A study of the uptake of Information Security Policies by small and medium sized businesses in Wales

Anthony Burns[1]; Anthony Davies[2]; Paul Beynon Davies[3]
1 Mr, eCommerce Innovation centre, burnsaw@ecommerce.ac.uk
[2] Prof, eCommerce Innovation centre, daviesaj14@ecommerce.ac.uk
[3] Prof, eCommerce Innovation centre, beynon-daviesp@ecommerce.ac.uk

Abstract — **Over the last few years the risks that threaten Internet connected computer systems and the business critical information stored on them have been widely publicised. To address these threats many companies have implemented security measures, to protect themselves.**

Current research indicates that use of an information security policy alongside the actual implemented security measures can greatly minimise such threats. However implementation of such a policy can be expensive and not feasible for Small businesses.

This paper presents a study of Small businesses in South Wales that use a mixture of Internet connected standalone computers and Local Areas Networks (LANs). It looks at the security measures they have in place and whether or not they have an information security policy. Findings show that most Small Medium sized businesses do not have such a policy document, but many are using components that would normally form part of such policy, within their staff employment manuals. This is a much cheaper and less time consuming way of using the more important and relevant components that usually make up such a policy.

Keywords — **Information Security Policy, Internet Usage Policies, eMail Use Policies, Password Policies and employment manual and staff manuals**

I. INTRODUCTION

An Information Security Policy is a document that is used to provide direction and support for a company's information security in accordance with a business's requirements and relevant laws and regulations [1]. In addition, it covers a series of rules, guidelines and policies that staff must abide by in order that security measures already implemented are as effective as they can be.

The main purpose of such a policy is to inform users, staff and managers of their obligatory requirements to protect technology and information assets. The policy should

specify the mechanisms through which these requirements are to be met.

Current research indicates that use of a formally defined and documented Information Security Policy alongside a company's or organisation's actual implemented security measures can greatly minimise potential security threats [2]. Unfortunately, many Small businesses fail to implement such a policy and so suffer the consequences of a security breach brought about by these threats. Often companies could have avoided such breaches if they had an Information Security Policy document in place.

Research conducted by the Department of Trade and Industry (DTI) showed that only 34% of Small businesses (1-49 employees) and 45% of Medium sizes businesses (50-249 employees) in the UK had a formulated, defined and documented Information Security policy [3].

In Wales, Small Medium sized Enterprises (SMEs), made up more than 99% of all businesses [4] in 2005. SMEs are defined as companies with less than 250 employees and less than €50 turnover. These provide approximately 60% of all private sector employment and more than 40% of turnover [5]. Increasing Information and Communications Technology (ICT) and electronic commerce (eCommerce) use by SMEs in Wales is expected to be an important driver of economic growth and productivity of these companies.

Research conducted by the DTI in 1999 revealed that Wales had the lowest use of Web sites and eMail in the UK [6]. This led to the creation of the Opportunity Wales (OW) programme in 2000 to address this problem. The purpose of this programme has been to help Welsh SMEs

increase their use of eCommerce and in turn help Welsh businesses catch up with their UK counterparts.

More recent statistics also reveal Welsh SMEs having a lower usage of the Internet and associated eCommerce activities than the UK average. Research conducted by OW [7] showed that Small and Medium sized companies in Wales generally had a lower uptake of Internet access when compared to the UK average [8] as shown in Table 1 taken from the ONS (Office of National Statistics) study. It is interesting to note that the average uptake of Internet access by Micro sized companies of 1-9 employees (Micros) was actually higher in Wales than the UK.

Table 1 Comparison of Welsh and UK SMES with Internet access

SME size	ONS 2004 UK [8]	OW 2006 Wales [7]
Micro (1-9 employees)	61.6%	66.1%
Small (10-49 employees)	82.6%	72.4%
Medium (50-249 employees)	97.3%	71.4%

By comparing the DTI's "Business In The Information Age International Benchmarking Study 2004 " [9] report figures for SMEs in the UK with a Web site, against figures for Wales gleaned from the State of the Nation Report 2005/2006" [7] report, it can be seen that less Welsh SMEs have a Web site than those on average in the UK [Table 2].

