Computer Security, Privacy, and Politics:
Current Issues, Challenges, and Solutions

Ramesh Subramanian
Quinnipiac University, USA

IRM Press
Publisher of innovative scholarly and professional information technology titles in the cyberage

Hershey • New York

Acquisition Editor: Kristin Klinger
Development Editor: Kristin Roth
Senior Managing Editor: Jennifer Neidig
Managing Editor: Jamie Snavely
Assistant Managing Editor: Carole Coulson
Copy Editor: Jennifer Young
Typesetter: Larissa Vinci
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
IRM Press (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033-1240
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.irm-press.com

and in the United Kingdom by
IRM Press (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanonline.com

Library of Congress Cataloging-in-Publication Data

Computer security, privacy, and politics : current issues, challenges and solutions / Ramesh Subramanian, editor.
p. cm.
Summary: “This book offers a review of recent developments of computer security, focusing on the relevance and implications of global privacy, law, and politics for society, individuals, and corporations.It compiles timely content on such topics as reverse engineering of software, understanding emerging computer exploits, emerging lawsuits and cases, global and societal implications, and protection from attacks on privacy”--Provided by publisher.
Includes bibliographical references and index.
ISBN-13: 978-1-59904-804-8 (hardcover)
ISBN-13: 978-1-59904-806-2 (e-book)
1. Computer security. 2. Computer networks--Security measures. 3. Computer security--Government policy. I. Subramanian, Ramesh.
QA76.9.A25C6557 2008
005.8--dc22
2007037717

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter VIII

Privacy through Security: Policy and Practice in a Small-Medium Enterprise

Ian Allison, The Robert Gordon University, UK

Craig Strangwick, ABC Awards Ltd, UK

Abstract

The chapter discusses how one small business planned for, and implemented, the security of its data in a new enterprise-wide system. The company's data was perceived as sensitive, and any breach of privacy as commercially critical. From this perspective, the chapter outlines the organizational and technical facets of the policies and practices evidenced. Lessons for other businesses can be drawn from the case by recognizing the need for investments to be made that will address threats in business critical areas. By highlighting the need for organizations to understand the nature of the risk and the probability of an event occurring, the security approaches highlight the need to address both the threats and actions in the event of an incident to reduce the risk to privacy.

Introduction

Privacy often is discussed in the literature as an ethical issue, whereby members of society are perceived to have a right to privacy and that right is considered to be eroded through the application of information technology. The Internet and supporting architectures are considered to make privacy more vulnerable because behaviour can be monitored, personal data can be commodified and exchanged, and data can be combined from different sources to enable analysis of individuals' records (e.g. Spinello, 2006; Tavani, 2004). The invasion of privacy is seen to occur through the access to, and control of, personal information.

Consequently, debates in the literature focus on what we understand privacy to be, the degree to which privacy can be taken as a right, to what degree privacy should be protected and how computer technology affects privacy. In other words, the morality of individual, organizational, and societal actions is evaluated. What is ignored in these debates is the business implication of privacy and how this shapes information security activity within organizations.

Security research, on the other hand, focuses on the threat of attack by hackers or malware, and the tools and technical solutions available to address these threats. The need to develop secure architectures or build applications that avoid security pitfalls, whilst important, mostly does not address the way in which such decisions affect privacy.

This chapter, therefore, seeks to straddle these two fields to show how organizations need to take privacy into account as a business issue in order that this shapes information security policies and practice. To achieve this we draw on the experiences of one small-medium enterprise (SME). The formal definition of SMEs varies from country to country, but for the purposes of this chapter we have defined SMEs as employing less than 500 people. This definition does not mean that the lessons are not applicable to larger organizations but that the focus of the study, and data drawn from previous studies, matches this definition.

The remainder of this chapter begins by outlining why privacy is a business issue, recognising the financial and legal imperatives organizations face. Current security policies and practices in SMEs worldwide are then reviewed highlighting the weaknesses currently evident in the way that SMEs approach their information security.

The focus of the chapter is a case study based on ABC Awards Ltd, a small UK-based assessment body who offers vocational qualifications through a variety of learning centres. The study relates to their development of an enterprise-wide information system and underpinning infrastructure. Policy and practice were developed to

support the business security needs in line with the legal and commercial need for protection of privacy of personal data. The analysis is structured to focus on people and organizational issues, and on technical issues, to show the inter-relationship between these aspects of information security management.

Privacy as a Business Issue

The violation of privacy through computer technology is often related to acts of snooping on individuals. Edgar (2003) gives examples of how computers have been used to identify potential prospective sales targets, verify the status of debtors' bank accounts, and find out about the activities of customers. These examples show how organizations are seen to invade privacy in order to make business decisions based upon private data. Moor (2004) therefore calls for increased legal protection so as to reduce excess harm and risk to the individual at the expense of the organization.

Organizations are already under a clear legal obligation, at least in some countries, to protect private data and to use it only in accordance within defined guidelines. Laws on data protection have developed since the 1970s. France (2004) noted the way that the European Directive (95/46/EC) in 1995 produced harmonisation of these laws across Europe. The resulting laws supported the free flow of data between businesses in different parts of the continent as the Directive provided a standard level of protection. However, she also highlights that it was not the moral but the trade imperatives that led to the development of the initial UK Data Protection Act (1984). Previous parliamentary investigations had been less than convinced by the ethical cause.

The current UK Data Protection Act (1998) is built upon eight principles that constrain the way that data is collected, processed, and stored. For example, organizations have to ensure the data is accurate, held only as long as necessary, not excessive, and secured.

