Designing Information Security for Small Businesses: Lessons from a Case Study

Dr. Terence Love

Edith Cowan University, Perth, Western Australia

ABSTRACT

This paper focuses on the different factors that impact on the design of information security for smaller businesses. A case study is used to identify issues, and costs of information attacks, preventative measures and remedial work. The paper identifies lessons for designing information security solutions for smaller businesses.

Keywords: Information Security, SME, Design, Human Factors

INTRODUCTION

Over the last five years, the use of computing and the Internet has become widely established in small businesses (NOIE, 2000, Australian Bureau of Statistics, 2001). There is increasing uptake by individuals and small businesses of online financial services such as online banking and share trading (NOIE, 2001). These changes, along with the fact that the most common computer operating systems used in small business (Windows 95/98) provide minimal data security (TheCounter.com, 2001, Schneier, 1999b, Schneier, 1999a), imply that information security issues are increasing in this sector. Resolving the information security issues of smaller businesses is important because they are the strongest growing area of the economy, they include the largest number of businesses, and their successful adoption of e-business is seen as a key factor in national economic and social development (NOIE, 2000, NOIE, 2001, Australian Bureau of Statistics, 1999, Australian Bureau of Statistics, 2001). This paper suggests, however, that currently, neither large nor small-scale information security solutions align with the realities of smaller businesses.

Information security and information warfare protection are important to all organisations. The increased role of computers and the Internet in business processes has increased the difficulty of providing information security, and increased opportunities for information warfare attacks (The SANS Institute, 2001). Traditionally, larger organisations have been earlier adopters of computers and computer networking, and have been the locus for aggregation of technical expertise in computing and networking. Together, these factors have shaped research into information security and information warfare, and the creation of information security solutions for large and small businesses (see, for example, The SANS Institute, 2001, Smith, 1997).

Computer and network information security products are, in the main, designed using a technical focus. Information security solutions designed for smaller businesses echo this preoccupation with technical issues, and as a consequence, most information security solutions for smaller businesses are "mini" versions of solutions aimed at larger organisations. For example, mini-firewalls have been developed for the small office/home office (SOHO) market, Internet browsers offer security settings, and a range of do-it-yourself file encryption solutions such as PGP are available.

This case study is aimed at identifying factors to support the design of information security solutions specific to small business through understanding the qualitative human issues and differences in the relative costs of information security problems to small and large businesses. The business owner in the

case study estimated that the cost of responding to two successful information attacks on the business' computer systems was equal to a year's profit (not including the risks or consequences from important information being illegally used to gain access to bank accounts or other assets, or act against the business). The relative cost to small businesses of responding to an information attack is proportionally bigger than for larger organisations.

OVERVIEW OF THE CASE STUDY

This case study analyses a real incident in which a computer in a small business was infected by a virus, infiltrated, and information transferred to an unknown location on the Internet. A rich picture is developed of the costs and resources associated with addressing information security at the smaller end of the business organisation spectrum. This offers the basis for identifying factors for improving the designs of information security solutions for smaller business organisations. An overview of the incident is as follows:

1. Business is protected by antiviral software.
2. A viral attack breaks through this protection.
3. This viral attack is identified (in part) and steps are taken to recover the situation.
4. It becomes clear it is possible that systems and important financial data have been severely compromised – almost certainly by a secondary attack.
5. All business processes are stopped. Steps are taken to secure the financial arrangements with other organisations.
6. Computer and information security is reviewed, and outcomes are implemented in the computer systems.
7. Computers are tested and business processes rebuilt for the business to resume using its amended computer systems.
8. Ongoing plans made for surveillance on computer behaviour and financial documentation, and research into security issues.

Each of the above stages involved time and resources, and, in some, significant risks that challenge the future viability of the business. Several stages require high levels of technical expertise. For many smaller businesses, understanding about information security protection is strongly shaped by the advertising of information security products for the SOHO market and newsagents magazines. A significant issue to emerge is management's decisions are often strongly dependent on an intuitive analysis of situations, artefacts, systems and risks. These intuitions depend on designers of computers, software and Internet systems providing sufficient clues.

