ThinkTank

SCOTLAND & NORTHERN IRELAND

ISSUE 2: July 2008 IT SECURITY

IBM express advantage™

NEW ARRIVAL AT IBM NORTHERN IRELAND

Following on from the last ThinkTank newsletter, Alison McNeill, IBM's General Business Executive for Scotland and Northern Ireland, is delighted to announce that Shelley Cleere has now joined the Northern Ireland office.

Shelley has many years experience in the IT industry and will add a significant benefit to IBM's presence in the province.

Shelley is a dedicated Software Sales Representative and can be contacted at CLEERES@uk.ibm.comor on 028 9051 2529.

'GREATER TRUST IN STAFF' SAYS SURVEY

UK companies have become increasingly aware of the need to have information security policies in place, with seven out of eight large businesses claiming to have one. However, the high priority given to information security by companies does not necessarily translate into improved security awareness among employees. Increasingly, companies are realising that to tighten up on information security, they have to change their people's behaviour.

These are among the early findings of the 2008 Information Security Breaches Survey (ISBS) carried out by a consortium, led by PricewaterhouseCoopers LLP.

The survey shows that companies are placing greater trust in their staff and they want their staff to use technology to improve their effectiveness. For example, 54% of UK companies now allow staff to access their systems remotely (up from 36% in 2006); every very large business gives remote access to at least some staff. The proportion of businesses restricting Internet access to some staff only has nearly halved (from 42% to 24%), and only 9% give no staff access to the Internet.

IBM SPEEDS UP DATA COMPLIANCE

Following the acquisition of Princeton Softech in August 2007, IBM can offer a set of tools for data archiving, test data management, data privacy, and data classification and discovery. The IBM Optim tools are designed to enable your business to better manage data, improve its database performance, and improve security. Optim works in three areas:

- Data Growth – Optim allows secure archiving of data and maintain links to the data. Additionally, standard query tools such as Cognos can still query the data even though it's archived
- Test Data Management – Archive just the specific data you need for development, rather than save the whole database
- Data Privacy – Allows application-aware data masking, with the ability to fictionalise data, like credit card numbers.

This product portfolio works with DB2, Oracle, SQL Server, Siebel, PeopleSoft, JD Edwards and SAP.

WELCOME

Welcome to the ThinkTank from IBM Northern Ireland, the newsletter that takes a fresh and pragmatic approach to real business concerns.

In this issue, we look at:

- **The importance of IT security**
- **How companies are placing greater trust in their employees**
- **The IBM products to speed up data compliace.**

Most businesses understand that anti-virus software is a necessary tool: however, many businesses have focussed too much on the threats of hacking and have neglected conventional security. The recent thefts of laptops and the loss of CDs containing valuable and personal data have brought this into sharp focus. In this issue we look at ways of securing your business data that could enable you to reduce risks and keep your reputation.

To discuss IT security, get in touch with your local support team at IBM.

Marcus Austin, Editor

ibm.com/businesscenter/uk/scotnihome

Produced by Crimson Business Tel: +44 (0)20 8334 1655 info@crimsonbusiness.co.uk www.crimsonbusiness.co.uk
Publisher Nicola Dundon **Managing Editor** Marcus Austin **Project Manager** Joanna Franaszczuk

Setting your boundaries

Security has always been a primary concern for businesses: however, companies have mainly concentrated on the entry points into and out of the business, leaving security elsewhere largely ignored - until HMRC lost two CDs…

If you have a mobile workforce in your business then your valuable data is constantly at risk. Laptops, PDAs and Blackberrys containing sensitive company information or valuable contact details are carried around and are inevitably lost or stolen. In addition, the PCs in your office - and the data they contain - are all also vulnerable to theft.

The cost of replacing the data – even if it's not sensitive information – can run into thousands or hundreds of thousands of pounds, and that does not take into account the loss of reputation. Even though the data on the HMRC disks was encrypted, the loss of reputation has been immense, and the cost to send out millions of letters to potential victims was huge.

Legal requirements

You could also be breaking the law by allowing unencrypted or even encrypted data off your business premises or by allowing it to fall into the wrong hands within your business. In February 2007 the Financial Services Authority fined Nationwide £980,000 for failing to manage its information security risks after a laptop containing customer details was stolen, and Orange was criticised for allowing staff to share passwords and have potential access to customer data.

In addition, The Information Commissioner's Office (ICO) who enforce and advise on the Data Protection Act have recently been given the powers to impose substantial fines on organisations that deliberately or recklessly commit serious breaches of the Data Protection Act.

