International Perspectives on Information Security Practices

Opinions, Preferences and Tools in the Financial Services Industry[1]

Prepared for red / McAfee

Dr. Jonathan Liebenau

With Patrik Kärrberg

Department of Management

Information Systems Group

London School of Economics and Political Science

October 2006

[1] We would like to thank all our anonymous interviewees and: Dr. James Backhouse (LSE); Dr. Ayse Bener (Bosporus U.); Greg Day (McAfee); Dr. Gurpreet Dhillon (Virginia Commonwealth U.); Ms. Camilla König Ekegren (Swedish Chamber of Commerce, Beijing); Ms. Laura Georg (U. Geneva/HEC); Dr. Karl-Olof Hammarqvist (Stockholm School of Economics); Ms. Ulla Lundqvist (Svenska Bankföreningen); Dr. Waldemar Grudzien (Bundesverband deutscher Banken e.V.) Mr. Jason F. Quigley (International Banker's Association, Japan); Mr. Bernd Schaefer; Dr. Frederick Wamala (LSE); and numerous current and former postgraduate students in the Department of Management at the London School of Economics who shared their views on information security.

I. Executive Summary

A unique perspective on information risk and its legal and economic context

ICT security practices and the attitudes and preferences of chief information officers continue to change rapidly as the pressures of compliance interact with the changing technical challenges and rising consumer expectations. In this study we have examined recent regulatory trends, "best practice" and "due diligence" responsibilities of US, Asian and EU firms. We analysed the relationship among such external forces and internal firm behaviours and conducted a small set of intensive, probing interviews with opinion formers and practitioners. In these interviews we asked responsible people in financial services firms questions about their responsibilities and powers, their relations with external bodies, their opinions about the costs and benefits of investing in certain kinds of information security tools or in tools they might wish to have available.

"The gap between theory (compliance rules) and practise in information security management has never been greater." *Banking security expert, UK*

Banking and other financial services not only are affected by all the major trends, such as the impact of the Sarbanes-Oxley Act and national data privacy legislation, they also are the leading sector with regards to the implementation of corporate security. Their influence extends in many directions by virtue of their close links with regulators, their key position with regard to standards setting, and their impact on consumer behaviour, especially through online banking practices. We analyze our findings so that we can come to a better understanding of these forces and their effects upon the profession. Our results will be of special interest to those concerned with benchmarking their practices from an international perspective.

Structure of the Report

Key findings

1. **Responsibility:** The role of the CIO is unclear, and few CIOs feel that their personal reputation is closely linked to the tools they use. In some countries (UK, US) the prevailing attitude is one of concern about non-repudiation, leading to a concentration on compliance and post-hoc responses, while elsewhere (especially Switzerland and Singapore) security is seen as an integral responsibility requiring proactive positioning. Very few information executives have lost their positions solely on the basis of breaches, although recent firings at AOL may mark the beginning of a trend.
2. **Branding:** Confidence in security products is somewhat high, but there is a strong desire to be vendor independent, so layers or rings or levels of security are typically designed to mix different kinds of tools and techniques. Some rely on systems integrators to do this, others construct their defences themselves. The basic security tools are trusted, but the array of regulations, standards, and expectations for compliance create resentment and a sense of incompleteness in the structure of secure systems.
3. **Risks Online:** Whereas banks may be satisfied with their own tools and processes, the vulnerabilities of customers who use online banking services are a source of constant concern. There is no consensus about how to bring the general level of security of personal computers up to the standards necessary to ensure that the whole system of service providers and customers is secure. Trojan attacks against customers are an increasing worry, although virus checking techniques are trusted in general. Bank-sponsored public promotions to encourage safe online practices are one approach.
4. **Paying for Security:** Some firms cross-subsidize or use internal debit systems to support special functions of IT security and especially business continuity, e.g. to reduce down-time recovery response. This is sometimes organised through "buying-in" systems where divisions might pay for additional levels of confidence. Premium security products could have a larger role in this market.
5. **Compliance:** The expectations of information security executives and managers is that tools will keep up with the changes in policies and regulations, but they resent the considerable effort on monitoring such changes in order to participate in defensive designs themselves. Information security policy is moving into compliance functions and as a consequence infiltrating into everyday business risk considerations.

Trends and growth areas

1. **Reputational Risk from Breaches:** Reports of breaches of personal data have been compulsory for two years now in the United States with the result that CIOs are acutely aware of each instance of exposure. When similar requirements come into force in the UK at the end of this year a new dimension of reputational risk will become apparent. This trend is expected to extend to all major markets.
2. **Changing Boundaries:** Information security managers in financial services companies can control their internal environments because they are able to purchase and manage products and processes at the highest level of quality. Private online customers, however, are use a wide array of products and have levels of security far below those applied within the banks. This raises the possibility that the realm of responsibility for security will extend beyond the traditional boundary between bank and customer.
3. **Authentication Systems:** Banks are searching for new means to authenticate remote users. Two-factor authentication systems are common in Scandinavia, are soon to become compulsory in Singapore and are likely to become widespread in the European Union. This changes not only some elements of security systems architecture, it alters customer attitudes and behaviour.
4. **Managed Services:** Managed services to customers could grow to accommodate the changing sense of responsibility for the boundaries between customer and bank. Other approaches are industry recommendations, guidelines or standards for supplying specific security software appropriate for customers to utilize when using online financial services.
5. **Central Controls:** Central control techniques are changing with most firms using automated processes to standardize updates and in some cases to control online activities. Software solutions that contribute to the enforcement of centralised policies will be quickly disseminated. In this way financial services companies are likely to lead among large firms because they are able to do so in an efficient and timely manner on a very large scale.

II. Introduction; An overview of legislation, practices and context

New forms of computer security threats are emerging just as the recognition of the strategic as well as the broader industrial and national economic significance of information integrity are attracting attention of the heads of corporations, industrial bodies, national and European Union regulators. The United States has paid special attention to information integrity as part of both data protection policies and national security, responsibility for secure computing has wide-ranging effects upon the behaviour of senior executives and is expressed in industry bodies generally. The consequences of flawed systems has already been seen in courts of law as well as in the judgement of investors; European firms, national governments and the European Commission have been forced to pay attention. European institutions are also likely to take action which will affect not only the roles and responsibilities of corporate CIOs but of company strategic behaviour more generally.

Information security products emerged in the 1980s when it became clear to government users, academics and to a limited degree commercial and personal users, that threats from viruses and intruders into systems needed to be countered. In general surveys of IT managers, security and privacy ranked well outside the top ten concerns throughout the 1980s and 1990s where strategic planning and staffing issues dominated. In recent years problems associated with security and privacy consistently held the second place in the list of concerns, after "IT and business alignment" and all sectors agreed that new security technologies were the most important developments of recent years[2]. Over the past two years security technologies have ranked first among respondents among significant application and technology developments, a position of glaring conspicuousness reflecting both the appreciation of new products and defensive techniques, and an indication of the high expectations of the IT professionals community. Both the appreciation of the difficulties and developments and the pressures associated with the increasing number of and higher expectations from regulations, industry standards and professional best practices have pushed security higher in company's priority list and brought unprecedented scrutiny onto information management executives.

The recent security breaches by ChoicePoint, Lexis-Nexis, Bank of America, Citigroup and many others have put nearly 10 million Americans at heightened risk of identity theft, and other sources estimate the worldwide cost of security breaches at $2 trillion worldwide.[3] According to the Federal Trade Commission, 27.3 million American were victims of identity theft between 1999 and 2003,

[2] J. Luftman, R. Kempaiah and E. Nash (2006), "Key issues for IT executives 2005" *MIS Quarterly Executive* 5(2): 27-45

[3] Quoted in Allen Holmes, "Riding the California Privacy Wave" *CIO Magazine* 15 January 2005

costing businesses and financial institutions $48 billion and consumers $5 billion. Victims pay an average of about $1,400 (not including attorney fees) and spend an average of 600 hours to clear their credit reports.[4] "The personal costs can also be devastating; identify theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs."[5]

The direct link between security and strategic business function is best seen in the reaction to requirements to give notice of a security breach. The California (and subsequent U.S. federal) requirement for swift notice creates reputational and other market incentives to improve internal security practices. According to news reports, after giving its third notice of security breach in fifteen months, Wells Fargo Bank ordered a comprehensive review of all its information handling practices. Wells Fargo's CEO stated, "the results have been enlightening and demonstrate a need for additional study, remediation and oversight. . . Approximately 70 percent of our remote data has some measure of security exposure as stored and managed today."[6]

Throughout the world, place still matters with regard to cybercrime. Countries and states differ in their laws and their approaches to enforcement, and when a virus wreaks havoc around the world it may be that no country will claim jurisdiction, since it has only suffered a fraction of the harm caused by the virus, and the country of residence of the perpetrator may not have the means or the will to prosecute.[7] One approach to this has been the Council of Europe's Cybercrime Convention, which has also been signed by the United States, Canada, South Africa, and Japan.[8]

---

[4] U.S. Federal Trade Commission, "Report on Identity Theft" 2003 http://www.ftc.gov/opa/2003/09/idtheft.htm

[5] Hillebrand, Gail and Susanna Montezemolo, "Identity theft" statement by Consumer's Union and Privacy Rights Clearinghouse, 16 June 2005.

[6] D. Lazarus, "Wells Boss Frets Over Security" *San Francisco Chronicle*, 23 Feb 2005, http://sfgate.com/cgi-bin/article.cgi? file=/c/a/2005/02/23/BUGBHBFCR11.DTL

[7] Bert-Jaap Koops and Susan W. Brenner, eds, *Cybercrime and Jurisdiction, a global survey* T.M.C. Asser: The Hague, p. 17

[8] Convention on Cybercrime, Budapest 23 November 2001 (CETS 185) available at http://conventions.coe.int/Treaty/EN/WhatYouWant.sap?NT-185

II. Thematic issues

Based on the background of the legal and business context, and as interpreted through the views of our interviewees, we can see the thematic issues in the following structure:

What are the real problems with information security today?

Reputation: Reputational risk from information security breaches are real, and as disclosure requirements become widespread the danger is felt throughout the organisation.

Lack of benchmarks: Although numerous metrics exist and consultancies offer benchmarking reports and services, practitioners nevertheless report that they feel unable to gauge appropriate levels of investment or degrees of technical sophistication.

> "We don't have time or capability to quantify risk probabilities in say 1% or 20%, so we simply acknowledge that we need to manage that risk. The lack of benchmarks makes it difficult for us to then assess the value or efficiency of our actions, since the only real indicator you have of your security levels are breaches. But breaches occur too seldom to be a reliable indicator."
> *Security executive, Sweden*[9]

> "Our evaluation of best practises is very subjective and we lack soft benchmarks. If security is a selling point in a given point of time we would invest, no matter the costs. Further, the rise of risk management as key activity, and the role of information security for Basel II capital ratio, contributes to security now showing up on the radar screen for top executives and the board."
> *IT security manager, Japan*

Risk of key staff losses: Very few competent specialists are available to manage information risks. Companies that lose the internal capabilities their teams provide cannot find alternatives either on the labour market or through outsourcing.

> "We are extremely dependent on a few key security experts. We have good results from the financial services authority inspections, but try and downplay this vulnerability during audits…"
> *Security officer, Sweden*

Flexibility: Large organisations need more flexibility to respond to and be proactive against emerging threats.

