IDENTITY THEFT - FACT OR FICTION?

STAND & DELIVER—

OR HOW I LEARNED TO STOP WORRYING AND LOVE THE WEB!

With apologies to Stanley Kubrick.

A WHITE PAPER ON THE ISSUES OF CORPORATE IT SECURITY MANAGEMENT

JAMIE RICHARDS, SUPPORT MANAGER, XuiS

Do you remember the days when they told us that the internet would set us free? We would all be working from home, in our own paperless office, setting our own hours and enjoying all that extra leisure time we were promised.

They sold us the dream of the Information Super Highway – they just forgot to tell us about the Super Highwayman!

Some thoughts on the problems of passwords

In this paper, XuiS explores the hazards of corporate identity theft and the increasingly complex methods we are using to combat these hazards.

We look at the costs, in terms of both money and credibility, of poorly enforced IT security and why the simple approach is often the most effective.

XuiS SOFTWARE

A Climate of Fear

Every time you open a newspaper, switch on the radio and TV or even log into your email account somebody is telling you about the perils of getting entangled in The Web. The statistics surrounding the issue of identity theft are undeniably frightening; **the UK Government has stated that identity theft costs the country £1.3 billion a year**; over a quarter of UK adults either know someone who has had their identity taken and misused or has experienced it themselves, according to the March 2005 'Which' survey.

The problem of corporate identity theft is equally worrying. Nearly three quarters of UK businesses use a website as an integral and essential part of their corporate strategy; official figures from the Department of Trade and Industry (DTI) reveal that nearly half of these use no form of encryption for transactions over the internet, despite all the risks this entails. Many claim that the costs of implementing these types of solutions is an unnecessary business expense; as **DTI figures show that the average 'cyber intrusion' costs a company in excess of £30000.** The real costs in lost productivity, in credibility, in brand image and in company status are simply incalculable.

"$38... The average cost of calling the help desk to reset a password."

Gartner, June 2004

So we all try to find ways to make sure it does not happen to us. At home we add passwords to stop people accessing our PC, purchase software to control viruses (another password), have separate email addresses for personal and general use (more passwords), more software to stop spam on those mail accounts (another password) – well, you get the idea! At work it is just the same. We're all using a variety of applications, often on a variety of different platforms, each one requiring its own password access. Company policy will mean that you need to change these passwords periodically, often on a monthly basis.

The problems of complexity

The cost mounts, the complexity increases. Far from being 'set free' we have to remember all of these extra things and understand all of these new technologies. And, let us face it, we have all got enough things to cope with anyway – so if we have to have all these passwords we will use the dog's name, or the kid's or write it down on a post-it which we will hide in our desk. Nobody will ever work any of that out, so it should be safe enough, right? And when it expires, we will just add a digit on the end, that's secure enough.

Statistic time again; **70% of network attacks start behind the firewall** – the recent news story about the attempted 'virtual' bank robbery at Sumitomo Mitsui is the perfect illustration. On this occasion the system had been infiltrated with key logging software which would have delivered passwords, account details and other sensitive information to the criminals virtually gift wrapped! As yet, the investigating authorities are not saying whether this was an 'inside' job or whether access had been gained by some other method – but that is beside the point, the real issue here is how relatively easily the system was infiltrated and the increased panic levels among groups of Network Managers worldwide. It goes without saying that emails will have flown around emphasising the importance of security, reminding people of company policies and (in all likelihood) instigating mass password changes – 3M's balance sheet will certainly benefit from all the extra post-it notes needed!

The Answer?

So what can we do? Some experts will tell you to use multiple passwords, avoiding the obvious and using a combination of letters and numerals – statistically, they say, this is the safest approach; other experts will recommend the single password approach, backed up by some personalised 'biometric' data – strangely they also have statistics to back up their claims. But whoever you listen to, they will undoubtedly be making suggestions that add to the complexity of an already complicated situation.

Although there is no easy answer, the latter is probably the most sensible method, the so-called shibboleth approach (for those who are not familiar with the word 'shibboleth', it is in the Bible, Book of Judges Chapter 12 Judges Chapter 12, verses 1-15, probably the earliest recorded example of effective use of passwords in security enforcement). But whichever methodology is used, the most important thing is for it be enforceable AND user friendly – for example, self-service password reset would be a useful facility. This will give your help desk administrators valuable extra time to deal with the REAL security issues, and properly enforce IT security policies to prevent attacks on your network (from without and within) and deal with inappropriate material being stored on your company servers.

"Gartner Group estimates that a 10000 person enterprise can achieve an ROI of nearly 300 percent and saving of $3.5 million in a three-year period by Implementing an automated provisioning system"

Roberta Witty

Research Director, Gartner

In summary, the Internet is both a useful tool and a potential hazard for our business growth. We do need to monitor and control who has access to our business critical data and systems, and we do need to formulate and enforce IT security policies to manage the malign attacks on our servers. However, we do not need to make things so complicated that we spend all of our time simply remembering how to log-in to our own networks and applications, giving the super highwaymen the opportunity to infiltrate our systems while our backs are turned. Identity management is not a product, it is a process! As the saying goes, keep it simple, stupid!

Shibboleth

The armies of the Ephraimites and the Gileadites met in a huge running battle in the area that is now modern Israel. The Gileadites triumphed, routing their enemy who attempted to flee through the passage of Jordan. But the Gileadites managed to take the passage and established a blockade before they could reach it.

All of those trying to pass the blockade had to prove they were not Ephraimites. The Gileadites established a "test phrase". The Ephraimite tongue did not allow for a "sh" sound, pronouncing it instead as an "ess". So, to catch out Ephraimites pretending to be Gileadites, everyone was forced to say the word "shibboleth" - an ear of corn. Those who pronounced it as "sibboleth" were slain immediately; those who did not were allowed to pass.

STAND & DELIVER

OR HOW I LEARNED TO STOP WORRYING AND LOVE THE WEB!

The Cost of Passwords

An organisation with 1000 employees.

Assumptions:

> Only 2 password related helpdesk calls per end user every year

> An average cost of €30 per call, in lost man hours and productivity

> Self service password reset cuts calls by 30%

Annual costs: 2 x 30 x 1000= €60000

30% reduction with self-service password reset

Annual savings: **€18000**.

Can you honestly say that your password reset calls are really that low? And what would be your costs in lost time?

PASSWORD STATION

Password Station is the foundation for the AIMS Identity Management Suite. It provides a straightforward, self-service password reset facility cutting calls to your Helpdesk by more than 30%, giving your administrators time to deal with the real issues. With an easy to use graphical interface it allows your end users to securely reset their forgotten password and to synchronise ONE strong password across multiple platforms through any web browser or automated telephone system without calling the help desk. With the use of biometric challenge questions, and without storing password history on a vulnerable database, passwords again become the safe and secure method to protect your systems. With the facility to integrate voice recognition technology and support for RSA SecurID without requiring end user identity enrolment, Password Station is THE answer to managing your password problems and reducing your Helpdesk costs. It does not require an army of consultants to deploy. Now you can quickly eliminate the number one help desk call by installing Password Station on your web server in a matter of minutes without any consulting service fees. Providing round the clock access to all networks and applications, without the necessity for 24 hour cover from your helpdesk, ensures an immediate and identifiable return on your investment.

XuiS SOFTWARE

Contact

XuiS
The Pavilions
Kiln Lane
Epsom
Surrey, KT17 1JF
United Kingdom

Phone +44 (0)1372 728881
Fax +44 (0)1372 722245

sales@XuiS.com
info@XuiS.com

www.XuiS.com