2005

My problem or our problem? Exploring the use of information sharing as a component of a holistic approach to e-security in response to the growth of 'malicious targeted attacks'

Aaron Olding

Paul Turner

My Problem or Our Problem?

Exploring the use of information sharing as a component of a holistic approach to e-security in response to the growth of 'Malicious Targeted Attacks'

Aaron Olding & Paul Turner
School of Information Systems, University of Tasmania
aolding@utas.edu.au - paul.turner@utas.edu.au

Abstract

There is now a growing recognition amongst e-security specialists that the e-security environment faced by organisations is changing rapidly. This environment now sees a situation where maliciously targeted attacks are conducted by 'guns for hire' (hackers) and/or criminal organisations (Illett 2005; Keiser 2005). As a consequence, conventional organisational approaches to e-security are becoming increasingly problematic and inadequate. There is a need to raise awareness of these issues amongst organisations and to contribute to the generation of effective integrated solutions that address this emerging e-security environment without sacrificing user privacy and/or breaching user trust. This paper considers the potential role of e-security information sharing between organisations as a key element in the development of the integrated responses advocated. By examining information sharing in other areas of business it is evident that there are mechanisms that can facilitate these behaviours and generate benefits for organisations. Despite this growing evidence however, there remains reluctance amongst most organisations to engage in e-security related information sharing (Gross 2005). In examining these issues this paper considers mechanisms for generating stronger evidence on the role and effectiveness of e-security information sharing and ways of overcoming organisational reluctance to implement them.

Keywords
Electronic Security, Cyber Attack, Information Sharing, Holistic Security Approach, Malicious Intent. Cyber Environment Shift, Electronic Neighbourhood Watch.

INTRODUCTION

The evolution of the networked society continues to open up new opportunities and pose new risks for organisations using the Internet. However the risks that organisations face have changed in recent times with cyber attackers having a much more malicious intent behind their actions (Illett 2005; Keiser 2005). Attacks are no longer arbitrary but are directed and focused on achieving a specific goal be it information theft, system destruction or network denial. Organisations that have not realised and taken steps to better protect themselves are at risk of having their organisational reputation and ability to undertake business tasks severely damaged.

Certainly some organisations have already recognised the changing nature of the threats posed, and responded variously through technology, management and the law. To date however, there has been a tendency for these responses to be limited to discrete sets of technical, organisational and/or legal approaches without effectively acknowledging the inter-relationships between them (Broucek & Turner, 2001; Hannan, Frigs, Broucek & Turner, 2003). There is now growing evidence to suggest that the fragmented nature of these responses are inhibiting the development of more integrated solutions and, through unforeseen interactions amongst different socio-technical factors, are actually failing to achieve the required e-security level (Broucek & Turner, 2005). By ignoring the requirement for more holistic responses to the challenges of the new e-security environment (both within and beyond the organisational boundary) there is an increasing reduction in the overall effectiveness of the discrete solutions being developed. What is being suggested is the need for a more integrated holistic approach to security that allows organisational e-security to balance its requirement of security against those for privacy, trust and digital evidence acquisition. While this is easy to say, it is a much more difficult task to actually define how to undertake this approach.

In this context, this paper considers the potential role of e-security information sharing between organisations as a key element in the development of the integrated responses advocated. Already, both

AusCERT and the CSI/FBI highlight the importance of information sharing for improving e-security and there is also strong anecdotal evidence emerging to suggest that where it does occur between organisations e-security is improved. More broadly, by examining information sharing in other areas of business it is also evident that there are mechanisms that can facilitate these behaviours and generate benefits for organisations. Despite this growing evidence however, there remains reluctance amongst most organisations to engage in e-security related information sharing (Gross, 2005). In examining these issues this paper considers mechanisms for generating stronger evidence on the role and effectiveness of e-security information sharing and ways of overcoming organisational reluctance to implement them.

In presenting this research-in-progress paper the concept of "Electronic Neighbourhood Watch" is used to frame the examination of mechanisms being deployed to generate stronger evidence on the importance of this proactive approach to e-security. It is hoped that the research into this area will provide a greater insight into the usefulness of information sharing as a proactive approach to cyber attack prevention and be one step toward determining the look of a holistic approach to electronic security.

