International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 2 –NOVEMBER 2014.

Improving an Organisations Existing Information Technology Policy to Increase Security

*1Shamim and #2Bharathi Devi Patnala

*HoD, Dept of M.Sc(CS),KBN PG College, Vijayawada
#HoD, Dept of MCA, KBN PG College, Vijayawada
[1]shamimkarima@yahoo.co.in
[2]bharathipatnala@gmail.com

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 noncompliance 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

I. INTRODUCTION

There can be little argument that policy should be creating a secure environment in an organisation. 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. 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. 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 being 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.

This research examined the security polices, their implementation and user awareness of a particular organisation as result of a number of perceived shortcomings. 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. This paper will explain why identified issues should be of concern, how they affect the organisation, and make recommendations to improve the current implementation.

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.

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

II. 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

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.

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.

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 hocand 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.

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 ata 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 apolicy is endorsed the subsequent associated brief if it misses the schedule for the next meeting results in a two monthdelay.

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

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 anyaction 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 foractivities which appear to breach the acceptable use policy. However, similar cases involving management have onlyresulted in minor disciplinary warnings.This apparent ad-hoc and non-consistent enforcement may have also contributed to the existing culture of theorganisation in which most policies are not viewed positively.

III. RECOMMENDED IMPROVEMENTSTO THE CURRENT ICT SECURITY POLICYIMPLEMENTATION

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

Improving the policy implementation by addressing these issues identified should not only create a greater acceptance ofICT security within the organisation but result in the production of better policies, provide management documentationon how the security measures are performing, and also enhance the existing implementation to be more aligned with theorganisation'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 dismissingpersonnel to a more positive one.

The organisation should educate employees on ICT security policies and ICT security matters using a well developed andformal 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 astatement in a high level policy informing managers that it is their responsibility. Awareness is to include a means toconfirm 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 changedalso 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 eLearningpackage for relevant policies for their role, when they last read the policies and when they are due to confirmthat 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 ICTsecurity policy awareness within this activity ensures that employees are made aware, but having in undertaken in a lessformal 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 isthe perception that a large number of employees haveAn education programme would assist the ICT Security Team in achieving this for the organisation. ICTsecurity policy personal should adopt a less judgmental, more objective mentality to communicating and enforcing ICTsecurity policies and this will improve the impact of information security policies and programs . Changingthe existing beliefs and attitude towards ICT security policies to a more positive one should also be beneficial when itcomes 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 astatement in a high level policy informing managers that it is their responsibility. The best security policy is ineffectual ifemployees ignore it, or are unaware of its existence. The key to success is education and all employees should be madeaware of the ICT security policies and the compliance process the organisation has implemented.

Awareness of policies needs to be established, as without it an employee can claim unawareness of the policy and theorganisation will have no way of proving otherwise. Without proof of awareness a dismissed employee could have acase 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 thepolicies. If not a dismissed employee may have a case against their dismissal. Result in the policy being ignoredor un-enforceable.

Before they are submitted for approval, policies should also be reviewed by the appropriate areas to ensure that the policysubject matter is correct, and that they can be implemented. This should eliminate any possibility that the policies areopen 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 orbreaching the policy. Failure to include this in the policies may result in a claim of unfair dismissal.

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

IV. 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 butnot be limited to what ICT security is, the benefits to the organisation and employees, the roles and responsibilities of allwithin the organisation, who the ICT Security Team is, what the ICT Security Team does, identify ICT security policies

and associated documents.

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 isdetermined that there is deficiencies in the suite new policies should be drafted as soon as possible. The ICT securitygovernance framework which has management approval and endorsement should be used as a guide for this activity.

Improve policy enforcement

The ICT Security Team should as part of the ICT security policy process advice HR of the requirements for uniformlyenforcing policies and to be mindful that the current perception within the organisation is that HR are not enforcingpolicies 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 draftedand sent to management.

Establish non-compliance reporting

A procedure should be developed and implemented for the reporting of ICT security policy non-compliance relatedmatters for the whole of the organisation. The ICT Security Team should as part of this process be made aware of thedetails 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 oftheir 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-complianceoccurred but also to management. This more than likely will take the form of an investigation report but also be includedin 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 everytwo to three months. At some of these meetings ICT is only allocated a few minutes which results in policy issues beingonly given a fraction of that if any at all.

V. 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..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 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 noncompliance 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.

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.

VI. REFERENCES

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

[2] 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

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

[4] .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

[5] Didier , D.I. (2008). Improving Information Security with Social Psychology. Retrieved October 10, 2009, from http://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

[6] .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