Elsewhere though, such as Australia, small businesses are exempt from privacy legislation. The US, too, has minimal legal protection for private data, with small business required to offer little security of data, and some make a profit from selling on that data. As a result some argue this leaves them "woefully behind" Europe (Tavani, 2004, p. 146). The US Government appears to side with business interests, who fear the cost of implementing data protection legislation would undermine economic efficiency. Tavani (2004) argues that this is alarmist and there is minimal overhead as most US organizations operating in Europe have done so without profits suffering.

Indeed, on the contrary, it could be argued not paying appropriate attention to privacy could be a detriment to business profits. As Holmes (2006, p. 2) puts it, "carefully thought-out privacy controls make good business sense" as it has a considerable impact on sales. He shows how getting this right has been beneficial at Bell Canada. Microsoft also has recognised that it needs to ensure privacy as part of its products and services (Fleischer & Cooper, 2006). In areas related to Internet activity, Microsoft's policies and practices have been overhauled to ensure compliance with the EU privacy rules. Fleischer and Cooper (2006) conclude by highlighting the importance of privacy for the business and the need to involve key stakeholders in decisions about privacy policy.

There are though many examples of organizations who have suffered loss of profits as a result of under-mining customer privacy; the "size of the monetary penalty should fool no one" (Holmes, 2006, p. 1). Nissenbaum (2004) gives the example of Lotus Marketplace, a software package that brought together publicly available information about individuals in one system. The package was due to be launched by Lotus and Equifax in the early 1990s. They did not anticipate the level of public complaint: 30000 letters of protest were received. The package was withdrawn from the market. Cartmanager, an online shopping cart software provider, broke its own privacy policy by selling customer data thereby infuriating both online users and the merchants who had incorporated the software on their Web sites; their reputation was damaged for some time (Holmes, 2006). Similarly, one of the UK's largest banks, HSBC, found itself on the front page of national newspapers in August 2006 because of a security loophole putting customer data at risk via its Internet banking systems requiring its CEO to write a strong rebuttal highlighting the potential impact of the article on its business (Guardian, 2006).

As a consequence, organizations need to focus on ensuring customer trust. "Trust means stakeholders feel safe in the hands of these enterprises and are confident in the secure delivery of their products and services along with protection of their private information" (Reece, 2007, p. 1). Reece (2007) goes on to argue that trust must be earned through excellence of operations and leading edge information protection. Good information protection requires organizations to recognise the value of the information and develop policies accordingly. Good privacy polices should not be seen as a dam but as a finely tuned control valve allowing business to continue effectively whilst maintaining the integrity and security of personally valued data (Holmes, 2006).

The financial implications of a lack of trust are significant. For instance, e-commerce usage has stalled because of a lack of trust (Holmes, 2006). Internet users place great value on security measures that make identity theft less likely (Poindexter, Earp, & Baumer, 2006). At The Woolwich, a UK bank, security was seen as a critical ele-

ment in their adoption of e-banking following the embarrassment suffered by their parent bank where security breaches led to huge media coverage (Shah & Siddiqui, 2006). Low information security effectiveness could have wide-spread implications for competitive advantage: "the enormity of potential losses arising from IS security abuses should motivate them to raise their deterrent efforts so as to enhance there IS security effectiveness" (Kankanhalli, Teo, Tan, & Wei, 2003, p. 152).

So in summary, if a business was to inadvertently release private data then the damage to the reputation and trust in the market that would have an immediate, and at least proportionate, impact on the business's finance. Even ignoring the possibility of litigation, the loss of custom could be substantial. This risk is all the more likely where trust is a paramount element of the service provided, such as in financial or other personal service organizations. Organizations are aware of these risks to their business: it is already seen as a major constraint on the growth of e-business. On this basis then, security of systems should be considered from a customer privacy perspective, as well as ensuring business processing can be maintained.

Security Policy and Practice in SMEs

The growth of e-business has increased the criticality of any security incidents, mounting risks to privacy through new forms of attack, and the legal implications of breaches. Large organizations therefore have become far more aware of the need to take action to address the security risks arising from using information systems, resulting in a drop in the number of incidents (DTI, 2006). Previous studies, however, (e.g., Kankanhalli et al., 2003) have shown that small businesses are less likely to address this issue and are ignorant of the technologies available. Such organizations have become more vulnerable therefore to the threats relating to their information systems and have seen a rise in incidents.

Equally, the security of business transactions and personal data is not simply dependent upon the security of the network. From a survey of SMEs in Hong Kong, Chung and Tang (1999) conclude security management is an important success factor for the adoption of information systems in SMEs. So as new customer-based information systems are designed, developed, procured and deployed the privacy related security issues of the information system need careful consideration.

With the increasing use of the Internet and mobile technologies by smaller organizations, enabling them to be more flexible and diverse in their operations, the threats are broadening. Effective security management is therefore essential for all organizations in this increasingly interoperable world in order to ensure that the

information remains confidential, available and retains integrity. Yet, Chang and Ho (2006) found the smaller business is likely to be less effective in the application of critical factors outlined in the security management standard ISO17799 with smaller organizations resisting making investments in this area. Here then we will review the extent of the issue.

Gupta and Hammond (2005) undertook a survey of SMEs in the USA. Their findings provides an insight into current information security practice within small businesses based on questionnaires drawn from organizations across a variety of sectors, including services, construction, utilities and finance. Keller, Powell, Horstmann, Predmore, and Crawford (2005), similarly, interviewed 18 system administrators in small businesses to evaluate systems security practice. Their findings provide a more personalized view from network professionals working in small organizations. There is a natural difference between these findings resulting from the variation in the type of samples: network specialists will be intrinsically more knowledgeable than the average SME manager. Below, these data sets are used to evaluate SMEs' security management policies and their use of security technologies.