CASE STUDY IN DETAIL

Setting the scene: In this business, the computers are used for financial management, document creation, and image manipulation. Like many micro businesses the organisation is acquiring small-scale e-business functionality: it has its own website, takes orders over the Internet and is an early adopter of Internet banking and share trading services. Information security precautions before the attack consisted of regular backups, good email and file hygiene, carefully chosen passwords, and anti-viral software from an international certified company. The anti-viral product was chosen because it updates from the Internet using spare bandwidth. The owner had tried other products and found that manual updating of virus signatures was often neglected. A large number of passwords were in use, and, because of this, were stored in an encrypted password database on this computer. At this stage it was not appreciated that encryption varies, and the level of encryption on this file was negligible. The business used three Windows 98/95 machines with a network printer in a small network whose structure changed frequently. Each machine acts as a backup for others (the main function of the network) with 100Mb Zip backups

stored off site. One computer was connected to the Internet (no Internet sharing). At the time of the attack, the Internet connected machine was physically disconnected from the network.

Information Warfare Attack: The attack concluded a hectic exchange of emails with another organisation. The last email contained a viral package. The message was from a trusted source. The title of the attachment was believable. The attachment was recognised as a virus because of the continuous sound of the hard drive transferring data. About two seconds after opening the attachment the power was cut and four seconds later (the APM delay) the computer shut down. It was restarted and a full virus scan undertaken. The scan showed several dozen files infected with a mix of viruses. The other organisation was notified. They confirmed they had not intentionally sent that attachment and later confirmed their machine was infected. Further investigation showed the anti-virus scanner had been reset from 'real time' to 'scheduled' (unclear whether due to the attack or due to an omission from the previous day when real time scanning was turned off temporarily to install software).

Remedial Action: The first stage in the remedial process (undertaken as part of the full scan above) was to instruct the anti-viral software to repair the infected files. This it did but leaving a small amount of doubt due to its screen messages being inconsistent. Most of the viruses were not described in the software manufacturer's virus database. An Internet search was undertaken to find out more about the viruses to understand the scale of security breach. The picture that emerged was complex: the infected email had contained many viruses each with different functionality (Trojans, bombs, backdoors).

In restoring files to bring the machine back to a pristine functional condition, the virus checker was reinstated and set to scan real time. In addition, a repeat full scan was initiated. To the owner's surprise, an even greater number of virus-infected files were identified, many different from first time round. Eventually, after using the repair function with full scan six times, all files were clear but dozens of systems files had been deleted that the anti-virus product could not repair. The computer would boot and run, but not to specification. The hard disk of the machine was reformatted and software and data were reinstalled. The backup regime meant that almost all the data was secure. The only significant loss was of two weeks of emails and appointments. The Outlook personal folder (85Mb) refused to load, and this necessitated using an archive

A this point, the concern that information security had been compromised was offset by the awareness the virus was not specifically targeted at this computer, and there was no evidence that viruses had propagated from this machine to colleagues whose addresses were stored on it. Precautionary measures included the removal of all banking information from the computer, and it was decided that for 6 months particular attention would be paid to financial documentation. It was concluded that the failure of protection against the information attack was probably due to real time virus checking being inadvertently disabled, and perhaps the heuristic virus identification process had confused sound files as infected. Details of the incident were sent to the anti-virus software manufacturers because of the failure of the software to clearly identify that it had not removed or neutralized the viruses it had found and a reply awaited.

The Second Attack: In the days following the incident, it became clear that things were not right but, at first, this was put down to paranoia. The sizes of downloads and uploads did not correlate with files being transferred; beyond differences expected from telephone line quality or poor server response. In addition, the computer did not behave in exactly the way it was expected. Suspicions increased in intensity when the machine was found dialing whilst unattended. The machine was isolated whilst further research into information security was undertaken, and again the hard drive was reformatted. Around this time, a similar failure by the same antiviral software was identified at another organisation. In this case, 'real time' scanning was fully functional: the software appeared to have failed to stop virus infestation.

Research into virus protection led to sites offering free security testing. This indicated a serious security failure due to its network configuration that allowed its drives (and those of any other machines on this network) to be viewed and manipulated remotely. This failure preceded the virus attack

Stop the Business: The business was stopped. An increased understanding of cracking software led to the realisation that that the password system and its encrypted storage was not secure. Along with other private information on the computer, this exposed the business and owners bank accounts. Banks were contacted, the situation explained, and advice sought. This process took considerably longer than expected due to lack of expertise by bank staff. The most common response was that nothing needed to be done, but that the bank was not responsible for any losses. Senior managers at banks revealed that they did not have processes for situations where customers' online security was compromised. The only secure solution was to close all online banking and other arrangements. This was done and new passwords obtained for all other accounts.

After turning off file sharing, and binding the network onto Netbeui and off Tcp/ip, file download sizes normalized and the computer no longer suffered fits of erratic behaviour.

