Global Information Assurance Certification Paper

Implementing a stronger password Policy
Paul O'Hara
September 20, 2002

Introduction:
The subject of this case study is the implementation of a minimum password length as part of introducing a strong password Policy within an Organisation, the objective of which was to provide better security of the corporate electronic data. It was noted we could improve security in this way for very little cost to the company, as there were no software or hardware purchases involved. However we had to take into account the impact on the user community and the possible increase in calls to the service desk (help desk) for password resets once the change was made live. My part as Security Officer in the implementation was to co-ordinate the change to the password Policy in an Organisation consisting of 3000 plus users primarily accessing three separate Microsoft NT4 Domains. Approximately one third of our users are laptop users who regularly dial in remotely while the remaining 2000 employees use workstations in either an Office or Production environment - in a few cases the workstations are shared and in some cases by shift workers.

The paper will show that the successful introduction of a minimum password length depended more upon preparation and user awareness than technical configuration. The paper will also document the desire to keep the password in synchronisation with other systems passwords in order that the users can remember their passwords more easily. In addition, in the absence of any particular security features for our laptops at that time, the implementation of power-on (BIOS) passwords for laptops as an initial security step (first line of defence) for our mobile force, will be covered. Again this proved to be an exercise in good preparation but exposed weaknesses with having BIOS passwords as the only defence for laptops.

Background:
The situation prior to the implementation was that we had a network user account policy that used default of a minimum of six characters for a network logon password. The Industry standard at the time was moving towards a minimum eight characters for the password length - various security papers had been published that proved that eight characters is much harder to break than six characters [http://support.microsoft.com/default.aspx?scid=kb;en-us;Q147706]. To support this view we ran our own checks against the SAM database using the L0phtCrack [LC4] [http://www.atstake.com/research/lc/] utility, and noticed that 70% of our users six character passwords were cracked in one hour.

In addition although we had a company Policy for power-on passwords on laptops at the time, it was not implemented. This meant that any laptop that was stolen was immediately accessible to the thief and any data stored on the hard disk could be read. It also meant that the dialup networking capability was open to abuse if the thief could guess the network logon password. We were well aware that a BIOS password in itself was not much of a deterrent to a

determined thief but that it was a quick step to take prior to introducing encryption on the laptop.

Preparation to secure the network password:

A decision was made to strengthen the users network password and once that implementation had been complete then prepare for the laptop BIOS password installation. The reason was we did not want to introduce too many changes at the same time that could confuse our users and could potentially alienate them.

The first thing we decided to do was clean up the SAM database and delete any user accounts that had expired as a result of slipping through the normal administration procedures. We found that our administration processes worked well most of the time but occasionally there were gaps in the information received from the HR Department, particularly when contractors or temporary workers left the Company. This was a key security initiative because although the passwords would have expired on those particular accounts, it exposed the possibility of ex-employees attempting to get their passwords reset. To help with this analysis we used the Hyena NT administration tool http://www.systemtools.com/hyena/hyena_main.htm and were able to list all expired password accounts together with those accounts that had non-expiry passwords. Having investigated the target accounts and expiring accounts where necessary, we deleted those that were redundant, we then felt that we could apply the new policy to a more reliable database.

Next some preliminary work was completed on the user account Policy such as lengthening the reset count so that no more than three attempts could be made to change the password. We also increased the number of remembered passwords to twelve to prevent the frequent re-use of passwords. In doing this we noted SANS advice given in their Top Twenty Vulnerabilities :- *Many organisations supplement password control programs with controls that ensure that passwords are changed regularly, and that old passwords are not reused. If password aging is used, make sure that the users are given warning and chances to change their password before it expires. When faced with the message: "your password has expired and must be changed," users will tend to pick a bad password.* http://www.sans.org/top20.htm. So we also made sure that warning notices appeared on the users screens 10 days before the password was due to change and on a countdown basis to the last day of the change.