Security Management Policies

Table 1 summarises level of adoption of security management policies by small businesses. The levels of planning and policy definition are low in comparison to larger organizations. Only 41 percent of small businesses have written a security policy that will protect customer privacy (Gupta & Hammond, 2005) in comparison to 76 percent of large organizations (Fulford & Doherty, 2003). The reasons for this difference relate to expertise, resources, and an understanding of the risk.

Table 1. Policies and procedures currently in place (adapted from Gupta and Hammond, 2005)

Document	% of respondents
Data recovery procedures	47
Computer use and misuse policy	43
Information security policy	41
Information security procedures	33
Business continuity plan	24
Data destruction procedures	21

SMEs lack the skills, knowledge and experience that would give the understanding and necessary motivation to develop comprehensive security policies (Gupta & Hammond, 2005). With little perception of the risks, managers focus their attention to other business priorities. It is difficult to overcome the lack of knowledge as small businesses often do not have the financial resource to hire consultants to address the skills gap.

The result of these resource constraints is more evident in some areas of security policy than others. Some types of planning activities such as data destruction procedures and business continuity planning are particularly low. However, privacy is especially vulnerable if obsolete data is not destroyed effectively or during a crisis situation, where it may be deemed a lower priority than recovering the systems.

Security professionals are more aware of these needs; Keller et al. (2005) found 50 percent of the companies interviewed had an emergency action plan and a further third had begun to develop one. However, they too found the quality of the plan was variable as the plans ranged from simple back up procedures to a full disaster recovery plan including copies of working machines at another site. With the emphasis being placed on the policies and procedures for security rather than on handling the situation in the event of an incident, unforeseen problems related to the loss or inadvertent disclosure of private data could easily occur in the moment of crisis.

Security Technologies

Whilst power surge protectors and back up systems were the most used technologies (Table 2), small organizations are generally most concerned about viruses (Gupta & Hammond, 2005). So the majority seek to protect themselves through anti-virus

Table 2. Security technologies in use (adapted from Gupta & Hammond, 2005)

Technology	% of respondents
Power surge protectors	79
Data back up systems	65
Anti-virus	57
Firewalls	43
Redundant systems	35
Intrusion detection system	25
Security evaluation systems	9

software. Keller et al. (2005) found that the systems administrators were less concerned about virus attacks, with only about a quarter of their interviewees believing that viruses were a major threat. This lower concern may be because they had taken action to militate against such problems by implementing an anti-virus tool and appropriate management policies. All the systems administrators had implemented some form of firewall, two thirds of which were a hardware solution.

Employees often are considered to be a major threat, either due to malicious attack or unintentional action. Trim (2005) highlights that hacking by internal staff is a growing problem, with a suggested figure of one third of hacking incidents resulting from internal activity. Privacy of data should not though be thought of in relation to security from external attack, but by ensuring integrity of data from all forms of unauthorised access and corruption (Spinello, 2000). So, integrity of the data requires that those who have a right to access the data can do when they need it, so as to be able to process business or make appropriate decisions based on that data, for instance.

Privacy of personal data can be put at risk by poor practice or premeditated action by employees. Gupta and Hammond's (2005) respondents, however, considered insider access abuse was of least concern. Whether this is because of the higher level of trust resulting from a perceived employee commitment or due to the ignorance of the business managers is difficult to say. What is evident is that, in contrast, the system administrators regarded internal personnel as the primary threat (56 percent of respondents) (Keller et al., 2005).

So, in summary, SMEs have tended to adopt off-the-shelf security technologies in the expectation that these will suffice in the protection of their business data and therefore the privacy of their client base. This ignorance leaves them vulnerable to the release of private information through either malicious attack or poor management practice. The business implications are similarly significant whatever causes the breach of privacy and client trust.

Small businesses therefore need to reevaluate their policies and procedures, and change their security technology, to be more effective in dealing with actual security concerns (Gupta & Hammond, 2005). The absence of such policies makes organizations more vulnerable to internal or external attack, and therefore a breach of privacy.

Small businesses should take better preventative measures so that the information remains confidential, available and retains integrity. The remainder of the chapter outlines how one small business set about changing the security culture to protect its business and the privacy of its clients, highlighting the lessons that other organizations might draw from this case.

Case Study

Company Background: ABC Awards

ABC Awards is a national awarding body, accredited by the Qualifications and Curriculum Authority (QCA) to develop and offer vocational qualifications eligible for public funding. ABC was formed through a consortium of four regional awarding bodies by pooling their existing qualifications and resources in order to compete with larger companies such as Edexcel, and City and Guilds. ABC is a non-for-profit company and although it receives no public funding most of its customers are publicly funded.

ABC award qualifications across a number of fields, such as in skill-based trades like welding, hobbies such as flower arranging and art, or general life skills such as foreign languages. The development of qualifications includes liaising with subject specialists, training providers, and sector skills councils and employers to determine programmes of study that meet the UK skills needs and then writing specifications for units and qualifications. The business currently has over 500 qualifications, and at any one time up to 200 under development, reflecting the pace of change in the UK skills market.

Accredited qualifications are offered to over 1,400 colleges, universities and private training providers. The services to customers include administering the whole process from registrations to certification as well as quality assuring the delivery of learning, the provision of tutor support and specifications for coursework and exams, external assessment and moderation of candidates work and certificate production. Data sharing services also are provided to the various government departments as a condition of national accreditation status.

