Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2009

Improving an organisations existing information technology policy to increase security

Shane Talbot
Edith Cowan University

Andrew Woodward
Edith Cowan University

Originally published in the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2021
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/18

Improving an organisations existing information technology policy to increase security

Shane Talbot & Andrew Woodward
Secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University

Abstract

A security policy which includes the appropriate phases of implementation, enforcement, auditing and review is vital to protecting an organisations information security. This paper examined the information security policy of a government organisation in response to a number of perceived shortcomings. The specific issues identified relating to the organisations security policy as a result of this investigation were as follows: a culture of ignoring policies, minimal awareness of policies, minimal policy enforcement, policy updating and review ad hoc at best, policy framework, lengthy policy development and approval process, no compliance program, no formal non-compliance reporting and an apparent inconsistent enforcement across the whole of the organisation. In response to these identified issues, the following recommendations were made to improve the information security of the organisation: changing the organisations culture, creating an awareness mechanism for policies, improving the organisations culture, create an ICT policy awareness programme, review and re-write existing policies, policy enforcement, policy compliance, policy non-compliance reporting, policy updating and review, improve the policy development and approval process, policy compliance checking and uniform policy enforcement. Whilst it is also likely that a lack of governance contributed to these issues, this aspect was not addressed in this paper. It is hoped that timely implementation of the remedies presented here will increase the organisations information security.

Keywords

Information security, security policy, user awareness, governance

INTRODUCTION

There can be little argument that policy should be creating a secure environment in an organisation (Hone & Eloff, 2002; von Solms, 2001). The reason that ICT security policies exist is to document the organisations information security requirements, to explain to employees their responsibilities for protecting information resources, and the reasons for secure communications (Dancho, 2003). ICT security policies are critical to the organisation protecting its information assets, reducing risk, enabling regulatory and industry compliance and protecting the privacy of employees and the organisations information. (Bacik, 2008) Improving the existing ICT security policies will only increase the effectiveness of the existing policies.

Security driven by technology rather than policy is an inadequate means of protecting information, and will likely not be in line with the business aims of the organisation. In addition to creating useful, appropriate policy, it is also important that the personnel that are subject to the policy are aware of its existence. Failing to make users aware of a policy can lead to a decrease in security through user behaviour that does not comply with the policy, be in intentional or not (D'Arcy, Hovav & Galletta, 2009).

This research examined the security polices, their implementation and user awareness of a particular organisation as a result of a number of perceived shortcomings. The organisation in question is a state/ territory government and encompasses over 16 agencies and sub-agencies, which due to exigent circumstances cannot be specifically named here. The security team with support of management developed and published an ICT security governance framework. This has been used as a guide to instigate changes to the existing policies for the ICT Security Governance Section. However, a number of issues being raised by other sections within the organisation are yet to be investigated. The existing ICT security policies and their implementation have been viewed unfavourably by many sections within the organisation. Over time the number of issues with the policies has escalated and the ICT Security Team is being made aware of more and more every day.

Many of the issues already raised directly related to the policy documents and their impact the on ICT security for the organisation. The investigation and paper intends to identify as many issues as possible in relation to the policy documents, their implementation, and other issues within the organisation which impacts the effectiveness of the policy

implementation (Zeltser, 2009). This paper will explain why identified issues should be of concern, how they affect the organisation, and make recommendations to improve the current implementation.

PROCEDURE

Investigation and research
The initial investigation into the existing situation involved the reviewing of the existing processes and documents. Included in the investigation was the consulting of employees to determine organisational awareness and attitudes. The research into the documented issues involved consultation with the ITSA, security colleges, publications, and the Internet.

Consultation
The initial consultation phase of this paper involved relevant sections within the department. Primary purpose was to inform them of the activity and request any input that they felt might be of assistance. Included in this were the Information Technology Security Advisor (ITSA) for the organisation and the Department's Policy Office.

Employees were consulted to identify issues not directly related to the format and content of the policies. These included attitudes of employees towards ICT Security policies and policy awareness.
On completion of the investigation and the results being documented the ITSA and Policy Office were informed of the findings and what the issues are which had been identified with the existing ICT security policy implementation. All agreed with the findings.

