process-related audits that were prevalent in some of the smaller firms.

5.16 IT IA practices varied across firms but commonly included the following indicators of an effective function:

- IT IA involvement with Risk Management function for key risk identification;
- IT IA involvement with systems development projects;
- Timely follow-up of outstanding issues and liaison with Information Security and/or IT management to ensure timely resolution;
- Training on new technologies and emerging risks; and
- Joint internal and operational audits.

Two firms showed a lack of commitment to fixing Information Security audit issues that had remained outstanding for two and four years respectively, exposing the firms to significant security risks.

5.17 ***Firms need to ensure that their IA function has the relevant IT skills to cover adequately the risks posed by their IT control environment. Firms can consider the use of external resources for audit work where in-house expertise is lacking. Firms' involvement of their IT IA function in internal projects may prove beneficial in terms of monitoring progress, identifying risks and ensuring requisite Information Security controls are built into the design.***

People

Resources

5.18 The financial services industry increasingly makes use of recruitment agencies for candidate search and selection, whether for full-time staff or short-term contractors.

5.19 There is evidence that organised crime groups deliberately target financial services firms in order to place staff to commit financial crime, in particular identity theft. It is therefore imperative that firms have a comprehensive vetting policy and follow it in recruiting employees.

5.20 In our visits, we observed a range of vetting procedures proportionate with the size of the organisation, such as:

- Tiered vetting according to sensitivity of job role;
- Service Level Agreements with agreed vetting standards for recruitment agencies;
- Random audit of recruitment agency vetted staff;
- Verification of complete school, university and employment history;
- Credit, address and telephone number checks;
- Bank of England terrorist list check;
- County Court Judgment checks;
- Equivalent vetting for all staff, contractors, overseas and outsourced employees; and
- Annual risk assessments for all staff.

5.21 We noted that some Human Resources departments also involved their Information Security and Compliance teams in assisting the vetting process.

5.22 However, in a number of cases, we observed poor standards of vetting. Several of the above vetting procedures were absent in a firm whose profile seemed to justify them. In other cases, the process was inconsistent between different types of employee.

5.23 ***Where firms recruit staff externally or make use of contractors / temporary staff recruited through agencies they need to ensure that an appropriate level of vetting is carried out, commensurate with the sensitivity of the individual's role.***

Processes

Passwords

5.24 We observed a range of password standards across the firms we visited that were generally reasonable. However, we found that even within the same firm there were

sometimes variations in standards between the firms' IT Policies for different areas of the business or where the use of legacy systems prevented the adoption of a common standard. Firms should have a single baseline password standard, which follows published Information Security standards. For data sets that are especially sensitive (see below) additional security measures should be considered.

A firm kept its system administrator and master passwords for all business critical applications and systems in a sealed envelope in a locked fireproof safe.

However, the firm also kept the passwords in a Microsoft Word document on a public area of the network that had not been password protected!

One firm reported a longstanding employee who had progressively carried out a fraud totalling about £80,000. As a payment clerk, he had identified a dormant account. He then repeatedly stole his colleague's password, by looking over his shoulder, and created payments from the dormant account to his own using his colleague's user account.

5.25 ***Firms need to wherever possible, adopt a single, consistent password policy based on published good Information Security guidelines.***

Data classification

5.26 Data classification was only observed at larger firms with small and mid-size firms rarely discriminating between different types of data. Where data was classified, firms generally had policies and procedures in place about the degree of protection employees should apply according to the data classification – from no protection for open source data, to encryption for personnel files.

Firewall management

5.27 For firewalls to be effective firms need to:

- Monitor for firewall vulnerabilities;
- Test and apply firewall patches in a formally controlled and timely manner;
- Issue instructions on what to do if a firewall fails;
- Ensure firewall resilience through failover capability to alternative firewalls. In the event of the firewall failing, another firewall operating in parallel will continue to protect a firm's network;
- Ensure that filter rules comply with Information Security policies; and
- Ensure firewall log review is conducted in a timely manner.

5.28 All the firms we visited had firewalls in place. However, the degree of patching to address the latest vulnerability or firewall log file monitoring, varied considerably.

One firm was unable to state how or what patches were applied. Another sent off its firewall log reports to a third party for analysis in monthly batches making real time analysis of external threats to their network impossible.