The Shift in the Cyber Environment

Despite the opportunities and advantages that the internet has brought to organisations, they have always had to deal with the threats that are part and parcel with the cyber environment; however the nature of those threats has changed in recent years toward a much more malicious orientation. Organisations now face threats which are more likely to severely damage the organisation causing financial loss, embarrassment and system downtime (The Daily Oakland Press 2005; Jeftovic 2005; Musil 2005; Hines 2005; Associated Press 2005). The threats that organisations are now facing include system penetration, information theft, extorsion, denial of service attacks, phishing, pharming, malware, social engineering, domain name hijacking and physical data theft. Make no mistake, the perpetrators of these actions are highly skilled groups that have discovered that their skills are in demand and they are willing to use them. According to both Miroshnikov (Illett 2005) and Gillespie (Keizer 2005), the skills of the hackers are now being offered for sale and Kaspersky Labs mentions that cyber attacks are now being heavily influenced by organised crime and the possibilities for financial gain (Kotadia 2005).

Some of the recent examples of maliciously motivated cyber attacks include:

- An employee of America On-line (AOL) sells 92 million email addresses to a spammer who runs an on-line gambling business; the addresses were then sold on to other businesses. (Oates 2005)
- The ownership of the Panix.com domain name is transferred to another unknown party and during that time users become susceptible to information theft. (Jeftovic 2005; Musil 2005)
- Scammers posing as a legitimate business manage to gain accounts with Choicepoint (an identification and accreditation company) and they used this access to gain information that has resulted in 750 cases of identity theft. (Hines 2005)
- 18 people were arrested in Israel for installing Trojan software onto the computer systems of competitors which allowed remote access and may have been used to undermine bids and steal customer data. (Associated Press 2005)

Holistic Approach to Security

This new breed of cyber threats has changed the way in which organisations need to undertake their organisational electronic security. The fortress approach being used by many organisations is becoming increasingly problematic and insufficient to adequately deal with the malicious cyber threats. This approach focuses on cyber incident prevention at the organisational boundary (Patzakis, Mann and LaBancz 2003) and the organisations that are still using this model are at serious risk of being successfully attacked. Fortunately many organisations have recognised the shift in the cyber environment and are taking steps to deal with the new threats.

While those organisations that are taking steps to better protect themselves from malicious cyber attacks should be commended, they are also facing a different set of problems with the approach they are taking. Broucek & Turner (2005) point out that the problem is with the discrete set of approaches that organisations tend to pursue in the areas of legal, organisational and technical. These approaches tend to be undertaken in isolation from each other despite the inter-relationships between them. For example an organisational policy banning the use of email for personal use will not be very effective if there are no legal procedures to monitor internet use or legal implications for such inappropriate use. It is the

fragmented nature of these discrete approaches that is inhibiting the development of more integrated solutions and that unforeseen interactions amongst a range of socio-technical (technological, organisational and legal) factors actually impairs the overall effectiveness of each approach (Broucek & Turner 2005). What is needed is an integrated holistic approach to electronic security that balances the needs for privacy, security and digital evidence in a hope to integrate all of the elements of the socio-technical approach to security together to come up with the best way in which to investigate and implement organisational electronic security solutions not just within the organisational boundary but beyond it as well. While it is easy to say that we need an integrated holistic approach to security, defining it however is another thing entirely. One element that has been identified that may play a role in a holistic approach to e-security is information sharing.

Information Sharing

There is an argument that one way to protect yourself is to protect the community that you are part of, similar in how a neighbourhood watch keeps the community safe by having its members watch out for each other. For a neighbourhood watch to work its members need to communicate and share information with each other, so that everyone is informed as to any possible risks and can take proactive steps to protect themselves. However at present organisations seem extremely reluctant to share any sort of security related information, not only with each other but government and law enforcement agencies as well. According to the 2004 Australian Computer Crime and Security Survey 75% of organisations surveyed who had experienced at least one security related incident decided not to report it to any sort of law enforcement agency, this statistic has risen from 62% in 2003 and 37% in 2002. This result is mirrored in the 2004 CSI/FBI Computer Crime and Security Survey with only 20% of organisations that had experienced a cyber incident reporting it to law enforcement.

There is some support for the importance of information sharing, as mentioned above both AusCERT and the CSI/FBI include information sharing as major components of their yearly security surveys but it is the fact that organisations already share information in other areas of their business and gain advantages from it that supports the possibility of a security approach working. For example a JIT (Just-In-Time) stock system allows savings by minimising stock levels and the costs of keeping that stock by having it delivered as needed (Johnston 1998). This stock system requires information be shared with suppliers about stock levels and usage. Information sharing is at the heart of not just this system but all electronic business undertakings. If organisations are able to gain benefits from sharing information in other areas then there is a possibility that the same can be said for sharing of security related information as well.