Review Information Security: The business was restarted using manual systems and a search undertaken for a better security model. At this stage it was clear that the major risks were banking and other assets, and major costs were the time and effort needed to respond to attacks. A rough calculation indicated the costs of responding to two similar attacks per year would neutralise profit margins. Two main improvements were identified: increasing protection against attacks and reducing the cost of responding to a successful attack. The first implied some form of firewall, protection against unauthorized access to files, and a change of anti-virus software. The second implied reducing time and labour costs to restore the computer system back to good working order.

Computer Changes: The solutions identified consisted of moving to Windows 2000 (for its file security, and, more importantly, its self-repairing ability), and installing a firewall and new anti-virus software. Identifying suitable software proved problematic. All of the major software manufacturers of SOHO level firewalls and anti-virus software make similar claims: that they will provide complete protection, and are easy to set up and use. The only significant differences are in the branding image presented, e.g. 'Cheap, Cheerful and Scary', 'Serious and Responsible', 'Corporate and Mobile Professional' and 'Professional but with Shareware origins'. The preferred solutions were chosen because their manufacturer offered a web-based security test, and because of comments in magazine reviews.

Testing and Rebuilding Business Processes: Windows 2000 and new firewall and anti-viral software installed apparently without problems. The system was tested using the manufacturer's web-based security tests and the newly hardened system came out as fully secure. New business systems were developed to avoid keeping on computer any financial and asset related information that might be used to illegally gain access to businesses assets. The operational software and data was reinstalled and configured. The 'hardened' machine was brought into action on the Internet.

Ongoing Surveillance: Attention was given to unusual machine behaviour or unusual events on bank and credit card accounts.

Ongoing Research into Information Security: Resources were committed to researching computer information security through subscribing to two electronic newsletters.

ANALYSIS

At its simplest, this case study describes a small business organisation caught with inadequate information security protection at all levels. Regardless of the anti-viral protection in place, the business's computer systems were open to identification via share sniffing software. Using this technology, the information attacker had full access over the Internet to the business's hard drive shares and files as soon as the IP address was identified.

The successful virus attack was useful because it drew the business owner's attention to resolving security issues and building stronger protection.

Lesson 1: Unless the system had been obviously and successfully challenged it is unlikely improvements would have been made.

==

The case shows how the usual advice about opening attachments is problematic in small business contexts. Many organisations that a business interacts with have imperfect security systems, and small businesses frequently do business with individuals and organisations of which they know very little. An email order from an unknown customer is not an unusual event, and, accepting occasional losses is preferable to having rules that block business.

Lesson 2: Small business arrangements are often insecure because they are co-located (same machine or same insecure network) with systems and information that require high security. Minimising this co-location is important (Smith, 1997).

==

It is not sufficient to rely on manufacturer's advertising claims as shown by the failure of the original anti-viral software, and by the new firewall. After a few days, the firewall was again tested - it failed. The manufacturer's recommended firewall settings lead to a failed condition by their own security tests. Resetting the firewall ports and services is not well explained in the manual but with technical support from a colleague the firewall was again secured. Even then, the firewall failed Gibson Research (www.grc.com) security tests.

Lesson 3: Processes by which small businesses are informed about security software are often flawed because software manufacturers are one of the major sources of information, and their information provision is biased by the need for its marketing and advertising role to act in in their favour. Small businesses need to be able to identify appropriate software through ways that are more successful than present.

==

Banks and other organisations have a significant role in information security for smaller businesses. Currently, banks are trying to maximize profits by reducing transaction costs, and as part of this process are encouraging small businesses to use online banking services. The move online results in significant shifts in security issues for businesses. Physical security solutions are well established and responsibilities well-delineated and accepted. In the move online, financial institutions have effectively transferred more of the share of risks of information sharing onto small business clients because more of the technical aspects of the processing happen at the clients' end of the network. More significantly, banks have reduced their participation in resolving practical aspects of information security. Their responses to a lost

chequebook and a lost set of internet banking passwords are different (they know what to do about a lost chequebook) and do not align with the differences in potential for losses to the business (a lost chequebook is less risky to the business).

Lesson 4: Improved designs for improved information security solutions for small businesses must include improvements to financial institutions systems in the areas of rights and responsibilities.

==

For smaller businesses, such as that described above, a substantial economic effect of the information attacks was in terms of costs of recovering the systems. Proportionally, the effort, labour costs and resources needed to recover business processes back to full functionality are much higher in smaller than in larger companies. This is intrinsic: total costs of ownership are dominated by economies of scale gained through the use of standard operating environments - a situation unlikely in small businesses using a variety of computers.

