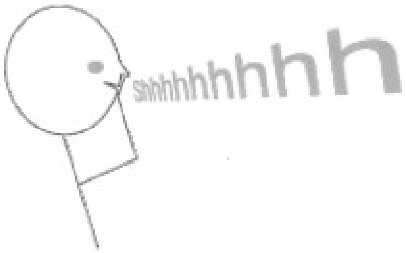
HUMAN RESOURCES JOINS FORCES WITH INFORMATION TECHNOLOGY

IT Accessed have teamed up with people and technology harmonisation specialists **Ryan Solutions** to produce a series of articles for the UK's Chartered Institute of Personnel Development (CIPD). This article originally appeared in the CIPD's April 2006 newsletter for North Yorkshire.

People connect every function within an organisation. Human Resources is therefore in a key position to influence the success of the organisation. In this new series of articles, Human Resources forges links with Information Technology to raise key issues of concern to our organisations. The issue chosen for this newsletter is security and passwords. One of our committee members, Linda Ryan joins with an Information Technology colleague Allyson Cole of IT Accessed Ltd to address this subject



Passwords

Are you concerned about the security of your organisation's data? Do you recognise a devil-may-care attitude to computer system passwords in your organisation? Do passwords cause resentment and stress in your company? It's probably time to consider creating a Password Policy, or review any existing policy. This should be a joint task involving Human Resources and System Owners in liaison with Information Technology. But, don't think this only applies to large companies; a very small or one-person business also needs to follow good policy - even if it's not one written down.

This is especially true now most companies have access to the Internet often via a permanent Broadband connection. It is not just colleagues and visitors who could misuse your identity; if you are connected to the Internet there are billions of people who could find and potentially abuse your computer access once they have your password!

Why you need passwords for each user of a computer system.

- To protect the information on the system from loss or corruption, inappropriate use (e.g. personal information), falling into the hands of competitors (e.g. sales data).

Data held by an organisation is often key to its future success. People collect and enter data remotely to form databases key to creating a competitive edge. Data held on people within the organisation is particularly sensitive; it must be protected and used appropriately. Remember data protection legislation and guidance.

- To protect the system from viruses, spyware and hackers.

Employees should be aware that visitors to the company or people communicating over the internet may harm the computer system - obtaining a valid password or gaining access to a PC left logged on and unattended will help them greatly. Many of our offices are now open plan, even if dedicated to one function or department; visitors from outside the department or temporary workers within it all have the opportunity to view screens as they move around.

- To identify the person carrying out the transaction.

Does the same person keep making errors; is there a problem with the workflow: who is deliberately sabotaging the system? Systems are now able to collect information about users and the transactions they are making; used wisely this can identify improvements in performance and detect inappropriate use which may need to be addressed by redial training or disciplinary action. It is therefore important to know who is doing what.

- To make it clear that each person is responsible for all transactions carried out under their I.D.

It is important that users understand that they are each responsible for transactions carried out using their ID and password.

What makes a good password?

- It must be changed regularly.

How often depends on the sensitivity of the data or systems and also on how good the system (firewalls, anti spyware programs) and the people are at keeping a password secret. A common gripe in organisations is that IT enforces very frequent password changes. However this is often the case because IT suspects the passwords are being shared and are doing their best to prevent security problems. All departments need to work together on this issue.
At a time when many HR tasks are being delegated to line managers, those managers need to be made aware that giving members of their team access to their personal password is not a safe way of coping with an extra workload - it is preferable to have separate user access.

- It must not easily be guessed.

There are many guidelines on what makes a secure password. A TOP TIP is to use an acronym that's at least eight characters long consisting of words (in both upper and lower case) and numbers, based on a song, quote or poem for example:

"Show me the way 2 Amarillo Peter Kay" becomes the password "Smtw2APK".

Employees find it particularly difficult to remember passwords for systems used infrequently. It may be best in these cases to look carefully at a process to see if there is a more effective way of gaining access to the information needed; for example, a senior manager who needs information each month is best provided with an emailed report or Excel worksheet that can be interrogated rather than being given direct access to the system.

- It must not be written down and must not be stored on your PC.

If a password is stored on your PC in any way - even if it appears on screen as asterix's the password can be identified.

How Can IT And HR Work Together On This Issue?

HR is a key support of change management, helping managers to identify and make changes in processes and introduce new systems. In many organisations a significant amount of IT's support budget is spent on resolving unnecessary password issues; if employees understood just how much money this costs then password practice might improve and system enhancements could be afforded - is this a good issue to build in organisation communication or performance based pay? We are all human, so any password policy should be practical as well as secure - there should be a quick but safe procedure to follow if passwords are forgotten or if someone suspects a password has been revealed. Quick reactions here from IT will help encourage users to change passwords when needed and not to misuse them. From an operational HR point of view, in circumstances where an employee is perhaps suspended pending investigation of misconduct, a speedy response is needed from IT to block user access. Equally, when an employee leaves the organisation for any reason, HR must notify IT immediately so that the User ID can be amended or removed.

Right from the beginning, the policy should be for processes and IT systems to be designed and used so that there is never a need for one person to know the password of another. No amount of education and lecturing will work if in order to get an important matter dealt with urgently for a customer, a password has to be divulged.

Note that IT support personnel often get so bound up in dealing with user passwords they forget that they should also change their system and administrator passwords appropriately! This should form part of any policy.

Senior Management Support

Lastly, and it should go without saying, any password policy needs to be supported by senior management. If managers are seen to act free and loose with passwords and to bend the rules to suit, the rest will follow

So the message to HR is get your board and management committee behind the policy at the outset.

Was this useful to you - let us know - are there IT mysteries you would like explained?

Linda Ryan
linda.ryan@ryansolutions.co.uk

Allyson Cole
www.itaccessed.co.uk
info@itaccessed.co.uk