These changes were made in agreement with our service desk so that the service desk analysts were prepared for any additional user calls. We decided not to force case sensitivity because if we had done so the users could not synchronise exactly with their SAP password, which did not recognise case. Also we did not want to introduce yet another password complexity at this stage.

To help with the synchronisation of passwords, preparation work was also done on increasing the SAP minimum password length to eight characters. SAP is the main application software suite in use within the company and 15% of our users require access at least once a week while 80% required access daily. We felt

that giving the users an opportunity to synchronise their SAP and network logon passwords was an important incentive for using an increased password length. All to often users are forgotten in the rush to improve security and this we felt would take away some of the concerns the users may have had regarding remembering an eight character password.

Another important check that had to be made at this time was to identify any service accounts or hard-coded application ids that used passwords of less than eight characters. This was sometimes difficult as we found that the existing passwords could not always be traced. In cases like this we used L0phtCrack (LC4) to identify the password length or if the password was under eight characters but could not be cracked, we substituted a stronger password of the correct length. We were also helped by the fact that any of our applications that used hard-coded ids and passwords used Service accounts and these were held on a separate resource Domain.

During this initial preparation stage we also made sure we got buy-in from the Business and agreement to the policies we were implementing. Meetings were held with senior Management both in the Business and Information Management Departments, where the need for better security was explained and what we intended to do to improve the current situation. Everyone was keen to improve security but it was most important, once we had decided to increase the password length, to advise our users first and to make sure there was minimal impact on our systems. To this end we sent all our users an email (all our users had email) explaining the reasons for the change together with instructions on how to change their passwords and to make them more secure. See Appendix 1.

Making the change to the user account Policy:
Another email was sent the last week before the change reminding users of the impending change to their passwords. The change itself was done outside of normal working hours and because it was only a small change to the user NT account policy, took just a few minutes. See Fig 1 below. Most of the work had been in the preparation and the wording of the emails sent to the users. The Primary Domain Controller was rebooted and the new Account Policy became live.

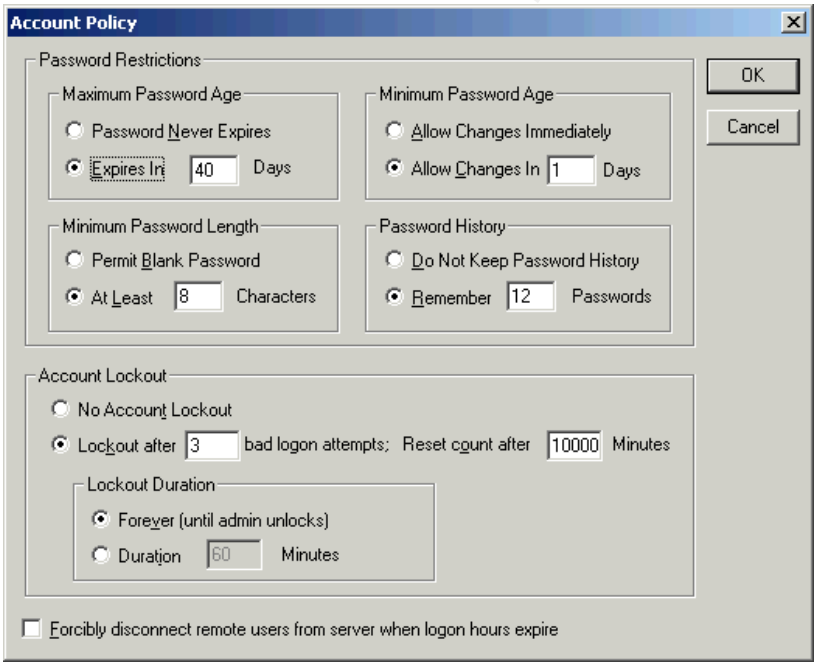
Changes in line with the user account domain were also made to the user account policy on our application role servers – those servers not governed by the policy on the Primary Domain Controller. Here we found that most of the servers had been installed using the Microsoft default policy settings, which for NT were very wide open and unsecured. This pointed not only to vulnerabilities with the installs but indicated that our procedures needed to be brought up to date. As the changes were transparent to the users (only administrators had access to the servers) it was relative easy to organise a system change. At this time we also took the opportunity of strengthening the administrator passwords on the servers and again using Hyena *[6]* we made sure that the passwords contained special characters and no complete words. *[8]*

