



the sales improvement specialists

IT SECURITY AND THE INTERNET: AN OVERVIEW FOR DIRECTORS



A White Paper from Koru Consulting

June 2006:

IT Security And The Internet: An Overview For Directors

1. INTRODUCTION

“Isn’t IT security the responsibility of my IT provider?”

“IT security is expensive. I know we need it, but we still get attacked by new viruses!”

“I am told that over the last year over 40% of organizations have had a security breach, and on average they cost £30,000” (see note 5 below)

First of all while IT security is the responsibility of the IT provider, it is fundamentally a business problem, as this paper will demonstrate. The second and third statements are undeniably true, but in well clichéd terms they represent the tip of the iceberg in cost and risk terms.

The objective of this paper is to identify the costs and risks associated with the “internet” aspect of IT security, and to appraise managers of the actions they can take to minimise their organization’s exposure.

2 DEFINITIONS

In the context of this document the “internet” is defined as:

- Web Sites
- Email/spam (electronic junk mail)
- Instant Messaging
- Peer To Peer communications

The technicalities of these are not relevant, the implications for an organization are.

3. BACKGROUND

The internet has transformed life. It has created new businesses and industries: it has simplified the customer interface: it has reduced selling and service costs, opened new distribution channels, improved communications and revolutionised education. Its benefits are immense. It is (relatively) cheap, pervasive, and easy to use; in a nutshell, it’s great. Few organizations today can live without it, and that in its own right is an issue.

On the down side it has spawned many less desirable and unwanted attributes such as IT diseases, unacceptable content and fraud.

4 THE COSTS AND RISKS

4.1 In a typical organization IT security is focused on the prevention of known problems such as viruses, and preventing unauthorised access. This is handled by a combination of anti virus and firewall software/appliances and perimeter security such as swipe cards, and even retina recognition. Most IT security expenditure is concentrated in these areas and in a 50 User organization this will cost around £4-5000. This is a reasonable price to pay for business continuity and protection of data. However, as identified above there are other issues with which to contend, which may render some of this investment a little ineffective.

4.2 Many organizations use the internet to place and receive orders, to deploy services personnel, and to conduct market research and business intelligence. Others use the internet as a means of receiving managed applications services, for Customer Relationship Management, financials etc as it is more cost effective than hosting their own system. As a result many office based staff have access to the internet; many have unrestricted access.

The natural consequences of this are to surf, use internet enabled email and instant messaging. Shopping and auction sites, music and video downloads, "chatting" with friends and personal email are favoured activities.

4.3 The risks and consequences of this are:

4.3.1 Increased costs through loss of productivity: Obvious as it seems, if people are employed on personal business, they are not working for you! In a 50 user organisation, just 20 minutes a day "surfing" will cost around £32000 per annum, or two extra/unnecessary people. (see note 1 below)

4.3.2 Loss of opportunity also arises. Using the same basis as above, but applying it to sales or revenue earning professional people an organisation could be losing up to 5% of additional revenue potential. Combined these two areas could yield up to an additional 6% in operating margins. (see note 2 below) In both these examples 20 minutes a day is a conservative estimate of time spent on personal business.

4.3.3 While an organisations IT infrastructure is being used for non work related activities, it cannot be used for its intended purpose. As most businesses today are IT enabled it is reasonable to say that business must in some way be damaged by personal use of the infrastructure. At the simplest level management may have to invest in additional/unnecessary infrastructure. At the worst level business can be damaged, particularly in commodity environments. If your web site is slow or unavailable customers can, and will go elsewhere. (see note 3 below)

4.3.4 Incurring legal action is expensive and damages an organizations reputation, and business prospects. Unmanaged use of the internet introduces the risk of legal liability. This is brought about by accessing, storing and circulating inappropriate content such as pornography. Such content can also lead to gender and/or minority discrimination and harassment. Illegal circulation of copyrighted material is also potentially bad for business.

IT Security And The Internet: An Overview For Directors

4.3.5 The use of instant messaging is growing in the corporate world. Use of instant messaging provides an open door to hackers giving them access to your intellectual property and confidential documents. Open email systems offer similar threats, allowing viruses and other malicious IT diseases into your systems increasing the risks of business discontinuity.

4.3.6 One of the largest and fastest growing threats to organizations and individuals today is SPAM (junk email). Spam is generated from multiple sources. These include access to web sites with auto responders, registration by individuals for newsletters and bulletins, malicious individuals and corporate bodies. Over the last year the volume of Spam has doubled (see note 4 below) and has implications and incurs risk and cost across all the areas above.

5 THE MANAGEMENT RESPONSE

Given that 22 million adults use the internet, and 85% use email, and 45% have access at work (see note 6 below) there is a good chance that it might be happening in your organisation.

Clearly virus protection and firewalls are no longer the solution, though they still form an integral part of IT security. Many of the issues above are generated from within the firewall and perimeter security systems, and are therefore under the direct control of management. The process is as follows:

- Understand the extent of non work related internet activity.
- Analyse the risks and costs associated with such activity
- Define your business priorities e.g. Security, legal risk, cost avoidance
- Define what is acceptable non work related usage and develop an acceptable usage policy (AUP)
- Identify the necessary IT tools (known as Content Security products) that will facilitate the implementation of your AUP, together with the best return on investment of the chosen tools
- Review your AUP in line with the development and needs of the organisation

6. SUMMARY

There is no doubt that an Acceptable Usage Policy, supported by appropriate Content Security products, will deliver cost justifiable business benefits and increased security while allowing organisations to continue to benefit from their internet investments.

7. NOTES

1. Based upon an average employee cost of £15,000 pa
2. Based upon assumption in 1 above. Maximum return would be in the professional services industries. In a product environment operating margin improvement would be lower
3. Source: Penn State University 2003
4. Source: International Data Corp., 2003
5. Source: PriceWaterhouseCoopers
6. Source: Office of National Statistics