Mobile and remote users: Ubiquitous computing, USB ports and mobile devices challenge the border between the company and its rules; we need to explain rules to users so that actions make sense.

> "The largest threats to information security practises for our mobile workers according to me are public wireless LANs and carelessness with flash memories. For both BlackBerries and laptops the data is encrypted and not a big security risk." *Banker in Singapore.*

[9] All quotes in text boxes are from interviews conducted for this study. They are presented as illustrative or exemplary of widely held views or strong opinions.

What differences are there internationally?

Governance and auditing: Non-US companies resent the pressures to comply with Sarbanes-Oxley Act procedures, although Japan is developing a consistent compliance system, referred to as J-SOX[10] and the European Union has a similar plan with it's so-called "8th Directive"[11].

Customer interfaces: Scandinavia and Singapore are ahead in two-factor authentication systems.

> "A difference between the US mentality and ours is that we are more wary and careful about data mining. Compared to the US, there is less utilization of customer data for this purpose, and therefore less sensitive data being extracted in processes that could be compromised."
> *Banking security expert, UK*

Varieties of technical architecture: There is not much evidence of convergence of technical practices; most convergence is seen in procedural standards of ISO 27001 ("Information Security Management System") and ISO 17799

How are things changing?

Security practices becoming routinised: The gap between information security theory and practice is wide and growing. Guidelines, standards and compliance concerns overshadow mechanisms for change.

> "Information security is of increasing concern. But more and more complexity comes into the picture too. We have a strong feeling that IT governance methods are increasingly important that we can control the cost of this increasing complexity."
> *Policy manager, Dutch Bank*

The rise and fall of the information security officer: As information security becomes routinised, it moves into a position where it is a subset of compliance-meeting activities. On the one hand this links it in with the core business functions as performed by chief financial officers, on the other hand it decouples it from the IT functions, perhaps to the detriment of the interests of chief information officers and their counterparts.

> "We don't see any convergence of the security practises as such among organisations. One reason being the people caring for customer data and policies are different to those who manage and maintain the system security. This is not only due to compliance reasons, but a more pragmatic one: You can't expect someone to be expert on both policy and implementation." *Policy manager, industry association in the EU*

[10] http://www.nri.co.jp/english/news/2006/060221.html; http://www.pm-global.com/news_1002_e.pdf

[11] Ernst & Young, "The EU 8th Directive New Rules for Statutory Audits in Europe" November 2005, http://www.tecbrand.com/eyrisk/151105/eynewsletter151105/feat_eu_8th_directive.html

How vulnerable do banks think they are to information security breaches?

Online banking: The greatest threat is to customers when using online services. User education takes time and banks will increasingly find collaborative efforts to speed up "national systems" necessary. Some banks respond by strengthening their internal systems, some by extending security to customers, some by collaborating in national campaigns, such as the "surf with confidence" campaign carried out by Sweden's bankers' association.

> "The boundary, 'blame line', between bank and customer in the international perspective is blurry due to different legislation in different countries."
> *Banking security expert ,UK*

Internal threats: Internal breaches are important considerations and the greatest fear of most information security managers. No technical solution can protect against any determined insiders with a grudge and the ability to alter intrusion-detection records or otherwise cover their tracks.

> The difficulty of intrusion detection is the manual interpretation of incoming "alarm bells". A lot more could be done, as it is the combination of many factors that signals a potential intrusion, and this should be automated much better than today."
> *Security officer, Scandinavia*

What is the place of information security tools in systems architecture?

Branding: There is no brand loyalty to security tools, and many adopt a layered approach to secure systems where tools from different vendors are used at different layers.

> "We have no loyalty towards certain vendors, and it's part of our strategy to rather strategise around technology choice (such as Java for internal development) to stay independent."
> *Bank security officer, Sweden*

> "We have no brand recognition locally for specific security tools, as they are procured centrally and only installed by us. We have a central server to which we connect new PCs and laptops and all software is installed from there. Also, all Internet traffic to our branch is routed via VPN tunnels to proxy servers in HQ, so the Internet pipe is centrally managed, and can be cut in case we have a virus attack."
> *Branch office, EU bank in Singapore*

> "We have high confidence in our total security system and need an overlap between different vendor products, as we don't trust individual anti-virus and spam products fully."
> *Security officer, Scandinavian Bank*

> "To counter the tendency to get stuck with any company, we make a point to change anti-virus software occasionally. That ensures we are independent of any one vendor."
> *Manager, IT Security Bank in Japan*

> "Symantec and McAfee have done the right thing, offering you the security packets. But Trend Micro is only anti-virus, don't know what extra value they offer. It's one of the pieces of the puzzle when I put together my security. At least the anti-virus guys have brand recognition towards the end-users. The people who operate on the network (the Cisco's) don't have that. A lot of consolidation is happening in anti-virus."
> *International security executive, Japan*

Does compliance add up?

Relations with regulators: The national financial services regulators must engage in constant dialogue with companies and industry representatives in order to interpret regulation for the application of secure systems. Large companies can rely on informal contacts and some use them on a daily basis. Smaller companies expect the national bankers associations or other industry bodies to represent their interests, since no matter what level of expertise is available in-house or through auditors and consultants, there are constantly questions about details of architecture or the reliability of software solutions that have to be checked.

> "We have good relations with the local financial services authority. We have some margin to argue our case, as sometimes what we do in Tokyo means breaking a local regulation when following a global regulation. E.g. we are not allowed to delete sent emails according to the Japanese regulator, but in Germany we must delete emails due to privacy laws. Good relations with the financial services authority is crucial and they know about this situation very well".
> *IT manager, Japan*

Compliance rules: Implementation practices are constantly working to satisfy compliance requirements. Information management professionals are sanguine about national regulations but complain about their need to satisfy foreign compliance requirements (especially with regard to Sarbanes-Oxley auditing procedures).

> "We understand SOX and what it's good for, but in practice you do what you can. You try to identify issues that affect SOX and eliminate these issues rather than regulate them."
> *Banking security expert, UK*

Can the range of outsourcing behaviours be sustainable?

No single model: A very wide range of arrangements currently exist from a complete absence of outsourcing arrangements to the outsourcing of network security, to comprehensive outsourcing of internal security arrangements and standard applications. These choices seem independent of size or character of technical reach or facility.

"We have a global outsourcing partner, who handles all storage of data, firewalls, other security software, and support request. We remain with [only] administration rights to our critical applications. We are very happy with this arrangement. Stringent processes and documentation have been built up for a smooth interaction between our outsourced IT department and the users in the bank. The outsourcee is on top of things and our automatic anti-virus system pulls updates every hour from the vendor".
Manager, operational risk, German bank

Acceptable risk?: The added security costs changes the risk equation and has contributed to a change in attitude towards outsourcing in general. Some banks assess the added risks to be sufficient reason to avoid outsourcing, others regard it as a means of spreading risks.

"We don't assess the benefits of due diligence and best practises as IT is an outsourced cost centre in our organisation. We are not going to pretend we create value in our IT operations."
Manager, operational risk, German bank

IV. Law and Jurisdictional Issues

The forces that impinge on each information management executive come from an idiosyncratic combination of internal corporate practices, industry standards, national laws and regulations, international laws and practices, especially as related to trade and financial activities, and the functionality of the technology that decision makers have chosen. We first turn our attention to the character of these effects as they relate on a high level to the organisation of work in information security in financial services.

> "The national financial service authority holds the key to standardization, as they handle ISO certification and coordinate international compliance legislation."
> *Security officer, Sweden*

Perhaps the two greatest changes in trends come in the form of compliance requirements for due diligence, the duty of care, and good governance generally, and in the form of national cyberlaw legislation, much of which addresses data protection and privacy. The first of these in its current form is associated with the Sarbanes-Oxley Act of 2003 and the interpretations, responses and measures to accommodate it throughout the business world. The second is associated with ISO 17799 and other procedural standards, and with data privacy legislation such as the "Financial Data Protection Act of 2006".[12] A third major factor is exemplified by the Bank of International Settlements' "Basel-II" framework by which banking risk levels (including information security risks) are directly linked to the amount of liquidity the bank must maintain, thereby directly coupling potential business profits with security investments and practices.

> "The regulatory influence is totally different between Japan, Hong Kong and China. In Hong Kong the financial services authority is non-intrusive and non-discriminatory business environment. In Japan the authorities sometimes discriminate against foreign firms; red tape is slower for them than for local companies. In China, subjectivity from the China Banking Regulatory Commission bogs you down, if you can't show how you benefit the Chinese state in a clear way."
> *IT manager, Japan*

Despite the changes in legislation and the introduction of many new standards, and indeed despite the attention that security is receiving in professional forums, conferences, specialist and academic writing, there is a general perception that action to counter threats remain inadequate. In a recent interview, the co-chairman of the U.S. President's Information Technology Advisory Committee said: "There is a big gap between what we already know about cyber-security and our deployment of technologies and processes to improve it…CIOs are partially responsible for the insecure state of today's operating systems, because they fail to see the handwriting on the wall and prioritize security. Vendors produce

[12] U.S. House of Representatives, "Financial Data Protection Act of 2006" H.R.3997, see Sec. 3. "Notification of information security breach" which extends the

what we are willing to purchase. CIOS are largely responsible for the failure of their organisations to operate at the current state of the art with respect to cyber-security, and very few organisations operate at the current state of the art…CIOs must demand that software vendors design and correctly implement [such secure] systems, and most importantly, CIOs must be willing to pay for it."[13]

Sarbanes-Oxley Act [SOX]

The Public Company Accounting Reform and Investor Protection Act of July 30, 2002 is aimed at strengthening the corporate governance of enterprise financial practices. Although most of the provisions of SOX apply only to U.S. domestic publicly traded corporations, non-public companies whose debt instruments are publicly traded, and foreign companies registered to do business in the United States, the knock-on effects are even larger than this. The effects on IT related activities is also great and include:

- Performing analysis and potential implementation/integration of software packages on the market that assist in SOX compliance.
- Providing authentication of data through the use of data integrity controls.
- Capture and document detailed logging of data access and modification.
- Securing data by means such as firewalls.
- Documenting and remediate IT application control structures and processes.
- Provide storage capacity for the retention of corporate data assets related to the law (i.e. e-mail, audits, financial statements, internal investigations documentation).
- Provide recoverability of the archive.[14]

"It costs a lot of money to work towards compliance, and sometimes this takes resources away from dealing with real risks. The Finance Services Authority recognises this problem as well. SOX regulates 5 aspects relevant to us, where 2 relates to governance and 3 relates to information security: Correctness, confidentiality, accessibility of data for financial reporting. We don't have to follow SOX today, but if we had to, we'd make SOX becoming a side effect of our normal practises."
Security manager, Scandinavian bank

The general consensus in the computer security profession seems to be that the Act has been a boon to information security in the U.S.[15] According to the Computer Security Institute, the effect of the

[13] Ben Worthen, "Security: The sky really is falling; interview with Ed Lazowska" *CIO Magazine* 1 October 2005
[14] G. Dhillon, *Principles of Information Systems Security* Hoboken, N.J.: Wiley, 2007
[15] E. Eugene Schultz, "Sarbanes-Oxley—a huge boon to information security in the US" *Computers & Security* 2004, 23:353-354

Sarbanes-Oxley Act was mainly to raise the organisation's level of awareness of information security.[16] However, our findings indicate that outside the United States the distinction between companies quoted on a U.S. stock market and those that are not still is the major differentiator, at least insofar as the issue has penetrated to information security professionals in financial institutions. Furthermore, there is a widespread view that the act is both too vague in its specifications and at the same time too prescriptive in its implications to be anything much other than a stimulus to an over-extensive set of compliance routines.