In addition to making the changes to the user account policy we felt it was appropriate to introduce a warning notice on all machines to advise anyone attempting to logon to our systems, that they must use an authorised (to them) logon id. We consulted with our Legal colleagues and after some discussion soon became aware that unauthorised users, potential hackers etc., if caught, could legally be exempt from prosecution if we did not display such a message before the logon screen appeared. It was a loophole that needed to be plugged - so the text for the warning message was agreed.

"Access to this computer system is strictly limited to those people who have been issued with a valid user id by xxxx and are bound by xxxx's Information Security Policy. Copies of the Information Security Policy can be obtained from the Service Desk on xxxx or can be viewed on the internal web at xxxxx.com/security. Any person who attempts to gain access without the correct authorisation will be committing a criminal offence and may be prosecuted."

A change was made to the system Policy, on the appropriate domains, that forced the warning message on to each user's PC screen prior to the network logon password prompt. Having read the message each user just pressed the Enter key to move the display to the normal logon screen. We advised all users before making the change, emphasising the warning message was aimed primarily at potential unauthorised users in case any were using "borrowed" ids and gave any offenders time to request their own ids

Fig 1. User Account Policy



Impact of changing the password length:

The impact on the users was very little because they had enough advance warning and many had made the change previously. Some did not have to do

anything as they already used eight or more character passwords. Also because of the 40 day password expiry period, the change only affected some 2500 users (500 users were on the other two domains) over that 40 day period – not all on the same day. In this way the service desk noticed only a small increase in the number of password reset calls during the following weeks.

Once the 40 day period had expired we knew that the majority of users were now using the eight character password. We could now move on to the other two domains that needed changing to the same standard. This was a bit more complex because one of the domains contained users from both the UK and the US. Therefore we had to pitch the change to suit both time zones. However we were able to make use of the emails we had used in the previous change and our US colleagues just made cosmetic alterations to the text to reflect their own service desk phone numbers etc.

We then set about changing our documented NT standards to bring them in line with the change. The standards became global standards and were adopted in the other zones of the Company. We also noticed that our Auditors were satisfied with the change we had made but we still had plenty to do and the next task was to introduce a power-on password for our laptop users.

Introducing a laptop power-on password:
After initial discussions within the security group it became apparent that the first thing we needed to do was to find out the make, model and number of laptops we had in the Company. The model was important because we wanted to make sure the laptops we had were capable of supporting a power-on (BIOS) password. The number was also important, as we had to decide if it was possible for the PC Support section to perform all the installs locally. We quickly realised there were far too many laptops to call in, plus they were dispersed far too widely. The users themselves would have to do the installs.

We used procurement records to obtain the details of the laptops we had but an Asset Management system could be used if available. Of approximately 1000 users who had laptops we found that 95% had IBM Thinkpads and better still all the Thinkpad models supported BIOS passwords. Where the laptop model types included very old or little used models we decided not to include that particular model type in the rollout. This was because it would be difficult to maintain the power-on password and in a very few cases the model type did not support a power-on password.

In preparation we decided on a password format that was secure but a format that users could easily remember, one that could be easily recovered should the password be forgotten and one that the service desk or administrators could track if the user left the Company without divulging the password. Therefore although the passwords had to be secure and unique to the user, we had to take into consideration the following :-

1 We did not want delays caused by users forgetting complicated

passwords.

2 If the users did forget their password, the service desk would not be able to reset it. A PC engineer would be required to do the reset, which would mean maintenance, costs etc.