Lesson 5: Designing information security solutions for smaller businesses requires a strong focus on minimizing the cost of keeping the system functioning securely. Hardware prices have reduced to the level that making a complete copy of a software environment on a hard drive (stored perhaps off site) is becoming economically practical.

==

Perhaps the most important issue to emerge in this case study is that the back door Internet access to the business' computers was discovered because of increased sensitivity to unusual events and behaviours. The realisation that security software does not guarantee information security came from detailed exploration of the literature

Lesson 6: Surveillance, research and reflection are important aspects of information security, and, hence, supporting them is an important issue in designing solutions for small businesses.

==

Some weeks after the final system was in place and functioning, it was discovered that all users had access to all files. Windows 2000 is not secure as installed. Over 300 changes are needed to secure its base configuration (Schneier, 1999a). Resetting file permissions was neither intuitive nor straightforward.

Lesson 7: In design terms, when users are told that software provides a service then it is necessary to tell them when it is not implemented - especially in relation to security.

QUANTITATIVE ISSUES

The direct costs of addressing the information attack were identified by the proprietor. The limitations of memory in these circumstances mean that the costs may understated. The proprietor's estimates are listed below:

Task	Time	Cost ($50/hr)
Identifying attack, researching virus details, redoing virus checks, reformatting computer rebuilding software and data	16 hrs	$800
Attempting to resolve problems with Outlook file	4 hrs	$200
Removing banking and other sensitive information – backing up and creating new manual system	3 hrs	$150
Move the business completely back to manual systems. Reformat the computer.	10 hrs	$500
Discussions with banks and other financial institutions	6 hrs	$300
Research into information security and security software issues	12 hrs	$600
Buying and installing new OS and information security software, rebuilding and reconfiguring system and testing	18 hrs	$900
Checking website for intrusion	3 hrs	$150
Reconfiguring firewall software	4hrs	$200
Final developments of new business system	8 hrs	$400
Resolving network issues and implementing file sharing restrictions	9 hrs	$450
New operating system software, information system software, replacement of programs that wouldn't work under Win2000, office material	(Approx)	$1100
	Total	**$5750.00**

Other costs, more significant than direct costs, include:

- Loss of business with the organisation that sent the virus laden email (and a significant loss of collaborative potential).
- Losses of efficiency from changing business and computer systems to more secure but less streamlined processes
- Losses from time business stopped trading.
- Potential future losses due to misuse of information transferred out of system.
- Costs of ongoing surveillance and information security issues research

CONCLUSIONS

Several conclusions emerge from this case study into a small business recovering from an information system attack. First, the most significant issues are non-technical, regardless of the fact that the attacks and response occur via computer subsystems that are essentially technical. These issues point to several lessons for those designing improved information security solutions for smaller businesses. Taken together, they suggest that designing improved forms of information security software or systems may be more effectively based on disciplines of ergonomics, organisational design and management systems design rather than having a purely technical focus.

REFERENCES

Australian Bureau of Statistics (1999) *Special Article - The information society and the information economy in Australia*, [Html file]. Australian Bureau of Statistics. Available: www.abs.gov.au

Australian Bureau of Statistics (2001) *Small Business in Australia Update 1999-2000 (released 30/4/2001)* (pdf file Report Number). Australian Bureau of Statistics, Canberra, Available: www.abs.gov.au.

NOIE (2000) *E-commerce beyond 2000 - Final Report*, National Office of the Information Economy, Canberra.
NOIE (2001) *The State of Play - June 2001*, National Office for the Information Economy, Canberra.
Schneier, B. (1999a) 'Back Orifice 2000', *Cryptogram*, (Aug 15, 1999)**,** pp.
Schneier, B. (1999b) 'Security Hole in IE/Outlook and Office', *Cryptogram*, (March 15, 1999)**,** pp.
Smith, D. (1997) *Improving Computer Security through Network Design*, [html file]. AUSCERT. Available: www.auscert.org.au/Information/Auscert_info/Papers/Security_Domains.html [2001, June]
The SANS Institute (2001) *How to Eliminate the Ten Most Critical Internet Security Threats - The Experts Consensus*, [html file]. The SANS Institute. Available: www.sans.org/topten,htm
TheCounter.com (2001, 1Jul01) *OS Stats*, [html file]. TheCounter.com,. Available: http://www.thecounter.com/stats/2001/July/os.html [2001, July]