Information sharing is already being recommended in efforts to stop a host of security related issues, some of the examples are below:

- One of the key recommendations to combat the increase in insider abuse based electronic crime from the 2004 E-Crime Watch Survey, was to establish a formal process for reporting and sharing information in an effort to detect pre-attack behaviour (Gordon et al. 2005).
- The U.S. GAO (Government Accountability Office) has found that inadequate information sharing between states and government agencies has led to criminals and terrorist having the ability to obtain U.S. passports (Amone 2005)
- U.S. Secret Service director Ralph Basham has urged greater information sharing in a presentation given at a conference organised by the Business Software Alliance. He said that information has value and that information sharing between private organisations and law enforcement agencies needs "significant improvement" if enforcement agencies are to successfully investigate and prosecute cyber crime (Gross 2005).

One example of where information sharing is playing a role in electronic security practise is described in Sherman (2005) in the story of how two Chief Information Security Officers (and friends) regularly meet to discuss electronic security incidents, insights and solutions. When one has some information on an electronic security threat or incident that the other may find useful the details are given to them either through phone call or email. The CISO's find this relationship beneficial and are trying to foster it amongst other security people they know, they acknowledge though that it is difficult to get past the culture of secrecy that surrounds organisational security. In the same article it was noted that while e-security professionals do not share information, the cyber attackers and hackers they face do and as such a notice of vulnerability is more likely to be known by someone who is willing to exploit it then someone who is able to fix it.

While security experts may be recommending greater information sharing as a method to improve overall security, the possible negative consequences are still of concern and include the possible generation of negative publicity and fear of competitors using information against them (AusCERT 2005; Gordon et al. 2005). There have been many examples recently of organisational reluctance to inform stakeholders about an electronic security incident. One such incident was reported by Poulsen (2005) in which a hacker managed to gain access to the T-Mobile network servers and all of the sensitive information they held (inc. all customer information, images from cell phone users and unclassified US Secret Service documentation and communications). Despite knowing about the intrusion (and required by law in California) the company did not inform their customers of the breech until US Secret Service investigations began months later.

The Electronic Neighbourhood Watch

The main driving force behind this paper is the belief that information sharing assists in e-security activities by allowing stakeholders (organisations, governments, law enforcement agencies, customers, etc.) to be better informed about the threats that they face. This knowledge allows a proactive approach to e-security that is more efficient, better directed and overall less costly to implement while better protecting the organisation from a new breed of cyber threat (Illett 2005; Keizer 2005; Kotadia 2005).

The purpose of this research is to generate greater evidence on the importance of information sharing in organisational security practise with a focus on how it can be applied to a holistic electronic security approach. The possible benefits that an organisation can derive plus the barriers to its successful implementation will also be a major component of the research.

What is being envisioned for this research is an information sharing concept that is being called the electronic neighbourhood watch (ENW). From the concept level the ENW is a proactive approach to e-security that is a way in which information sharing and cooperation between organisations, governments and law enforcement agencies can be promoted and undertaken successfully following the same basic model as a traditional neighbourhood watch.

At this early stage the approach that is being put forth to examine information sharing will focus on how it is undertaken successfully in other organisational areas most specifically in the areas of electronic commerce. The idea is that since organisations are more willing to undertake information sharing in the e-commerce/e-business area, by examining the advantages, barriers and driving factors behind them we can determine how these factors apply to e-security information sharing and whether it is a valid security concept.

CONCLUSION

The cyber landscape in which organisations now operate has always been a wild and unpredictable place but in many ways it was like the frontier, dangerous but filled with enough opportunities to make the effort worthwhile. However, as cyberspace has become more populated the nature of the threats that organisations face has changed and the environment is now more threatening and malicious than ever. As the motivations and technical skill of those looking for vulnerabilities has grown, so too has the focus from the criminal element that have seen the possibilities for profit by exploiting these vulnerabilities and are more than willing to develop the resources required to do so. Due to this shift, organisations now need to change the way they deal with cyber threats, moving away from a fortress mentality to one in which a holistic approach to security is used. The intention of this research is to determine the role of information sharing in organisational electronic security practise in the context of an holistic approach. There will be a focus on inter-organisational sharing as a proactive approach to incident prevention.

The head of the U.S. Secret Service has said “An intrusion for one represents a collective threat for us all” in response to the need for greater information sharing and cooperation in dealing with cyber based threats (Gross 2005) yet it remains to be seen if information sharing will play a part in improving e-security. While there is anecdotal evidence that information sharing plays an important role in security, what sort of benefits, if any, can be expected? Does it play a role in a proactive approach? What barriers are present that are restricting e–security information flows? And (if advantageous) how can we best implement information sharing into the electronic security processes that organisations already undertake? These are but some of the questions that need to be answered and it is hoped that by doing so a better, more holistic, approach to e-security protection can be promoted for the benefit for all stakeholders.