5.29 Many corporate networks have alternative methods of entry such as through Wireless Access Points or Virtual Private Networks. With alternative access points the reliance upon firewalls as a security choke point may be misplaced. Indeed, we noted some firms are – or have considered – hardening their network infrastructure so that all servers and PCs have firewalls and Intrusion Detection, irrespective of the external-facing firewalls in place.

Incident management

5.30 Effective incident management and its escalation to senior management has become increasingly important with firms relying on technology to be available around the clock. For larger firms, this has meant that traditional problem management procedures are inappropriate when a rapid response is required. This is the case for incidents impacting customer service delivery channels such as ATMs or web applications.

5.31 We found that although small firms had limited formal incident management capabilities, it was relatively simple for them to escalate the issue to senior management because of the firms' small size.

5.32 We found larger firms, and particularly those that had been subject to 'phishing' attacks, have well-developed incident management procedures. These have been repeatedly tested, reviewed and enhanced with each attack experienced to produce an effective incident management response and escalation procedure.

5.33 While the incident management process reflects the size and nature of the organisation, we observed some common practices such as:

- Having a documented incident response process that covers the reporting, recording, categorisation, investigation and resolution of all incidents with guidance on how incidents should be escalated;
- An incident response plan describing the roles and responsibilities of the participants and involving representatives, where appropriate, from: IT, fraud, communications, customer liaison, call centre, marketing and legal and providing out of hours contact numbers and nominated deputies.

5.34 ***Firms need to have incident management procedures commensurate with the size of their operations that define the roles and responsibilities for the staff involved and provide the escalation route to senior management.***

Penetration tests

5.35 We noted that, without exception, all the large firms we visited had carried out some form of penetration test to assess their resilience against attack. The tests carried out were a mixture of internal and external and conducted by both internal staff and external consultants, ranging in frequency from monthly to annually. However, we also discovered two small firms that had never undertaken a penetration test.

5.36 Industry experience suggests that penetration tests always lead to findings such as the discovery of old, un-patched software or dangerous services running on web servers that would permit a hacker to enter a system.

5.37 Some firms raised concerns over what 'white hat hackers'[2] did by night using the knowledge gleaned from their day jobs. To address this, some firms conducted both corporate and personnel due diligence on external consulting staff used when doing penetration tests.

Due diligence of vendors is important as one firm found out when the confidential results of a penetration test were sent to the firm in an unencrypted email. Unsurprisingly the firm did not retain the vendor as a preferred supplier.

5.38 Our understanding of industry practice is that:

- Penetration tests should be regularly conducted;
- Internal and external penetration tests should be carried out;
- A penetration test should occur before the firm implements any internet application;
- There should be an independent check to ensure that exceptions identified are addressed appropriately; and
- Third party firms should be vetted using due diligence and regularly rotated to ensure that tests are not restricted to a particular third party's skill set.

5.39 ***Regular penetration tests are useful to identify vulnerabilities.***

Systems

Wireless Networks

5.40 Of the firms we visited, none had Wireless Local Area Networks (WLAN) installed as there was no perceived business need based upon firms' existing arrangements. However, a few firms told us that if they were moving to a new location that did not have pre-existing cabling it would be an option they would consider. One firm had

2 'White Hat' hackers are skilled technicians employed to conduct ethical hacks, i.e. attempting to gain entry into a firm's systems at its request to determine and report on system vulnerabilities.

installed a WLAN for testing purposes, but subsequently removed it following a risk assessment by a newly-appointed Information Security Officer.

5.41 A small number of firms have recognised the potential of WLANs and are starting to, or have already, updated Information Security policies and procedures to include the control requirements for using WLAN technology. This is important, as firms are starting to deploy wireless-enabled laptops when they replace IT equipment, which, unless the functionality is restricted, will look for wireless networks and potentially share or receive files over the WLAN. Some issues firms would need to consider include:

- Authorisation, authentication, encryption and access permitted from only approved locations;
- Controls, with appropriate policies and procedures to ensure that only authorised users can gain access e.g. through mapping a user's internet address to the user's computer's unique hardware number (MAC or Media Access Control);
- Laptops should be configured not to share or accept files using a wireless card, as this may represent a backdoor into the corporate network;
- The prevention of unauthorised wireless access points;
- Access point security;
- Implementation of encryption and authentication measures such as in a Virtual Private Network (VPN) where data is encrypted at the sending end and decrypted at the receiving end. Originating and receiving network addresses are also encrypted;
- Establishing and enforcing wireless network policies;
- Intrusion detection.

