Wigley & Company

BARRISTERS and SOLICITORS

COMPUTER USERS FACE FOOT & MOUTH RISK: CYBER-CROOKS

November 2004

P O Box 10842 • 11-17 Bolton Street • Wellington • New Zealand • Ph. + 64 (4) 472 3023 • Fax. + 64 (4) 471 1833

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

Computer users face Foot & Mouth risk. Organisations face on-line legal risk in many areas. In this Telecommunications Review article, Michael Wigley identifies the legal risks and answers to those risks, including in respect of virus attacks, employee Acceptable Use Policies, and minimising exposure to third parties.

INDEX

1 Introduction

1.1 The Foot & Mouth Disease Research Institute had an experimental farm in Surrey in the early 1960s. Some virus that the Institute had imported from Africa escaped, infecting cattle in the neighbourhood. Accepting that the Institute had inadequate sanitation, an English court said that it would be liable to nearby farmers whose cattle got Foot & Mouth.

1.2 What on earth has this got to do with the on-line and telecommunications world?

1.3 This situation is similar to an organisation passing on an electronic virus it receives to someone else, when it has inadequate on-line security and anti virus measures. It's a relatively easy step to hold a company liable if it negligently fails to stop an on-line virus or other intrusion from affecting another organisation. Liability could be multi -million.

1.4 Judge-made law tends to move incrementally by applying earlier cases to deal with commercial and technical developments. Applying the Foot & Mouth case to on-line viruses is a typical way this happens. There will be debate about what level of security is adequate to avoid liability, how closely related to the organisation the affected party must be before the organisation would be liable, and so on. But risk remains. For example:

1.4.1 It's unlikely an organisation is liable for failing to install the latest patch in anti-virus software (because it's prudent practice with software to defer installation until upgrades have been operating commercially for some time);

1.4.2 The Foot & Mouth case shows there are limits as to who can sue. There, the business of local cattle auctioneers was affected by the outbreak. But they had no claim as there were too far removed from the Institute.

1.5 There are stronger operational than legal drivers for having robust security and anti-virus protection and procedures in place. Add legal risk to the list as well, as one of the basket of risks.

1.6 Other legal reasons why organisations should have strong on-line security include, for example, the Privacy Act and the general law of confidentiality. They require an organisation to protect confidential information it holds, using a level of security that is appropriate in the circumstances. In addition to other risks (such as reputational), the organisation could be liable to pay money to affected parties if information is hacked out of the organisation.

2 External online attacks

2.1 What can organisations do to reduce legal risk of being hacked by an outsider, other than limiting liability to the people about whom information is held?

2.2 Apart from having robust systems, there's not much from a legal perspective that an organisation can do to reduce this risk (after all, it can't contract with a hacker it doesn't know). Perhaps the only area where hacking risk in relation to an external party can be lowered by way of contract is in respect of those known to be dealing with the organisation. For example, where external contractors have online access to the LAN through the fire wall, typically, and appropriately, they will sign up to an agreement that they will abide by the organisation's security policies etc.

2.3 Using those contractors as an example, a common failure is that an organisation has fancy legal words in place but they won't work because not enough has been done to get legal buy-in by the contractor to the contract and the security policy. It's generally not enough to have documents kicking around either in hard copy (such as a procedure manual) or on-line. The contractor should hand-sign an agreement unless great on-line acceptance procedures are in place. The agreement will typically deal with the contractor's relationship with the organisation (such as quality of work, what's to be done, price payable and so on) as well as issues around security compliance.

2.4 It's okay for that contract to cross-refer to, say, the organisation's security and acceptable use policy. If there are unusually onerous terms in the policy, it's prudent specifically to refer to those in the contract.

3 Prosecutions

3.1 A desire to be able to prosecute a contractor for hacking into the system and, say, misusing the system, illustrates this point about getting clear agreement

from the contractor. New Zealand for a long time has had an array of crimes that can be used against cyber-crooks. More recently, specific computer/telecommunications crimes have been added to our Crimes Act. A pivotal component of those new crimes is the issue of *authorisation*. A cyber-crook can be prosecuted if she goes somewhere she is not *authorised* to go. If it's intended that a contractor have on-line access to, say, the HR system, ideally it should be clear that she is not authorised to access the accounts payable system. This doesn't have to be done in so many words, but ideally there should be clarity around the degree to which the contractor is authorised to access parts of the LAN. That makes prosecution easier.

4 Employees

4.1 What about employees? As well as being able to prosecute crooked staff for online crimes, employees will have employment law concerns, and other issues such as privacy and copyright compliance.

4.2 Clarity around where the employee is authorised to go on the LAN (to facilitate computer/telecommunication crime prosecution) is one reason why there should be a contract covering on-line activities. Others include reducing the organisation's risk arising out of the employee's misuse of porn, breach of copyright, defamation, and so on. All these add up to a compelling argument that there should be a contract and an Acceptable Use Policy (AUP) in place with the employee to cover on-line activities.

4.3 Unless there is a strong online process, there should be clear handwritten agreement, not just reference to obligations in some on-line or hard copy manual lurking somewhere in the office.

4.4 We are emphasising the need to hand-sign something. When the organisation wants to take action against the employee, he might successfully say he knew nothing of the particular policy (even if in fact he did know). So, for example, generally a simple on-line *click accept* acknowledging acceptance of the relevant policy is not enough. How can the organisation or a prosecutor later prove that it was in fact the employee that click-accepted when he denies that he did it?

4.5 It is easier to have an automated and streamlined on-line system for accepting AUPs. Paper-based systems tend to be problematic anyway (signing of the contract/AUP documents is frequently botched, the paperwork gets mislaid and so on). The point is that, if an on-line system is set up, it has to be sufficiently robust to be able to prove later that the employee truly signed up.

5 What types of documents to use with employees?

5.1 These are different ways of getting employee buy-in to terms governing on-line usage. This could all be spelt out in the contract of employment. Typically however, AUPs need to change to respond to new technology and threats. A

common and good approach is to specifically refer to the AUP in the contract of employment, noting that it will change from time to time. Get the employee to hand-sign the existing AUP (or use robust electronic buy-in). Otherwise the organisation needs a strong audit trail to be able to prove later that the particular on-line AUP was the one in place at the time and it was readily accessible by the employee (it is common for organisations to fall down on this aspect).

5.2 Each time there's a change to the AUP, repeat the employee buy-in process. To say that the AUP applies, as it changes from time to time, is not particularly strong. This is hard work if done by signing, so a robust self-contained electronic system is better in practical terms.

6 Getting Acceptable Use Policies Right

6.1 Documents such as AUPs can be hard to draft. Take porn for example. AUPs will often use porn legislation as the benchmark for what is or isn't acceptable in an office environment. But porn legislation covers only nasty stuff. There is a whole bunch of material which would be unacceptable in an office which comes nowhere near the porn legislation (for example a photograph of a topless woman sent by male employee to a female employee). Another approach is needed.

7 Conclusion

7.1 Putting all this in context, the organisation's main focus of course should be around operational drivers such as external and internal on-line security, availability of service, etc. But there are additional and related risks in the legal area. It's worth taking steps to minimise those (and that's consistent with the key operational requirements anyway).

We welcome your feedback on this article and any enquiries you might have in respect of its contents. Please note that this article is only intended to provide a summary of the material covered and does not constitute legal advice. You should seek specialist legal advice before taking any action in relation to the matters contained in this article.