Within ABC, the organization records 500,000 enrolments per annum to their qualifications from candidates at the various centres of study. The required confidentiality of the data is high as the database contains sensitive personal data related to the studies (covered under the UK Data Protection Act) and company financial data related to payments for the assessments. The privacy issues relate to physical representations of the data (e.g., candidate transcripts, certificates) as well as the electronic, and with the distributed nature of the business the issues relate to securing the data in all potential locations. Privacy of candidate data was acknowledged as a strategic priority given that a small lapse could result in significant loss of business in a saturated market, where reputation is a vital component for qualification providers competing fiercely to win and retain market share.

As a non-for-profit entity with the stated objectives of contributing to the UK education system, ABC is actively involved in many partnerships including the development of new national diplomas, and various Government collaboration projects involved in reducing bureaucracy and duplication across the education sector. ABC also has in the past entered into partnerships with related private sector service providers such as authors of study guides and learning resources that can accompany its qualifications when being sold to colleges.

The four regions each have their own offices and local area network. Each regional body runs as a separate business in addition to the ABC activities. ABC operates as a stand-alone commercial entity. It is therefore necessary to maintain legally separated networks whilst providing the necessary inter-connectivity for the personnel.

The business employs approximately 50 staff members located across the four regional offices. Functions include business development, marketing, ICT systems, finance and administration, with approximately half of staff involved in administration and customer support. In addition the business has over 700 contractors involved in development and delivery. Roles include consultants, lead examiners, script markers, question authors, and visiting moderators. A small number of personnel work from home or travel extensively so need remote access.

Systems

ABC has an internal development function that recently replaced the individual legacy systems of the four member organizations. In response to the strategic need to create an enterprise-wide awards management system, a project was established to create a new software and hardware architecture, supported by appropriate information management practices. The company has deployed a wide area network capable of supporting the short term and high priority business processing requirement. The network connects the four offices to servers located in Nottingham which hosts the company's bespoke Awards Management System (AMS) used for transaction processing and document production.

Table 3. Principles adopted to ensure security of data

	Security Management Policy Development	Security Practice
Organizational Issues	Manage risks	End user education
	Total cost of ownership	Least privilege access
Technical Issues	Develop security policies	Defence in depth
	Use of external resources	Monitoring of systems

The company also has recently introduced an e-commerce Web site that takes registrations data from colleges and integrates with the AMS. ABC recently outsourced its email and collaboration systems with an externally hosted Microsoft Exchange Server.

The current systems development strategy is based on further extending the services to customers with more features available online and a staged move towards e-assessment and support for e-learning including real-time online invoicing, on-screen results entry, support for electronic portfolios and e-moderation and on-screen testing.

This chapter does not detail all of this work, but focuses on the way that privacy issues shaped the approach to security, and how security was designed into each area of the system. Our policy throughout was to ensure privacy of data by ensuring the system and organization were secure from accidental, deliberate and opportunistic attack. The security policy was based on the international information security standard for best practice (ISO17799). The practices were relevant to ABC partner companies, and capable of being implemented by most SMEs.

The approach taken can be categorised into issues focused on addressing people and organizational aspects of ensuring security, and the technical underpinning to support those needs. The following sections are organized on this basis highlighting how for each aspect the policies were formed and put into practice. Table 3 outlines the principles adopted and discussed below.

It will be shown that organizations need to understand the real risks and build security management policies on them; evaluate technological solutions and external hosting decisions on the total cost of ownership; build systems with defence in depth where the first line of defence is users who are aware of the issues; and to minimise the chance of unauthorised access by defaulting to a policy of least privilege access and monitoring the network to maintain confidence to ensure the security policy is working.

Organizational Issues: Policy and Practice

Manage Business and Security Risks

Undertaking e-business is a considerable risk: interruption of financial transactions, revealing sensitive data or intellectual property to competitors, or logistics information can be used to disrupt normal distribution operations (Shih & Wen, 2005).

Organizations need to invest in information security measures to ensure security incidents do not undermine the advantages that the technology brings, especially across e-business operations. The threat of security breaches hinder the expansion in e-business (Fulford & Doherty, 2003). New technologies increase this concern; wireless communications and mobile devices are now integral elements of the supply chain. The benefits of such technologies also are their biggest vulnerabilities: network exposure and rogue access can be achieved without need for physical access to the network infrastructure (Shih & Wen, 2005).

So, the information security professional should always assume that the systems will at some time be compromised and therefore plan appropriate defences and recovery strategies. Their key task is how to avoid, mitigate, and manage the risks that this places on the business. So, security managers need to be risk aware. Kankanhalli et al. (2003), however, found that SMEs applied fewer security deterrents than larger organizations. Yet, where greater deterrents and preventative measures were applied by organizations then greater information security effectiveness resulted. To judge the survivability of an organization's systems it is necessary to judge the level of disruption caused to essential services as a result of any incident (Redman, Warren, & Hutchinson, 2005). For system survivability it is necessary to ensure protection against threats and quick response to the effects when one occurs.

Early in the requirements engineering phase of the project, information privacy was considered as a key requirement for the system and a risk analysis was conducted in line with the recommendations of ISO17799 to determine the high priority risks that needed to be considered. Prior to this project, as with many small businesses, risk analysis was not a mature, evolving process within the business but more of an ad-hoc tool used after the event or a paper based exercise used to satisfy regulators or requirements for a continuous improvement program.

