Edition 2003-16

SIFT Notes

In this issue…

These Security Intelligence Notes are issued fortnightly by SIFT - a boutique Australian information security consulting company - looking at the regulation of information, and the implications for industry. SIFT combines a knowledge of security with understanding of individual industries' regulatory & business requirements.

The Internet Industry Association provides this research as a service to its members in the interest of developing awareness and understanding of regulatory and risk issues in information security.

Subscribe to SIFT Intelligence at www.sift.com.au.

internet industry association

a SIFT Information Control Publication

THE ECONOMIC CONSEQUENCES OF SHARING SECURITY INFORMATION

Earlier this year, SIFT issued a note highlighting research suggesting that companies that share security-related information make less attractive targets to hackers. Further research is now available on the the costs and benefits to companies that participate in such information sharing. This note provides a summary of the paper *"The Ecnomic Consequences of Sharing Security Information"*, by Ester Gal-Or and Anindya Ghose.

Gal-Or E & Ghose A, The Economic Consequences of Sharing Security Information, http://www.cpppe.umd.edu/rhsmith3/papers/Final_session7_galor.ghose.pdf

The US federal government has encouraged the formation of Information Sharing & Analysis Centers (ISACs) with the goal of helping to protect critical infrastructure assets that are largely owned and operated by the private sector, in industries such as banking and finance, chemicals, telecommunications, oil & gas, and electricity. Focusing on these Centers, the article investigates the competitive implications of sharing information about security breaches and investments in technology which promote security.

Security measures and correct implementation of security technologies have never been more important than in today's economic climate. Companies with poor online security measures have experienced negative effects not only in regards to online sales, but similarly with offline sales as customers shift to competitors with a higher "perceived" security.

For a while now, it has been recognised that a key factor required to improve information security is the gathering, analysis and sharing of information related to successful and unsuccessful attempts at computer security breaches. Shared information of information system vulnerabilities, threats, incidents, best security practices and solutions amongst member groups provides an impetus for continuos improvement in security standing. However, revealing details of information security breaches entails both costs and benefits for the disclosing firm.

Firms revealing information regarding security breaches in a public forum can suffer losses through loss of market share or stock market value from negative publicity. Private and listed companies can be reluctant to release information about attacks and vulnerabilities for fear of regulatory breach. Additionally, companies are reluctant to share information if there is a risk of the breach notification itself being compromised – Sun Microsystems was subject to criticism when hackers intercepted documents from CERT detailing a flaw in a software package.

However, as suggested in our original SIFT Note article, there are also good reasons for sharing security incident information. The most obvious benefit of such sharing is the improved preparedness against further attacks and fraud, and secondary benefits can arise from increased sales due to a better security reputation and goodwill amongst consumers. For trust-based industries such as financial services, this can be crucial. Additionally, by reporting security breaches, a firm can send a strong message to its customers that the company takes information security seriously, providing a strong branding message. Such actions can boost consumer comfort level while dealing with such firms, in terms of alleviating their "perceived security risk".

An example of this comfort is provided by research suggesting that the customers of organisations in the IT-ISAC have greater confidence in their

vendor's security products due to their information sharing behaviour. Flow on impacts include an increase in the overall confidence in stopping or apprehending cyber criminals, leading in trun to greater demand for IT security products. Information security investments and sharing of security information can thus result in positive outcomes for the industry as a whole.

Industry benefits can accrue when increased trust in dealing with a particular firm online also expands the overall market size within the industry. A number of industries have experienced positive demand shocks by successful attempts at cross selling and up selling as a consequence of mitigating consumers' fears of privacy and information security related issues. An example of this is Amazon.com's efforts in protecting the integrity of consumer data, supporting the growth of this market.

Overall, information sharing is still in its infancy. However, done correctly, it will enhance the security of organisations and broader "national information infrastrcutres," bringing us closer to the fabled "Culture of Security".

Key Research Findings

- A higher level of security breach information sharing by one firm leads to a higher level of security breach information sharing by another firm and to a higher level of security technology investment by the other firm.

- As the number of substitutes within an industry increases, the level of information sharing and amount of security technology investment by firms in that industry increase. That is, the more competitive an industry is, the more likely it is to share.

- In direct correlation to the finding above, the more duopolistic an industry is, the lower the optimal amount of security breach information shared and investment in security will be.**

  *[** SIFT Note: This point is of particular note given the duopolistic nature of many of Australia's major industries. Such a research finding suggests that within a small market where only a few key players can operate successfully, information sharing of security incidents is unlikely]*

- If an increase in investment does not lead to greater demand for the industry's goods it discourages a higher level of information sharing.