5.42 ***WLAN may be a low cost option for communication within firms, but security controls should be defined and implemented before any installation.***

External events and emerging risks

Instant Messaging

5.43 Instant Messaging (IM) applications provide text, voice, and video communication and file transfer facilities between IM users across the internet. Common public IM providers include Yahoo, Microsoft and AOL. They use unencrypted communication over the internet while business IM applications typically employ secure solutions.

5.44 Although IM improves the productivity of staff within a firm, it also exposes the firm to whatever provider software and infrastructure weaknesses exist when allowing IM traffic through the firm's firewall. Furthermore, public IM communications are not archived nor provided with standard disclaimers as with corporate email. The use of

public IM has the potential to facilitate financial crime as it allows the unrecorded exchange of potentially market sensitive information as well as providing a conduit for virus transmission.

5.45 We noted many firms that either did not have a policy on the use of IM or have a policy on business internet usage did not adequately address the use of IM. Those firms which addressed IM risks employed some, or all, of the following security practices using non-public IM products or else banned the use of IM at the firm:

- Block on IM traffic (text, file transfer, video conferencing and voice);
- Enforced authentication;
- Centralised archiving and backup of IM traffic;
- Authentication and encryption of messages;
- Automated addition of company logos and disclaimer messages;
- Provision of a centralised audit trail of all IM traffic and the production of Management Information;
- Monitoring for IM vulnerability alerts;
- Applying patches in a timely manner and treating IM as a formal communication tool subject to the same usage restrictions as email through effective policies and procedures; and
- When selecting between competing IM systems weighting selection towards the security of the product.

A particular firm did not have a policy on IM, or any control in place to prevent the installation of the application on the firm's systems. This firm stated that the unauthorised use of IM was a big problem outside of the UK where IM use formed up to 50% of the cyber investigations carried out.

The only firm visited where the use of IM was permitted had limited the use to a non-public IM for a restricted group of staff and had incorporated additional controls to enforce message non-repudiation.

5.46 ***Firms need to understand the Information Security risks associated with the use of public IM versus proprietary IM as well as being mindful of the FSA's Systems and Controls Handbook rule 3.2.20 regarding the ability to retain adequate records of matters and dealings that are subject to the requirements and standards under the regulatory system.***

Personal Digital Assistants (PDAs), USB pens and Smart phones

5.47 The increasing use of personal or corporate PDAs, USB pens (portable storage devices that can be plugged into a PC) and Smart phones has changed firms' Information Security risk profile. While these devices can usefully store and transfer data, they can also be used to steal corporate information or potentially act as virus vectors. PDA and phone viruses, such as the WinCE4.Duts.A and the Cabir worm, were created as a 'proof of concept'.

5.48 However, in August 2004 a Trojan virus called 'Brador' was discovered that infected PocketPC based on the Windows CE operating system. When it is downloaded from the internet in the form of an email attachment, it emails the device user's IP address to the creator and allows remote control of the device.

5.49 In the sample of firms we visited only large firms had policies or procedures specifically relating to the use of devices such as corporate PDAs. Medium and small firms had no policies or procedures in place regarding the use of these devices. However, policies and procedures did cover removable media such as diskettes and CD-ROMs, which would suggest that firms do not yet recognise that such devices pose as much risk as removable media.

5.50 Firms should be alert to the risks posed by such devices and ensure that appropriate policies and procedures are in place where their use is sanctioned. And they should provide user education to alert employees to the risks associated with connecting personal devices to corporate networks.

It was encouraging to note the actions of a member of the IT Department at one firm who observed a contractor about to connect a USB storage device to one of the firm's networked computers. He stopped the contractor, informed her this was not allowed and asked her not to bring the USB storage device onto the premises.