The draft of the final document including the list of issues, solutions, recommendations, justification, and implementation plan for improving the policy implementation was then presented to the managers of the Policy Office and the ICT Security Team. This final stage of consultation was to ensure that management had no other issues or recommendations for the paper. The issues identified were accepted and the associated solutions and recommendations endorsed.

Collating findings and investigation results
The Security Team had been made aware of a number of issues prior to the commencement of this paper and these had been documented. The result of the investigation undertaken for this paper into the existing implementation issues was also documented and the two documents combined to form the list of issues.

The following investigations were documented:

- Possible solutions to address the issues
- Possible impact the issues have to the organisation and justification for recommended solutions
- A suitable implementation plan for recommendations

These documents then formed the basis for the associated sections within the final paper.

IDENTIFIED ISSUES WITH ICT SECURITY POLICIES

The investigation into the existing ICT security policy implementation identified a number of issues. These have been combined with those already identified by sections within the organisation and are presented here. The issues presented are not limited to the policy documents themselves, but include issues which impact policy effectiveness and the ICT security of the organisation. They have been summarised in the following list, with further information relating to each finding presented below:

- A culture of ignoring policies
- Minimal awareness of policies
- Minimal policy enforcement
- Policy updating and review adhoc at best
- Policy framework
- Lengthy policy development and approval process
- No compliance program
- No formal non-compliance reporting
- Apparent inconsistent enforcement across the whole of the organisation

A culture of ignoring policies
The history and how the organization has dealt with policies have resulted in a culture within the organisation in which employees ignore policies which they do not wish to comply with. This is major hurdle which needs to overcome before any policy implementation can be effective. Currently a number of information security policies are scoffed at when they are ready for implementation.

Comments such as "who cares about the policy – you can't enforce it" and "no one cares about policies because they're crap" are common place within the organization.

The existing view of many within the organisation is that policies are only in place as a means of disciplining employees or hindering development and operational advancement.

Minimal awareness of policies
The Policy Office has created an Intranet site as an advisory for all within the organisation. Policies are listed with associated links to download the relevant policy document.

Awareness of relevant policies is next to non-existent. A walk around of the major ICT building within the organisation highlighted this issue. Employees were asked what ICT security policies they were aware of. Most could only sight the "Acceptable Use Policy". It is assumed that this is only because it is mandatory for employees on induction to sign that they have read and understood the document.

Awareness of the overarching Security Policy for the organisation was minimal. This policy was approved only two years ago and within the last six months a flyer had been produced and handed out to all employees.
A number employees questioned also added that since joining the organisation they have not had a refresher on this policy. The policy had a major re-write in the last year which has since been approved and published.
The most widely known ICT security policy, the "Acceptable Use Policy" simply addresses awareness with a statement pointing out that it is the manager's role to ensure that personnel are made aware of all relevant ICT security policies.

Consultation with the Policy Office on the awareness issue resulted in a proposal to make the sponsor or owner of any new policy responsible for making all relevant employees aware of its existence.

Minimal policy enforcement
The department is responsible for providing ICT resources to the whole of the organisation. The operational side of this seems appears to have taken precedence. Policies, especially information security related policies, have often been ignored if they might impact quick and simple implementation of ICT services. After this has occurred the department then continues this practice by using the original example as a precedent.

Raising policy breaches with management has often resulted in claims that the policy cannot be enforced; or the policy should be re-written. Most policy breaches or non-compliance related issues in which an investigation or action undertaken are in relation to blatant breaches of the Acceptable Use Policy. At times this has also appeared to be ad hoc and not enforced uniformly across the whole of the organisation.

Policy updating and review ad hoc at best
The Policy Office was recently established and one of their initial tasks was to re-write all ICT policies using the new organisation's policy template. Many policies which had up until this date remained in draft where now approved.

The content of these policies however were not reviewed in depth before all the policies where published. Since then a number of policies including the ICT Security Policy has not been updated and their contents reviewed. A number of these policies were originally written by the now disbanded IMB nearly 10 years ago and their usefulness is almost non-existent for the current organisation.

Policy framework
The ICT Security Governance Section was tasked soon after it was established to assist in the creation of the ICT security governance framework. This framework was endorsed by the ICT Security Manager and it was approved by the organisation's management shortly afterwards.