Table 2 Comparison of Welsh and UK SMEs with a Web site

SME size	DTI 2004 UK [9]	OW 2006 Wales [7]
Micro (1-9 employees)	51%	57%
Small (10-49 employees)	77%	68.4%
Medium (50-249 employees)	89%	72.7%

The comparison of UK and Welsh studies showed that SMEs in Wales have a lower use of eCommerce than the rest of the UK. Those that do use eCommerce need to have good security policies in place to help protect their Internet connected IT systems from the risks that threaten them. Due to Welsh SMEs having a lower use of eCommerce compared to the UK average it has been assumed that Welsh SMEs would also be less inclined to use such policies.

Companies not using such policies are less well protected leaving their IT systems more at risk to security breaches. Examples of security breaches include viruses, hackers and staff misuse. This increases the likelihood of IT systems facing down time which, in effect, threatens their day-to-day eCommerce capability.

In 2004 the DTI produced UK average figures showing the numbers of Small and Medium sized businesses that have Information Security policy documents [3]. Unfortunately the results were not split into regional areas and hence no figures exist for Wales.

Extensive searches were conducted across the Internet for reports, conference papers and journal papers, detailing the numbers of Welsh SMEs with a formal Information Security Policy document. Unfortunately, it was not possible to determine any figures detailing this information. Hence, one of the main objectives of this study has been to find out these figures and also to find out what barriers might be preventing businesses developing such policy documents.

II. Research Method

The main goal of the study was to investigate whether Welsh businesses are adopting Information Security Policy documents at a slower rate than other regions of the UK. The study also aimed to find out to what extent Welsh SMEs were using Information Security Policy documents or alternatives. The study also looked into how Welsh SMEs were implementing the various IT usage policy components usually found in Information Security Policy documents.

Research was conducted by contacting 500 SMEs residing in Wales. Details of suitable SMEs were supplied by OW.

To answer the question of whether Welsh SMEs were less likely to have an Information Security Policy document than those on average in the UK, we used figures attained from the DTI Information security breaches survey 2004 to acquire the UK statistics and carried out a two staged survey for the Welsh statistics.

For the purpose of this research into how Welsh businesses are using Information Security Policy documents, our survey examined only one category, defined as a SME. However, unfortunately, the DTI's UK figures were split up into two categories of Small and Medium sized businesses in order to make a comparative study a weighted average of the two DTI categories was determined. This weighted average was then used to compare the results with the proposed Welsh average from the proposed study.

To determine the content and prevalence of Information Security Policy document usage amongst Welsh SMEs the study was broken into two phases:

Phase one
A total of 30 companies were initially selected from the list of 500 SMEs supplied by OW. In March 2006 a letter requesting an interview was sent to each, followed up by a telephone call requesting an interview. A total of fifteen SMEs agreed to be interviewed at their own premises, conducted using a preset questionnaire. Phase one was conducted as a pilot study. The questions asked concentrated on finding out the security measures that the SMEs had in place and whether or not they were using Information Policies and their components.

Phase two
Based on the answers given by SMEs in the pilot phase, a more detailed questionnaire was devised. This questionnaire used more specific questions than previously used in phase one as it was now known to what extent Welsh SMEs were using an Information Security Policy.

The resulting questionnaire was then used to carry out the research for phase two by means of a self administered postal survey to the remaining 470 SMEs in July 2006. The main aim of the survey was to gain a much larger sample of answers from SMEs across Wales and their usage Information Security Policies.

The survey enquired whether the companies used traditional constituents of an Information Security Policy e.g. an Internet usage policy, and whether these were documented within an Information Security Policy, an Employee/Staff manual or some other source, and whether these also contained specific user responsibilities. It also enquired about barriers that might be holding them back from formulating these constituent policies and how these policies were enforced if they did use them.

