CYBER STOR

global security for your data

CASE STUDY

The Client

AMP Insurance (in a phase of global expansion, branching out from Australia to Hong Kong and acquiring businesses in Europe) represented by Warwick Foster, CIO and Director of AMP (UK).

The Problem

How was AMP Insurance, now operating on a global scale, to ensure that differing national regulatory requirements for the protection of client data are not violated within an environment necessitating information exchange flexibility? As a result of published data indicating 60% of non-internet fraud being perpetrated by in-house personnel, (minimum cost) forensic audit capabilities were to be a component of any solution.

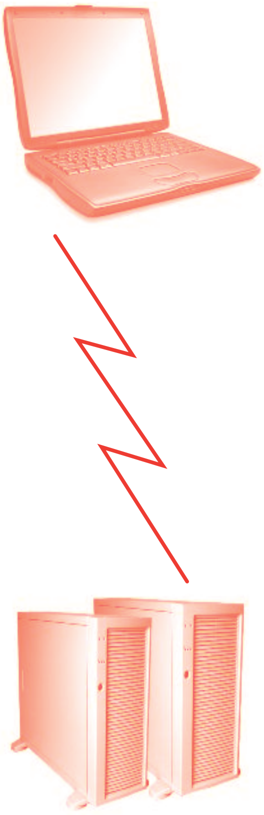
The Solution

The solution began with the acceptance that traditional “file updating“ in a thin-client environment would be unsatisfactory since this is not amenable to forensic auditing. On the other hand, storing all changed files would cause prohibitive data-storage costs and would, in any case, necessitate additional means for time, date and device “stamping“ to be recorded along with each file. The solution proposed incorporates an automated capability to store compressed sequential changes only, where merely the changed bits of information are stored, and simultaneously records a device-time-date “stamp“. This way, storage costs are minimized but, if any information is fraudulently altered, by running an audit the change as well as time and date of the change and the PC on which it was made can be readily ascertained. From this information, the person who used that PC to perpetrate the fraud can be identified.

Next, while for obvious security reasons encrypting the data being stored and exchanged had to be foreseen, standard “drive/file encryption” resulting in a minimum number of encryption keys was considered unsatisfactory since too many users would have access to the small number of keys (an obvious security risk) and also internal confidentiality might be breached by breaking passwords to access files locked under any one encryption key but not intended for access by lower echelons of employee. The solution proposed incorporates both variable encryption-level capabilities and the ability to set encryption keys at the file, rather than disk, level. This way, the larger number of keys required decreases the security risk and, by managing file-sharing based on encryption key, rather than merely on password, avoids at the same time any possible breach of confidentiality.

Finally, to ensure global regulatory conformance, a simple requirement – namely that no data ever remained resident on a user’s PC and was always resident on the secure corporate server – was stipulated so that any lost, stolen or damaged PC would never result in data loss nor unauthorized third-party access. However, this necessitates a user-independent (automated) means of transferring the data from the PC and which, itself, does not permit any breach of security, together with a means of subsequently erasing (wiping) the data in a manner to prevent future recovery. The solution proposed provides for automated data-transfer, first establishing bit-level changes to the data and then encrypting these on the PC, prior to transfer, thus ensuring that if subsequently intercepted nothing will be comprehensible. The data-wipe component utilizes overwrite sweeps of randomly generated characters thereby meeting US Department of Defense data-erasure standards.

The CyberStor client-server solution necessitated “pushing out“ a locked, pre-configured, version of the client software to each user via the corporate LAN, with the self-extracting client install necessitating merely a few seconds. Each user had preset server-access-authentication (and password) provided and initial, randomly-generated, (software) encryption keys were provided separately. Installation, configuration of, and training on, the server software necessitated one person-week of dedicated IT personnel time. For external personnel, in particular those based in Hong Kong, and travelling with laptops, GPRS wireless cards were recommended to obviate any necessity for land-line or Wi-Fi hot-spot access.



Return on Investment

In the words of Warwick Foster: “The primary objective was to ensure global regulatory conformance and this has been achieved in a neat and unambiguous manner by ensuring no data remains on any user’s PC. While other solutions might have achieved this, only CyberStor could convincingly demonstrate maintenance of security throughout the process and independent of PC location. An added plus is the ability to share files according to encryption key as a result of file-level key specification.“

“With regard to ROI, although there is no additional administrative overhead because existing servers run the CyberStor server software, it is clear that if we have to maintain a history of file-changes this will create additional storage costs. With CyberStor at least storage volume requirements are minimized in this case. But the real ROI has to be measured in the context of the cost of NOT installing a solution such as this – we will now avoid any potential class action lawsuits resulting from misappropriation of client information. CyberStor themselves have compared the cost of our one-off purchase of their seat licences plus server software (amounting to US$ 400,000) against the hidden cost arising from potential data loss, as established by the FBI and resulting from PC theft, loss or damage. Depending on how the figures are interpreted, we have a fivefold ROI, with the potential hidden-cost saving being in the region of US$ 2 million.“