The Basel II Accord

"The Basel II Framework describes a more comprehensive measure and minimum standard for capital adequacy that national supervisory authorities are now working to implement through domestic rule-making and adoption procedures. It seeks to improve on the existing rules by aligning regulatory capital requirements more closely to the underlying risks that banks face. In addition, the Basel II Framework is intended to promote a more forward-looking approach to capital supervision, one that encourages banks to identify the risks they may face, today and in the future, and to develop or improve their ability to manage those risks. As a result, it is intended to be more flexible and better able to evolve with advances in markets and risk management practices."[17]

"Due to Basel's capital rules, we need to have full control of related information, therefore information security is vital"
Bank security officer, Sweden

Gramm-Leach-Billey Act

The Gramm-Leach-Billey Financial Modernization Act of 1999 requires companies to give consumers privacy notices that explain the institutions' information-sharing practices.[18] Most of the provisions of the GLB Act address the procedures for collecting and utilizing personal information, but there are significant security implications, also. These include the enhanced requirements to ensure that information gathered cannot be used for unauthorized purposes and holds implications for all sorts of breaches of data security that have the effect of disclosing customers' account numbers to, for example, non-affiliated companies. "Another provision prohibits "pretexting"—the practice of obtaining

[16] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson (2006), "11th Annual CSI/FBI Computer Crime and Security Survey" Computer Security Institute, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

[17] Bank for International Settlement web site: http://www.bis.org/publ/bcbsca.htm

[18] www.ftc.gov/bcp/conline/pubs/buspubs/glblong.pdf

customer information from financial institutions under false pretences. The FTC has brought several cases against information brokers who engage in pretexting."

Where privacy is concerned, the onus falls clearly on financial services organisations to ensure that their systems are secure. However, home banking services and related e-banking operations have blurred the boundaries between the system of the banks themselves and those of their customers. Indeed, although it is common practice to bar the attachment of non-bank devices to an internal system, every remote user becomes vulnerable in relation to their use of the services when they are protected at a lower level than the bank itself. As one interviewee put it with regards to Trojans and viruses, "our main vulnerability comes from customers' computers. Their lack of protection is a major concern. As a bank we have enough resources to protect ourselves, but our customers do not." A similar point was made by Hillebrand and Montezemolo: "Identity thieves are able to operate in large part because consumers don't control who has access tot heir credit files. That is, identity thieves who have stolen information about the consumer are able to apply for credit, and the creditor evaluating the fake application examines and relies on the real consumer's credit record to approve credit for the thief."[19]

Requirement to give notice of breaches

Emanating from California state law implemented in July 2003, the US requirement to give notice of a security breach has brought new attention to information security within companies. Indeed, Consumer's Union considers that "a requirement for swift, no-exemption notice of security breaches should create reputational and other marketplace incentives for those who hold sensitive consumer information to improve their internal security practices." This certainly seems to have been the case for Wells Fargo Bank, which ordered a comprehensive review of all its information handling practices after three notices of security breaches in fifteen months[20]

Although the ChoicePoint case was the first to be notified under the new acts, it was neither the largest nor unusual in the manner of breach. Ten days after the ChoicePoint breach was made public, the Bank of America office in Charlotte, North Carolina, reported the loss of backup tapes with 1.2 million records. On that same date PayMaxx made public a breach which exposed 25,000 records online and during the following month ten further breaches were made public. Throughout 2005 one breach was made public on average every third day, but by the middle of 2006 reports of breaches were numbering

[19] G. Hillebrand and S. Montezemolo, Report on identity theft, Consumers Union and Privacy Rights Clearinghouse, 16 June 2005

[20] D. Lazarus, "Wells Boss Frets Over Security" *San Francisco Chronicle*, 23 Feb 2005, http://sfgate.com/cgi-bin/article.cgi? file=/c/a/2005/02/23/BUGBHBFCR11.DTL

between 8 and 10 per week and to date almost 94 million records containing sensitive personal information have been involved in security breaches.[21]

> "Privacy laws and obligatory disclosure of data breaches is a trend in developed countries. First the US, then other countries like Singapore, and soon the UK. Regulators in undeveloped markets such as Malaysia, the Philippines, Indonesia, Taiwan, and China will not be too keen on this, as they know they are behind."
> *IT manager, Japan*

In banking the most direct measure of the effects of security breaches is in the loss of customers directly linked to breaches, and the recent Ponemon Institute study showed that 34% of customers would change their bank after one breach, and 45% would leave after two breaches. Reputational risk is a real and present danger. [22] As requirements to notify affected individuals and the public of database breaches become more common we expect to see major reconsiderations of reputational risk at the highest levels of all large corporations. Britain is expected to require notification by 2007, and other countries are expected to introduce similar legislation in the coming years.

> "From January 1st, it will be compulsory with token authentication in Singapore, and some banks will struggle to get their systems up and running on time".
> *Banker in Singapore*

European Union activities

The EU legal framework that applies to information security dates from the Council Decision 92/242/EEC of 31 March 1992 and then and subsequently has focussed on evaluation criteria, with primary implications for e-government, procurement and related processes. In recent years EU-wide defence policy addresses combating cyber crime and cyber terrorism. The European Union response to the Sarbanes-Oxley Act is emerging in the form of parallel guidelines under development, known as "EU 8th Directive". Nevertheless, an analyst from the European Network and Information Security Agency has written:

> "Failure to implement appropriate information security measures might have severe consequences for the implicated organisation. Under private law, failure to implement security measures might result in damages for breach of contractual obligations (e.g. negligence or breach of a fiduciary relationship). The increasing statutory obligations that have been introduced through laws on banking, data protection and healthcare are an additional source of

[21] (Privacy Rights Clearinghouse, "A chronology of data breaches" www.privacyrights.org/ar/chrondatabreaches.htm; updated regularly, last accessed 12 Oct. 2006
[22] Vontu, Inc. "Ponemon Institute names most trusted retail banks", press release 26 January 2006 http://www.ponemon.org/press/2006PTSiRetailBankingFinalrelease.pdf

security requirements. Security has become an issue of concern for shareholders and management that affects the positioning towards corporate liability." [23]

The combination of these elements adds up in the European context to a set of activities that so far are superseded by national laws and activities, especially as regard financial services, and international practices, such as compliance with SOX.

> "The EU cybercrime convention disseminates to national level, and it's a worry that different countries implement it differently"
> *Security Expert in a European Bankers' Association*

[23] Mitrakas, A, "Information Security and Law in Europe" *Information and Communications Technology Law* 15 (1) 33-53

V. Breaches and Responses

The context of security is that "in 2004, nearly 115 million computers were infected by 480 new species of malicious code, including the worms MyDoom, NetSky, SoBig, Klez, and Sasser, which cost at least $166 billion" [24]

There are even claims that in 2005 the dissemination of new malicious code continues at an exponential rate, and increasingly the drive towards profit rather than destruction, and by implication increasingly targeting financial services or consumers of financial services, including credit card and electronic banking facilities.

ChoicePoint

The ChoicePoint case was revealed due to the data breach disclosure laws of the United States. On 14 February 2005, identity thieves accessed personal information of more than 145,000 consumers contained in databases compiled by ChoicePoint in Atlanta, Georgia. Although this led to a landmark ruling in July 2006, it was by no means the largest such breach so far reported. That was the breach disclosed on 16 June 2005 after identity thieves exploited vulnerabilities in databases complied by CardSystems Solutions Inc. in Tucson, Arizona, accessing personal information of more than 40 million consumers.[25]

CardSystems Solutions

The fundamental legal basis for information security is the legal duty of care that transacting parties must show in their daily or business dealings. However, when CardSystems Solutions of Tuscan, Arizona, suffered a cyber break-in and 40 million debit and credit card accounts were exposed, they were found to have an unsecured network, "even though the network had been certified secure to a data security standard, according to Visa."[26] CardSystems provided 119,000 small and mid-sized merchants with products and services used in "authorization processing", which in 2005 amounted to 210 million card purchases, totalling more than $15 billion. Despite the very large amount of personal information they stored, they were found by the Federal Trade Commission to have failed to provide reasonable and appropriate security. They were found not to have adequately assessed the vulnerability of its network

[24] Sean B. Hoar, "Trends in Cybercrime: the dark side of the internet" *Criminal Justice* Fall 2005 (20:3) 4-13. *2004: Year of the global malware epidemic—Top ten lessons*, IT Observer, 23 November 2004; http://www.ebcvg.com/press.php?id+679
[25] Kim Zetter, "CardSystems' Data Left Unsecured" *Wired* 22 June 2005 http://www.wired.com/news/technology/0,1282,67980,00.html
[26] Ibid.

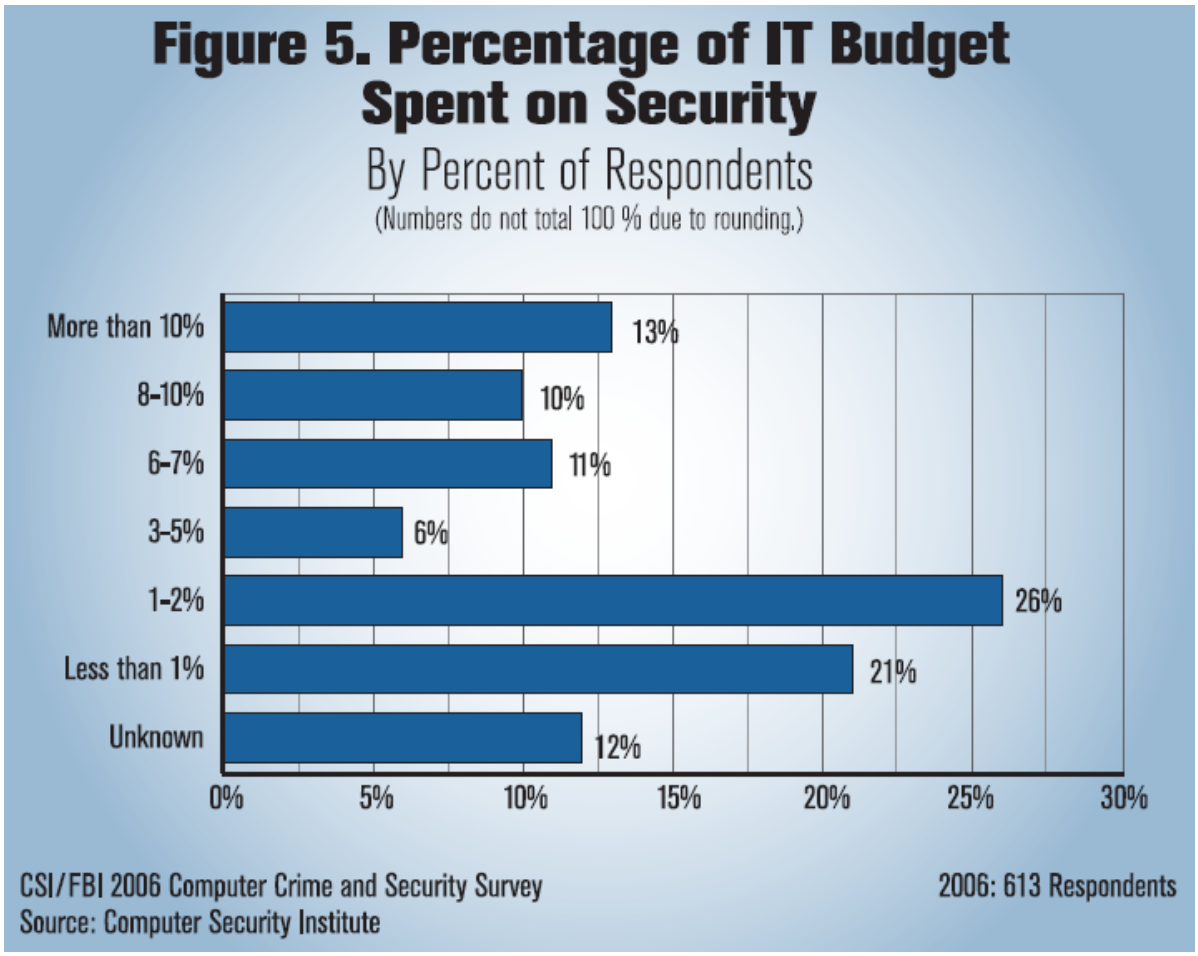
to commonly known or reasonably foreseeable attacks, did not implement "simple, low-cost, and readily available defences", did not use "readily available security measures to limit access between computers on its network and between its computers and the Internet…"[27] Nonetheless, Visa had certified CardSystems Solutions in June 2004 that it was compliant with the standard, but when audited after the breach it was found that they had even failed to apply a firewall or maintain virus definitions. "The Payment Card Industry Data Security Standard… consists of 12 requirements …, such as installing a firewall and anti-virus software and regularly updating virus definitions. It also requires companies to encrypt data, to restrict data access to people who need it and to assign a unique identifying number to peple with access rights in order to monitor who views and downloads data."[28]