- Security breach information sharing and security technology investment levels increase with firm size and industry size.

    - Sharing information is more valuable to larger firms and in bigger industries. However, larger firms are not a measure of size outright, but rather in comparison to other firms within the industry.

    - This may be because larger firms may assign a higher value to such information because the marginal cost-benefit ratio of sharing information is higher for them.

ASEAN & CSCAP STRESS IMPORTANCE OF E-SECURITY

The Association of South East Asian Nations (ASEAN) announced in late September plans to share information on computer security next year and create a regional cyber-crime unit by 2005. Each country would form a Computer Emergency Response Team (CERT) to provide timely sharing of information on viruses, worms and hackers. The teams would also work collaboratively to both identify and respond to new forms of cyber crime. It is planned that by next year a framework will be in place to share information so that all parties involved will receive early warning information and can take action accordingly.

While at this stage we are yet to see the effectiveness of such a model, the proposal has impacts on the enire region as such agreements help to tie the countries of ASEAN closer as they work towards creating a single economic space. As we move closer to greater ASEAN economic integration, it will be essential to achieve harmonisation of key information security policies, laws, and approaches. Currently, ASEAN have five key contractual agreements with China, Japan, India, Australia, New Zealand and the United States which when complete will merge the ASEAN economies to become a single market of 500 million people.

With these key contractual agreements, it is hoped that the best practices of cyber crime fighting can be implemented across geographic boundaries. Countries like India are helping to lead the fight against cyber crime and cyber criminals by opening up "virtual police stations" in Bangalore from as early as 2000. More recently, China has made agreements with ASEAN to jointly combat non-traditional security problems such as cyber crime, stemming from Free Trade discussions between the two economic bodies.

The Draft report from the 13th meeting of the Council for Security Cooperation in the Asia-Pacific (CSCAP) Working Group on Transnational Crime in Manila also highlighted the sharing of intelligence and the harmonisation of legal systems as ways in which the region could forge stronger ties both economically and as a stance against cyber crime.

CSCAP (2003) Draft Report on the 13th Meeting of the CSCAP Working Group on Transnational Crime Manila, 26-28 June 2003 URL http://www.cscap.org/documents/13%20TNC%20DRAFT%20REPORT.doc Date Accessed [20/10/03]

BBC News (2000) India tackles Cyber Crime, BBC World URL http://news.bbc.co.uk/1/hi/world/south_asia/847727.stm Date Accessed [20/10/03]

Kazmin, Amy (2002) Beijing looks to bring Neighbours Under its Wing, Financial Times URL http://www.globalpolicy.org/globaliz/econ/2002/1105asean.htm Date Accessed [20/10/03]

SANS INSTITUTE UPDATES TOP 20 VULNERABILITIES

This list highlights the 10 most commonly exploited vulnerabilities on Windows and Unix systems over the last year. Whilst there are thousands of attacks on systems each year, the ones listed below are the target of the majority of successful attacks.

The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus, version 4.0, 8 October 2003, http://www.sans.org/top20/

Top Vulnerabilities to Windows Systems

- W1 Internet Information Services (IIS)
- W2 Microsoft SQL Server (MSSQL)
- W3 Windows Authentication
- W4 Internet Explorer (IE)
- W5 Windows Remote Access Services
- W6 Microsoft Data Access Components (MDAC)
- W7 Windows Scripting Host (WSH)
- W8 Microsoft Outlook / Outlook Express
- W9 Windows Peer to Peer File Sharing (P2P)
- W10 Simple Network Management Protocol (SNMP)

Top Vulnerabilities to UNIX Systems

- BIND Domain Name System
- Remote Procedure Calls (RPC)
- Apache Web Server
- General UNIX Authentication Accounts with No Passwords or Weak Passwords
- Clear Text Services
- Sendmail
- Simple Network Management Protocol (SNMP)
- Secure Shell (SSH)
- Misconfiguration of Enterprise Services NIS/NFS
- Open Secure Sockets Layer (SSL)

Each vulnerability is listed along with remedial step-by-step instructions at the Sans Top 20 website. It is imperative that organisations guard against these vulnerabilities to ensure that “reasonable steps” are taken towards protecting from known vulnerabilities.

