

Identity Access: Yesterday's Thinking About Today's Risks

Norman Fraser
CEO, Tricerion Group plc
www.tricerion.com

It has been said that “change is inevitable - except from a vending machine”. It is certainly true that the identity access risk landscape has changed beyond recognition in recent years, with respect to both the scale and the types of threat. Identity access – or the process of establishing user identity in a system, e.g. through login – is now a front page news story, and an accepted topic of conversation amongst ordinary citizens.

Global businesses have responded to these changes by doing more to strengthen identity access: more security policies, more identity management solutions and more authentication layers. But all too often, the increased activity masks a troubling lack of change where it really matters: between the ears.

How we think about identity access risk drives what we do to protect the identities of our stakeholders, and this has implications for the bottom line. My colleagues and I enjoy frequent opportunities to discuss this topic with executives of respected companies. It is striking how often we hear them report that they are satisfied with their organisation's management of login risk, when a few carefully-chosen questions can expose quite serious holes in their logic.

We call this “*yesterday's thinking about today's risks*”.

Identity access risk isn't what it used to be. Yes, the *scale* of risk is larger than it was and it's still growing, but the *nature* of the risk has changed as well. Yesterday's undisputed orthodoxy for maintaining login security doesn't work anymore. Too many corporate boards are receiving and acting upon recommendations that apply old thinking to a new threat landscape, and are thus failing to diagnose the risks properly or to implement adequate solutions.

In what follows we will review some examples where out-of-date thinking fails organisations, and see how fresh thinking can help put them back on the winning side in the identity access arms race.

Optimism is never going to work

Hoping for the best has never made sense as an approach to managing corporate risk. It's not so much outmoded thinking – it's always been a bad idea. But with every new identity theft exploit someone, somewhere thinks of a new way to rationalise the “optimism defence”.

The COO of a well-known global financial institution once reassured me that his organisation had only incurred modest losses to phishing attacks, so he saw no need to take action to protect against further attacks. The relatively modest losses could be written off as part of the cost of doing business. I asked him two simple questions:

Question 1: What is the total cost of phishing attacks to your organisation?

Question 2: If you have suffered only modest direct losses to date and you propose not to take any further action to protect your organisation against phishing, what will keep your losses from growing massively?

I've had variants of this conversation with other executives, and the two *faux pas* illustrated here crop up again and again.

First, it's tempting to assume that the total risk exposure is equal to measurable direct losses. It has been estimated that \$3.2 billion was directly lost to phishing in the US alone in 2007¹, so the scale of the problem is worth taking seriously. But it is the indirect losses that are really frightening and these are frequently overlooked.

In the Ponemon Institute's 2005 survey on US data security breach notification², it was reported that 19% of individuals surveyed who were aware that they had suffered a data breach had already terminated business with the service provider in question, while a further 40% were considering doing so. Given the cost of winning new business, this represents a truly substantial level of indirect loss. Further, a 2004 Congressional Research Service Report showed that companies identified as victims of cyber-attacks in media reports suffered stock price drops of 1%-5% in the days immediately following the reports. For the average New York Stock exchange corporation, price drops of these magnitudes translate into shareholder losses of between \$50 million and \$200 million.³

Second, any successful small-scale phishing attack against your organisation demonstrates that it is vulnerable to large-scale attacks. We at Tricerion started talking with one financial institution when they were experiencing modest phishing losses which they were willing to tolerate without further action. Suddenly, their monthly losses jumped by an order of magnitude and they were not able to protect themselves. In due course we helped them to eliminate the losses altogether, but only after they had sustained several months of unnecessary loss and damage to their brand reputation.

Thinking about identity access risk in terms of the risk of direct financial loss can be deeply misleading. Any level of loss should be taken as evidence that systems are vulnerable and need to be fixed before the loss levels explode. Direct losses are just one part of the story – the much higher cost of polishing up a tarnished brand may be hard to estimate, but it must be taken into account.

Password policies that make things worse

Many organisations continue to implement password policies based on yesterday's thinking. Once upon a time, discussion about passwords was all about cryptographic strength. For example, if an ATM PIN consists of a sequence of four digits then there are

1 Avivah Litan, Gartner Report on Phishing, December 2007

2 Ponemon Institute, *National Survey on Data Security Breach Notification*, September 2005

3 Brian Cashell, William D. Jackson, Mark Jickling and Baird Webel, *The economic Impact of Cyber-Attacks*, Congressional Research Service Report to Congress, April 2004.

