Swiss organizations take proactive measures to ensure data security

Business

With the 2004 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) “ Computer Crime and Security Survey” finding that 53 per cent of the 494 organizations surveyed had experienced unauthorized access to company data over the previous year, and the total financial losses from those breaches totaling a staggering $141, 496, 560, it is no surprise that the Swiss government has placed such a high priority on protecting personal data. But, it is more than simply the financial cost to organizations of data theft that has driven the new Data Protection Laws. The survey also found that as a result of the possible negative publicity associated with a security breach, and not wanting competitors to utilize the information to their advantage, a staggering 58 per cent of the participating organizations did not report unauthorized access to data at all. While not reporting data theft can avoid bad publicity, it also means that personal information can go unreported – and it is for this reason that governments are concentrating on new laws designed to protect the rights of the individual. In no area is the risk of data theft more evident than in mobile computing.

With organizations becoming increasingly dependant on laptops to provide ubiquitous access to company networks, protecting data on these very portable devices poses significant security challenges. In fact, the FBI estimates that the 53 per cent of network penetration due to data derived from stolen laptops, results in an average cost of $25, 000US per device – far exceeding the value of the computer itself. And, with consulting firms estimating that organizations typically lose between five and eight per cent of their notebooks per year, the very portability of laptops can come at a very high price. One company has even admitted that the loss associated

with the theft of a single laptop cost a staggering $2 Million dollars!” More than the obvious privacy issues caused by unauthorized access to sensitive data via a stolen laptop, numerous retired hard drives with sensitive security and business information in clear text have appeared on sites such asEbay,” said Jens Albrecht, CEO of Swiss IT security company, insinova ag.

“ As a result, with a total price for encryption estimated to be less than CHF 230 per computer, organizations are beginning to understand that encryption technology is actually not a cost, but a necessary security investment,” Albrecht continued. “ And, with improved management features lowering administration costs and increased competition lowering acquisition costs, the total price of ownership is expected to fall by 10 per cent per year until 2008 – further improving the already-significant Return on Investment!” In recent years, Swiss organizations have taken proactive steps to ensure that stolen or lost laptops do not provide unauthorized access to sensitive data. One such company is Suva, the accident insurance company, which approached Swiss IT security experts, insinova ag, in 2004 to help them integrate encryption technology within its existing security architecture. Suva’s Security Requirements: Protection of Confidential Client Data” Being an insurance company, Suva’s 800 mobile employees must carry highly-confidential personal and health information on their laptops,” explained Albrecht. “” Understanding that its portable devices posed a data security risk, Suva approached insinova ag to help it ensure its clients’ personal information could not be accessed via a stolen laptop,” Albrecht continued.

“ Suva understood that encrypting all data would not only prevent unauthorized access to a client’s personal information via a lost or stolen laptop, but would also conform to the requirements of the Swiss Data Protection Laws.” Swiss Data Protection Laws state that personal information must be appropriately protected to prevent disclosure of the data due to unauthorized access, and if appropriate precautions are not taken an organization is open to a law suit in the event of involuntary publication of information. Before recommending an encryption solution, insinova ag explained that data encryption solutions can be basically divided into two distinct categories – “ full-disk” or “ file/folder” encryption solutions.” insinova ag explained to Suva that while file/folder encryption products did offer encryption of certain files specified by the user, other files such as paging/swap files, temporary files, offline folders of the email application, the recycle bin, or in disk sectors that are not fully written (Slack Space) could still be accessed in plain text,” noted Albrecht. “ As these unencrypted files would still enable unauthorized access to data, Suva decided to focus solely on full-disk encryption solutions that ensure that the entire hard-drive is always encrypted.

“ Suva then sat down with insinova ag to explain what additional functionality it would require from the selected full-disk encryption solution.” Suva wanted to be able to combine the data security benefits of encryption with the identity management advantages of positive user authentication,” said Albrecht. “ This meant that the selected encryption solution would have to be able to integrate seamlessly with today’s multi-factor authentication solutions, such as smart cards and tokens.” It was also decided that the

selected encryption solution should make it simple to manage configurations, such as the boot logon screen, keyboard layout, and password rules from a central location. This would make it quick and easy for administrators to instantly distribute the encryption software to Suva's distributed client laptops. The selected solution should also provide support for multiple keyboard languages at the pre-boot logon, and be easy to integrate with its existing virus scanners and system tools.

Suva also felt that in order to guarantee data security, the selected encryption solution would have to ensure that every user could be allocated a key file which may contain multiple encryption keys – a unique hard-disk key as well as multiple individual and shared keys for encrypting increasingly-popular removable media, such as USB memory sticks and micro drives." By ensuring that every user has access to the shared key, Suva would be able to make it simple for users to securely transfer and exchange removable media, such as USB devices," explained Albrecht. " And, in the event that the removable media device gets lost, the information contained on the device cannot be accessed by anyone outside Suva." insinova ag Meets Suva's Data Encryption RequirementsAfter a strong recommendation from insinova ag and an extensive evaluation process, Suva selected WinMagic's SecureDoc full-disk encryption solution." insinova ag has no hesitation in recommending WinMagic's cost-effective SecureDoc full-disk encryption solution," commented Albrecht.

" As SecureDoc supports every major PIN protected USB token and smart card, for pre-boot user authentication, it makes it simple for any organization

to integrate full-disk encryption with an existing PKI infrastructure by utilizing the same smart card and PKI certificates," Albrecht continued. " As a result, insinova ag has successfully installed SecureDoc for many high-profile Swiss users that required high-level data protection, including BIT [The Federal Office for Information and Telecommunication]." Not only has the selected full-disk encryption solution enabled insinova ag to meet all Suva's budgetary and timeline constraints, but also Suva's management requirements. SecureDoc enables administrators to create user dependent configuration files with only a few mouse clicks, and as these files can be copied onto dispersed laptops using any software distribution application, the task of distributing the encryption software to Suva's highly-dispersed users could not be simpler. Also, as the solution makes it simple for Suva to seamlessly integrate full-disk encryption with authentication technology at pre-boot, it has proved a hit with users as it has not slowed down the log-on process." In order to avoid the usual user resistance associated with implementing an additional level of security, the process has to be completely transparent to the user," explained Albrecht.

" When a user turns on his laptop there is no additional step to the log-on process," Albrecht continued. " After the initial encryption of the entire hard-drive(s), the user is simply prompted to enter their password in the boot logon screen, and the user will then be able to logon as normal into the PC and into Windows. insinova ag Meets Suva's Data Security Requirements With WinMagic's SecureDocAlbrecht is quick to point out that the SecureDoc full-disk encryption solution has enabled insinova ag to meet all Suva's data security and budgetary requirements." SecureDoc ensures that no

unauthorized user can access Suva’s internal data, makes it simple for authorized users to access information, and has proved simple to integrate with all virus scanners, backup systems, and compression programs,” concluded Albrecht. “ And, there has been no noticeable performance degradation to the user in day-to-day computer operations,” Albrecht continued. “ Simply stated, SecureDoc has made it simple for insinova ag to meet both Suva’s and the Swiss Data Protection Laws’ data security requirements without inconveniencing staff, partners, or administrators.”