Risk analysis began by clearly understanding what information security means, ISO7799 defines information security as the preservation of information confidentially, integrity and availability. The high level system and user requirements were then considered against these categories to determine security requirements for the new system.

It is important in such analysis to ensure the risks are based on actual, rather than perceived, threats. So, previous incidents that had occurred across the business's systems over recent years were analysed before considering the planned systems and any additional risks that would result from the implementation. Previously, the perceived risk to confidentiality had been focused on unauthorized access and theft of data, and loss of data and systems through virus infection. These are not to be dismissed, but the historical analysis showed that most incidents had concerned information integrity and availability. Also upon resolution of information avail-

ability problems, an information integrity problem was common and related to the loss of availability.

Incidents affecting information integrity included corrupt database files and documents through unplanned outages and failure of UPS, data processing errors through lack of training and incorrect software functions. There had been no reports of unauthorized access or theft of data and incidents of infection by virus were minor and resolved easily by updating virus definitions and removing the virus before any real damage had been done. However, the business was aware that this risk to personal data could not be ignored as it moved towards an integrated e-business solution that would enable transactions to be processed across the regions and eventually direct by assessment centres.

Total Cost of Ownership

SMEs do not have a culture of security management and have tended to resist the need to invest in information security technologies and practices (Giannacopoulos, 2002). Indeed, Gupta and Hammond (2005) found that a variety of international surveys highlighted that nearly half of organizations stated budget considerations as the reason for poor security procedures and implementation. However, this culture is slowly changing as managers realize that even the smallest business is becoming prone to attack (Giannacopoulos, 2002).

Even where organizations are willing to invest in physical security devices such as firewalls, many small companies struggle to appreciate the return on investment for an integrated security policy. The reason for this in part is due to marketing within the IT security industry, with vendors marketing products as a single solution to security, but products can only be as good as the configurations and the configurations only as good as the policies they implement.

One way to overcome this perception is by moving to a financial model that uses total cost of ownership (TCO), or life-time cost, as the basis for making judgments. Many small businesses are not familiar with the concept of TCO and frequently make decisions based on the purchase price alone or purchase price plus some well understood maintenance costs. The broader organizational costs, such as inability to process business, loss of client trust, loss of data integrity or confidentiality, should be part of the costing model. Security threats might devastate an organization's financial position with single incidents often costing more than £30,000 (approximately US $60000) and occasionally as much as £500,000 (US $1m) (Shih & Wen, 2005). Only by being aware of these costs will managers recognize the potential savings

of their investment in an overall security infrastructure. So as well as using these broad outline costs, security managers need to estimate the cost of impact on their own enterprise and in the event of an incident calculate the actual cost as a way of evidencing the value of preventative measures.

By understanding how well the security supports the overall business objectives or the risk involved in each solution then management are able to make more informed decisions. Also, due to the high degree of coupling involved in networks and software layers there are many other costs to be considered even when simply adding a firewall. These include the cost of impact on existing systems and any reconfiguration that may need to be done, impact on future upgrades to the network, increased use of network resources, bandwidth and power, more points of failure in the network, additional insurance.

One example of the use of total cost of ownership at ABC was in the selection of firewalls. Identifying the overall cost and benefits of the various options meant assessing different combinations of firewalls. Issues considered in the decision included the level of capability of particular technologies; how selection of vendors could improve the bundled costing; whether the technology would require consultancy support due to the level of complexity; and the long-term availability support and trouble shooting. So, in terms of the costs, it was the whole solution, not just parts, that was measured, so taking into account support factors, staff costs, dependency and impact (e.g., implications for other new purchases), ongoing monitoring and support, and the risk of downtime or breach of confidentiality.

Least Privilege Access

Many security incidents are caused by user error when the user has inappropriate access to systems. In SMEs, there generally is poor user account management, for example, active user accounts for staff that have left, unrestricted remote access and local user accounts. These vulnerabilities provide easy targets for hacking or malware intrusion to go un-noticed. Policies were created whereby members of the consortium agreed to ensure that a named member of staff was accountable for account creation and deletion.

While least privilege access is an ideal to aim for, implementing it in an SME is usually very difficult as default access is usually the norm. Previously at ABC all users could do anything. In order to move from one extreme to the other, new systems being deployed can begin to follow a methodology whereby all users begin with very limited access whilst learning and training and then progress through security levels in a structured manner. Access privileges were changed in the design of the network

and the enterprise-wide awards management application. For example, application permission rules were defined based on roles such as a "centre administrator" and granting of the permissions to individuals is administered by authorized users. The advantage of this approach is that it protects staff from mistakes and unintended privacy infringement.

For the design of the application detailed task analysis during the requirements stage enabled permissions to be defined clearly prior to implementation. For each type of record being stored by the system the four basic operations (create, read, update, delete) were used to define the permissions on each area. As part of the solution, ABC recognized and considered the trade-off between the need to make the system secure but not at the expense of making the roles of the employees so difficult that they could not operate effectively.

End User Education

Earlier we noted that employees are a significant risk to the security of the business. End users pose a threat to a company both through intended and unintended actions. In addition to deliberate attack, end users also provide a risk through their actions and ignorance. It therefore is logical to assume this would be addressed through employee training and awareness. However, Keller et al. (2005) note that surveys show that training and awareness were the lowest on the list of priorities for companies. Users, though, also are your best ally in detecting problems and are therefore the first layer in the defence. They can spot problems early. To enable employees to assist in the defence of the network, managers need to share more information relating to attacks, malware, and other vulnerabilities.