Within the framework was outlined the ICT security policy architecture for the whole of the organisation. The document also identifies sections of ICT security in which policies need to be in place. A number of these policies are in existence, many requiring major re-writes and some need to be developed.
A number of these policies are currently in draft and some have entered the approval process.

Lengthy policy development and approval process
Currently on average it takes a year for an organisational wide policy to go from the initial brief to being approved and published. The process involves a lengthy consultation process which is necessary, however a number of mandatory endorsement stages tie up the approval process for months.

Currently it is a requirement that policies once endorsed by middle management have to return to the same committee at a later stage to ensure that the supporting brief for the policy (for the upper management committee submission) is also endorsed.

The middle management committee only sits once a month with an agenda which is published well in advance. Once a policy is endorsed the subsequent associated brief if it misses the schedule for the next meeting results in a two month delay.

The upper management committee is only held once every two months. ICT related issues have only been allocated a 15 minute window for discussion. Consequently ICT policy related matters are often not heard or delayed until the next committee meeting.

No Compliance Program
Compliance checking within the organisation has not been implemented. Compliance reporting and metrics are not produced and made available to relevant levels of management.

There is no reviewing of compliance to determine if the security controls and policies employed are effective and being used correctly.

No formal non-compliance reporting
The reporting of policy breaches and non-compliance in a formal, published and recognisable process does not exist. Employees are not aware of what their responsibilities, how they should report issues, and who to report them to. Consequently many issues are not referred to the appropriate areas and ICT Security Team was often not involved.

Numerous issues have eventually come to the attention of ICT Security Team long after the event and long after any action should or could have been taken.

Apparent inconsistent enforcement across the whole of the organisation
A number of examples exist within the organisation where employees are aware of colleagues being dismissed for activities which appear to breach the acceptable use policy. However, similar cases involving management have only resulted in minor disciplinary warnings.

This apparent ad-hoc and non-consistent enforcement may have also contributed to the existing culture of the organisation in which most policies are not viewed positively.

RECOMMENDED IMPROVEMENTS TO THE CURRENT ICT SECURITY POLICY IMPLEMENTATION

The identified issues with the ICT security policy implementation is affecting the effectiveness of the policies and the ICT security which the implementation was intended to provide.

Improving the policy implementation by addressing these issues identified should not only create a greater acceptance of ICT security within the organisation but result in the production of better policies, provide management documentation on how the security measures are performing, and also enhance the existing implementation to be more aligned with the organisation's ICT security business requirements.

Changing the organisations culture
The organisation has to change the existing culture of ignoring policies or viewing them solely as a means of dismissing personnel to a more positive one.

The organisation should educate employees on ICT security policies and ICT security matters using a well developed and formal process. This process of educating and awareness should be carried out uniformly across the whole organisation. All presentation and handouts developed within this process should be published and made available to all employees.

Creating an awareness mechanism for policies
The Intranet site whilst an instrument for access to policies is not an effective way of ensuring awareness. Nor is a statement in a high level policy informing managers that it is their responsibility. Awareness is to include a means to confirm that personnel have been made aware of IT security policies.

An automated system whereby personnel are made aware of all relevant policies and when policies have been changed also assists with the refreshing of policies.

An e-learning package which uses the organisations network and domain authentication is a possible solution. Employees on logging into the network would before gaining access to network resources first be checked by the e-learning package for relevant policies for their role, when they last read the policies and when they are due to confirm that they have been aware or refreshed their knowledge of the policies.

Another solution to assist with the awareness is the utilisation of the work centre periodic meeting. The inclusion of ICT security policy awareness within this activity ensures that employees are made aware, but having in undertaken in a less formal way and if structured along a "micro-training" format should provide a valuable tool with minimal expense.

Improving the organisations culture
The sole purpose of policies is not to empower the organisation with a means of dismissing employees; however this is the perception that a large number of employees have. Critical to the success of ICT security is the changing of beliefs, attributes, and behaviour of the employees and the organisation to that which aligns with the business and it requirements (Didier, 2008). An education programme would assist the ICT Security Team in achieving this for the organisation. ICT security policy personal should adopt a less judgmental, more objective mentality to communicating and enforcing ICT security policies and this will improve the impact of information security policies and programs (Didier, 2008). Changing the existing beliefs and attitude towards ICT security policies to a more positive one should also be beneficial when it comes to policy awareness and other supporting documents supported by the policies i.e. standards and procedures.