5.51 ***Firms need to be alert to the Information Security risks introduced through the use of hand held devices. If hand held device use is permitted, firms need to consider educating their users in how to use devices safely and updating their Information Security policy accordingly.***

Virus attacks

5.52 The increase in the number of viruses released was evident – one large firm reported it had blocked 1,000 viruses in January 2004 and 7,000 in June 2004. Furthermore, the time between system vulnerability being published and exploited in a virus release is declining. For example NIMDA took 11 months from publication to be exploited in September 2001 while ASN.1 in February 2004 took only three days. It is likely to be only a matter of time before a 'zero day' virus is released where there is no immediate anti-virus fix or even knowledge of what the underlying vulnerability is with potentially hundreds of vulnerabilities being reported each month.

5.53 In the case of predicted zero day viruses, anti-virus updates will be unable to protect a firm's infrastructure from infection. Firms will instead have to rely on their incident management response plans in order to contain infection until a patch is developed and obtained.

5.54 In attempting to protect a firm against harmful programs or files ('malware') the traditional approach has been to harden the perimeter through the use of devices such as firewalls and mail filtering. However, the use of devices such as Personal Digital Assistants, USB pens, Smart telephones and Wireless Local Area Networks means that external-facing anti-virus controls can be bypassed. This potentially exposes a firm's infrastructure to internal malware risks, reinforcing the importance of up-to-date anti-virus patches and user anti-virus education.

5.55 All the firms we visited employed some form of anti-virus procedures. These encompassed anti-virus updates to varying levels of anti-virus precautions described in staff policies and procedures manuals as well as user education.

5.56 In practice, firms' abilities to deploy anti-virus updates quickly varied from fully automated to manual, with some smaller firms relying on a manual 'sneakernet' roll-out (e.g. loading an anti-virus disk on each PC), potentially extending the window of vulnerability.

5.57 We understand that industry anti-virus practice is to:

- Produce policies and procedures that describe the anti-virus precautions and the process for dealing with virus attacks;
- Install virus protection software on servers, mail gateways, and workstations, including laptop computers and handheld computing devices;
- Update virus definitions whenever a new version is released and distribute to key servers within a short period of time;
- Educate staff on the risk posed by computer viruses with particular emphasis on laptop risks; and
- Notify staff of new virus risks, giving details of who they should contact in the event of an infection or query over the alert.

An employee made a link between his firm's laptop and his home PC using a crossover cable to transfer files.

As the firm's laptop was only infrequently connected to the corporate network it didn't have the latest anti-virus update and therefore when connected to the home PC, it picked up a virus. When the employee reconnected the laptop to the firm's network the virus spread before the latest update could be applied to the laptop. This caused system downtime.

5.58 ***Even with traditional anti-virus precautions, a firm's network remains vulnerable to viruses introduced through novel, alternative routes. Although timely automated distribution of anti-virus software will help protect a firm's infrastructure, it needs to reinforce user anti-virus education.***

Denial of Service

5.59 Denial of Service (DoS) attacks are where a system receives many simultaneous instructions and either cannot cope with the volume of requests and fails or slows its processing down so that a user cannot get a timely response when loading a web page, for instance.

5.60 DoS attacks can be launched from single machines or as a 'distributed' attack using many computers simultaneously, frequently hacked home PCs with broadband connections, to create a flood of messages directed at a specific target.

5.61 DoS attackers have been targeting online gaming firms due to their reliance upon their websites for certain dates in the sporting calendar, but have also shown interest in attacking firms who rely on the internet as a service delivery channel. This impacts on consumer confidence.

5.62 Among the small sample of firms we visited, none had experienced a DoS attack or been threatened with a DoS attack. Firms who are likely to be targets should consider what their incident response plan would be to a DoS attack and who they would call on for help if this occurred.

5.63 ***Regular vulnerability tests and threat assessments should identify system weaknesses and the probability that a firm may be targeted in a DoS attack.***

Physical security

5.64 We are aware that many firms donate retired computers as part of asset refreshment cycles to local good causes. However, the corporate confidential data remaining on these computers has resulted in embarrassment for some firms and potentially exposed them to regulatory or statutory sanction. Firms need to ensure that they do not just delete files, but use specialist software to delete data from computer hard disk drives securely and permanently.

Business Continuity Management

5.65 Firms should identify critical systems that are essential for the business to operate in the event of a disaster. Generally, all the firms we visited had some form of Business Continuity arrangements, varying in complexity according to the nature and scale of their business.