Countering risks

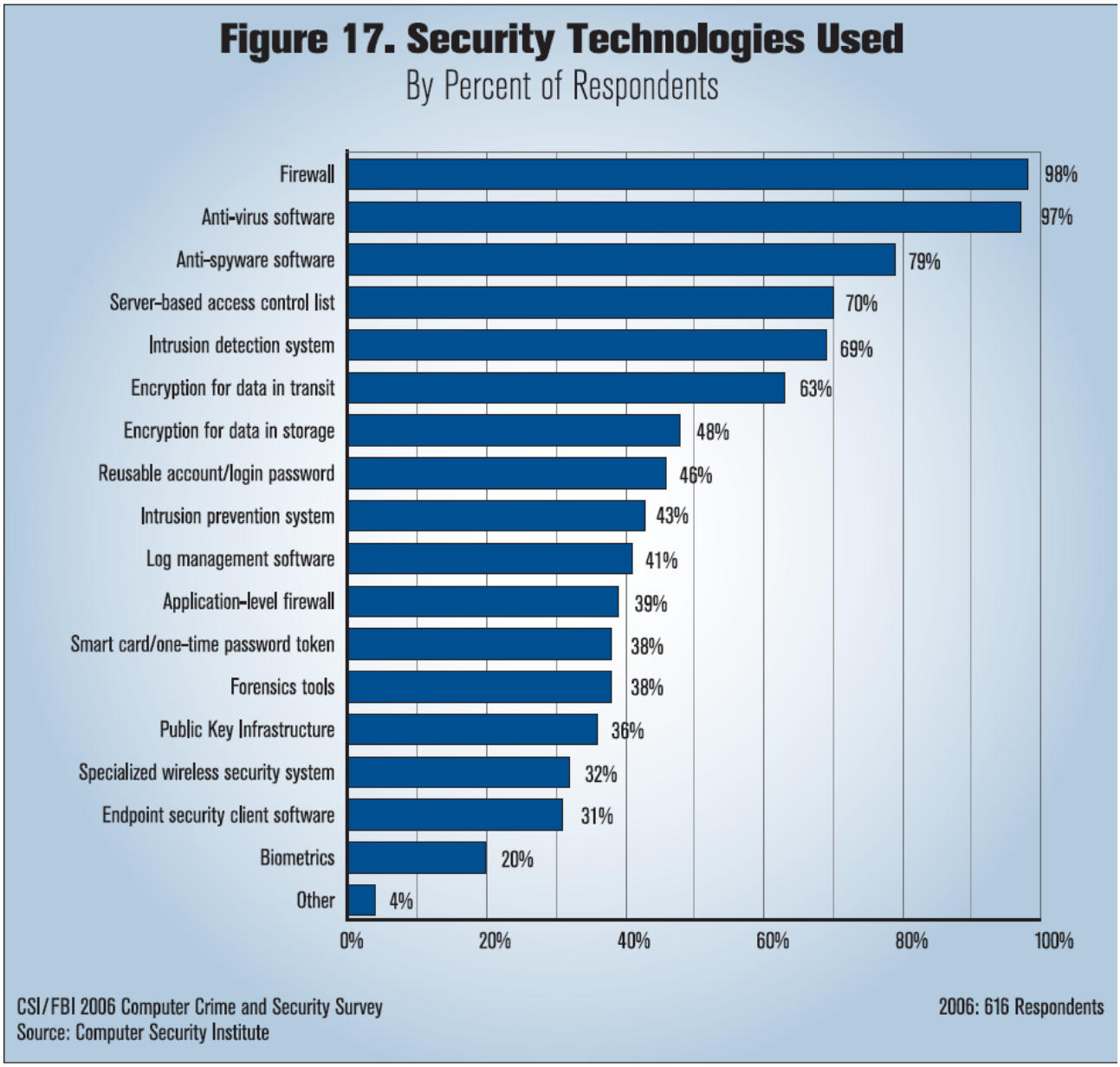
One measure of the response to this is seen in the amount of spending on security, as expressed for the U.S. in the figure, below:

[27] Federal Trade Commission, "CardSystems Solutions Settles FTC Charges" news release 23 February 2006 www.ftc.gov/opa/2006/02/cardsystems_r.htm; FTC "Complaint" and "Decision and Order" Docket No. C-4168

[28] Zetter, op. cit.



The SCI/FBI Survey emphasises that "projects designed to increase an organisation's information security. . . need to be justified in economic terms". (p. 7), but found that although return on investment calculations were popular (42% of respondents claimed to use it), only around one fifth used net present value or internal rate of return metrics.



The 2006 survey of the Computer Security Institute provides the best overview of the kinds of technologies that organisations tend to use, with the vast majority employing firewalls and anti-virus software and between about 70-80% using anti-spyware software, server-based access control, and intrusion detection systems [see Figure 17]. Most also encrypted data in transit. However, fewer than half of respondents used technologies for encryption of data in storage, reusable account/login passwords, intrusion prevention systems, log management software, application-level firewalls, smart cards or one-time password tokens, forensics tools, public key infrastructure, etc. It is notable that this emphasis on technical solutions maps reasonably well into the relative level of losses, where respondents indicated that over 30% of losses in dollar terms were caused by virus contamination and over 20% by unauthorized access to information. Theft of laptops or mobile hardware and theft of

proprietary information accounted for a further 24%, but all other categories of losses accounted for less than 6%, with password sniffing, phishing (in which the organisation was fraudulently represented as sender) and system penetration by outsiders in aggregate accounted for less than 3% of total losses.

> "I'm satisfied with our virus protection. The key is automated patching as you need to buy time. A new patch to Microsoft Windows on the Friday, and a virus could kill you the next Monday if you don't have your updates installed. Compared to 5 years ago a lot has happened and I expect it to improve further the coming years."
> *IT security manager, Japan*

That survey also elicited opinions with the question: "What do you think will be the most critical computer security issue(s) your organisation will face over the next two years?" and found that data protection and application software vulnerability attracted the highest number of respondents, but that policy and regulatory compliance was a second high category, followed by identity theft and then viruses and worms.

> "Patch management for virus updates could be done quicker. Manual processes to log actions on each server hold us back and we'd like to further speed this up"
> *Sweden*

A further perspective can be seen from the Ponemon-Vontu Survey[29] on actions taken to counter risks**:**

Table 11 With respect to your organization's current information security priorities, please rank the following seven (7) key activities from *1=highest priority to 7=lowest priority*. If possible, please avoid tied ranks.	Average Rank	Forced Rank
Protecting sensitive or confidential data in motion (transfer)	3.11	1
Identity and access management	2.23	2
Protecting sensitive or confidential data at rest	3.42	3
Protecting against viruses, malware and spyware infection	2.52	4
Training and certification of employees	2.08	5
Protecting against external penetration (hackers)	2.21	6
Disaster recovery planning	2.15	7

Banking specific responses

"Two-factor authentication systems" are regarded as the major technical addition to banking security and constitute a clear trend in the financial services sector. These can take a variety of forms including one-time password tokens, scratch pads with single use passwords, SMS transmitted codes that have short usage periods, biometrics, etc. These constitute the second factor in addition to common forms of

[29] Ponemon Institute, "US survey: Confidential Data at Risk" 15 August 2006 http://www.vontu.com/uploadedFiles/global/Ponemon-Vontu_US_Survey-Data_at-Risk.pdf

online log-in processes. One paradox of their usage is that they run the risk of stimulating hackers and crackers who regard it as an attractive challenge to supersede any new technique.

> "We perceive two major security threats in our operations: One being virus, the other being investigated without notice by the Chinese financial services authority."
> *Small branch office of EU bank in China*

All of the commonly available forms are currently in use, although national practices differ very widely. In Scandinavia one-time password tokens, scratch pads, SMS transmitted codes and other mechanisms are common. In the United Kingdom, HSBC currently provides one-time password tokens only to business users who wish to participate in a pilot scheme, which seems likely to be extended and offered to private customers in the near future.

> "It's expensive being test rabbit for new security technology, and dangerous to be a lagger. We choose to be on the forefront in some areas, but support and customisation needs for older legacy systems hold back quick transitions"
> *Security officer, Sweden*

Whether banks announce intentions to extend such schemes is to some degree associated with local as well as international interpretations of where responsibility ends for the security of extended systems that include customers' private devices. If the model of credit cards is applied then we may find US and UK banks readily reimbursing fraud victims, while continental European banks may continue to regard each incident as a crime worthy of investigation and contention with regard to liability. This may provide differential incentives in the short run whereby US and UK banks continue to invest heavily in all manner of anti-fraud techniques, while others place more of an onus on customers.