III. RESULTS

The data from phase two of the research was analysed in August 2006. The response rate to the postal survey sent out to 470 OW clients was 15.5%. The respondents were a mix of sole traders, Micro, Small and Medium sized companies representing a broad spectrum of all industry sectors from tourism to manufacturing.

The results, as were predicted, show that Welsh SMEs do indeed lag behind the rest of the UK in terms of using Information Security Policy documents. The weighted average of the DTI survey conducted in 2004 for Small and Medium companies in the UK with an Information Security Policy document was 34.1%. The comparable Welsh SME figure from phase two study was considerably lower at 5.5% as shown in Table 3.

IT usage policies are component policies that usually form the contents of an Information Security Policy document. Our results show that a large proportion of Welsh SMEs do not actually have any IT usage policies (53.4%) and those that do, favour documenting them within a staff/employee manual (12.3%) rather than an Information Security Policy document (5.5%) [Table 3].

The phase one pilot research also found that those SMEs that documented their IT usage policies used them as part of an Employee/staff manual much more frequently than they did in a full Information Security Policy document.

Table 3 How Welsh SMEs document their IT usage policies

Response	% of Businesses
Have an Information Security Policy document	5.5%
Staff/Employee Manual	12.3%
Other	2.7%
Not documented	35.7%
Do not use any IT usage policies	53.4%

Just under half the SMEs that responded to the survey stated that they used IT usage polices to help protect their IT systems from security breaches 46.6% [Table 4].

Table 4 Welsh SMEs that use the sort of IT usage policies that are likely to form part of an Information Security Policy document

Response	% of Businesses
Use constituents	46.6%
Do not use constituents	53.4%

Research results show that 64.7% of Welsh SMEs that use IT usage policies within their businesses do not have these documented in any way [Table 5]. The most usual way of documenting these policies appears to be within a Staff/Employee manual (29.4 %) with only 11.7% keeping them within an Information Security Policy document [Table 5]. Many of the companies who did not document the IT usage policies that they use within the company stated that their staff are made aware of the policies orally via management and colleagues.

Table 5 How companies using IT usage policies usually found in an Information Security Policy document keep a record of them.

Response	% of businesses
Information Security Policy document	11.7%
Staff/Employee manual	29.4%
Other	5.9%
Not documented	64.7%

The most popular IT usage policy used by Welsh SMEs are Password policies. It was found that 79.4% have a Password policy [Table 6]. It is encouraging to see that so many Welsh SMEs are taking on board the importance of a Password policy, as passwords are the computer system's front line defence against being breached by an intruder. This is why it is important to have a Password policy that specifies that staff use adequately secure Passwords.

Other popular policies used by Welsh SMEs are for Computer equipment usage (52.9%), eMail usage (50%)

and Internet usage (50%) [Table 6]. Rather worryingly though are the low numbers of companies using Instant Messaging policies, especially in recent times when virus writers, hackers and phishing scammers have targeted users of these services.

More than 15% of respondents stipulated that they used other sorts of policies within their companies. These included:

- Data protection policies;
- Equal opportunities policies;
- Environmental policies;
- Staff sickness policies;
- Disciplinary policies;
- Grievance policies;
- Fire safety policies;
- Health and safety policies.

Table 6 Constituent IT usage policies usually found in an Information Security Policy that Welsh SMEs are using

Response	% of businesses using IT usage policies
eMail usage policy	50%
Internet usage policy	50%
Instant Messaging usage policy	20.5%
Password policy	79.4%
Intellectual property rights policy	32.3%
Computer equipment usage policy	52.9%
Other	15.2%

Results for the survey question asking how SMEs make staff to adhere to their IT usage policies, were gathered in our survey through an open question. In this qualitative data gathering exercise respondents were requested to give their own answers rather than choose from a selection of pre-written answers.

Research results show that the most popular ways for Welsh SMEs to enforce their IT usage policies on their staff is through staff training (38.2%) and trust (38.2%) [Table 7].

