Wigley & Company

BARRISTERS and SOLICITORS

ENSURING YOUR LEGAL & IT SECURITY

9th ANNUAL IT SECURITY SUMMIT

5th & 6th April 2004
Auckland

BrightStar CONFERENCES

P O Box 10842 • Level 7 • 11-17 Bolton Street • Wellington • New Zealand • Phone: + 64 (4) 472 3023 • Fax: + 64 (4) 471 1833

also at Auckland • Phone +64 (9) 307 5957 • www.wigleylaw.com

Wigley & Company presented last year and this year at the Annual IT Security Summit in Auckland and this paper supplements the 2003 paper, updating security issues including corporate governance, Electronic Transactions Act and proving cases in court. See http://www.wigleylaw.com/LegalComplianceAndITSecurity.html for the paper on which this supplement is based.

INDEX

1. Introduction

1.1 This paper supplements our paper to this summit last year. That paper dealt with issues such as the Electronic Transactions Act (ETA), new crimes legislation, virus and other risk to organisations (eg: liability to third parties when a virus is passed on), privacy, employees and AUPs. If you want a copy of that paper, please email: mwigley@wigleylaw.com.

2. Electronic Transactions Act: an update

2.1 The Act came into effect in November 2003, with the introduction of Regulations. The Regulations don't affect many areas. One of significance is that documents which the IRD require to be kept on paper can now be retained instead by being scanned (as opposed to being retained in some other electronic form).

2.2 The position remains that the ETA affects mainly Acts and Regulations. So its implications outside the public sector are generally not major (for some however it will be and each industry needs to check). It's very important however for the public sector including G2P and G2B.

3. Proving cases in court

3.1 IT and security generally involves balance of various issues such as business needs, cost, technical solutions, security and privacy. Often

in the mix are legal needs. For example a public sector funding agency will want to be able to prove on-line fraud. There are no perfect legal solutions. Often the legal needs are ignored when systems are designed. Those needs should be fed into the mix when systems are being designed.

3.2 Criminal cases generally need to be proven beyond reasonable doubt. That's close to 100% proof. This is a real issue. Take a key feature of a prosecution such as for on-line fraud. Proving that the accused person actually was the person who used the computer (ie: authentication) is not simple. Typically the person is authenticated by a key such as a digital certificate or a username/password. With the old system (a handwritten signature) the identity can be proven 100% (ie: forgeries can always be detected). That's not so on-line with currently used technology in practice. For example, many just assume that the most robust practically available key (PKI digital certificates) is powerful evidence that the person using Joe Smith's digital cert is in fact Joe Smith. It's not. All it does is provide evidence that someone has used Joe Smith's digital cert. In the inherently insecure and typical Microsoft environment, someone else such as an external hacker or an internal ragbag could access and use the cert, which of necessity (as the string is so long) is loaded on the PC. Worse than that, authorised use of someone else's digital cert would be common in many office and home environments, and encouraged. For example, a doctor's cert might often be used by her practice nurse.

3.3 So, to successfully defend a prosecution, which must be proven beyond reasonable doubt (ie: near 100%) a defendant might get off by raising enough questions. It only takes one person to succeed on this for defence lawyers to raise the defence time and again. So, design needs to take this into account.

3.4 For these reasons there's an argument that username and PINs are stronger from a legal perspective than so-called robust PKI. The PIN is (theoretically) stored in someone's head and so is not accessible to others. The banks after all, with their huge fraud risk, use PINs (sometimes but not always with a token (an EFT-POS card)). This may be seen as controversial and of course there are other solutions (eg: multiple level keys, biometrics etc). The point is: it's quite wrong just to assume that digital certificates and other keys prove that Joe Smith is Joe Smith.

3.5 To fully meet prosecution needs would unduly stymie the move to on-line. Some risk is needed. Importantly:

3.5.1 there's risk anyway in the off-line world;

3.5.2 on-line transactions create a lot more evidence and ability for widespread audit/evidence gathering (ie: on balance the ability to prosecute may be enhanced);

3.5.3 generally authentication is not the only evidence (for example, the fraudster getting money paid into his account is potent evidence and such evidence means authentication is less likely to be needed).

3.6 For non-criminal cases (such as $ claims), the standard of proof is generally "on the balance of probabilities", which is nearer a 50/50 standard of proof, not 100%.

4. Evidence

4.1 Our existing evidence law is relatively responsive to on-line evidence. However a new Evidence Code is likely to be introduced as a Bill later this year. It will be even more flexible in relation to electronic evidence.

4.2 One issue for NZ is whether there should be new law that presumes certain types of electronic signatures (ie: authentication) are valid unless the contrary is proven. This is the path the EU has taken in relation to PKI. There are pluses and minuses. There is a low-tech provision in the ETA on this aspect, which generally won't apply on current technology.

5. Corporate Governance and IT Security

5.1 Failure to meet appropriate security standards can lead to all sorts of types of liability such as:

5.1.1 liability to customers where a service fails (the Mercury Energy type of problem;

5.1.2 privacy breach (eg: inadvertent release of personal information in breach of the Privacy Act or other legal duties as to confidentiality);

5.1.3 business failure or downturn leading to financial problems, business failure etc;

5.1.4 liability to third parties where viruses etc are passed on when good systems would have stopped that.

5.2 IT and IT security is increasingly becoming a very significant issue for businesses, senior managers and directors. Directors owe a duty of care at least to the company. If they fail in that duty by failing to ensure adequate security is in place, they may be sued by shareholders, losses or others.

5.3 As part of the international trends in this area, New Zealand's Institute of Directors produced Directors' Guidelines for IT (including security)

in December 2003. These Guidelines expect close overview by directors, including by way of the audit committee or, where risk is particularly significant, a specifically appointed IT committee of the board. Senior managers are expected to be closely involved and directors need strong reassurance about security and system availability.

5.4 See also the higher level corporate governance paper just released by the Securities Commission (see http://www.sec-com.govt.nz/publications/documents/governance-principles/handbook.shtml).

5.5 Public sector has comparable governance obligations and issues. SSC's Guidelines for large IT projects and the Auditor General's report on the same topic are helpful.