5.66 For Business Continuity Planning, firms need to consider Information Security risks when establishing how access to archived data and User Administration will be managed if users are relocated and are using back-up systems. Typically, this is handled through defined roles and responsibilities with documented procedures for managing the process.

5.67 Regular testing and updating of Business Continuity arrangements is important, as some firms reported that initial tests highlighted problems with system interfaces and application recovery times exceeded recovery time objectives.

A firm had not invested in developing a Business Continuity plan. The business would have had difficulty in continuing if its premises were damaged.

5.68 *The FSA Systems and Controls Handbook states in 3.2.19G that: 'A firm should have in place appropriate arrangements to ensure it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. These arrangements should be regularly tested to ensure their effectiveness'.*

6. Industry and law enforcement agencies

NISCC

6.1 NISCC is an interdepartmental organisation set up by the Home Office to minimise the risk of electronic attack against the UK's Critical National Infrastructure (CNI). It works in partnership with the owners of the systems that support critical services in both the public and private sectors. And it offers a wide range of information and advice on best practice in protecting organisations' information systems. NISCC advises on how best to protect information systems and, through investigation and work with UK and international partners, it assesses the threat of attack. It also issues alerts and warnings, manages the responsible disclosure of new vulnerabilities, undertakes research and development work with partners, and promotes information sharing.

NHTCU

6.2 The National Hi-Tech Crime Unit plays a key role in combating serious and organised hi-tech crime covering e-crime prevention, reporting and investigation. To facilitate police and industry co-operation, outreach teams have been formed to provide dedicated points of contact. Through these, firms can talk to experienced and technically competent staff who ensure that any reports or questions relating to hi-tech crime are handled directly and quickly.

6.3 The NHTCU also has a confidentiality charter that allows firms to report crimes knowing that the source of the information will be protected and the information sanitised before being disseminated within industry intelligence briefings.

6.4 Several firms stated that they had initially passed on intelligence about potential e-crimes to the NHTCU, but they had received little intelligence in return and that it had appeared a 'one way street'. However, firms reported that since the e-crime congress in February 2004 the issue had been addressed with an effective 'two way flow' of intelligence between firms and the NHTCU.

DTI

6.5 The Department of Trade and Industry aims to increase the productivity of UK businesses and encourage confidence in the use of new information and communications technologies. It has responsibility for all businesses, including small-medium enterprises, and includes customers in the Critical National Infrastructure (CNI). The DTI works with business and industry bodies such as APACS to raise awareness of the importance of effective Information Security management and to encourage the adoption of security standards such as ISO/IEC 17799 and British Standard 7799.

CESG

6.6 The Communications & Electronics Security Group (CESG) is the national technical authority for information assurance. It provides security guidance such as IT Health checks, IT Security Assessments and assurance over security functionality of products and systems for government departments, agencies, local government, public sector and the private sector to help them achieve their business aims securely.

6.7 CESG has initiatives that may assist private sector firms, such as:

- CESG Listed Advisor Scheme (CLAS), which approves private sector consultants to provide Information Assurance advice to government departments and other organisations; and
- The IT Health Check Service (CHECK), a collection of firms that have been approved to supply Information Security work to the standards required by CESG.

APACS

6.8 The Association for Payment Clearing Services (APACS) has 33 members and 29 affiliate members and is the trade association for institutions delivering payment services to end customers. APACS financial crime initiatives include:

- Facilitating the 'E-banking fraud liaison group' consisting of APACS banking members plus BBA and NHTCU input where intelligence is shared between banks and NHTCU.
- Sending advisory emails to its members when it is aware of a new threat.

6.9 In addition to the initiatives above, it was also clear that there APACS has informal communication channels through to their industry members which worked well in exchanging intelligence.

6.10 APACS has also worked with other bodies on providing advice and information sharing such as working with the DTI to discuss the content of a DTI website on Information Security.

BBA

6.11 The British Bankers' Association (BBA) represents banks and financial services firms operating in the UK. It has about 250 members, plus associate members who fund its not-for-profit activities.