4

10 possible PINs to be tried by someone trying to crack the login. Small search spaces were deemed to be unacceptably risky, so policies were implemented to make large search spaces mandatory. To reduce the risk further, users could be forced to change their passwords frequently. Thus, password policies such as the following were introduced:

Password Policy

Passwords must be at least eight characters long and must consist of a mixture of letters and numbers. Letters are case-sensitive. Password change will be enforced at the end of each month.

This kind of policy makes perfect sense if the main threat to identity access security is brute-force password cracking. But it is not, and it has not been since the invention of the “three strikes and you’re out” policy which only allows a maximum of three failed login attempts before locking an account down.

In the context of *three strikes and you’re out* it makes little difference whether a password search space is 10^4 or the 62^8 mandated by the password policy above; in either case it is overwhelmingly probable that any three ‘brute force’ login attempts will fail. Thus the password policy does nothing significant to strengthen the identity access security, but it does make it harder for the user to choose memorable passwords, and this is compounded by frequent enforced password changes.

The longer and more arbitrarily structured a password is, the less memorable it will tend to be. The less memorable the password, the more likely the user is to write it down. Indeed, some industry leaders are even rejecting the conventional wisdom that passwords should never be written down. For example, Microsoft’s Jesper Johansson has observed that the security industry has been giving out the wrong advice about passwords for 20 years: “I claim that password policy should say you should write down your password. I have 68 different passwords. If I am not allowed to write any of them down, guess what I am going to do? I am going to use the same password on every one of them”.⁴

Johansson is correct that hardly anyone can reliably remember all the “strong” passwords the average user has to manage. But he is also straying into perilous territory. A shelf-full of research shows that the majority of identity thefts begin with the theft of personal information by people close to the victim – family, friends and colleagues. For example, it has been claimed that up to 70 percent of identity theft occurs within companies.⁵

When Richard Smith explored a number of workplaces to see what he could find, his results were alarming:

Coincidentally, mouse pads are shaped like miniature doormats. Just as some people hide house keys under doormats, some hide passwords under mouse pads. [I] occasionally perform “mouse pad surveys” at companies using computer systems. The surveys look under mouse pads and superficially among other papers

4 Kotadia, Munir (2005) Microsoft security guru: Jot down your passwords. *CNET NEWS.COM*, May 23.

5 Collins, Judith (2005) Identity Theft: Now It’s Your Problem. *Microsoft.com*.

near workstations for written passwords.⁶

Smith's desktop surveys discovered ill-concealed passwords in up to 9% of workstations in companies that placed no requirement on users to change their passwords periodically. But amongst the companies Smith surveyed that force regular password changes, he discovered poorly hidden passwords at between 16% and 39% of workstations.

Increasing the length, complexity, and frequency of change of passwords may increase the cryptographic security of passwords, but these measures dramatically increase the probability that real users will compromise their own password secrecy.

Prevention rather than cure

Yesterday's concept of "strong passwords" has become today's bad joke, since passwords are not cracked any more, they are simply harvested by means of fake phishing sites or Trojan spyware planted on the user's PC. Against these widespread and fastest growing threats, the cryptographic strength of passwords has become irrelevant.

Online service providers have concentrated on strengthening the defences of their own systems, but as Figure 1 shows, many of today's identity credential thefts take place outside of these defences. For example, in phishing exploits the user's login details are stolen during an interaction in which the genuine service plays no part. In Trojan spyware exploits the theft happens locally on the user's PC, over which the genuine service has no control.