3 The password could not be synchronised with the users network logon password because the maximum number of characters allowed was seven whereas the logon password was now a minimum of eight.

The format we decided upon was to use a combination of the user's NT account name for the password. Although this may have seemed unsecured to the users, the purpose of the password was to deter an opportunist thief from accessing data on the laptop, and it probably would not have occurred to the thief to try that particular combination. The thief would also need to know whose machine he had stolen and our particular 'formula' for the password.

Next we had to get agreement from Business management and explain to them why we were implementing yet another password. It was not difficult to convince them of the security benefit but it was more of a concern to the service desk who had a requirement to reduce the number of password resets they were already handling. However when we explained the format to them and what we intended to do to prepare our users, they were more relaxed about the implementation.

Having got the agreement of Business management and the buy-in from the service desk, we then advised the PC Support and PC Engineering Groups. This was necessary as these were the groups who would be installing and maintaining laptops and on occasions would need to know the format of the BIOS password.

In addition we had to prepare processes and procedures for :-

Service desk - to include in their existing laptop procedures the need to ask the users for their power-on password.

Users - issuing of power-on passwords to new users.

PC Support - making sure service level agreements were in place for any BIOS password resets.

Once the laptop model types had been identified we then traced the power-on password installation instructions for each Thinkpad type. This was done via the IBM website http://www.pc.ibm.com/qtechinfo/PFAN-3U7NCR.html. Each model was tested to see if the instructions were appropriate and where necessary we modified them to suit our needs. We then ran a pilot in the PC Support section and with a few key Business users to check the accuracy and user friendliness of the instructions and made adjustments where necessary.

At this time we broadcast a news article on the company Intranet advising users of the need for security and the forthcoming implementation of the laptop power-on password. Because the instructions were quite lengthy and because there were several different model types, we decided that an email would also be sent to our users (see appendix 2) advising them of the need to install a power-on password. A second email (see appendix 3) would also be sent a week later reminding them of the need to install the password and with links to the install instructions on the company web site. This would allow the users to download and print the instructions for their particular model type. See appendix 4 for an example of the instructions.

We thought it was important that the second email set a date for the installation so that the users had a definite target day to perform the install by. Although in reality we knew most users would not or could not do the install on that day, it would give the security team a start date by which we could measure the success or failure of the implementation. The day was carefully planned with the service desk so that it did not coincide with other changes or their most busy days.

Having advised all our users of the "go-live" date via email and Intranet, it gave us time to take note of their concerns and respond to questions they had regarding the installation. We found that many of them were quite knowledgeable on the BIOS password and some pointed out how easy it was for a thief to get round it. However when they put it to the test they found that bypassing the password was not as straightforward as first thought and that it would go some way in deterring most opportunist thieves.

Impact of implementing a power-on password:

During the first week of the change we had 20 calls from the service desk, half of which related to the model 560 and 570 laptop series. Those 10 calls resulted from the original email message not mentioning the two model types, an administrative error that was soon corrected by pointing the users to the correct set of instructions on the intranet.

The remaining 10 calls were mostly users having a problem following the instructions although the instructions were about as clear as we could get them. However there were three calls that resulted form hardware errors when the password was installed. Of these, either disconnecting the port replicator or disconnecting the external keyboard solved the problem.

Apart from the 20 calls we had 4 emails from users referring to the model T series that had not been accounted for. Three of these were for Contract users based at a Customer site but were connected to our network. Further investigation showed that we could include the T series together with the A series and the users were advised accordingly. Also there were 4 Panasonic laptop users who were issued separate instructions.