David Smith, Deputy Information Commissioner said: "This change in the law sends a very clear signal that data protection must be a priority and that it is completely unacceptable to be cavalier with people's personal information."

Worryingly, in a recent McAfee poll of 1,400 IT professionals with at least 250 employees in their companies, a third said that a major security breach could put them out of business.

Most businesses seem to regard themselves as the lucky ones, or that there isn't very much likelihood of data being stolen from them. However, when examining the figures for theft and loss it's a much bigger issue than expected.

Until recently the number of “data losses” reported were relatively small, but since the disclosure that HMRC had lost two CDs containing 25 million child benefit records, the flood gates opened. In March, it was disclosed that more than 1,000 government computers had been lost or stolen in recent years. The Ministry of Defence admitted 503 laptops or PCs missing in the past decade.

Flexible working

It’s an issue that in all probability will get worse, with employees increasingly choosing to work more flexibly, resulting in more and more data taken out of the workplace to potentially less secure areas.

While the situation sounds bad, there are ways to avoid the threats to data outside a business. The first way to protect data is to make sure that only those users with the correct security passwords and the correct privileges have access to corporate data. In order to be able to do this you need to be able to authenticate the person using the PC or laptop, either through passwords, biometrics or by using a security authentication device.

Password-based systems are the first line of defence. However, many employees have so many passwords that they cannot always remember them, resulting in lost time and effort contacting the help desk or IT managers to reset passwords. This affects the IT user productivity and the IT department.

Help desk costs become greater as the number of calls to reset and help manage multiple passwords increases. A June 2008 survey by Nasstar showed that IT staff spent as much as 70 percent of their time doing minor tasks such as password resets. Passwords tend to get written down or are chosen because they’re easy to remember which creates a security risk rather than a solution.

Safer systems

The alternative is to use a purpose-built package that is designed to make sign-on simple for the user and IT staff, and keeping administration to a minimum.

In March 2008 it was disclosed that more than 1,000 government computers had been lost or stolen in recent years. The Ministry of Defence was the worst offender…

By using a package such as IBM Tivoli Access Manager, users get a single sign-on, so they only have to remember one password, or can use fingerprint recognition to get access to their applications.

It can also be set up to restrict access to applications and data without a lengthy and complex implementation effort, it’s simple to maintain and administer, and happily for the IT department it is easy to reset passwords.

The system also has the ability to link in with HR systems, so that any changes in an employees work status are immediately reflected in their access rights.

It also enables the IT manager to:

- Enhance productivity by simplifying user experiences
- Reduce help-desk costs related to passwords
- Optimise security by eliminating poor password management.

Sophisticated software

Products such as IBM Tivoli Identity Manager allow users to reset and synchronise their own passwords without going to a help desk, saving time for both the users and technical support. The software can also identify unauthorised and malicious changes that would give users access to more applications than necessary to do their jobs, remove the illegitimate access, and alert designated business leaders to the threat.

Access tools such as Tivoli Identity Manager and Access Manager provide an audit trail of who has accessed what, and at what time, and will reduce the amount of time needed to gather the information required to comply with any security audits. Another way of authenticating a user is to move to two-factor authentication, which combines a password with a secure token. The secure token is normally provided by a small device about the size of a USB key, or from an application run on a mobile phone or PDA. So, to get access, a user needs to know the password and have the physical device.

An alternative to the secure token is to use a biometric security device such as a fingerprint reader. Fingerprint readers are now built-in to many devices including mice, keyboards, PDAs and laptops, and are simple to setup and easy to use.

Security policies must be adopted: employees need to understand why security is in place. The loss of the entire child benefit records data base was down to a lack of policy.

Reduce data loss

Another way to reduce the risk of data loss through lost or stolen devices is to remove the need to carry data around. By using thin-client diskless devices the data never leaves the server, so should a thin-client laptop or PC be lost or stolen all the data can be found, as everything resides on the server. Systems that lock-down the device's USB ports, CD and DVD drives so that data can't be copied from the devices onto USB Flash drives, CDs or MP3s ensure a near perfect secure system.

Lastly, but importantly, security policies must be adopted. Employees must understand why the security is in place. The loss of the entire child benefit records database was down to a lack of policy and training and best practice in handling and processing sensitive data. According to the investigation by the Independent Police Complaints Commission (IPCC) published in June 2008, the IPCC found that staff worked on confidential data without adequate support, training or guidance and had a "muddle-through" ethos. The information commissioner, Richard Thomas, has said that he will take formal enforcement action against HMRC over the loss of CDs which could cost millions in fines.

Avoid getting into a legal quagmire; it's time to start thinking about IT security now.