Aaron Olding would like to acknowledge ICS for their continuing support of the research that is being undertaken. http://www.icsmultimedia.com.au/

REFERENCES

Arnone, M. (2005). "GAO: Don't Give Criminals Passports." Federal Computer Week. http://www.fcw.com/artilce89461-07-05-05-web, Accessed: 7 July 2005.

Associated Press. (2005). “Israel Charges 18 with Industrial Espionage.” Security Pipeline. http://www.securitypipeline.com/163702148, Accessed: 2 June 2005.

AusCert (2005). AusCERT Computer Crime & Security Survey 2004, Australian Computer Emergency Response Team**:** 43.

Broucek, V & Turner, P. (2001). “Forensic Computing: Developing a Conceptual Approach for an Emerging Academic Discipline.” In H. Armstrong (Ed.), 5th Australian Security Symposium (pp. 55-68). Perth, Australia: School of Computer and Information Sciences, Faculty of Communications, Health and Science, Edith Cowen University, Western Australia.

Broucek, V. & T., P (2005). 'Riding Furiously in All Directions' - Implications of Uncoordinated Technical, Organiational and Legal Responses to Illegal or Inappropriate On-line Behaviours.” EICAR 2005.

Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R. (2005). 2004 CSI/FBI Computer Crime and Security Survey, Computer Security Institute**:** 17.

Gross, G. (2005). "Secret Service Heads Call for Cybersecurity Cooperation." Computerworld. http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,101820,00.html, Accessed: 21 May 2005.

Hannan, M., Frigs, S., Broucek, V., & Turner, P. (2003). Forensic Computing Theory & Practice: Towards Developing a Methodology for a Standard Approach to Computer Misuse. In S. A. Knight (Ed.), 1st Australian Computer, Network & Information Forensics Conference. Perth, WA, Australia.

Hines, M., (2005). "ChoicePoint Data Theft Widens to 145,000 People," CNET News.com. http://news.com.com/ChoicePoint+data+theft+widens+to+145%2C000+people/2100-1029_3-5582144.html, Accessed: 21 February 2005.

Ilett, D. (2005), “Russian Hackers ‘The Best in the World’”, ZDNet Australia. http://www.zdnet.com.au/news/security/0,2000061744,39187427,00.htm, Accessed: 9 April 2005.

Jeftovic, M., (2005). "Hijacking of Panix.com: A Call for An Emergency Rollback Procedure," CircleID. http://www.circleid.com/article/896_0_1_0_C, Accessed: 18 January 2005.

Johnston, R. B. (1998). Trading Systems and Electronic Commerce. Eruditions Publishing, Emerald, VIC, Australia.

Keizer, G. (2005). "Hackers Write Spyware for Cash, Not Fame." Security Pipeline. http://www.securitypipeline.com/shared/article/printablePipelineArticle.jhtml?articleId=160500232, Accessed: 6 April 2005.

Kotadia, M. (2005). Virus Authors Choosing to Infect Fewer Computers. ZDNet Australia.

http://www.zdnet.com.au/news/security/0,2000061744,39193414,00.htm, Accessed: 27 May 2005.

Musil, S., (2005). "ISP Suffers Apparant Domain Name Hijacking," CNET News.com.

http://news.com.com/ISP+suffers+apparent+domain+hijacking/2100-1025_3-5538227.html, Accessed: 18 January 2005.

Oates, J., (2005). "AOL man pleads guilty to selling 92m email addies," The Register. http://www.theregister.co.uk/2005/02/07/aol_email_theft/, Accessed: 9 February 2005.

Patzakis, J. M., Scott; and LaBancz, Melisa, (2003). "Computer Forensics in the Global Enterprise," 1st Australian Computer, Network & Information Forensics Conference.

Poulsen, K., (2005). "Hacker Penetrates T-Mobile Systems," Security Focus. http://www.securityfocus.com/news/10271, Accessed: 13 January 2005.

Sherman, E. (2005). "Peer-to-Peer." Information Security. http://informationsecurity.techtarget.com/magItem/1,291266,sid42_gci1042652_login,00.htmlAccessed: 12 May 2005.

The Daily Oakland Press, (2005). "Southfield Teenager Accused in Computer Attacks," The Daily Oakland Press. http://www.theoaklandpress.com/stories/031905/loc_20050319015.shtml, Accessed: 22 March 2005.

COPYRIGHT