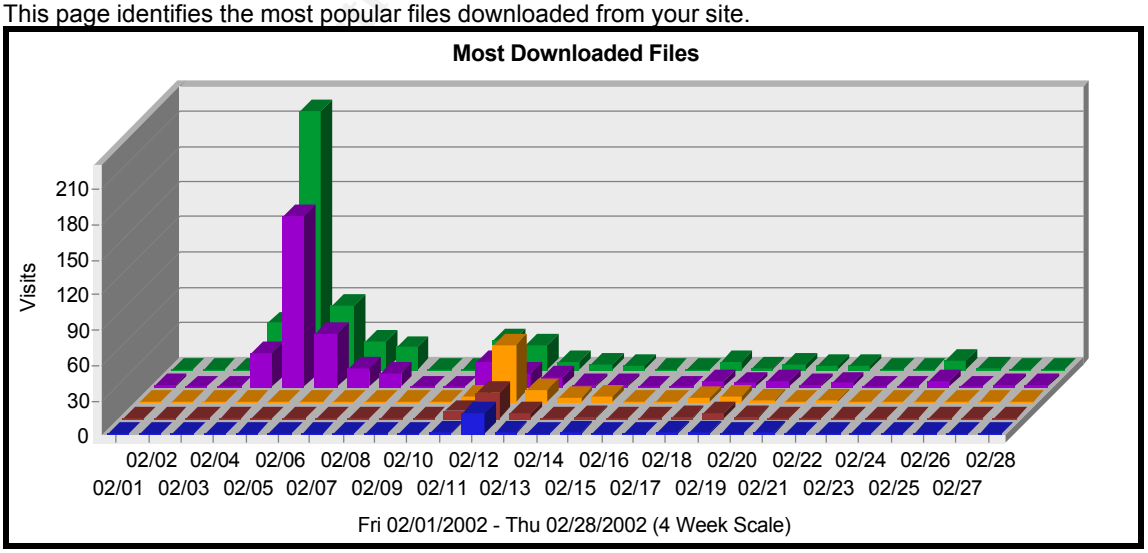
First indications were that quite a few users had installed the password without problems but it was difficult to tell at that stage what percentage of the user population were actually installing the password. Therefore after one month we carried out some analysis of the implementation to gauge the success of the rollout. Indications were that a majority of users had installed the password - this was based on the web traffic analysis tool WebTrends http://www.netiq.com/products/was/reporting.asp report produced for the Company Intranet that contained the user instructions. See Figure 2 below.

For reference, the histogram "Most Downloaded Files" in Figure 2 below shows that the number of Visits for the two Help Cards totals 795. (Visits are the important statistic. The number of downloads figure is not an indicator because scrolling the screen is considered a download by the WebTrends software). If a further 100 Visits is added because of the pilot installs and the model types that did not appear in the original message that went out and which were installed by the PC Support group and service desk, a total of 900 is a potential figure.

Given that some users probably did not install it even after downloading the Help Card(s) and some users got the instructions from other users, we could still estimate that at least 800 users had probably installed the BIOS password on their laptop in the first few weeks of the implementation. In addition, judging from user visits, engineering calls and conversations in the subsequent weeks following the implementation, the numbers rose significantly. Further security publicity, good practice and user instructions indicated that over 90% of users completed the installation. Now whenever a laptop is returned to the PC Support Centre it is checked for a BIOS password and new laptops are issued with installation instructions. All loan laptops have a default password installed.

Fig 2. WebTrends Report - Most Downloaded Files

This page identifies the most popular files downloaded from your site.



	File	No. of Downloads	% of Total Downloads	Visits
1	/learning/reference_cards/thinkpadAX_series_powerpassword.pdf	2,493	37.53%	464
2	/learning/reference_cards/thinkpad3_7xx_PowerPassword.pdf	1,517	22.84%	331
3	/learning/Reference_Cards/Changing+SAP+Password_b.pdf	386	5.81%	93
4	/learning/Reference_Cards/Changing_NT95b.pdf	212	3.19%	50
5	/learning/Reference_Cards/Change_bopw.pdf	139	2.09%	35
6	/learning/Reference_Cards/Up2Speed_OWA.pdf	115	1.73%	32
7	/learning/reference_cards/change_eroompw.pdf	162	2.43%	26
8	/learning/Reference_Cards/Changing_Outlook_b.pdf	88	1.32%	25