A survey by Ernst and Young in 2001 (cited in Fulford & Doherty, 2003, p. 107), however, found that the dissemination of organizational security policies and knowledge to employees is a low priority. The reason for this lack of dissemination is a lack of trust in the employees. Managers perceive that there is a risk from malicious employees as well as the possibility of anyone being approached and coerced by outside agencies. Also, "managers are reluctant to share or divulge sensitive and in many cases confidential data and information. This is because unnecessary leaks can result in inappropriate publicity for the organization that has been targeted by hackers or organized crime syndicates" (Trim, 2005, p. 494).

The development of usage policies is essential to both educate staff and protect the employer. However, policies are insufficient as a vehicle for education. Direct communication of defined policies and practices to all employees is necessary to ensure they become more knowledgeable about the risks involved.

The approach used at ABC was three-fold. Firstly the organization sought to raise awareness and understanding of the issues. It then provided alternative methods that could be used to achieve the same business goals. Finally, it re-configured systems and changed some policies to make it less likely that the practice would continue.

One example issue was Internet usage. Activities such as the receipt of e-mail and downloading materials from the Internet had become a major risk. These were addressed through security policies and technology, but making users aware of the risks was essential. User training began with awareness of the issues including information on high and low probability and high and low impact Internet threats. The concept of trusted and non-trusted sources was discussed, as well as high level principles of packet filtering, firewalls, and malicious code. Next users were trained on the safe use of the Internet and e-mail, for example the opening of attachments that are not from trusted sources, browsing safe and restricted sites, and managing their own security settings after making informed decisions about the threats. Permissions were then changed on the network with administration rights being removed to reduce the potential for intrusion by spyware in the event of an intrusion occurring.

In summary the organizational issues are:

- Ensuring that risk management is core to the ongoing privacy of client data. Risk management should be based on actual rather then perceived risks, therefore historical analysis of incidents should be monitored. At ABC this identified the need to focus on data integrity and availability as well as unauthorized access.
- Security selection and justification should be based on the total cost of ownership that models in the potential cost of loss of client data privacy or integrity.
- Ensure personnel access and education policies focus on the business implications of the erosion of privacy and therefore trust. In an SME end user staff can be a vital part of the security of the system as well as a potential risk.

Technical Issues: Policy and Practice

Security Policies

As discussed above, the literature shows that small businesses are less likely to have security policies than larger businesses, and where policies do exist the quality of those policies varies significantly. Fulford and Doherty (2003, p.106) recognize

that effective information security management is "predicated on the formulation, dissemination and operation of an information security policy." They report that whilst the importance of security policies is well understood, many surveys show that there is a low level of uptake and the policies that do exist are often inadequate. Many smaller organizations focus on the technical solutions, but Trim (2005) shows that policy and technological solutions go hand-in-hand.

Changes in technological solutions should be based upon a security policy. Without a policy, security practices will be undertaken without any clear strategy, purpose or common understanding. So important is this area of management that there is now an international standard (IS0 17799) that states the principal tenants of information security management policies, such as ensuring that the policy is aligned to business objectives.

In line with the section above, a starting point to developing policy is to start with risk assessment; specifically identifying those risks and likely causes that could compromise the information systems availability, confidentiality or integrity. One survey found that organizations ranked this as the second most important factor affecting the success of information security policy, after management commitment (Fulford & Doherty, 2003).

In an SME the risk management activity also can be used to address some of the other key factors related to understanding security requirements and communicating the policy to employees. By involving the organization's management team in developing the risk assessment they are made aware of how the business objectives and priorities are related to security.

The process of developing a security policy is an educational experience for a small business, and will bring a higher level of awareness and understanding; these are

Table 4. Policies developed at ABC

Policies Developed at ABC Awards
Organizational security policy: business priorities and responsibilities; the ABC infrastructure including all significant hardware and networks from an ABC user workstation to the ABC servers and backup device; the system users and types of services that each requires; the different services and protocols that need to be supported by the systems and infrastructure. Access and permissions: the authentication and access controls required. Service level agreements: systems availability and response times; agreed minimum standards at each regional office in order to connect to the systems. End user policy: use and misuse rules Archiving: destruction of obsolete and retention of historical data Data recovery: data Back up and recovery; business continuity plans and decision protocols in the event of incidents; testing procedure Monitoring: policy for checking for activity and utilization on network and servers.

essential if the business requires the higher level skills in application that are needed to implement security measures. Implementing any security measures without an underlying policy will lead to problems in both understanding and configuration.

Policies are not fixed and should be revisited as part of the regular review and control process. Each policy should state what the review cycle is and the responsibilities for undertaking that review. The reviews at ABC are informed by current experience, business changes or future plans, and new technologies or known good practice.

External Resources

As we recognised earlier, small businesses can lack the knowledge and skills to ensure the security of their systems. There are, though, many sources of assistance available for small businesses. Some of this may come at a cost, if it is necessary to engage consultants with specific knowledge of products and systems. ABC, though, took advice from many free or relatively cheap sources by attending relevant conferences and workshops, working with a local university, and discussing options with vendors in pre-sales activity. Knowledge was developed by discussing concepts, technologies and policy decisions.

When developing procurement strategies it is important to understand the location of value in different types of products and services. For a large company the location of value in a service might be the economy of scale it provides for cost reduction whilst for a smaller company it may be the ease of implementation.

External hosting of business applications in state of the art data centres is becoming popular for companies without existing skills to manage servers and firewalls and can be cost effective when the total cost is considered. Alternatively, in-house management can be more cost effective for bespoke requirements if existing skills are available and the scalability is not too large. Both approaches can be used by selecting the functions to outsource.