SIFT NEWS & UPDATES

Training: Introduction to Encryption & PKI

Canberra: 24-25 November 2003

Introduction to Encryption & Public Key Infrastructure has been developed by SIFT in conjunction with Aspect Education Services, and in consultation with the National Office for the Information Economy (NOIE). The course provides a vendor and solution neutral view of PKI, presenting a realistic and thorough examination of the topic as well as identifying risks, unanswered questions, and future directions.

Full course outline available online, at
http://www.sift.com.au/downloads/SIFT_Aspect_PKI_Outline.pdf

Training: Information Security – Tactical Information Control (ISTIC)

Sydney: 3-5 December 2003

Information Security: Tactical Information Control (ISTIC) has been developed by SIFT in conjunction with Aspect Education Services. Developed in line with Australian and International standards including ACSI 33 and ISO 17799, this course addresses business, technology, and regulatory aspects of information security.

Full course outline available online, at
http://www.sift.com.au/downloads/SIFT_Aspect_ISTIC_Outline.pdf

For further information or other locations/dates, contact Nick Ellsmore (nick.ellsmore@sift.com.au).

RECENT SIFT NOTE CONTENTS

SIFT Note 2003-15 (12 October 03)

- Cybercrime Tracking or Making Cyber-Spying Legal?
- Security ROI: Round Peg, Square Hole
- Australia Takes the Fight to Spam

SIFT Note 2003-14 (3 September 03)

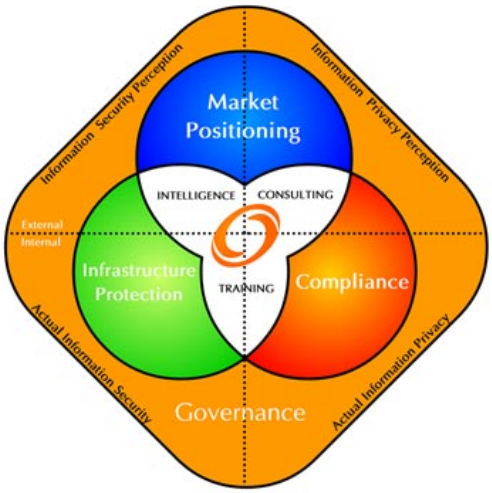
- Security Reponse: A Critical Component of BCP
- Draft Cybercrime Code & Law Meet Resistance
- Australian Government to see Windows Source Code

SIFT Note 2003-13 (8 August 03)

- Data Protection Laws Stifle Research
- Developments in Infrastructure Security: US & AUS
- MMS Technology Creates More Headaches

All SIFT research is archived at the SIFT website: *www.sift.com.au*

ABOUT SIFT



SIFT is a boutique Australian information control consulting company that provides tactical and operational support for information control and governance programs, within highly regulated corporate environments.

SIFT takes a tactical approach to information control: **concrete, specific, and measured steps, providing tangible information assurance**. Security you can understand.

Leveraging our unique perspective of information security issues in the Australian context, SIFT offers its clients a range of services:

Consulting

- Penetration Testing
- Information Security Governance, Compliance & Reporting
- Board & Executive Level Support
- Security Reviews, Audits and Benchmarking
- Privacy Strategy & Audit
- Risk Assessment

Intelligence

- Policy & Procedure Development & Review
- Policy Outsourcing
- Information Availability & Aggregation Reviews
- Product & Vendor Reviews/Recommendations
- Custom Research Reports

Training

- Introduction to Encryption & PKI
- Information Security: Tactical Information Control
- Industry Based & Custom Training Progams

Contact Us

SIFT Pty Limited
Level 67, MLC Centre
Martin Place
Sydney NSW 2000

P: (02) 9236 7276
F: (02) 9236 7271
E: info@sift.com.au
W: www.sift.com.au

ABOUT THE INTERNET INDUSTRY ASSOCIATION

The Internet Industry Association is Australia's national Internet industry organisation. On behalf of its members, the IIA provides policy input to government and advocacy on a range of business and regulatory issues, to promote laws and initiatives which enhance access, equity, reliability and growth of the medium within Australia.

SIFT Notes

Subscribe: www.sift.com.au or
Email: subscribe@sift.com.au
Publisher: SIFT Pty Ltd

ABN: 42 094 359 743
Level 67 MLC Centre
Martin Place
Sydney NSW 2000
Australia

t: +61 2 9236 7276
f: +61 2 9236 7271