Summary:

Having strengthened the password Policy and completed the implementation of a BIOS password we then accessed the password security currently in place. It seemed clear that although we had improved the security for our users, there was still a great amount of work to do to improve password security. The initial audit we had done on the user passwords and a subsequent survey revealed vulnerabilities elsewhere. We knew that at some stage we must increase the strength of our passwords by forcing more complexity – LC4 proved that. Case sensitivity and special characters will be introduced in stages so that our users can adjust to the changes more easily and avoid reset calls to the service desk. To prepare for this we have posted password remembering tips and techniques to the internal web – all of which include special characters in the examples.

Among the risks identified were the weakness of administrator passwords, third party application passwords and customer passwords. Each of these groups has their own particular security problems and will need to be tackled in their own way. In addition, none of the precautions we had taken so far had reduced the number of laptop thefts we were experiencing and we could not accurately gauge what affect the BIOS password was actually having on protecting the Company data. It was evident that further work was required on user awareness, physical security, encryption and perhaps the introduction of laptop tracking systems. However since the implementation, one stolen laptop was recovered (prior to the change , no stolen laptops had ever been recovered) and the password was still in place and there was no evidence of tampering. As SANS has shown, defence in depth is essential and although we had only taken the first step in improving the password security for the Company, it had given us the confidence to make the other necessary security changes in the future.

Appendix 1

Example of the email sent to users informing them of a change to their network logon and SAP passwords :-

IMPORTANT REMINDER REGARDING IM SECURITY

This is to let you know that **the minimum length of your Network Logon and SAP passwords will be set to eight characters with affect from xxxx**. This means that from the xxxx onwards when the system prompts you to change your Network Logon or SAP password - it will not accept a password that is less than eight characters. The reasons for the change are as follows :-

- **Your passwords are the first line of defence against unauthorised access to XXX's data.**
- **Every person who has been given access to XXX's data including Contractors, Agency staff, Outsource Companies as well as XXX employees has the responsibility to protect the Company's information.**
- **The longer the passwords are, the more difficult it is for unauthorised users to guess or 'hack' the passwords and gain access to the Network and its associated applications.**

We know it may be more difficult for all of us to remember eight or more characters but this is now both the industry recognised standard and recommended minimum password length, used by Companies to make their data more secure. When using passwords follow these guidelines :-

- Use numbers as well as letters.
- Do not use obvious words such as people's names or months of the year
- The maximum length of the Network Logon password is fourteen characters - SAP is eight characters.
- The Network Logon password is case sensitive ie. you can use a combination of upper or lower case letters.

If you do not already use a **Network Logon** password with a minimum of eight characters it is recommended that you **change your Network Logon password now** to a minimum of eight characters. This will prepare you for the change and make it easier when you are next prompted to change the password. Please follow the instructions below to change your Network Logon password to a minimum of eight characters.

Appendix 1 Continued

Windows 95 users

- Close down all applications
- Click on the Start button and select the Settings icon
- Click on Control Panel
- Double click on Passwords icon
- Click on Change other Passwords button
- Highlight Microsoft Networking and click on Change
- Type in your existing password and then press [Tab]
- Type in your new password using a minimum of eight characters and then press [Tab]
- Type in the new password again to confirm the change and press OK
- Click OK again when you see the success message and close the Password Properties dialogue box
- Close the Control Panel and restart your PC using your new password.

Windows NT users

- Close down all applications
- Hold down the [Ctrl] + [Alt] keys and press the [Del] key
- Click on the Change Password button
- Type in your existing password and then press [Tab]
- Type in your new password using a minimum of eight characters and then press [Tab]
- Type in the new password again to confirm the change and press OK
- Restart your PC and logon using your new password.