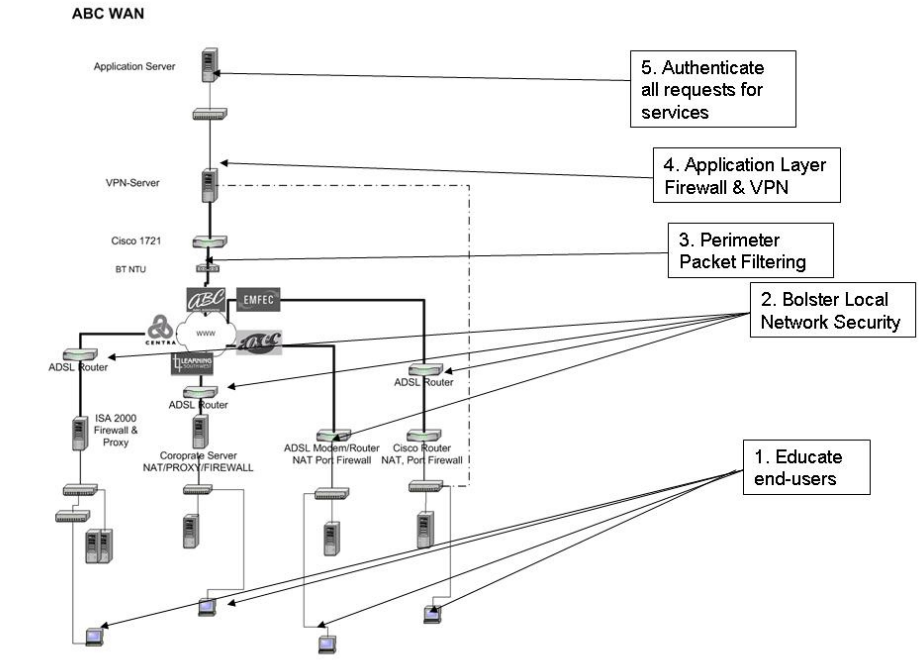
For the SME, hosting e-mail and Web site services internally are sometimes considered as a low cost option but this is based on several incorrect assumptions and lack of understanding of the TCO. There sometimes is a desire to increase utilization of existing investments in servers and this drives the decision to host on existing equipment. Many SMEs assume that if they have purchased a server and it has spare disk space then hosting e-mail services on it is beneficial as it makes use of spare capacity and reduces costs. The problem is that this approach reduces the redundancy in the server and increases the risks.

Defence in Depth

Security is an ongoing and normal concern when offices use interconnected IT systems. SMEs should define their boundaries and ensure the security on that perimeter because vulnerability at one office is capable of being exploited to allow unauthorized access to another office. Often organizations have inadequate firewall management and any physical security measures are often circumvented to suit the business and staff.

At ABC, the first objective was the deployment of an Intranet capable of supporting the short term and high priority business processing requirements for employees at each regional office. ABC used Virtual Private Network (VPN) connections between the offices. So it was decided that all communications taking place over public infrastructure (Internet) should be encrypted between the two network perimeters using industry strength IPSec. For a site to site connection this was done between the host firewall/VPN appliance and the client sites firewall. In this case the users

Figure 1. Defence in depth: Network security



are known and can be validated. The defence of the network was designed so that it was protected at different levels, as shown in Figure 1.

Due to the costs of wide area network infrastructure, users at the remote offices needed to access the system by routing requests over the public, un-trusted Internet. The systems also needed to send potentially confidential information back to users over the same un-trusted Internet. This was protected using current industry standard tunnelling and encryption protocols.

The ABC firewall was implemented in two levels, the first level for packet level inspection and the second level for application level inspection. A global access schedule was implemented on the packet level firewall so that all traffic is blocked during specific times. The ABC application level firewall was capable user level account management, thus only allowing access for authorised users. Additionally, the application server was designed to perform user level authentication. The authentication was performed transparently to avoid the user having to re-enter their username and password.

Monitoring of Systems

Misconfiguration of security devices is common in SME's due to the skills needed to translate a written security policy into a set of unambiguous firewall rules. SMEs typically invest in the security device but not the required configuration and testing. Regular monitoring and hardening of the servers and network became a normal part of the network administrator's tasks. Similarly, as the application vulnerability is more important, arguably, the application audit logs are checked, and security features are retested with new releases.

Monitoring of access logs gave confidence that the security policy was both correctly defined and implemented thereby ensuring the ongoing confidentiality of client data. This process also helped to identify areas of the policy that needed clarifying and changing. A key part of the monitoring is testing. Attempting to gain access to services that should not be allowed, and then checking the access logs, enabled areas of the company's security policy that were not implemented properly to be found.

Policies and technical solutions are not all-time solutions. They are evolving in line with business needs, perceived threats to privacy, new technologies and known good practice. In doing this monitoring it provides ongoing information to the senior management about the value of their investment, and areas that need further investment.

So in summary, the technical issues are:

- Development of a security policy that can be used to support the technological decisions so that client confidentiality, data integrity, and system availability are maintained.
- Use of appropriate external resources to help improve business resilience against the threat of a breach of privacy.
- Design the systems so that they are secured at the boundaries and at different levels thereby reducing the business vulnerability to a loss of client trust.
- Monitor the system for potential breaches of confidentiality and adjust the policies and technical solutions accordingly.

Conclusion

Whilst privacy legal obligations vary from country to country, organizations have a financial, as well as moral, motive to minimize the chance of an inadvertent release of private data. This case is a contrast to practice in many SMEs that leave many risks unmanaged and bring little benefit other than protection from well understood and low probability risks. A key lesson from this case is that privacy needs to be understood from a business perspective: a breach of client confidentiality can have a significant impact on the reputation and therefore the income of an organization. Dealing with information security as a core business issue provides greater confidence that data privacy will be maintained.