> "We consider our ability to effectively updating our virus protection a strategic asset"
> *Security officer, Sweden*

When Barclays Bank announced that they would buy all its online banking customers anti-virus software, it implicitly extended its acceptance of responsibility for secure systems.[30] They sent letters to all 1.6 million online customers in the UK providing them a code to download and unlock an anti-virus program licensed from the Finnish software developer, F-Secure. Their reasoning is clearly stated in their announcement:

> "We have a guarantee that if anyone is defrauded through no fault of their own we guarantee their money is safe. . . We're trying to stop fraud happening in the first place which is beneficial to them and us."[31]

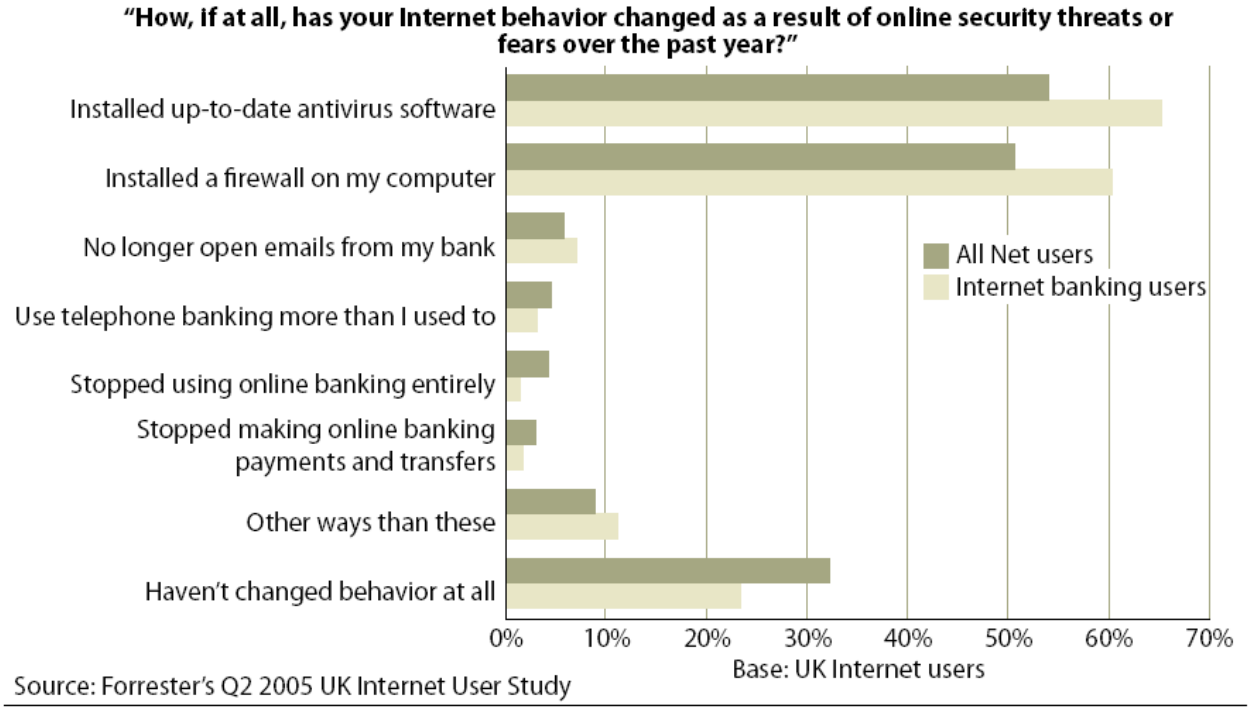
[30] BBC News, "Barclays banks on anti-virus deal" 26 May 2006 http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/5019856.stm
[31] Ibid.

This was not regarded as an appropriate move by all bankers we interviewed, some of whom pointed out that taking such responsibility invited customers to assume that they would receive software support, and they pointed out that there was a real possibility that one anti-virus program could interfere with others that users had independently installed.

> "The next wave of malicious software is Trojans. As a bank, we always have the possibility to protect ourselves, but the big problem is many of our Internet bank don't have necessary protection. Trojan viruses will increasingly cause a lot of problems for these customers."
> *IT officer, Scandinavian Bank*

> "The banks are afraid of becoming a helpdesk for Internet customers, as you will get all kinds of support requests. It's a balance to strike, because at the same time we want to consult and give advice. The second challenge regarding issuing recommendations of say anti-virus software to customers, is that we get involved in vendor choice, and run into possible questions of, at least morally, liability."
> *Security officer, Scandinavia*

Figure 2 Net Users Are Installing Firewalls And Antivirus Software Rather Than Giving Up Net Banking



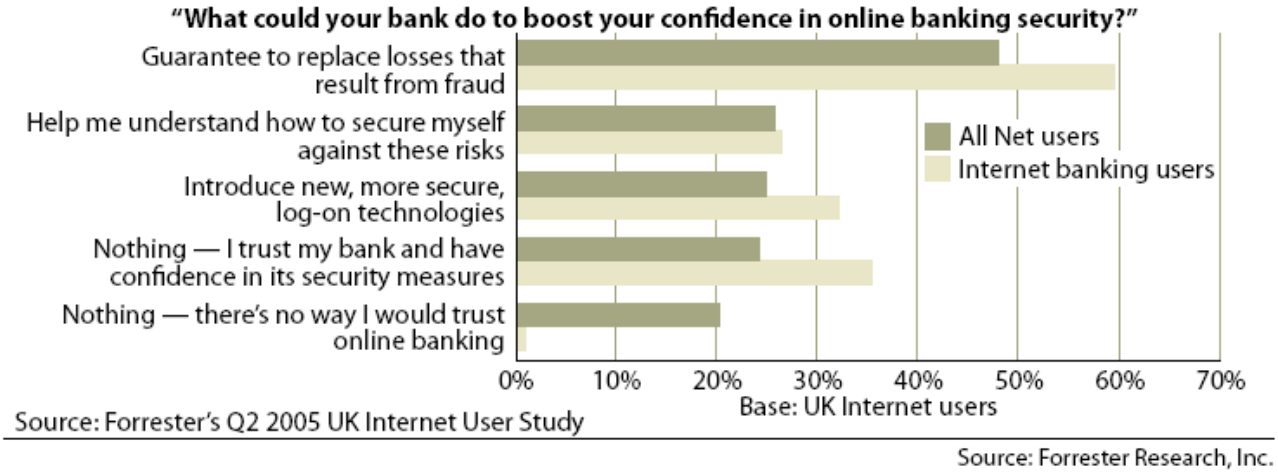
Source: Forrester Research, Inc.

As seen in the chart above from Forrester Research's study of last year,[32] UK users are concerned but few are willing to cease using online banking services. This is in contrast to US online consumers, of whom Forrester reports 14% said that they had altogether stopped paying bills or using bank services online. The report further informs us that half have installed or updated firewalls and antivirus

[32] Benjamin Ensor, "What UK Net Users Think about Phishing", Forrester Research, 16 August 2005

software, although many of these have recently acquired new PCs or had their firewalls and antivirus software upgraded automatically by their service providers.

Figure 3 Net Users Hope Banks Will Solve The Problem For Them



Source: Forrester Research, Inc.

However, the report points out that there is no expectation that electronic tokens will significantly change behaviour, a finding that seems premature given the very low level of experience with such technologies to date. In general banks cannot rely on customers to be vigilant and they must reconsider the balance between security and customer convenience.[33]

Virtualisation of financial services

One survey sponsored by Nortel,[34] focused on UK-based organisations that conduct business across Europe. The overwhelming majority of respondents, 83%, believed the adoption of virtual enterprise solutions will increase costs savings and production efficiency. Most of the corporations, 91%, have already deployed remote access, with some degree of security, to their employees. That survey is an indicator of the fact that sustainable competitive advantage in the financial services sector increasingly comes from the ability to manage the entire value chain both in the production and distribution of financial products.

> "Proprietary software used for example in remote Video Conferencing sometimes contain security holes, so in a way we become path dependent to current products due to resource limitations in testing new products."
> *Security officer, Scandinavian bank*

However, it also adds complexity to IT governance practices among security officers, and makes it evident that successful corporate security is the responsibility of all employees.

[33] Ibid, Forrester p. 7, 11
[34] Nortel/CMA, 2006, www.nortel.com/promotions/emea/virtualenterprise/index.html

"We don't use PDAs and mobile phones connected to the Internet, as we don't consider these products fully mature yet from a security point of view."
IT manager, Scandinavian Bank

VI. Professional Perspectives

Increasingly it is the case that leading corporations have executives who are responsible for information technology on the board of directors of corporations, and there is a growing trend for positions such as chief information security officers to report to chief financial officers, especially within financial services organisations. One example from outside of the financial services industry is in Volvo, where the president of Volvo Information Technology, Ulf Nilsson, serves as CIO of the Volvo Group and has the security functions reporting directly to him through the member of the executive management team responsible for global infrastructure & operations.[35]

> "Arguments to superiors for changes in information security are formulated in terms of risk, rather than in terms of direct cost."
> Security manager, Bankers' Association, EU.

The hierarchal position of chief information officers has been changing and is different in different industrial sectors. Overall, just over 40% report to chief executive officers, with one fifth reporting to chief financial officers and the same proportion to chief operating officers. Only 6% report to business unit executives, with the rest scattered elsewhere through the structure of the organisation. There is a clear correlation between those who report directly to chief executive officers and centralized IT structures.

> "Security policies are decided on top level, as it should, but it's sometimes a problem for IT departments that decisions are not taken close enough to its implementation".
> *Scandinavian bank's branch office in Asia*

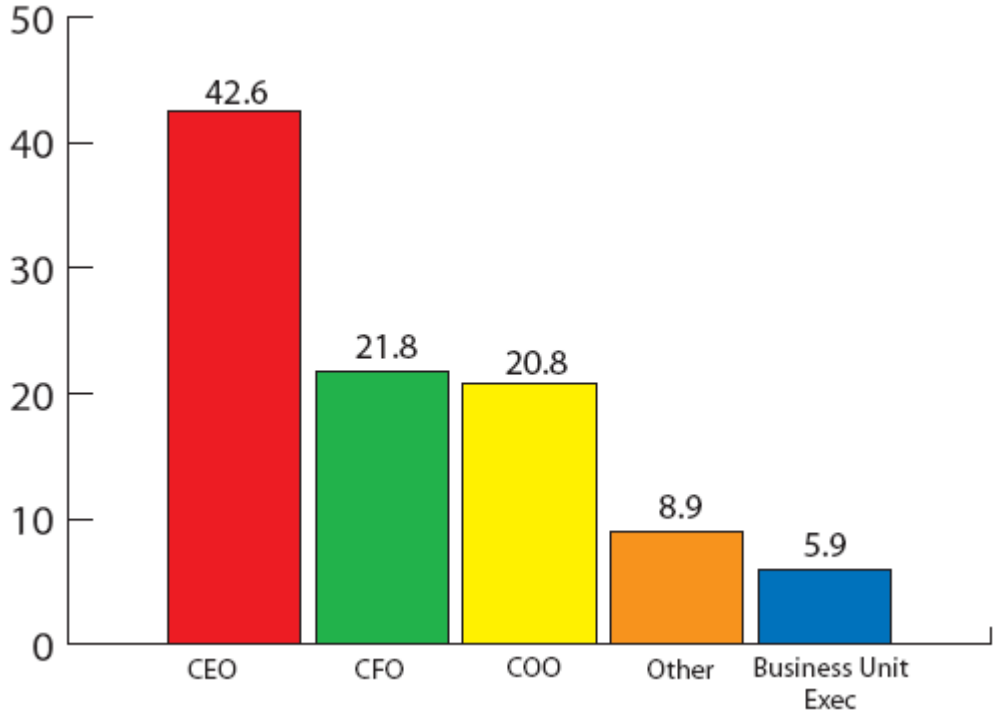
Information security responsibilities can be traced in a variety of ways, and the Ponemon Institute survey provides this distribution of reporting structures:[36]

[35] Ulf Nilsson, "From the Local IT Department Towards the Global IT Service Provider", presentation to European Conference on Information Systems, Gothenberg, Sweden, June 2006
[36] Ponemon Institute, "US survey: Confidential Data at Risk" 15 August 2006 http://www.vontu.com/uploadedFiles/global/Ponemon-Vontu_US_Survey-Data_at-Risk.pdf

Table 18 Who within your organization is responsible for protecting or securing sensitive and confidential data at rest?	Freq.	Pct%
No one person has this responsibility	134	28%
Chief Information Officer	96	20%
CISO/CSO	77	16%
Chief Risk Officer	32	7%
Compliance/Ethics Officer	32	7%
Chief Privacy Officer	31	6%
General Counsel	27	6%
CEO/Executive Committee	21	4%
Chief Financial Officer	14	3%
Other	13	3%
Human Resources VP	7	1%
Total	**484**	**100%**

Placed in the context of overall information management, another recent survey in all sectors showed that it was most common for CIOs to report directly to chief executive officers. In our interviews in banks, however, it was more common, and increasingly so, that information security reporting went directly to chief financial officers rather than through chief information officers.