Table 7 How SMEs get staff to adhere to their IT usage policies

Response	% of businesses
Surveillance	8.8%
Supervision	8.8%
Staff Training	38.2%
Trust	38.2%
No answer	17.6%

Over 25% of respondents said that as they were a sole trader they had no need for an Information Security Policy document or IT usage policies. The main reason for this is because they had no staff on which to enforce such policies. [Table 8].

Many SMEs also thought that such policies were not needed within their businesses because they were too small (2.6%) or were family run (10.3%) [Table 8]. Many family-run businesses may feel they do not need to use IT usage policies as they expect family members to be trustworthy. It is not always about trustworthiness; it is often about staff having the knowledge to know how to use Internet connected computer systems in such a way that they avoid making the possibility of computer breaches more likely. That is why it is still important to have some IT usage policies in place even if you do not enforce them. The same applies to the 2.6% of respondents that thought their businesses were too small to warrant using IT usage policies.

Just over one fifth of respondents put the barriers down to a lack of time (20.5%) but only 2.6% cost [Table 8].

One respondent to our survey who did not have an Information Security Policy or any IT usage policies documented quoted the following:

"If we were sent a standard small business policy document we would probably adopt it but have not time to sit and think something like this through at present."

Table 8 Barriers stopping Welsh SME developing an Information Security Policy document or IT usage policies that normally form constituents of such a policy document.

Response	% of businesses
Family run	10.3%
Business too small	2.6%
Lack of time knowledge	20.5%
Sole trader	25.6%
Cost	2.6%
No business benefit	7.7%
No answer	25.6%
No need	13%

Half of SMEs [9] that took part in the survey who were using either an Information Security Policy document or Employee/staff manual had incorporated compliance within employee contracts.

Table 9 SMEs using an Information Security Policy document and/or a staff manual that have incorporated compliance to these within employee's job descriptions within their contracts.

Response	% of businesses
Yes	50%
No	50%

Half the businesses using Information Security Policy documents or staff/employee manuals include some user responsibilities within these documents. Examples of these responsibilities provided by SMEs taking part in the survey include:

- "To backup data once a month this will change to once a day from 1st of September and for Anti-virus software to be updated every four weeks;"
- "The need for vigilance in all aspects of Internet use;"
- "Backup and Security awareness;"

- "Varies depending on the role of the Person in the organization;"
- "Responsibility for downloads, content. Virus and backup protection;"
- "General rules on Running of Anti-virus and Spyware software."

Table 10 SMEs that include user responsibilities in their Information Security Policy document or staff manual.

Response	% of businesses
Yes	50%
No	50%

IV. Discussion

Internet, eMail and computer equipment usage policies all serve the purpose of providing guidelines to company employees on their acceptable and unacceptable usages. If followed, these policies should reduce the likelihood of users falling foul of eCrime e.g. hackers, virus writers, phishing scammers etc. who target users of Internet connected computers. Encouragingly, 50% [Table 4] or more of SMEs in Wales that have IT usage policies actually implement them. This figure needs to be increased over time as they can help play an important part in protecting a company's Internet connected IT systems from the sort of security threats just stated above. One would certainly recommend that SMEs do take the time to develop these policies.

Instant messaging service users are often the target of attack through malicious code and phishing scams, making it important that companies make sure their staff use these services in a way which minimises the potential of security breaches. A good way to do this is by developing an Instant Messaging Policy for staff to follow, outlining how they can and cannot use such services on company computer systems. Unfortunately, as our results show, only 20.5% [Table 4] of Welsh SMEs that use IT usage policies within their businesses have one for Instant messaging services.

Many of the SMES taking part in the survey said that the biggest barriers to them developing and using IT usage policies were "Lack of time and knowledge." One company even stated "If we were sent a standard Small business policy document we would probably adopt it but have no time to sit and think something like this through at present." In addition to this and the known importance well written IT usage policies can play within a business as part of an Information Security Policy document or a Staff/Employee manual. It looks like these barriers could easily be removed by SMEs being provided with advice on how to draw up such policies, maybe using a template detailing the likely contents for policies. Thus, allowing them to draw up their own policies and use them in either an Information Security Policy document or as seems more the case in Wales a Staff/Employee manual.