Client information security needs to be at the forefront of the design of the architecture and the applications. Too often security is considered as an add-on feature after the initial developments, and therefore it is difficult to achieve. As was shown here, security management for SMEs is required from the early stages of systems development through risk assessment and then designing solutions that can evolve over time. Focusing on it from the beginning meant the purchase and development decisions were informed by surfacing the organizational risks and priorities, as well as the technical or functional requirements, thus providing the agility to respond to business level decisions without compromising the security.

In the assessment of risk, information security managers should plan for a breach of the system not just try to minimise the threat. The risks can inform the development of a range of policies, which should be evolving documents that reflect the ongoing nature of the business and the risks it faces. Policies and business priorities should shape the selection of security solutions and decisions on external hosting, but a final solution will encompass a mixture of technologies that needs to be evaluated by looking at the total cost of ownership.

Defence in depth gives the SME the ability to implement a comprehensive security policy within a constrained budget by defining multiple areas to focus efforts. Additional benefits are that the organization can use the approach to start a process of continuous improvement. The first line of defence is a knowledgeable user. User training is a vital element of the implementation process, as a change of culture is often required in small businesses.

Further work is required at three levels to build on this case study. In the company there is need to assess the impact of the approach adopted over time to ensure the business benefits were as anticipated. In the industry, we need to recognise the way that privacy issues are potentially business critical, and apply the lessons from this case elsewhere to test if the concepts are transferable. Finally, researchers should pay more attention to information security in SMEs as these are potentially the weakest link in the e-business supply chain. In particular, further codification of knowledge from other examples of good practice should be developed that are useful for other businesses, and in due course seek a common body of knowledge for information security in SMEs.

References

Chang, S.E. & Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management and Data Systems*, *106*(3), 345-361.

Chung, C-W & Tang, M-ML (1999). Computer based information systems (CBIS) adoption in small businesses: Hong Kong experience and success factors. *Journal of Global Information Technology Management*, *2*(2), 5-22.

Department of Trade and Industry (DTI) (2006). *Information Security Breaches Survey.* Retrieved on May 17, 2006 from www.dti.gov.uk/sectors/infosec/index.html

Edgar, S.L. (2003). *Morality and machines (2nd Ed)*. Sudbury, MA: Jones and Bartlett Publishers.

Fleischer, P. & Cooper, D. (2006). EU Data privacy in practice – Microsoft's approach to compliance. *Computer Law and Security*, *22*(1), 57-67.

France, E. (2004). Data protection in a changing world. In T.W. Bynum & S. Rogerson (Eds.), *Computer ethics and professional responsibility*, pp. 263-273. Malden, MA: Blackwell Publishing.

Fulford, H. & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: An exploratory investigation. *Information Management & Computer Security*, *11*(3), 106-114.

Giannacopoulos, P. (2002). Why IT security matters for small and medium sized businesses. *New England Printer and Publisher*, *65*(3), 30-32.

Guardian Newspaper (2006). Security flaw leaves 3m HSBC online accounts open to fraud., August 10. Retrieved from http://business.guardian.co.uk/story/0,,1841853,00.html

Gupta, A. & Hammond, R. (2005). Information systems security issues and decisions for small businesses: an empirical examination. *Information Management & Computer Security*, *13*(4), 297-310.

Holmes, A. (2006). The profits in customer privacy, *CIO*, March 15. Retrieved in May 2007 from http://www.cio.com/article/19070/The_Profits_in_Customer_Privacy

Kankanhalli, A. Teo, HH., Tan, B.C.Y, & Wei, K.K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23, 139-154.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management*, Spring, 7-19.

Moor, J.H. (2004). Towards a theory of privacy in the information age. In T.W. Bynum & S. Rogerson (Eds.), *Computer ethics and professional responsibility*, pp. 249-262. Malden, MA: Blackwell Publishing.

Nissenbaum, H. (2004). Toward an approach to privacy in public: Challenges of information technology. In R.A. Spinello & H.T. Tavani (Eds.), *Readings in cyberethics (2nd Ed)*, pp. 450-461. Sudbury, MA: Jones and Bartlett Publishers.

Poindexter, J., Earp, J., & Baumer, D. (2006). An experimental economics approach toward quantifying online privacy choices. *Information Systems Frontiers*, *8*(5), 363-374.

Reece, J.C. (2007). Forget about security and privacy: Focus on trust. *CIO*, May 23. Retrieved in May 2007 from http://www.cio.com/article/112051/Forget_About_Security_and_Privacy_Focus_on_Trust

Shah, M.H. & Siddiqui, F.A. (2006). Organisational critical success factors in adoption of e-banking at the Woolwich bank. *International Journal of Information Management*, 26, 442-456.

Spinello, R. A. (2000). Information integrity. In D. Langford (Ed.), *Internet ethics*, pp. 158-180. London, UK: Macmillan Publishers

Spinello, R. A. (2006). *Cyberethics: Morality and law in cyberspace (3rd Ed.)*. Sudbury, MA: Jones and Bartlett Publishers.

Tavani, H.T. (2004). *Ethics and technology: Ethical issues in an age of information and communication technology.* Hoboken, NJ: Wiley.

Trim, P.R. J. (2005). Managing computer security issues: Preventing and limiting future threats and disasters. *Disaster Prevention and Management*, *14*(4), 493-505.