Managing content filtering for a Remote work force

INTRODUCTION

The Internet provides access to the widest variety of information content, from the obscene and misleading (hereafter referred to as 'illegal' content) to that which is widely considered as tasteful and 'good'. Information may be downloaded as video files, sound files, graphics files and/or text files, or more recently 'streamed'. Until relatively recently staff operated from company premises and were subject to centralized application-level checks.

What is not so well known are the implications and risks arising from remote working (e.g. at home or hotel) including the availability of broadband (e.g. 8Mbs) and WiFi, and coupled with little if any 'local' content filtering, i.e. by-passing corporate content checks.

And should an organization be concerned? Yes, because they are responsible for the actions of their staff.

FURTHER DETAILS

Broadband-related problems:

1. Higher bandwidths mean that staffs have the opportunity to download content than was otherwise unavailable (to an acceptable standard) at slower speeds. Higher speeds also mean that staffs adopt a more 'suck and see' approach to downloading content, spending less time comparing the 'time to down load' versus the benefits and implications (including 'breaking the law').
2. Remote workers more often than not have 'local' administration rights to their laptop (and certainly with regard to any PDA), which means that security controls may be 'disabled' (or reconfigured) in contravention of the corporate security policy – and without anyone knowing. Furthermore security controls (including anti-virus, content filtering, patches, etc) on laptops and PDAs used are often 'out-of-date' or indeed missing.
3. Remote workers, because they are away from the office environment, may lack training and awareness with regard to the corporate security policy. Alternatively staff may simply choose to ignore the policy on the basis that they are not subject to corporate monitoring. ***It should be noted that the IWF monitor Internet activity***.

WiFi-related problems:

4. WiFi networks within homes are not always configured in accordance with the latest industry standard (e.g. WPA2). This situation may arise because of mis-configuration by staff (i.e. 'non-IT experts') or due to the implementation of

'older' wireless access products; note the provision of such products is usually the responsibility of staff themselves.

Police authorities initially monitor access to illegal content on the basis of the 'requestors' public-IP address, which itself is mapped to a particular house address (e.g. 2, Rosemary Lane) by the broadband provider for the length of the session, and a record is retained. Unfortunately the same IP address may be used by several internal hosts, through 'Port address translation', including any intruders WiFi enabled device. Although the lack of illegal material on a laptop/workstation would subsequently exonerate innocent individuals (unless the intruder had uploaded illegal material maliciously, i.e. a 'stitch up') any police investigation would be embarrassing and impounded equipment would of course be unavailable for the duration of the investigation.

5. WiFi networks in hotels and cafes (e.g. Starbucks) usually have their security controls 'disabled' to aid access by the public (or at least the password is 'shared' by several parties).
6. Bluetooth-based LAN products are also appearing which may be exploited in similar manner toWiFi products. However unlike for WiFi, personal firewall products do not protect Bluetooth ports.

WHAT CAN BE DONE?

1. Probably the simplest solution, applicable would be to:

(i) Deny 'local' administration rights to laptops (not applicable to 'Personal Digital Assistants')

(ii) Have the IT department configure the personal firewall / VPN client such that staff may browse the Internet….<u>but only via the corporate network</u> *(i.e. VPN to the corporate network and then out via the corporate Internet firewall and content filtering solution)*.

(iii) Disable Bluetooth 'LAN' profile

The recommendation covers broadband, WiFi and 3G technologies.

2. Where (1) is not feasible, implement a 'local' content checking solution that blocks access to inappropriate web sites from laptops.

3. Log access to potentially inappropriate web sites, <u>ideally</u> 'centrally' under (1), or 'locally' under (2)

4. Implement a rolling programme of annual (remote) 'health checking' that:

- Check the integrity of security controls on laptops / PDAs.
- Check log files, cache, history and temporary files for evidence of 'inappropriate' browsing
- Check permanent storage for evidence of 'inappropriate' browsing (requires the use of recovery facilities)

Share findings with staff member in a confidential manner and in accordance with well-defined policy, noting that staff may have inadvertently accessed some ‘inappropriate’ content or web sites.

5. Procure wireless access points for laptop users working from home, and following configuration in accordance with the latest ‘industry security standards’, disseminate them to staff. Replace wireless access points as necessary to remain compliant with industry standards.