6 Smith, Richard E. (2002) *Authentication: From Passwords to Public Keys*, Addison-Wesley.

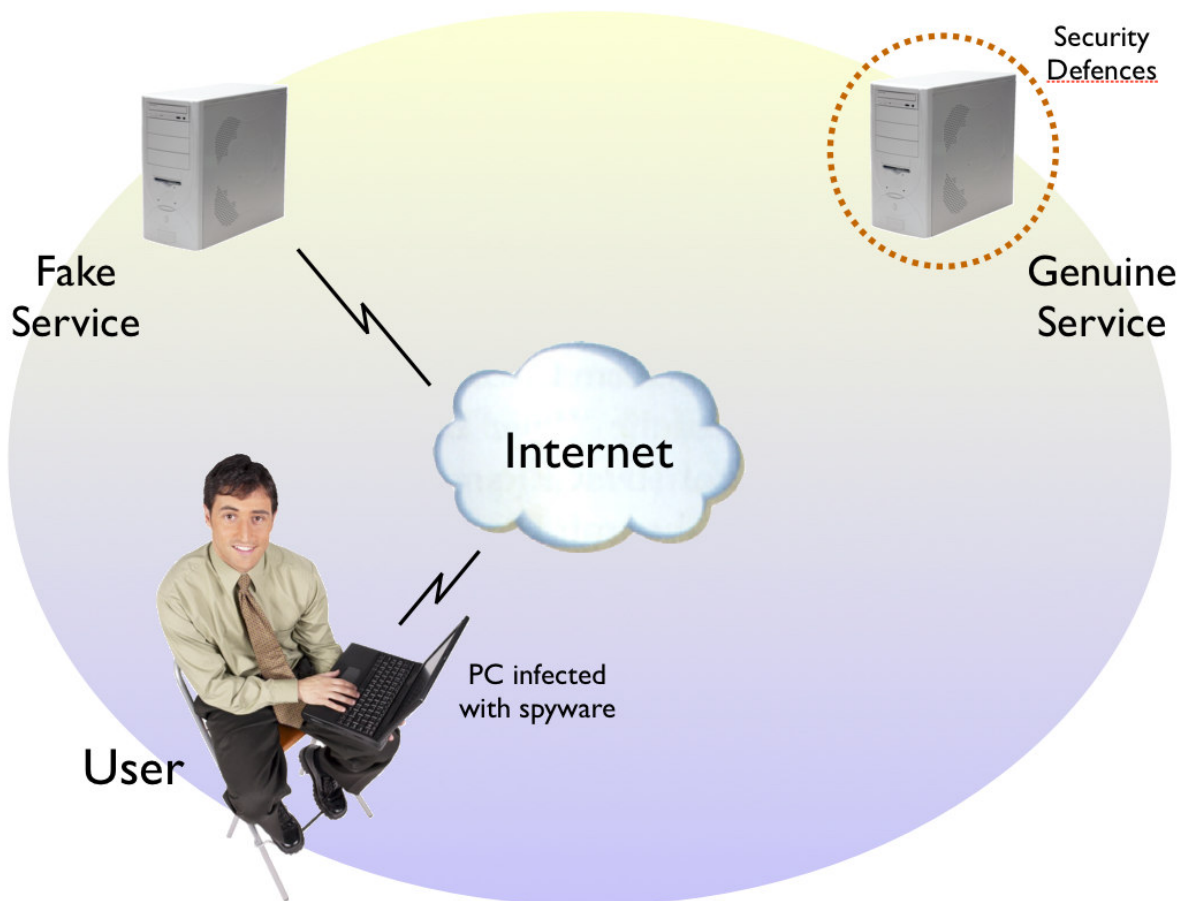


Figure 1: Many credential thefts take place without the involvement of the genuine service

For these reasons many service providers have given up on the possibility of preventing credential theft and have instead directed their energies towards “curing” the problem of stolen credentials, e.g. by deploying risk analysis systems that try to spot suspicious behaviours. These are inexact by definition and inevitably allow some criminal activity to occur.

However, we don't have to be restricted by yesterday's limitations. Today there is no good reason why service providers cannot protect their users by deploying credential systems that place credential theft somewhere on a scale between very difficult and impossible. One-time password generating tokens or smart cards are well known and can be highly effective, but they also involve significant capital outlay and logistical overhead. They may be appropriate for some applications but certainly not for all.

Tricerion's SafeLogin solution provides users with a personalized login environment, which is delivered entirely from the server side, requiring no special user training, and providing highly effective protection against all current credential theft exploits, including phishing and Trojan spyware attacks.

Woodrow Wilson once said, “If you want to make enemies, try to change something.” Service providers can be very nervous of being seen to change anything in the user's login experience. They opt to invest massively to buy partial protection systems that try to fix

credential thefts after they have happened, because this can be done less visibly to the user. But for a fraction of the cost these identity risks can be effectively eliminated using methods that users have been found to accept readily. Today's solutions really do work.