In fact "Business eye" do provide free advice and templates to businesses in the Wales area on such matters to enable SMEs to develop such policies so such barriers should not have less of an impact. More likely it is a lack of knowledge of how important such policies can be to businesses which prevents these businesses developing them

Some of the businesses that took part in our survey said the biggest barrier to them developing IT usage policies was a lack of perceived benefit [Table 6]. However, if they looked at the cost of developing such policies within an Employee/Staff manual or Information Security Policy document compared to the costs suffered by companies that have suffered a security breach, they would see that the cost benefits would fall heavily on the side of developing such a document.

Only 50% [Table 9] of businesses that took part in our survey who have an Information Security Policy document or Employee/staff manual have made sure that compliance is written into staff job descriptions and within their contracts. By doing this if a staff member breaks one of the policies he or she has broken their contract and hence is legally in breach of it. Without doing this the policies carry no weight and cannot be used for any legal purpose or disciplinary procedures.

It is important that companies include user responsibilities - procedures they have to carry out, for example each computer user is responsible for downloading patches for their operating system and backing up their own work files onto a CD-ROM every week. These help protect company IT systems from possible security breaches. Unfortunately, only 50% of those SMEs with such policy documents included such responsibilities.

V. Conclusions

Welsh SMEs that have IT usage policies tend not to have them documented and those that do appear to favour keeping them within a Staff/Employee manual rather than in an Information Security Policy document. This probably stems from this seeming a more practical place to store these. Especially when you consider that many would already have such a manual containing company non IT usage policies and guidelines, so adding IT usage policies would be a fairly straight forward task. Whereas drawing up an Information Security Policy document from scratch would more than likely seem a much larger task than developing and adding new IT usage policies as and when they are needed to your company's Staff/Employee manual.

Those companies in Wales who currently state that they use IT usage policies but do not document them need to start doing so. It is important that company IT usage

policies are documented so staff are aware of them and adhere to them.

The findings as a whole suggest more work is needed to encourage Welsh SMEs to use Information Security Policies, or as seems more likely from this research, Employee/staff manuals as part of a strategy to address their company's IT security. This could perhaps be achieved by carrying out research looking into the costs endured by SMEs that have previously fallen foul of security breaches, which they would have been protected from if they had a policy document in place. This research could be used to show SMEs in Wales the potential costs of not having such a policy document in place and used in conjunction with business support services to help and encourage businesses in the development of a policy document.

ACKNOWLEDGEMENT

This paper is an output of the Opportunity Wales Advance project (Ref 55255), an Objective 1 programme funded through the Welsh European Funding Office and was produced by members of the eCommerce Innovation Centre research team. The authors wish to acknowledge the financial support given by the Welsh European Funding Office.

REFERENCES

[1] BS ISO/IEC 270001:2005 BS 7799-2:2005
[2] Laura Willis, 2002. Security Policies Where to begin. SANS whitepapers. http://www.sans.org/rr/whitepapers/policyissues/919.php
[3] DTI Information security breaches survey 2004. figure 16
[4] Small Business Service. 2005. *Small and Medium-sized Enterprise (SME) Statistics for the UK 2004*
[5] Office of National Statistics (2003), 'Size Analysis of Welsh Businesses'.
[6] Department of Trade and Industry (1999), 'Moving into the Information Age 1999: Regional Benchmarking Study', London, HMSO
[7] eCommerce in Welsh SMEs: the State of the Nation Report 2005/2006
[8] Information and Communication Technology (ICT) Activity of UK Businesses, 2004. National Statistics. Page 18 Table 14 http://www.statistics.gov.uk/downloads/theme_economy/ecommerce_report_2004.pdf
[9] Business In The Information Age International Benchmarking Study 2004. Page 51 figure 6.2c.