

THE IT SECURITY PORTFOLIO

A SERVICE FROM KORU FOR IT COMPANIES

This compendium of articles relate to the ITC security issues facing the SME market today. The objective of this document is to identify the opportunities for IT services companies.

Half of British businesses report attacks by cyber-snoopers

- *46% of UK businesses knowingly affected by Spyware*
- *Growing prevalence of Spyware poses major strategic threat to business, survey finds*

Spyware, the disruptive software that covertly gathers user information through an Internet connection, is a significant threat to British business, according to research from PC World Business. One in two (46%) businesses reported that they have been affected by this extremely dangerous software. PC World Business estimates that the figure could be considerably higher, given the covert nature of the malicious bug.

Research of more than 250 businesses by PC World Business has found that the majority are open to spyware attacks, giving hackers a relatively clear run at confidential and business-sensitive data held by a business. More than a tenth (14%) admitted they were unaware of spyware and its effects; 26% said they were unsure if they were protected from attacks, and two in five IT managers stated that their staff are unaware of the types of website from which spyware can be picked up.

Spyware is typically bundled as a hidden component of freeware or shareware programs that can be downloaded from websites. However nearly half (47%) of UK businesses do not educate staff about the risks of spyware or impose safeguards to avoid websites where spyware can be downloaded.

“We’re more worried about the 54% of businesses that report no affect,” said Richard Harrison of PC World Business. “The nature of Spyware is that it is mostly invisible and it is likely that many thousands of UK businesses are being impacted by malicious software without any knowledge of it.”

“At its worst, Spyware can effectively steal the crown jewels of a business from under its nose,” said Harrison. “There’s no obvious sign, no fingerprints or CCTV footage – it’s a remote and stealthy threat that all businesses should put at the top of their security risk list.”

79% of the IT professionals surveyed think that spyware attacks will get worse in the coming years.

Spyware is a time-consuming and costly problem. Setting aside the costs to business of lost data, there is the cost of resource spent removing the hazard from the enterprise. Of the

businesses that reported being affected by spyware, 28% stated that it took up to one hour to get rid of the problem, while 10% said that it took between two hours and one day to get rid of spyware software from their business IT network.

The right security is the key to beating the hackers and the viruses

The productivity gains and rapid return on investment offered by new IT equipment and software, such as wireless networks and internet-based telephony, have never been better. The downside is that the work practices this new equipment and software introduces can create security risks.

A recent survey by the Institute of Directors revealed that IT security came top of the list of technology worries among British SMEs in the UK, and for good reason.

As wireless networks and more flexible and mobile ways of working proliferate, there is greater potential for hackers and viruses to breach your systems risking lost work, downtime, information theft and even fraud.

Yet a few simple precautions should help mitigate risk to your business, according to Paul Bodgers technical operations manager of PC World Business.

“Many people neglect to do the simple things such as activating firewalls or anti-virus and anti-spyware filters on their operating system together with ensuring their system downloads automated updates.”

Wireless working may require additional security measures, although the simplest wireless networks should be straightforward to protect, said Mr Bodgers. Encryption to a standard known as WEP should be all you need to set up a secure-password protected network. Some equipment, such as new all-in-one wireless router and access point equipment with built in firewall software, is now secure out of the box.

Working remotely from home or on the road brings additional risks, according to Stefan Foster, managing director of the National Computer Centre. Ensure your IT department or supplier sets up a virtual private network (VPN) to introduce more secure access for home-based workers if they are working with particularly commercially sensitive information. “If you can afford it, add higher levels of security using what are known as secure ID fobs, which offer more heavily protected and encrypted access.”

Staff awareness is just as important as having the right electronic safeguards and levels of encryption. It is important to introduce clear IT security processes, policies and awareness training, said Mr Foster. Staff need to be educated to not leave passwords stuck on Post-It notes and to not store sensitive documents on their home PCs’ hard drives.

“Training and engaging staff is vital. They need to realise that not following these sorts of precautions can do damage, cost money and even threaten their jobs. They should also be made to feel that they are all empowered to point out security breaches or weaknesses.”

Security does not just mean protecting your data from intruders either, it also means backing it up in case disaster does strike, added Mr Bodgers. This can be on CDs or DVDs, tape-based systems, or to secure locations over a broadband connection, a service offered open to a range of providers.

Small businesses live in fear of technology failure

IT tops AXA's Business Risk Survey.

For the third year running, small businesses have told AXA that IT systems failure is the most feared threat to their ongoing health and profitability. 91% of respondents identify IT failure as a threat with 23% of these believing it to be significant. IT problems were also identified by a quarter of respondents as the most common cause of total business failure.

