Passwords are virtual, have no on-cost, cannot be physically lost or broken and, in the current climate, where money is tight, they are the only real alternative to the modern and expensive biometrics, passkeys and active swipcard-based solutions. Bearing these facts in mind Darren James, Product Specialist, Specops UK, asks: are passwords a necessary risk to the security of your business?

So what can be done to increase data security without embarking on an expensive spending spree? The answer is to examine your current process and adopt best practice. This can be a simple case of increasing password length by an additional couple of characters, adding complexity by constraining the current password to have a mix of upper and lower-case alphabetic characters and numbers and a special character such as !£% or eliminating the use of ‘soft passwords’ such as Admin1, Passw0rd from the business. Another option is to introduce passphrases to replace passwords. These are in effect long passwords that the user can easily remember.

Many sectors have audits where the incumbent password policy is inspected and brought into question. This today is one of the main catalysts that cause companies to revisit their existing password structure; another is an actual security breach – which can lead to impulse spending on a system that may be unsuitable for your organisation.

A recent BBC news article entitled ‘Call to improve password security’ addresses the growing security problem caused by computer power costing less. Research suggests this makes it easier to crack passwords and access data, with devastating results, both in terms of cost and reputation! Plus with the growing use of graphics cards as surrogate supercomputers, the continued use of short passwords and soft password content will leave your company vulnerable to attack. A well-known technical research institute recommends we all move to a 12-character password comprising of a combination of upper and lower case, symbols and digits. This is simply a case of longer passwords taking longer to crack and therefore offering better protection, suggest the researchers. Another well-known organisation recommends moving to a 28-character passphrase.

Costing money and reducing user uptime?
It is very well documented that introducing an increase in password length and/or complexity will generate more requests for password reset calls to your IT support team, as well as generating a lot more user downtime.

The process can be as short as five minutes or as long as many days, all dependent on your local conditions. In the UK, the average reset per person per year is 1.5 hours, so apply this to your user base to understand the amount of call traffic and downtime within your business.

This scenario can be alleviated by making use of what most companies already have in their server room: a Windows server and an active directory, a powerful and secure database that is self-replicating and heavily encrypted. Microsoft, as well as many third party vendors, provide tools that snap into the active directory and give the protection and solutions needed for increased password complexity and security. Adding an effective form of password self-reset as a counter-measure to the increase in users forgetting their more complex passwords provides the business with what it needs.

Utilising these tools and features, a business can effectively apply different password lengths and/or complexities to various parts of the business based on the access rights of the user groups. The net result is less calls for password resets.

Soft words
The next area where a business can improve the security of the password is to remove the use of ‘soft’ words. We all know of users who simply use something such as Passw0rd or 12345678, or their name followed by a couple of digits, such as David12 or Debbie27.

Implementing a tool with a dictionary feature will allow you to eliminate all those common words used as passwords. It takes only seconds to download a list from the internet containing 1,000’s of common passwords and implement this list as ‘not allowed’. This type of feature, along with other sensible features such as the elimination of passwords that are dictionary words, can add a significant layer of security to your password system.

So how do you implement these changes? The first step is to decide which users need to have stronger passwords – this could be based on access rights, or a blanket rule for all users. Once this is decided, the password policy can be revised to enforce these rules. This can be done using the tools provided by Microsoft and third party vendors.

In conclusion, it is clear that passwords are here to stay, but with the right tools and policies, they can be made much safer and more secure. By implementing these changes, businesses can reduce the risk of data loss and improve the overall security of their systems.
of the user name, incremental characters and fill characters, will ensure that your passwords are strong and complex without implementing an excessive password length.

The business can now implement complex and or longer passwords for users who have higher access rights and implement standard or simpler passwords for those users with limited or no elevated access rights.

The last thing to address is providing a solution to allow the users to ‘self-reset’ their password. This has many advantages and very few, if any, disadvantages. A self-reset solution allows the user to authenticate themselves against the system and then reset their password in the event of it being forgotten or expired. By self-resetting their own password, only one person in the organisation will know that password, which is a major security gain. Using the traditional method of resetting a password, both the user and the service desk operator will have knowledge of the same password for a certain period of time.

Other advantages of a self-reset password solution include the huge reduction in calls to the IT service desk by typically 90 per cent. The user self-resets in less than a minute, so is up and running quicker, is more productive and the IT service desk can deploy their resources in a more efficient manner. Also a good self reset password product will have more than two methods of user authentication. This is to ensure that any user who does call the service desk for a manual password reset can be authenticated to eliminate beyond reasonable doubt that the person actually asking for a reset via the telephone is who they say they are, again enhancing the security aspect of the reset.

Other good features allow remote or external users to self-reset their password. This will address those annoying occurrences when a key member of the business is working on a Sunday night on that special presentation for Monday morning and attempts to log-on only to find that their password has expired. As the self-reset service is software-based, it operates 24 hours a day, every day, giving coverage outside normal support hours.

Different systems
One must then consider all the other systems in the organisation outside of the primary active directory and those that do not support Windows authentication, for instance SQL, SAP, LDAP and so on, and then the cloud-based systems that lie outside of the organisation such as Windows Azure, Office 365 and Google Apps. Suddenly users may have to remember many passwords for many different systems and these external passwords may well have relaxed or no password complexity rules. So again it’s important to consider these challenges and find a solution that can replicate your user’s secure and complex active directory (AD) password for these other disparate systems. By enabling this technology in your organisation the user only needs to remember one strong password. There’s less chance of that password becoming compromised as users won’t need to write it down, and finally when they self-reset their AD password all of the other systems passwords that they log into can be seamlessly synced, instantly.

Increasing data security within the business is crucial as any breach can be very costly and damage the reputation of the business. Organisations need to implement stronger passwords now by using what Microsoft and other vendors offer. The increased data security will leave you less vulnerable and selecting the right secondary tools to minimise the anticipated increase in password reset requests will keep users active and provide a return on investment within a few weeks.

The process to increase password security outlined above takes place thousands of times every day and the software tools described are numerous with many vendors offering anything from basic password enhancements to complete password suites with prices to match.