CIO Reporting Structure



(J. Luftman, R. Kempaiah and E. Nash (2006), "Key issues for IT executives 2005" *MIS Quarterly Executive* 5(2): 27-45

Reputational issues

Although there is little evidence of direct personal reputational risk being associated with security breaches in banks, and still less that such a link might be extended to the choice of security technology, there are indications that this may emerge soon. The top-level resignations at Hewlett-Packard were associated with the misuse of privacy controls on databases, and the dismissal of AOL's chief technology officer and two others was a consequence of the massive data breach in July 2006.[37]

> "The cost of reputation risk are higher than that of financial risks"
> *Security Expert in a European Bankers' Association*

Budgeting is related to risk

As there are differences in reporting systems for security management, there are also differences in budgeting procedures, and here again we see inconsistencies and transitions throughout the industry. Increasingly information risk is seen as a cost item different from IT systems costs, but some firms have established an internal market in which different levels of coverage are provided, much in the way that insurance risk are calculated based on separate functions.

> "We use an internal debit system where the business units are charged for their chosen IT support levels. This visualises costs for security, response times when servers go down, etc. It's interesting to see that most business units are willing to pay a high price for short response times, as business contingency is vital and costs of reputation risk very high."
> *Security officer, Scandinavian Bank*

[37] Ellen Nakashima, "3 Leave AOL Over Security Breach; company pledges to review its privacy practices" *WashingtonPost.com* 22 August 2006

VII. Responses from interviews

The interviews yielded a wide variety of extremely rich evidence of preferences, attitudes and experiences with practice. Below we summarize the feedback from all interviews, organised in the structure of the interview template, as seen in Appendix 2.

Section A: Organising for information security

Our questions at the outset of each interview covered aspects of responsibility for information security, reporting structures, stakeholders in the organization and trends of change. All interviewees referred to a division between security policy making and IT implementation. The structure of hierarchies and the use of staff functions, typically organizing around operational, IT and financial risk respectively, differ among companies. Within the organisations, group functions strive to enforce similarity between markets in order to carry out compliance controls, but small and medium sized banks have achieved a higher grade of centralization of IT functions, such as practices of outsourcing, group intranet access, and security software updates. As a response, large organisations have developed a careful attitude towards outsourcing to third parties.

Interviewees reported that there is a trend towards security functions merging into compliance functions. Many experienced the rise of the information security officer in the organisation around year 2000 was a response to a lack of security practises during the 1990s. As information security becomes a ubiquitous practise among banks in coming years, some contend that the information security officer function will disintegrate to encompass all aspects of the operations.

There is a difference between retail and business banking that became apparent in the interviews. Some from small banks that specialize on business banking stated that they chose to avoid many problems by not having a web presence; their customers cannot log on to the bank.

Size also matters. Judging from patterns of responses, whether a company has a CISO is based on size, but even a small financial services organization is more likely to take security seriously than in typical manufacturing firms, and that difference is typical of the extensive use and maturity of applications in banks. We also saw a general shift from technology-driven, bottom-up security provision towards top-down, policy and compliance-driven direction.

Our respondents are greatly influenced by the converging practices and the influence of cross-national mergers among large banks. There are bigger differences between firms than nations, but corporate culture has traces back to its national origin.

Data mining: Attitudes differ towards customer data mining, which is extensively used in the United States. However, European respondents regarded it with apprehension and ascribe database breaches to the involvement of many third parties in associated activities.

Contractual agreements: In US and UK companies contractual agreements rule the behaviour and attitudes of what corporate security practices are. On the other extreme, Japanese companies have a very high trust in their employees, and expect everyone to be flexible in order to interpret the best interests of the company. In each cultural context respondents confirm their preference for their own approaches to reaching agreements and ascribing responsibility.

The meaning of information security: It is apparent from respondents that the meaning of information security differs with corporate function. To a certain extent and depending on the respondent's function, the role of security is more up to the interpretation of individuals than a clearly expressed corporate policy.

Section B: Regulation, standards and best practices

Sarbanes-Oxley and Basel II: Firms with no major activities in the US resent SOX, but nevertheless claim that they work to close the gap between their national and US practices with the expectation that similar regulation will soon apply elsewhere. Most knowledgeable respondents felt that Basel II requirements tend to mitigate against outsourcing. They also agree that it is impossible to follow exactly all diverse compliance requirements.

Intrusiveness: In China, the regulator and its control mechanisms are perceived as more intrusive than elsewhere, while respondents working in Japan report that the regulator favours local banks when dealing with requests. In most other advanced markets, the relationship between regulator and firm is characterized by a well understood trust-relationship. US firms are guided by more narrow compliance concerns than European firms.

Most respondents report that their organizations use ISO standards as guidelines for practice, but there is bewildering variety of assessment methods used and industry forums fail to satisfy the perceived need to align best practices.

Section C: Practices of information security executives

Reluctantly, some of the most knowledgeable respondents revealed that security at the highest level is an area of rare expertise. Only a few people can be relied on to implement and manage systems. For a smaller bank this is a major risk, because the loss of a few key personnel could make it extremely difficult to remain compliant. Information security is commonly described as a "craft" rather than a technical/professional function.

The lack of industry-wide benchmarks for the efficiency of security and its related effect on real risk makes financial firms rely on auditors for requirements setting. "SOX is a conspiracy of the auditors", one auditor jokingly expressed it. The subjectivity of auditing practises is a concern for developing real benchmarks. Some respondents agreed that an internal debit systems for IT resources can be a proxy to estimate costs in companies and this can develop as an alternative way of estimating risk, independently of auditing practices.

Section D: Security threats and tools to counter them

Common security products are becoming regarded as necessary commodities to compliment the "hard shell protection", and we believe that at the higher level there is not much evidence of brand loyalty, at least as it might enter strategic discussions. Most respondents expressed a high level of trust in anti-virus software and consider reliable and timely updates a strategic functionality. Further, respondents have noted the consolidation among vendors. They perceive top-tier players with sufficient support and expertise in anti-virus patching the only viable procurement option. The opinions about the reliability of intrusion detection methods varied among respondents. Some respondents claimed that current intrusion detection products lack appropriate automated reporting outputs to account for a prioritisation of warnings. This flaw led them to adopt inefficient manual monitoring methods. Some believe that locking functions in commonly attacked applications (especially in Windows) would be a useful innovation.

Section E: Coping with networks, mobility, and virtuality

The largest information security problem for retail banks is reported to be online connections, but flash cards and wireless LANs are of great concern to some. Surprisingly to us, mobility in the work force is not considered of strategic importance in the financial sector, and some firms have even banned Internet access from PDAs and mobile phones. Data on BlackBerries and laptops are encrypted and almost everyone interviewed agreed that they pose no major data threat if stolen. New ways of using "thin clients" where central controls ensure better security through central storage, and could reduce the risks associated with lost physical storage (laptops, flashcards, phones, BlackBerrys. Some of the IT managers stated that even if laptops themselves are secure, certain applications (such as web conference software) could compromise security and must be checked before being deployed. Many banks do not allow external devices to connect into their networks: "the nightmare scenario would be the bank as a source of infection for internet banking customers," as one IT manager expressed it. Network access control and policy generation for new devices connecting to the network are also regarded as a high administrative burden.

VIII. Discussion: innovation and the ecology of information security

Innovation

How can we understand the innovation processes operating as information security changes over the coming years; where does the incentive and the know-how come from to change security? Administrative innovation and adoption often lags technical innovation in an organisation.[38] It comes as no surprise to security officers that managerial practises related to new security tools take time to develop. In our study we see these trends of administrative innovation, with internal debiting systems as an example, coinciding with an increasing interest among financial institutions to keep IT systems in-house to control operational risk.

As compliance becomes a by-product of overall risk management, security risks become a main interest for the compliance officer. To find out details of IT risk, the compliance officer could contact the IT department directly. It follows that security functions will be a subset of compliance and risk management, as organisational routines related to security become standardised. However, the dissemination of security functions into everyday practises must be supported by employees well educated in "everyday risk" for this delegation of responsibility to take place. It is clear from the majority of our interviews that inter-organisational benchmarking would increase the understanding of real risk and the education of employees. It would balance the current dependence on a few security experts in the organisation (which is an organisational risk in itself) and further a transition of current administrative processes.

Internal debiting systems put the IT resources "up for sale" to the business units within a firm. Business units receive offers of service levels from the IT department with an associated cost. Scandinavian banks in the study report on the introduction of such internal IT debiting systems for security and recovery operations. Initial results indicate e.g. that business units develop a monetary evaluation of different start-up times (after a server goes down) and its associated reputational and financial risk. This becomes a subjective, or soft, benchmark.

Such soft benchmarks result from "collective action" among employees and complements methods of deliberate risks assessment, which often involves an estimation of risk probability (e.g. the "Sprint" method used in many banks). Soft benchmarks result in internal cost estimations of particular service

[38] Swanson, E, (1994), "Information Systems Innovation", *Management Science*, vol 40, 9, 1069-1092

levels (based on both perceived value by the business unit and internal costs for the IT department). The minimum service requirement for critical processes would be set by a national financial services authority or the auditor. However, internal "price lists" could develop to form an initial input for knowledge exchange in inter-organisational comparisons.

Resource-based theories in management economics focus on the capabilities of organisations and deal with innovation in just this sort of way. We could regard the collective action of participants as a means of accumulating organisational capacity, as expressed by one management scientist in the following way: "Outside sources of knowledge are often critical to the innovation process, whatever the organisational level at which the innovating unit is defined… prior related knowledge confers an ability to recognise the value of new information, assimilate it, and apply it to commercial ends. These abilities collectively constitute what we call a firm's *'absorptive capacity'*". [39]

The absorptive capacity among employees contributes to administrative process innovation. We can envisage a scenario where educated employees will increasingly value security software functionality as they develop a higher collective and individual absorptive capacity and understanding for new concepts of "everyday risk". The information security arena could gain new dynamics through interaction between vendor-driven security product innovation and customer-driven administrative process innovation. Vendors who take advantage of this trend could attain competitive advantage.