SAP users only

Please note that if you are a SAP Session Manager user, the following instructions do not apply - you will only be able to change your SAP password when your current password expires.

If you do not already use a SAP password of eight characters it is recommended that you change your SAP password now to eight characters. As SAP has a maximum of eight characters for the password it will mean that you cannot have more or less than an eight character new password after the xxxx. Please follow the instructions below to change your SAP password to eight characters now.

- From the SAP Logon screen type in your current SAP ID and password but do **NOT** hit Enter
- Select the New password button
- Type in your new password of eight characters
- Type in the new password again to confirm the change and select confirm.

Appendix 1 Continued

For Information - SAP password rules

- Minimum length 8 characters after xxxx
- Maximum length 8 characters
- Expiration 40 days
- All characters that can be typed on the keyboard can be used
- First character cannot be ! (Exclamation) or ?
- First three characters may not appear in the same sequence in the users ID
- First three characters may not be identical
- Space character not allowed within first three characters
- Password is not case sensitive
- Password can be changed no more than once a day
- Cannot use last five passwords

Please reply to this email if you have concerns about changing your password to a minimum of eight characters or contact the Service Desk on xxxx if you experience logon problems after the change.

Appendix 2

Example of the email sent to laptop users informing them of the introduction of a power-on password.

Protection of Laptops by installing a power-on password

Following the recommendations of our external Auditors, Group Security and IM Service Governance, it has been agreed with XXX Senior Management that we will re-introduce power-on passwords for all Laptop computers. Although it is another password to type in, there are very important reasons for re-introducing this security measure.

- It is every employee's responsibility to protect Company data.

- The Data Protection Act 1998 also states that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"

- Approximately two laptops a month are lost or stolen from XXX employees. Apart from the physical loss there is a serious risk that any data on the laptop can be used by unauthorised users to adversely affect XXX's Business.

The power-on password is primarily a protection against the opportunist thief should the laptop be lost or stolen.

It has been decided that the password will be your *******.

In this way it will be easy for you to remember, will make it easier for IM to administer but will still be secure.

Therefore to implement the above security measure we will be issuing instructions next week for all laptop users to install a power-on password on their laptop. It will be a one-time install procedure that takes just a few minutes of your time and once the password is installed you will not be prompted to change it.

If you have any concerns or related problems please either e-mail Service, Desk or contact the Service Desk on xxxx.

Appendix 3

Example of the second email sent to users informing them of the introduction of a power-on password. This email contains the links to the Intranet for installation instructions.

Protection of Laptops by installing a power-on password

Following the security announcement emailed last week, it is now time to install a power-on password on your laptop. Please follow the instructions below to implement this important security measure. Although it is another password to type in, there are very important reasons for re-introducing this security measure.

What do you need to do?
Firstly, identify which type of laptop computer you use (the model number is normally located between the top of the keyboard and the bottom of the laptop screen), then print the relevant instructions below and follow the procedures in the document.

Instructions:
IBM Thinkpad A20, A21, X series please click here:
http://xxxweb10.group.xxx.com/learning/reference_cards/thinkpadAX_series_powerpassword.pdf

IBM Thinkpad 365, 380, 390, 760, 770 please click here:
http://xxxweb10.group.xxx.com/learning/reference_cards/thinkpad3_7xx_PowerPassword.pdf

Why are we introducing power-on passwords?

- It is every employee's responsibility to protect Company data.
- The Data Protection Act 1998 also states that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"
- Approximately two laptops a month are lost or stolen from XXX employees. Apart from the physical loss there is a serious risk that any data on the laptop can be used by unauthorised users to adversely affect XXX's Business.

The sending address for this email is an automated account. This message is for notification purposes only, and should not be replied to.

If you have any concerns or related problems please either e-mail Service, Desk or contact the Service Desk on xxxx.

Appendix 4

Example of ThinkPad power-on password instructions on the Company Intranet.