The stability and availability of IT systems is considered a key business continuity issue. Despite recognising the importance of IT systems to their businesses, 39% of those questioned had no plan in place to protect them in the event of IT and other business failure issues.

In addition to the risks, respondents also recognised that investment in the right technology is a key factor influencing their success - 94% considered it important with 20% saying extremely important.

Doug Barnett, risk control strategy manager, AXA, commented on the findings: "Fear of IT failure keeps small businesses awake at night. It has consistently topped our list of major worries. One thing is clear, if your IT systems fail and you aren't prepared, this is probably the one risk most likely to put you out of business. Businesses need to consider all the risks they face and prepare a business continuity plan. How you would cope with an IT failure is one of the most important areas to consider. If you plan for it you can cope with it."

AXA advises all small business people to look closely at the impact IT failure would have on their business and put solutions in place without delay. Factors for consideration include:

- How long could you afford for your systems to be unavailable? Do you have a backup solution in the event of your main systems failing?
- What does your IT system control? If you are a retailer and have your products linked to electronic scanning & payment tills do you have procedures understood by all staff what they should do if the IT system fails?
- What level of IT support do you have access to; do you have a formal contract? Is it sufficient? Do you have access to expertise out of office hours? Can critical support be accessed quick enough to get you back online before severe damage is done to the business?
- Is your most important data regularly backed up, stored offsite and available to you quickly in the event of system failure, theft or damage? Have you kept information on key services you may have to reinstall e.g. broadband account details; security settings.
- Are you systems protected from theft, virus infection or systems hacking? Do you have up to date virus software and internet firewalls installed? Do you control what access your people have to the internet and what they are permitted to open or download?
- Do you have up to date copies of all your software easily available should you need to reinstall them on new systems - do you know how to reinstall software? Have you kept details of all required documentation e.g. licensing agreements? How often has the original software being updated and do you have licence to upload the most recent updates? Have you installed protection against Spyware?

The Security Portfolio

- If you have custom designed software is the supplier still in business should you need it reinstalling or updating?
- When did you last test your back-up procedures or your business continuity plans?

Businesses unprotected against corporate ID theft

Small businesses are being advised to take action against corporate identity theft, after an Institute of Directors (IoD) survey revealed that 64 per cent of them were not adequately protected against the crime.

The IoD also found that 47 per cent of businesses could not correctly define corporate identity theft - the crime of obtaining personal and financial information from a business, and assuming its identity in order to make transactions or for financial gain.

To avoid falling victim to identity theft, identity protection expert at insurer CPP, Owen Roberts, advised businesses to get online. "If businesses bank online, they can check their accounts for any irregularities at any time of the day," he said.

Roberts also recommended that businesses check with website domain name registries, such as NetNames and Nominet, to check if anyone has set up a copy of the site. "Customers might order goods from the spoof website which will never arrive and so ruin the reputation of the legitimate business. Or customers might respond to a spam email from the fake website asking them for personal details," he added.

A recent identity scam involved small businesses receiving calls from people claiming to be from Companies House, UK's registry of businesses, asking for business details. The callers then re-registered the legitimate business and used its identity to gain credit.

To avoid this, businesses can sign up for the free, protected electronic filing system (PROOF) on the Companies House website to help prevent fraudsters changing their details.

For further protection against identity theft, CPP recommends businesses also:

- check their details held at Companies House to ensure they have not been changed by fraudsters;
- sign up to the 'Monitor' email alert system on the Companies House website to get notification when any changes are made; and
- never respond to unsolicited calls from people purporting to be from Companies House asking for authorisation codes or other details.
- *To sign up for PROOF visit the [Companies House website](#)*
- *To sign up for Monitor email alerts visit the [Companies House website](#)*
- *For more information on avoiding fraud visit the [Metropolitan Police website](#)*

Koru Comment

There is no doubt that the subject of IT security is a major issue to businesses of all sizes. The number and types of threats are growing rapidly and can have a catastrophic effect on businesses, even to the point where companies can go out of business if they are not adequately protected. Many smaller organisations believe that they are less at risk than large companies because they have less value to steal than say FTSE, or international companies. This is absolutely not the case as the big organisations are generally well protected, and the smaller ones are less so. There is also a myth that most, if not all threats are external. The reality is that unmanaged internet usage introduces all sorts of IT diseases, not to mention potentially huge productivity losses. However, one man's problem is another's opportunity. Koru strongly believes that there is a major opportunity for IT services companies serving the SME market to provide consultancy led, easily cost justifiable managed security services. These will give providers initial and recurring appliance, software and services revenue. There is a significant market to address and while most organisations have anti virus protection, fire walls and data back up, few have content management and dynamic data recovery solutions.