The ecology of information security

Firm-level

The use of information security technologies is part of an array of control mechanisms that can be deployed to help further the interests of groups or organisations. Most commonly we see it deployed within a company as a defensive mechanism, and in response to outside pressures to comply with expectations that regulators or industry agreements apply to responsible firms. That is the most clear instance of a differentiation between a safe internal environment versus a dangerous external environment. That might extend to the provision of a secure web interface that improves login security, but not much further. Some financial services firms differentiate themselves as especially security conscious in their advertising or by cultivating a reputation as being more cautious than competitors.

[39] Cohen, W, Levinthal, D (1990), *Administrative Science Quarterly*, Vol. 35, No. 1, Special Issue: Technology, Organizations, and Innovation (Mar, 1990), pp. 128-152

Authorised users

We have seen that the boundaries between the internal and the external are not well fixed in practice, even if in various ways they can be defined in law. So that when Barclays Bank provides anti-virus software to all its online banking customers, it goes beyond a polite request to them that they might try to cooperate. Indeed, it implicitly extends its system to encompass its customers' computers and accepts that by providing a particular product, they take on various responsibilities ranging from the endorsement of that brand to the added customer support that might accrue. A similar blurring of boundaries occurs when password generating tokens are used, such as those issued by Lloyds TSB from October 2005 and HSBC (for business customers only so far) from early in 2006. The longstanding experiences with two-factor authentication systems of Scandinavian banks, their imminent extension to all banks in Singapore, and their likely spread throughout Europe in the coming years will force further discussion of the boundaries and the increasing discontinuity between technical feasibility and the managerial and legal resources that should accompany it.

All users

Public awareness campaigns aimed at all online financial services users, such as the one mounted by the Swedish banking association and the U.K. Financial Services Authority, define another community. Vendors of security software products generally target this market when they try to reach individual, retail buyers. Insofar as surveys reveal that the vast majority of people using online banking are aware of security software we might imagine that these activities are successful, but the actual rate of usage is much smaller than the level of awareness might suggest, and consistently secure user behaviour is a rarity.

All of us

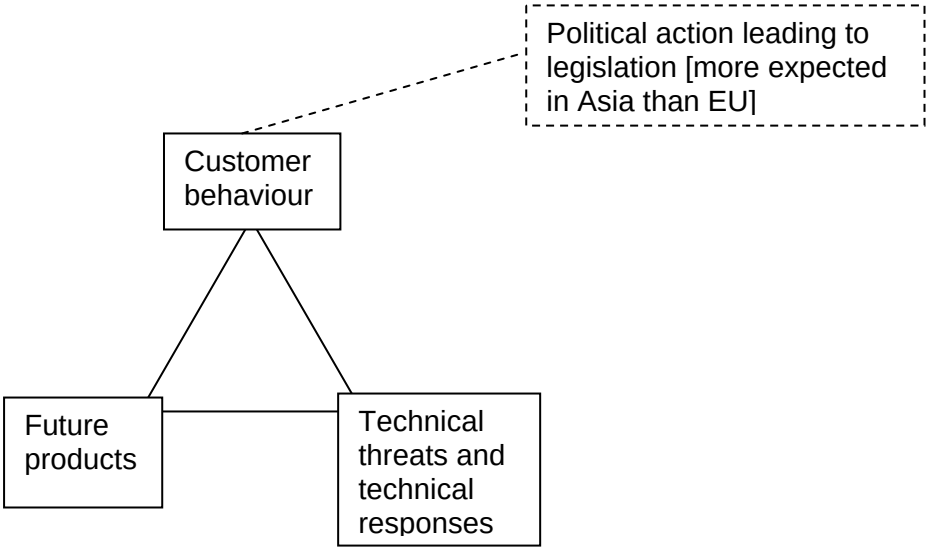
There is a larger community that includes all of us, or at least addresses the general level of security of the internet as a whole. Much is being done along these lines, by law enforcement agencies in their efforts to apprehend criminals who use the internet, by those engaged in the governance of the internet such as the Security and Stability Advisory Committee of the Internet Corporation For Assigned Names and Numbers (ICANN), by the European Union and some national governments. However, aside from cooperation with industry bodies, this level of activity does not appear in any mainstream firms' business plan within the financial services sector.

This perspective on the ecology of information security is useful not only in helping to understand the concept of boundaries of responsibility, it also hold implications for strategic behaviour for all of the

stakeholders in the industry. It clarifies roles and responsibilities and can guide in decision making for levels of investment. There is also, in theory, a relationship between success in disseminating secure practices at a higher level of community and the spending that might be necessary at a lower level.

IX. Conclusion

Despite the international character of the financial services industry, local differences abound. Although some of these emanate from national legal and enforcement systems, others are associated with differing ways of doing business. A general model of the relationships we perceive among information security tools, customer behaviour and the legal environment can be expressed in the following way:



One way to think of this is as a relationship among customer behaviour, technical threats and their countermeasures, and the manner in which innovative activities lead to future products. This is neither a "technology push" nor a "market (or regulator) pull" argument, but a recognition of the embeddedness of security within a nexus of social relations.

This relationship becomes especially indicative of future activities as most firms have a tendency to approach security regulation as a matter of non-repudiation.[40] For managers there, security is an operational cost and defence against attack is approached in a passive, post-hoc matter. This is usually explained as a response to the combination of external obligations to comply with regulations and standards plus internal assessment techniques, budgeting and reporting procedures. However, this is not the only possible result of this set of relationships. In Swiss banks, and some other leading financial services firms the approach is more to take concepts of "duty of care" as a matter of active responsibility, leading to an attitude supporting ex-anti action. If information security is to emerge as a contributor to the strategic functioning of firms, and especially if it is to be regarded as a contributor to

[40] L. Georg, "The Function of Corporate Security within Large Organisations: The interrelationship between information security and business strategy" PhD Dissertation , Universite de Geneve, 2006, p. 147

competitive advantage, it is likely to benefit most from imaginative extensions of these proactive interpretations of the “duty of care”.

Who is really responsible?

The underlying issue concerns where responsibility lies. This is variously defined, differently in different countries and by their behaviour differently among banks. Legal responsibility for the most part is limited to the boundaries of the banks and their internal systems. This is supported by the behaviour of customers, who increasingly act as if responsibility for their own devices rests with them, even if they resent it. However, this behaviour is changing. Forces for change can be seen in the move towards increasing responsibility for secure devices where “one-time password tokens” or similar bank-owned, remote customer used security devices are presented. Within banks a similar boundary is breaking down between the information security organisation and its internal environment. This changing ecology provides the largest challenge to any firm that wants to keep up with the forefront of information security.

Appendix 1: Research Methodology

The report presents the combined findings emerging from data on information security practices and opinions worldwide, with specific attention to the financial services sector. These data were obtained by:

1. Literature review

The aim of the literature review was to identify the key issues discussed in relation to the trends and changes expected in information security practices and their regulatory, standards, and policy environment internationally as well as nationally. The review sought to differentiate among most influential contextual factors and those which are less likely to be of great significance for the actions of chief information officers and other responsible information security executives.

In particular, three key areas of literature were surveyed:

Standards and legislation: The relevant legislation stems from three sources: governance, privacy and risk. The first of these, best exemplified by the U.S. applications of the Sarbanes-Oxley Act and related foreign requirements to ensure that record keeping and reporting processes are inviolate. There is considerable literature on this, originating in government sources which describe and advise on how to meet the compliance requirements, in consultancy advice on how to go through the necessary processes, and from the trade literature that addresses trends and challenges in practice. Privacy policies have emerged in different forms in many places, but the key effect has been laws requiring public notification of every breach of data security where personal information is revealed. In the financial services sector in the United States the Gramm-Leach-Billey Act similarly places the onus on financial services organisations to ensure that their systems are as secure as possible (sometimes defined in terms of the "duty to care") from risks of data theft. While UK and US standards and legislation provided a starting point, we were able to see the international trends and to put into perspective European Union legislation and policies.

Academic and expert studies: The general area of computer security is well developed in two forms, one based on computer science and software engineering and providing technical insights into the design and operation of secure systems. The other focuses on the legal and business context and includes studies of management practices and attitudes, liability and risk analysis, and the relationship with business strategies. These are found in numerous newsletters, conferences, and specialist journals such as *Computer Security*. A handful of specialist consultancy companies complement the computer security research centres publishing reports of relevance to this study. Especial help was available from the many doctoral studies conducted at the London School of Economics or in some way associated with researchers there.

Trade journals and professional bodies: A wealth of information is available from news sources and the guidance available from professional bodies and their outlets, including numerous specialist web sites and magazines such as *CIO Magazine*.

2. Expert interviews

Almost 20 interviews and discussions with experts were conducted, most of them structured in a formal manner following the template in Appendix 2, below. The people were interviewed under condition of confidentiality, but we have quoted extensively from them. We made an effort to speak with people at the appropriate level of seniority and responsibility but also to gather opinions from people some who

had special expertise in technical aspects of banking security, some who had high level responsibilities for corporate policies, and some from industry associations, lobby groups and official bodies, representing 10 countries [41] in order to gauge their opinions and learn of their expectations for the future of information security tools and practices. Our template for questioning is appended below.

[41] The countries included: China, Germany, Netherlands, Japan, Singapore, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

Appendix 2: Interview Template

I want to ask you some questions about your work as CIO, especially as it relates to information security matters. My questions are organized in the following way:

- First I will ask about your position, responsibilities and powers within your company.
- Second I will ask about your relations with external bodies such as regulators and industry and professional organisations.
- Then I will ask about the work of the CIO's office
- Then we will turn to security specific matters, including costs and benefits of investing in security, your perception of current and future threat levels, and the kinds of tools you have available or would wish to have to assist in ensuring security.
- Finally I will ask about your views on security specific to networks, mobility and virtuality [e-business, m-business, distributed work, etc.)

I want to assure you that I am not interested in any proprietary or commercially sensitive information. I am not going to ask you about details of your defences or your level of security, or anything about your experience of security failures.

A) Responsibility for information security in the organisation

Questions	
A1	Who is ultimately responsible for security within your organisation (short of the Chairman of the Board)?
A2	Please describe the reporting structure for improvements and changes to information security. Is this the same reporting channel as would apply in problem escalation?
A3	Who do you see as the main stakeholders in information security? What are their expectations of you?
A4	How would you present an argument to superiors for changes in information security, for example if you wished to increase expenditure?
A5	Do you perceive expectations and willingness to provide resources changing?

B) Regulation, standards and best practices

Questions	
B1	What relations do you have with industry bodies and standards setters with regard to information security?
B2	How do you deal with government regulators?
B3	The US Department of Homeland Security defines financial services to be part of "critical infrastructure". How does this affect your activities?
B4	Do you anticipate the EU or your national government emulating such controls and oversight?
B5	Are suitable consultancy services and other forms of intermediation, or buy-ins adequate and reliable for your needs?
B6	Which of these are your familiar with and concerned about complying with? USA: Sarbanes-Oxley Act (re accountability and due diligence) Gramm-Leach Billey Act (re privacy of consumer financial information) Security & Exchange Commission Expectations of "critical infrastructure" status by Dept. of Homeland Security UK: Financial Services Agency guidelines Data Protection Act ISO/BSI (1)7799 on secure systems management Europe: 8th Directive Council of Europe treaties

C) Practices of the CIO's office
(we need to classify available tools into groups: client software, server software, network hardware – firewalls, load balancers(?) etc),

Questions	
C1	What assessments are made of IT assets in need of protection? What methodology is used for this?
C2	Implementing "best practises" and "due diligence" is costly. How do you assess the benefits?
C3	Is the role of the information security executive moving towards routine, commodified practices, or towards directors' level strategic functioning?
C4	What is the confidence (how do you perceive the reliability) that you have in your security tools?
C5	How are particular products integrated into the management of practises for the business?
C6	Are you satisfied with the routines you use for virus definition updates, password shifting and similar frequent changes? Can you rely on automatic adjustments?
C7	What effect might current trends have upon your procurement and use of information security products?
C8	Do you expect industry standards to emerge that will limit your choices?
C9	Are you likely to have influence on the process of setting such standards and recommending particular products?
C10	Do you use custom security software? If so, for what purpose (virus/spam/spyware/site marking etc.)?
C11	Do you use outside service providers for strategic security functions?