The Identity Access Lifecycle

At Tricerion we find it helpful to think in terms of the Identity Access Lifecycle (Figure 2).

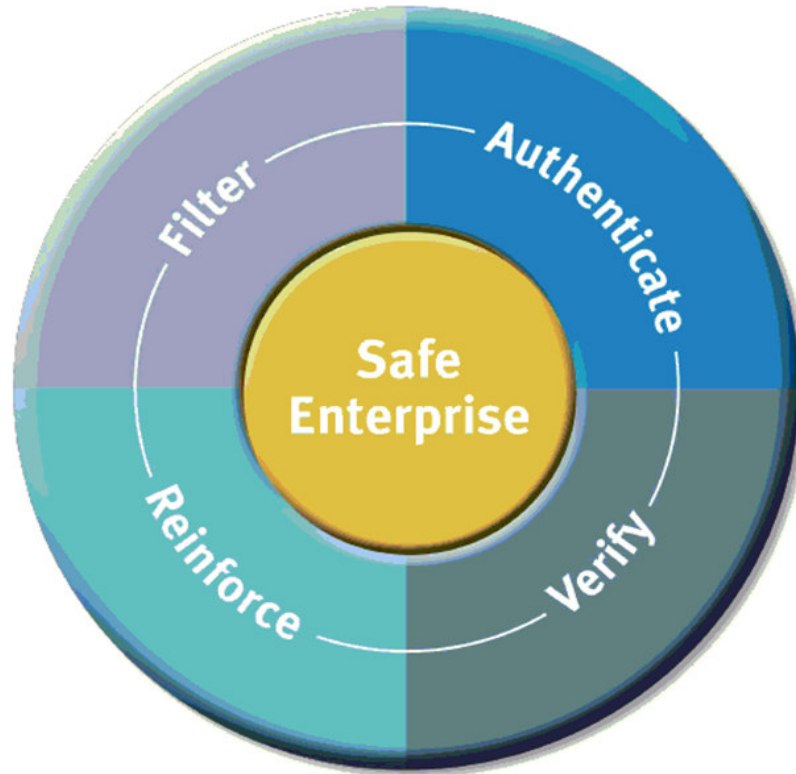


Figure 2: The identity access lifecycle

Filter	Assume you will face concerted attack, and take active steps to discriminate between human and automated identity access events, filtering out the robot logins.
Authenticate	Assume that attackers will target your login systems, and deploy an authentication model that actively excludes as many credential thefts as possible at this stage. Prevention is better than cure, and sophisticated, user-friendly alternatives exist today that make it difficult to justify continued use of the problematic conventional username and password method.
Verify	Assume that attackers will attempt to intercept your communications channel, so actively monitor for exploits such as man-in-the-middle attacks and disallow transactions where channel verification fails.
Reinforce	Assume that attackers will target your infrastructure, so actively reinforce against network exploits, such as distributed denial of service attacks, and interface device attacks such as browser hijacking.

At Tricerion we recognise that the identity access threat landscape has changed dramatically and will keep on evolving. Our SafeEnterprise solution effectively maintains identity integrity through all phases of the identity access lifecycle, applying up-to-date thinking to manage today's risks, and constantly evolving to keep our customers ahead of tomorrow's threats.

As the great genius Francis Bacon said as long ago as 1597, "He that will not apply new remedies must expect new evils; for time is the greatest innovator."

About the Author

Norman Fraser Ph.D. is CEO of Tricerion Group plc, identity integrity solution providers with an active presence in Europe and the USA. Born in Scotland and educated at Edinburgh and London Universities, he has been active in pushing the boundaries of secure human-computer interaction for more than 20 years. He has been involved in the start-up of several successful IT businesses, including Vocalis, Endava, and Tricerion.

About Tricerion Group

Tricerion specialises in identity integrity solutions, securing enterprises against all major threats to identity security, including dictionary attacks, phishing, pharming, Trojan viruses, and man-in-the-middle attacks. Ease of installation, simple logistics, low cost of ownership and excellent ongoing support combine to make Tricerion's SafeEnterprise an unparalleled proposition in the usable security space. Offering protection through the whole identity access lifecycle, Tricerion is able to deploy the right solution to filter, authenticate, verify and reinforce user access to valuable corporate assets. www.tricerion.com