Create an ICT policy awareness programme
The Intranet site, whilst an instrument for access to policies, is not an effective way of ensuring awareness. Nor is a statement in a high level policy informing managers that it is their responsibility. The best security policy is ineffectual if employees ignore it, or are unaware of its existence. The key to success is education and all employees should be made aware of the ICT security policies and the compliance process the organisation has implemented (Heathcote, 2003).

Without an effective awareness programme any employee who is disciplined because of a policy breach or non-compliance could have a case against the organisation (Chuvakin, 2008). An employee who is dismissal for a breach of a policy in which it can be determined that they were unaware of the policy has a case for unfair dismissal (Just Relations, 2009). The outcome of such a case could include compensation and costs which in some cases has exceeded $500,000.

Awareness of policies needs to be established, as without it an employee can claim unawareness of the policy and the organisation will have no way of proving otherwise. Without proof of awareness a dismissed employee could have a case for unfair or wrongful dismissal. Policies also need to be understood by employees, and the organisation needs to show that they have done everything possible to ensure employees have read and understood the obligations of the policies. If not a dismissed employee may have a case against their dismissal (HR Report, 2006).

Review and re-write existing policies
Reasons to update the policies include deployment of new technology, decommissioning of old software or hardware, or the introduction of new or updated regulatory requirements. In theory any changes to the organisation which the security policies are in place to protect should result in a review or re-write. Not reviewing and updating can result in the organisation not addressing risks to their information resources (Chuvakin, 2008). The ICT security governance framework which the ICT Security Team developed and has been approved by management should be used as a guide in this activity.

The entire ICT security policy suite should be reviewed and maintained regularly. An automated system of review scheduling with timely alerts will assist however the policies should also be reviewed or amended when a significant change to the existing practices occurs. A number of policies have not been amended with the result that they are no longer enforceable.

Policies should be written so that they are clear and concise as ambiguity and doubt can result in the policy being ignored or un-enforceable (Chuvakin, 2008).

Before they are submitted for approval, policies should also be reviewed by the appropriate areas to ensure that the policy subject matter is correct, and that they can be implemented. This should eliminate any possibility that the policies are open for interpretation and in some cases the enforcement could lead to legal action.
All ICT security policies are to be re-written to include explicitly the maximum consequence of no-compliance or breaching the policy. Failure to include this in the policies may result in a claim of unfair dismissal. (NSW IR, 2009)

A final review of the policy should be undertaken by the organisations legal department to ensure that the policy is enforceable and not open to legal interpretation.

Policy enforcement
Policies should be enforced uniformly across the whole of the organisation. Whilst it is the task of the ICT Security Team to investigate and report on ICT security policy non-compliance it is the role of HR Department to enforce the policies.

Policies which are not enforced uniformly become ineffectual. Any of the policies which are then used to dismiss an employee due to non-compliance exposes the organisation to an unfair dismissal claim (Giardini, 2003; Hughes, 2007).

Policy compliance
The ICT security policy suite will become irrelevant, unenforceable, and possible legally useless if the organisation does not implement a means of tracking if the policies are being followed (Ungerman, 2005; Chuvakin, 2008).

Compliance checking and reporting not only is a tool to identify when there is non-compliance but also is a reporting tool for management to show that the security measures in place have been implemented and adhered to.

Policy non-compliance reporting
A formal process should be established for the reporting of non-compliance of ICT security policies. Investigation reports should be detailed a containing such information as the alleged non-compliance event, the resultant impact on other employees or the organisation, whether any previous warnings have occurred, and the maximum severity of the non-compliance. Failure to document this information may result in the organisation making disciplinary decisions based on insufficient information leaving them open to possible legal action. (VTA HR update, 2006).

Policy updating and review
The existing practices need to be improved to ensure that the policies are maintained and reviewed appropriately. An automated system of review scheduling with timely alerts will assist however the policies should also be reviewed or amended when a significant change to the existing practices occurs.

Policies before they are submitted for approval should also be reviewed by the appropriate areas to ensure that the policies can be implemented and are concise.

