COMMAND HUB

20 January 2003

The Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Dr Carter

INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

CommandHub has developed innovative technology that facilitates the secure exchange of sensitive electronic information in a manner that is extremely easy to use, even by the 'technically challenged'.

By way of example, this technology has recently been deployed by a high-profile public company for the exchange of board and strategy documents as a complete, externally managed service that was successfully implemented with ***no*** user training. In was also the subject of a recent highly successful trial with a major government department where the issues of ensured privacy and external user acceptance were paramount.

The lessons learnt from these and similar environments, plus extensive prior experience with the strategy and deployment of key Internet and intranet initiatives for some of Australia's largest corporations, leads to the issues that are particularly related to the exchange of sensitive and private electronic data:

- in most instances the greater security risk is from internal rather than external parties;
- email attachments are a most inefficient and unsafe means of exchanging electronic data;
- the effective management of electronic data is best accomplished by using technology to keep the user interface a simple as possible rather than have the technology dictate the environment; and
- a *balanced security* approach is essential to maintain the privacy, confidentiality and integrity of electronic data.

Internal Threat

While most people assume that electronic data is most at risk while traversing the Internet as files or email, the sheer volume of traffic and easily available encryption tools mean that there is a far greater internal threat of unauthorised exposure. When the data reaches an intranet or web server, the volume of traffic has reduced by orders of magnitude and the percentage of people who have an interest in the material has increased dramatically.

As recently noted by Sun Microsystems, “Computer viruses and hacker attacks may grab the headlines but it's a well-known fact in IT circles that internal threats pose the greatest risk to enterprise information.”

As numerous studies and 'war stories' reveal, most internal attacks on sensitive electronic data are from an 'interest' rather than a fraudulent perspective but this does not make them any less threatening to the effective management and maintenance of confidentiality levels.

Email

Many organisations have a significant 'over-use' of email and this is nowhere more apparent than when Word or similar electronic documents are attached to email messages. This practice, often used when the extranet / intranet process is too complex - not only exposes a severe security breach but usually means that version control of documents is also compromised.

While the positive 'cultural' aspects from a high degree of 'people networking' need to be retained, a far more appropriate balance of content distribution via the intranet is invariably needed.

The volume and size of e-mails (often repeatedly containing the same attachments) present both a security hazard as well as unnecessary, increased bandwidth-hogging. What needs to be instilled throughout the organisation is a culture of sending short e-mails with an embedded link to an intranet page where the relevant content or file can be found. In this manner items of interest can be clicked on when the recipient is ready or just deleted if not - without clogging up e-mail boxes or network bandwidth.

Keep it Simple

With more and more electronic data becoming available via intranets and the proliferation of email, the vulnerability of sensitive data is of increasing concern in both the corporate and government arenas. Unfortunately, the most common scenario found in most larger organisations is an over use of security such that the technology and processes get in the way of what most users will actually use.

The use of passwords for access and encryption purposes is essential. But this use must be *appropriate* to the information concerned and must be implemented in a manner that is conducive to its use. Not all information requires a password or encryption - that would be the equivalent to locking every room in your home or office and having to unlock them every time you need access.

It is also no good having so many keys to the rooms in a building that people start leaving them in doors - yet we often see the electronic equivalent, where passwords can be readily found by just opening a desk drawer where they have been listed for easy reference.

Balanced Security

There are many levels of security that can be applied to data accessed via the Internet, from the electronic to the physical as well as the logical. The overriding consideration should be to have a consistently high base level of security and then have the appropriate tools available to apply even higher levels of security where appropriate.

Our experience has revealed many instances where the technology is overly visible and the processes too complex such that normal human nature results in compromises rather than compliance with the intended purpose and outcomes.

Yours sincerely,

Richard Cousins
Managing Director