D) Security threats and tools to counter it

Questions	
D1	Which kinds of external threats concern you most?
D2	To what extent do available software tools support your measures against general (external) threats? Against internal threats?
D3	How do you deal with “patch management”? Can you rely on automated updates for virus definitions, etc.?
D4	Is outsourcing an additional information security risk? Do you feel sufficiently in control of information security in outsourcing arrangements?
D5	Have you created routines and reporting systems and automatic alerts on external threats using intrusion detection software?
D6	Do you feel that business continuity (backups, redundant facilities, etc.) are appropriately aligned with information security concerns?

E) Coping with networks, mobility, virtuality

Questions	
E1	Is there a direct connection between security budget incentives (for the CIO/security officer) and an increased mobility among users of business applications (email, ERP system, teleconferences etc)
E2	Do your information security practices expand to encompass mobile work as it grows and changes? Are some areas more problematic than others (email, teleconferencing, etc.)
E3	What happens when an employee loses a portable device such as a BlackBerry or laptop with sensitive data, email, etc.?
E4	Which mobile devices pose highest levels of external (attacks) security threats?
E5	Which mobile devices pose highest level of internal (employees breaking rules, portable storage etc) security threats?
E6	To what extent are you involved in making your company a central actor as a virtual enterprise in the financial services value chain.

Appendix 3. "Quotable Quotes" from Interviews

Section A: Organisation around information security

"Arguments to superiors for changes in information security are formulated in terms of risk, rather than in terms of direct cost."
Security manager, Bankers' Association, EU.

"We are extremely dependent on a few key security experts. We have good results from the financial services authority inspections, but try and downplay this vulnerability during audits…"
Security officer, Scandinavia

"We have a global outsourcing partner, who handles all storage of data, firewalls, other security software, and support request. We remain with [only] administration rights to our critical applications. We are very happy with this arrangement. Stringent processes and documentation have been built up for a smooth interaction between our outsourced IT department and the users in the bank. The outsourcee is on top of things and our automatic anti-virus system pulls updates every hour from the vendor".
German bank, manager, operational risk

"We don't see any convergence of the security practises as such among organisations. One reason being the people caring for customer data and policies are different to those who manage and maintain the system security. This is not only due to compliance reasons, but a more pragmatic one: You can't expect someone to be expert on both policy and implementation."
Policy manager, industry association in the EU

Section B: Regulation, standards and best practices

"It is important as the national umbrella organisation to make sure the regulator doesn't make statements which gets very expensive for our members"
Security Expert in a European Bankers' Association (the Dutch)

"Due to Basel's capital rules, we need to have full control of related information, therefore information security is vital"
Bank security officer, Sweden

"The national financial service authority holds the key to standardization, as they handle ISO certification and coordinate international compliance legislation."
Bank security officer, Sweden

The practical implication of being part of the "critical infrastructure" is that banks keep payment flows going after a catastrophe"
Bank security officer, Sweden

"We have good relations with the local financial services authority. We have some margin to argue our case, as sometimes what we do in Tokyo means breaking a local regulation when following a global regulation. E.g. we are not allowed to delete sent emails according to the Japanese regulator, but in Germany we must delete emails due to privacy laws. Good relations with the financial services authority is crucial and they know about this situation very well".
IT manager, Japan

It costs a lot of money to work towards compliance, and sometimes this takes resources away from dealing with real risks. The Finance Services Authority recognises this problem as well. SOX regulates 5 aspects relevant to

us, where 2 relates to governance and 3 relates to information security: Correctness, confidentiality, accessibility of data for financial reporting. We don't have to follow SOX today, but if we had to, we'd make SOX becoming a side effect of our normal practises.
Security manager, Scandinavian bank

"The regulatory influence is totally different between Japan, Hong Kong and China. In Hong Kong the financial services authority is non-intrusive and non-discriminatory business environment. In Japan the authorities sometimes discriminate against foreign firms; red tape is slower for them than for local companies. In China, subjectivity from the China Banking Regulatory Commission bogs you down, if you can't show how you benefit the Chinese state in a clear way."
IT manager, Japan

"Privacy laws and obligatory disclosure of data breaches is a trend in developed countries. First the US, then other countries like Singapore, and soon the UK. Regulators in undeveloped markets such as Malaysia, the Philippines, Indonesia, Taiwan, and China will not be too keen on this, as they know they are behind."
IT manager, Japan

Section C: Practices of the CIO's office

"The cost of reputation risk and Basel 2 related issues are higher than that of financial risks"
Security Expert in a European Bankers' Association

"The EU cybercrime convention disseminates to national level, and it's a worry that different countries implement it differently"
Security Expert in a European Bankers' Association

"The gap between theory (compliance rules) and practise in information security management has never been greater"
Banking security expert, UK

"We understand SOX and what it's good for, but in practice you do what you can. You try to identify issues that affect SOX and eliminate these issues rather than regulate them."
Banking security expert, UK

"A difference between the US mentality and ours is that we are more wary and careful about data mining. Compared to the US, there is less utilization of customer data for this purpose, and therefore less sensitive data being extracted in processes that could be compromised."
Banking security expert, UK

"We foresee a disclosure law for data breaches, like the US one, in the UK before year-end."
Banking security expert, UK

"The boundary, 'blame line', between bank and customer in the international perspective is blurry due to different legislation in different countries."
Banking security expert, UK

"Banks collaborate on a list of convicted fraudsters, but it's tricky to exchange this kind of information, so it's mediated by the FSA."
Banking security expert, UK

"Security policies are decided on top level, as it should, but it's sometimes a problem for IT departments that decisions are not taken close enough to its implementation".
Scandinavian bank's branch office in Asia

"We don't assess the benefits of due diligence and best practises as IT is an outsourced cost centre in our organisation. We are not going to pretend we create value in our IT operations."
IT manager, German Bank

"Information security is of increasing concern. But more and more complexity comes into the picture too. We have a strong feeling that IT governance methods are increasingly important that we can control the cost of this increasing complexity."
Policy manager, Banker's Association

"A strong concern regarding the EU legislation is that it shouldn't deal with too much minimum standards, and it's important to remain a "bottom up" approach. We don't like regulation that ends up getting very expensive. Here we use a national approach, and work through the employer's organisation to counter similar expensive regulation in other markets."
A Bankers' Association, EU

"Social engineering utilises weaknesses in the "open environment" that Windows provides. If we could grant much more detailed access control within Windows, many of the current security risks could be eliminated."
A Bankers' Association, EU

"We don't have time or capability to quantify risk probabilities in say 1% or 20%, so we simply acknowledge that we need to manage that risk. The lack of benchmarks makes it difficult for us to then assess the value or efficiency of our actions, since the only real indicator you have of your security levels are breaches. But breaches occur too seldom to be a reliable indicator".'
Security executive, Scandinavia

"Our evaluation of best practises is very subjective and we lack soft benchmarks. If security is a selling point in a given point of time we would invest, no matter the costs. Further, the rise of risk management as key activity, and the role of information security for Basel II capital ratio, contributes to security now showing up on the radar screen for top executives and the board."
IT security manager, Japan

D) Security threats and tools to counter it

"We have no loyalty towards certain vendors, and it's part of our strategy to rather strategise around technology choice (such as java for internal development) to stay independent."
Bank security officer, Sweden

"Patch management for virus updates could be done quicker. Manual processes to log actions on each server hold us back and we'd like to further speed this up"
Bank security officer, Sweden

"It's expensive being test rabbit for new security technology, and dangerous to be a lagger. We choose to be on the forefront in some areas, but support and customisation needs for older legacy systems hold back quick transitions"
Bank security officer, Sweden

"We consider our ability to effectively updating our virus protection a strategic asset"
Bank security officer, Sweden

"We perceive two major security threats in our operations: One being virus, the other being investigated without notice by the Chinese financial services authority"
Small branch office of EU bank in China

"From January 1st, it will be compulsory with token authentication in Singapore, and some banks will struggle to get their systems up and running on time".
Security officer, Bank in Singapore

"We have no brand recognition locally for specific security tools, as they are procured centrally and only installed by us. We have a central server to which we connect new PCs and laptops and all software is installed from there. Also, all Internet traffic to our branch is routed via VPN tunnels to proxy servers in HQ, so the Internet pipe is centrally managed, and can be cut in case we have a virus attack."
Branch office, EU bank in Singapore

"The largest threats to information security practises for our mobile workers according to me are public wireless LANs and carelessness with flash memories. For both Blackberries and laptops the data is encrypted and not a big security risk"
Security offer, in Singapore.

We have high confidence in our total security system and need an overlap between different vendor products, as we don't trust individual anti-virus and spam products fully.
Security officer, Scandinavian Bank

The next wave of malicious software is Trojans. As a bank, we always have the possibility to protect ourselves, but the big problem is many of our Internet bank don't have necessary protection. Trojan viruses will increasingly cause a lot of problems for these customers.
IT officer, Scandinavian Bank

"We use an internal debit system where the business units are charged for their chosen IT support levels. This visualises costs for security, response times when servers go down, etc. It's interesting to see that most business units are willing to pay a high price for short response times, as business contingency is vital and costs of reputation risk very high."
Security officer, Scandinavian Bank

"To counter the tendency to get stuck with any company, we make a point to change anti-virus software occasionally. That ensures we are independent of any one vendor."
Manager, IT Security Bank in Japan

On Internet banking boundaries:
"The banks are afraid of becoming a helpdesk for Internet customers, as you will get all kinds of support requests. It's a balance to strike, because at the same time we want to consult and give advice. The second challenge regarding issuing recommendations of say anti-virus software to customers, is that we get involved in vendor choice, and run into possible questions of, at least morally, liability."
Security officer, Scandinavia

The difficulty of intrusion detection is the manual interpretation of incoming "alarm bells". A lot more could be done, as it is the combination of many factors that signals a potential intrusion, and this should be automated much better than today."
Security officer, Scandinavia

"I'm satisfied with our virus protection. The key is automated patching as you need to buy time. A new patch to Microsoft Windows on the Friday, and a virus could kill you the next Monday if you don't have your updates installed. Compared to 5 years ago a lot has happened and I expect it to improve further the coming years."
IT security manager, Japan

E) Coping with networks, mobility, virtuality

“Proprietary software used for example in remote Video Conferencing sometimes contain security holes, so in a way we become path dependent to current products due to resource limitations in testing new products.”
Security officer, Scandinavian bank

“We don’t use PDAs and mobile phones connected to the Internet, as we don’t consider these products fully mature yet from a security point of view.”
IT manager, Scandinavian Bank