Improve the policy development and approval process
The process for development and approval of policies needs to be reviewed and refined to ensure that policies can be developed and implemented efficiently and a more timely manner.

The requirement to obtain endorsement for the supporting policy brief to upper management is unnecessary and its removal would reduce the time taken from endorsement to approval.

Policy compliance checking
Policy compliance checking and reporting should be established as soon as possible. A procedure for reporting of non-compliance related matters should also be developed and implemented.

Uniform policy enforcement
The organisation should ensure that policies are enforced uniformly across the whole of the organisation to ensure that the observed inconstancies in implementation and enforcement are addressed.

A PLAN FOR IMPLEMENTING RECOMMENDED ICT SECURITY POLICY IMPROVEMENTS

Detailed below is a number of action items which if introduced should address the issues presented in this document and improve the organisations ICT security policy implementation. In a few cases a number of the recommended improvements can be addressed by the same action item. These identified remedies can be summarised as follows:

- Create an ICT security education programme

- Create an ICT security policy awareness program
- Review and re-write existing policies
- Improve Policy enforcement

Create an ICT security education programme
The ICT Security Team should develop an education programme for the organisation. The programme should include but not be limited to what ICT security is, the benefits to the organisation and employees, the roles and responsibilities of all within the organisation, who the ICT Security Team is, what the ICT Security Team does, identify ICT security policies and associated documents.

Create an ICT security policy awareness programme
The ICT Security Team should draft a business case for the organisations management. This business case should outline the options recommended by ICT security for the ICT security policy awareness implementation they being an e-learning package or the introduction of policy awareness in team meetings. Depending on the management decision a formal programme should then be developed and implemented throughout the whole of the organisation.

Review and re-write existing policies
At the earliest opportunity the ICT security policy suite should be reviewed and re-written where appropriate. If it is determined that there is deficiencies in the suite new policies should be drafted as soon as possible. The ICT security governance framework which has management approval and endorsement should be used as a guide for this activity. When undertaking the review, re-write and creation of policies it may require dedicated resources to be allocated to this task such as personnel. The ICT Security Manager should be advised if this is perceived to be the case.

Improve policy enforcement
The ICT Security Team should as part of the ICT security policy process advice HR of the requirements for uniformly enforcing policies and to be mindful that the current perception within the organisation is that HR are not enforcing policies uniformly across the entire organisation.

Establish policy compliance checking and reporting
An ICT security policy compliance mechanism should be requested from management. A business case should be drafted and sent to management.

Establish non-compliance reporting
A procedure should be developed and implemented for the reporting of ICT security policy non-compliance related matters for the whole of the organisation. The ICT Security Team should as part of this process be made aware of the details of the issue and authorised to investigate.

The procedure should include a number of documents which should be published and employees are to be made aware of their existence and how to access them.

The ICT Security Team should then report the issue and the findings to not only the area in which the non-compliance occurred but also to management. This more than likely will take the form of an investigation report but also be included in the weekly ICT security metrics which is presented to the General Manager.

Introduce auditing
The organisation should utilize the existing internal audit team to audit the ICT security policy implementation. Included in the audits can be the process for refreshing policy awareness, current state and correctness of the policy suite, compliance checking, and non- compliance reporting.

Simplify and streamline the policy development and approval process
The process for development and approval of policies needs to be reviewed and refined to ensure that policies can be developed and implemented efficiently and a more timely manner.

The current process results in an average timeline of twelve months from policy development brief to policy publication. A number of stages in the approval process require documents to be tabled at management meetings that only sit every two to three months. At some of these meetings ICT is only allocated a few minutes which results in policy issues being only given a fraction of that if any at all.

The process needs to be refined so that policies can be drafted and approved in a more timely fashion. It is recommended that management at all levels of endorsement and approval agree on a process which is specifically for policy matters and not a subset of other issues such as ICT or planning. This may result in an out-of-session type of consultation however if management approve this new process then policies can be developed and published much more quickly.

CONCLUSION

The organisation has an ICT security policy implementation that has evolved over some time, and the present management requested the ICT Security Team investigate and identify areas for improvement. The investigation into the current ICT security policy implementation has resulted in a number of recommendations, as have been presented in this paper. These recommendations for the ICT security policy implementation will not only improve the policies but also the security of the organisations information and supporting infrastructure.