This reference card covers how to set up, change and use a power on password with IBM Thinkpad computers models 3xx or 7xx (to check the model open the lid of the computer and look between the screen and keyboard). Note: if you have a Thinkpad 560 please contact the IM Service Desk 6555 for special instructions.

Contents:

Why have a Power on Password?

- It is every employee's responsibility to protect Company data.
- The Data Protection Act 1998 states that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"
- Approximately two laptops a month are lost or stolen from xxx employees in UK. Apart from the physical loss there is a serious risk that any data on the laptop can be used by unauthorised users to adversely affect xxx's Business.

How to set up the password?

The password only needs to be set once on a computer and it does not change. The password to be installed must be your *******. This is very important as it will help you remember the password, but will still be secure against people from outside xxx. Please follow the instructions below to install the power-on password.

Make sure your laptop is switched off, undocked and not using an external monitor.

Hold down the **F1 key** and switch on the laptop (Keeping the F1 key depressed until “Thinkpad” appears on the screen.)

The Easy Setup program appears. Select the password icon (padlock symbol) by pressing the **Right arrow key** and press **Enter**.

- The Power-on icon is already selected (black shading)
  Press **Enter** key.
- Do **not** select the HDD icon.

Type your password (key symbols appear in the password box as you type) then press **Enter**.
NOTE: The password must be your *****

- If you type a wrong key, use the Backspace key to erase it and then type the correct key.

Type your power-on password again to verify it; then press **Enter**

Press **Escape** and select **Restart** and then press **Enter**

At the OK prompt press **Enter**

- The next time you start your laptop you will be prompted for the password.

How to change the password?

To change the password you have to remove the current one first and then install a new one.
To remove the password :-
Switch on the laptop
At the padlock symbol type in your current power-c password and press **Space Bar** and then press **Enter**
The padlock symbol changes to unlocked and the laptop powers up. The old password has now been removed
To set a new password see “How to set up the password?” above.

When the power-on password is set, the password prompt (locked padlock symbol) reminds you to enter the password when turning on the computer (or returning to normal operation from suspend mode.)
When the password prompt appears (padlock symbol) at the top left corner on the screen, type your power-on password and press the **Enter** key. If the password is entered correctly, OK appears and the computer starts normal operation.

If the password is entered incorrectly, X appears. Retry entering the correct password.

If you fail to enter the correct password after three tries, you must turn the computer off, wait at least seconds, and turn it on to try again.

When will I be asked for the password?

Normally, this will happen when the computer is switched on, however the following should also be noted:

- To resume from standby mode when the computer is attached to the Dock I or Dock II, you may be prompted for the power-on password.

What if I forget the password?

If you forget your power-on password, you cannot reset it. You have to contact the IM Service Desk: 6555 to have the password reset. Note: A charge may be levied for the service.

- If you have had 3 failed attempts you may switch off the computer, wait 5 seconds and retry.

References:

[1] IBM site to list ThinkPad T560 for password install instructions.
URL: http://www.pc.ibm.com/qtechinfo/PFAN-3U7NCR.html?

[2] NetIQ site giving information on the Webtrends web site reporting tools.
URL: http://www.netiq.com/products/was/reporting.asp

[3] L0phtCrack (LC4) information for Windows Administrators.
URL: http://www.atstake.com/research/lc/

[4] Microsoft Knowledge Base article on NT password strengths.
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q147706

[5] SANS How to eliminate the twenty most critical Internet security threats – G2 weak passwords.
URL: http://www.sans.org/top20.htm

[6] Hyena main page
URL: http://www.systemtools.com/hyena/hyena_main.htm

[7] Windows password Filtering
URL: http://support.microsoft.com/support/kb/articles/Q161/9/90.asp

[8] Microsoft TechNet Article - Creating Strong passwords
URL: http://www.microsoft.com/technet/prodtechnol/winxppro/proddocs/windows_password_tips.asp?