6.12 The BBA's activities include:

- Participation in the E-Banking Fraud Liaison Group, whose membership includes financial institutions as well as agencies such as the NHTCU. This runs facilitated workshops and distributes intelligence to its membership; and

- Producing leaflets for retail and commercial customers such as 'Protecting your financial details' and 'Your money and the internet' as well as providing a list of links to bodies such as APACS and Association of Certified Fraud Examiners. The BBA collates data on certain types of fraud which is reported in the BBA's Fraud Prevention and Intelligence Unit's quarterly publication, Crimewatcher.

7. References and useful links

- **Anti-Phishing Working Group** (APWG) (www.antiphishing.org) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing.
- **APACS** (www.APACS.org.uk) is the UK trade association for payments and the banking industry's voice on payments issues such as plastic cards, card fraud, cheques, electronic payments and cash.
- **Bank Safe Online** (www.banksafeonline.or.uk) is the UK banking industry's initiative to help online banking users stay safe online. The site is run by APACS.
- **The British Bankers' Association** (BBA) (www.bba.org.uk) is a trade association in the banking and financial services industry representing banks and other financial services firms operating in the UK and provides consumer publications.
- **British Computer Society** (www.bcs.org/bcs) is an industry body for IT professionals. It plays an important role in establishing standards and training needs for Information Security professionals.
- **Business Link** (www.businesslink.gov.uk/) provides advice for businesses on implementing and managing Information Security.
- **British Standards** (www.bsi-global.com) is among the world's leading providers of standards and standards products. Through engagement and collaboration with its stakeholders, it develops standards and applies standardization solutions to meet the needs of business and society.
- **Central Sponsor for Information Assurance** (CSIA) (www.cabinet-office.gov.uk/CSIA). The CSIA in the Cabinet Office pulls together the various projects across government. It works with partners across government and the private sector to help maintain a reliable, secure, and resilient national infrastructure.
- **CESG** (www.cesg.gov.uk) is the Information Assurance arm of GCHQ and is the UK Government's National Technical Authority for information assurance.
- **The Department of Trade and Industry** (DTI)) provides advice for businesses on protecting their information (www.dti.gov.uk/bestpractice/technology/security.htm.
- **Financial Services Authority** (www.fsa.gov.uk/consumer/01_WARNINGS/scams/mn_scams.html) is a site aimed at consumers and gives details of the latest reported scams.
- **The High Technology Crime Investigation Association** (HTCIA) (www.htcia.org) is designed to encourage, promote, aid and affect the voluntary interchange of data,

information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership.

- **The Home Office** (www.homeoffice.gov.uk) is responsible for ensuring the UK's national infrastructure is protected as well as for policing for hi-tech crimes and gives internet crime prevention advice.
- **The International Information Integrity Institute®** (I-4®). www.i4online.com is a group of industry-leading organizations who share their expertise on managing information-related business risks.
- **The Institute for Communications Arbitration and Forensics** (ICAF) (www.theicaf.com) is an incorporated, professional institution for Information and Communications Technology professionals who aim to promote best practice in the security of information, the resolution of related disputes and the solution of technology related crime.
- **The Information Assurance Advisory Council** (IAAC) (www.iaac.org.uk) brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection.
- **The Information Systems Audit and Control Association** (ISACA) (www.isaca.org) publishes on information governance, control and security matters for audit professionals.
- **The Information Systems Security Association** (ISSA®) (www.issa.org) is an international organization for Information Security professionals and practitioners providing educational forums, publications to enhance the knowledge, skill and professional growth of its members.
- **The Information Security Forum** (ISF) (www.securityforum.org) is an international association of more than 250 leading organisations which fund and co-operate in the development of practical research about Information Security.
- **The National Computing Centre** (www.ncc.co.uk), a membership and research organisation for IT professionals, is playing a role in promoting Information Security best practice and guidance.
- **National Hi-Tech Crime Unit** (www.nhtcu.org) plays a role in combating serious and organised hi-tech crime. The unit covers electronic crime prevention, reporting and investigation.
- **Security Alliance for Internet and New Technologies** or SAINT (www.uksaint.org) brings together industry leaders and government to exchange information and best practice.
- **UK Government CERT** (www.niscc.gov.uk) is the UK Government's Computer Emergency Response Team, part of NISCC (National Infrastructure Security Co-ordination Centre).

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000 Fax: +44 (0)20 7066 1099
Website: http://www.fsa.gov.uk

Registered as a Limited Company in England and Wales No. 1920623. Registered Office as above.