The reviewing and re-writing of a number of existing policies, along with the possible creation of a number of new policies is a priority. A number of issues highlighted will be addressed by this, including reducing avenues for legal dispute when policies are enforced and the alignment of the policy suite with the current business security requirements. The creation and deployment of an education programme throughout the organisation will assist in creating a culture which is supportive and understanding of ICT security. The acceptance of ICT security policies should also reduce the number of security related incidents. The creation and implementation of compliance checking and monitoring will not only detect and report on non-compliance but also enable security to provide metrics to management, and issues of non-compliance can now be addressed instead of going unnoticed. The metric reports enable management to determine how the organisation is travelling in regards to the policies and security requirements of the organisation.

Whilst this work has identified remedies for the policies and their implementation, which was required as a matter of urgency, what needs to be examined in further work are the governance issues which lead to these issues arising in the first instance. If these governance issues are not addressed, then there is the very real risk of such policy issues occurring again in the future. Such a reoccurrence would similarly leave the information security of the organisation exposed, and insecure.

REFERENCES

Bacik, S. (2008). *Building an Effective Information Security Policy Architecture.* CRC Press, Taylor & Francis Group. Boca Raton, FL, USA.

Chuvakin, A. (2008). *Five basic mistakes of Security Policy.* Retrieved October 3, 2009, from http://www.computerworld.com/s/article/9065202/Five_basic_mistakes_of_security_policy

Dancho, D. (2003). *Building and Implementing a Successful Information Security Policy.* Retrieved October 10, 2009, from http://www.windowsecurity.com/pages/security-policy.pdf

D'Arcy, J, Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* **20(1):** pp79-98

Didier , D.I. (2008). *Improving Information Security with Social Psychology.* Retrieved October 10, 2009, from *h*ttp://www.netsecureia.com/whitepapers/Improving%20Information%20Security%20with%20Social%20Psychology.htm

Giardini. (2003). *Nd549 – Decision.* Retrieved October 10, 2009, from http://www.great.greattab.nsw.gov.au/pdfs/GREAT/nd549.pdf

Heathcote, P.M. (2003). *A2 ICT.* Gutenburg Press Limited, Malta.

Hone, K. & Eloff, J.H.P. (2002). Information security policy — what do international information security standards say? *Computers and Security* **21(5):** pp402-409

HR Report. (2006). *Policy sign-off needs more than click of a mouse.* Retrieved September 26, 2009, from http://srac.com.au/hra.htm

Hughes, S. (2007). *Latest Unfair dismissal, harassment, discrimination and termination cases.* Retrieved October 6, 2009, from http://www.thymac.com.au/files/pdf/Latest%20Employment%20Law%20Cases.pdf

Hunter, B. (2000). *Information Security: Raising Awareness.* Retrieved October 14, 2009, from http://www.iwar.org.uk/comsec/resources/canada-ia/infosecawareness.htm

Just Relations. (2009). *FAQ.* Retrieved October 10, 2009, from http://justrelations.com/j15/index.php?option=com_content&view=article&id=50&itemid-56

NSW IR. (2009). *Avoiding Unfair Dismissal.* Retrieved October 6, 2009, from http://www.industrialrelations.nsw.gov.au/Employers/Dismissing_staff/Unfair_dismissal/Avoiding_unfair_dismissal.html

Sapphire. (2008). *Policy Awareness – Why?.* Retrieved September 19, 2009, from www.sapphire.net/technical_consultancy/policy_why.html

Von Solms, B. (2001). Information Security – a multidimensional discipline. *Computers and Security* **20(6):** pp504-508

VTA HR update. (2006). *Recent tribunal decisions of interest.* Retrieved October 12, 2009, from http://www.vta.vic.edu.au/docs/News/HR%20Update%2011%20Aug%2006.pdf

Ungerman, M. (2005). *Creating and Enforcing an Effective Information Security Policy.* Retrieved October 14, 2009, from http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=28014

Zeltser, L. (2009). *How to suck at Information Security*. Retrieved October 15, 2009 from http://isc.sans.org/diary.html?storyid=5644

COPYRIGHT

Shane Talbot & Andrew Woodward ©2009. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors