Information security needs more than legislation

There may be a wealth of infosecurity legislation, but **Jason Hart** questions whether it is enough to fully protect your organisation.

In the last few years, we have witnessed scandals that have resulted in new legislation. Enron, WorldCom and Tyco are three high profile examples. We have also welcomed new legislation designed to foster the progression of, and protection from, the information age. In North America, the Sarbanes-Oxley Act requires that CEOs and CFOs vouch for the validity of their company books. The Health Insurance Portability and Accountability Act (HIPAA) aims to protect electronic patient information and sets guidelines for the exchange of that information (see p.18). The Gramm-Leach-Bliley Act enacted by the Federal Trade Commission protects consumer financial information. In October 1998, Bill Clinton signed the Electronic Signatures in Global and National Commerce Act. Also known as the Digital Signatures Act or eSign, this law states that electronic signatures on commercial contracts are the equivalent to handwritten signatures. European Telecommunications ministers approved similar legislation in 1999. In the European Union, the Data Protection and the Electronic Communications Directives set out guidelines for privacy and security governing electronic transactions.

The good news is that our governments have recognised the need to create new legislation. The digital signature acts aim to foster the information age. HIPAA and Gramm-Leach Bliley and other privacy laws serve to protect us from the pitfalls of the information age. Sarbanes-Oxley protects employees and shareholders from company executives.

If this legislation aims to protect us from the information age, what legislation or standards exist to ensure that the CEO who has to vouch for the validity of his books is protected from the network administrator who set up his password to the company's accounting application? What legislation or standards exist to prove exactly who authorised a multi-million dollar transaction or prescribed a drug to a patient? Alternatively, consider Bill Clinton who signed the Electronic Signatures in Global and National Commerce Act in 1998 with a password protected smart card. A network administrator set up his password (which, by the way, was "Buddy", the name of his Labrador retriever - a very poor password choice as it could be easily guessed). All of this new legislation assumes that we trust the strength of current authentication methods. ("Authentication" in this sense is the process a user undertakes to identify who they are to the network, and to "guarantee" they are who they say they are.)

> What legislation or standards exist to prove exactly who authorised a multi-million dollar transaction or prescribed a drug to a patient?

SECURITY VS USABILITY

A major security problem that most organisations encounter is ensuring the legitimacy of access to the network and the information stored. Logon, which is the authentication to the computer network or application, is often secured by nothing more than a password. Passwords have three significant downfalls: they can be easily guessed; they are prone to a culture of sharing; and users have a tendency to write them down - often in obvious places (see p.22).

Traditionally, high security and "user-friendly" have been poles apart. Users have always wanted easy access to their applications and the information they need to perform their daily work. They authenticate to the network, then they must authenticate with different usernames and passwords to their applications. They are fed up with forgetting passwords, being locked out of systems and generally wasting valuable time with password management issues. IT administrators are just as tired of all the Helpdesk calls associated with passwords. Security experts want "strong" password policies that require a password length of at least eight characters, a combination of both numbers and letters, and that enforce changes every 15 - 30 days. While these "stronger" passwords are harder to guess or crack, ironically they contribute to the problem because even more users write their passwords down as they are often too hard to remember.

The inherent weaknesses of traditional password systems render the network and the information it contains insecure, making it impossible to prove fraudulent activity because the level of proof of identity for the user is insufficient. A person can simply say someone guessed, changed, or hacked their password and the case is thrown out of court.

PASSWORD ALTERNATIVES

Thankfully, implementing advanced authentication methods, combined with single sign-on (SSO), solves these problems and puts your organisation back in control. Through the use of tokens (small authentication devices), smartcards, and/or biometric devices, user identity can be much more firmly established. While passwords are based solely on what a user knows (their username and password), advanced authentication methods offer multi-factor authentication based on combinations of the following security principles: what the user knows (password, pin), what the user has (token

generator, smartcard, biometric reader), and who the user is (fingerprint, retina, voice). Instead of using a password to logon, a person authenticates using an advanced authentication method, which is also logged and audited. Once that person authenticates to the network, SSO kicks in, providing people with fast and seamless access to their applications. SSO remembers a person's application logon credentials (such as usernames and passwords) and handles logon to the application, entering the user's credentials so they do not have to. SSO also handles password changes, password policies and any other messages that are generated by an application. Before granting access to an application that attempts to transfer money, for instance, you can force the user to re-verify who they are by prompting them to authenticate with an advanced authentication method. From a user point of view, all that is necessary is to logon to the network and all applications with a simple fingerprint scan.

Implementing single sign-on with advanced authentication (1) ensures proof of identity by forcing users to logon with strong authentication methods, (2) eliminates passwords altogether, (3) reduces administrative overheads saving time and money, and (4) makes sure transactions and events can be "proven in court" if necessary. At the end of the day, the needs and requirements (often legislative) of your management and staff, administrators, auditors and security experts, have all been addressed for the first time in the history of Information Technology.

AUTHOR: Jason Hart is is CEO of Protocom Development Systems, a global developer and provider of network security solutions (www.protocom.com).

CONFERENCE INFORMATION: Protocom are exhibiting at Infosecurity Europe, the largest and most important IT security event in Europe. Now in its 8th year, the show features Europe's most comprehensive FREE education programme, and over 200 exhibitors at the Grand Hall at Olympia, London from 29th April - 1st May 2003. www.infosec.co.uk

Continued from p.3

PRACTICAL APPLICATION

In practice, the arrangement would need to be negotiated in the country of the company's European headquarters and with the DPA of that country. For the system to work, the arrangement would need to be accepted by DPAs in the other EU countries in which the company operates. This is because, in the event of a complaint in another country, that country's DPA would still have the right to investigate the problem and give a ruling as necessary.

The business community is likely to support the project, as Hustinx explained: "Model contracts do not cover every situation and so there is a need to look at the issue from the company viewpoint." Currently, this arrangement is being assessed by the DPAs in Austria, Germany, the Netherlands, and the United Kingdom.

> "Model contracts do not cover every situation and so there is a need to look at the issue from the company viewpoint."
>
> - **Peter Hustinx, Netherlands Data Protection Commissioner**

The first initiatives will hopefully generate a number of common structural elements, such as those described above, which would then become a prerequisite for approval.

At that point, there is a good chance that other DPAs will accept the corporate rules scheme. Hustinx stated that "the scheme does not need the unanimous consent of DPAs in all the EU member states, as the EU Data Protection Directive does not impose an identical implementation framework on all member states." Companies would still have to work with DPAs in whichever EU countries they do business. Some DPAs would need more time than others to develop the concept because of differing priorities. Hustinx added that "the Data Protection Working Party likes to reach consensus."

For transfers outside a group of companies, it is likely that contracts would still be needed. However, Hustinx summarised the attractions of this imaginative corporate rules scheme:

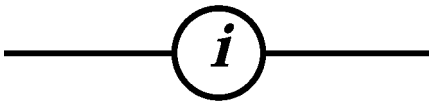
"1. it gives companies a sense of ownership backed by a solid structure and a management agenda with checklists for action, something which some leading companies are already claiming to do in any case

2. it is ideal for intra-corporate transfers, for example, for human resources data because it offers data subjects a legal commitment in a flexible format

3. it could work alongside solutions for specific countries, such as the US Safe Harbor scheme. In this case, the corporate rules commitments could be adopted as part of a company's Safe Harbor policy to which it would then be accountable to the US Federal Trade Commission; and

4. its impact could be global in that it could work in all countries, with or without data protection laws."

Han Kooy, senior legal counsel for Shell International, was emphatic about the benefits to the Netherlands/UK-based Royal Dutch/Shell Group of more than 2,000 companies around the world. "It is in the interests of Shell to work with a set of internal policies and procedures rather than a complicated set of externally formulated legal agreements which have no added value."



WORKING PARTY INFORMATION: For the Article 29 Data Protection Working Party document on data transfers: http://europa.eu.int/comm/internal_market/privacy/workingroup/wp1998/wpdocs98_en.htm

ADDITIONAL INFORMATION: There will be a presentation by Peter Hustinx and Han Kooy on the "corporate rules" scheme at PL&B's 16th Annual International Conference, July 7th - 9th, 2003.