

Security - a minefield or a 'walk in the park'?

Roger Wilkins

Security is one of the major challenges facing all businesses in an environment where more and more focus is being applied to the protection of personal and corporate information while users continue to demand easier access to ever increasing volumes of data.

Add to this mix stories of hackers gaining unauthorised access to sensitive data and viruses afflicting workstations, and the problems facing the executive responsible for security appear to present an overwhelming hurdle.

It is easy to make a system totally secure. However, that would require isolating it from all your users and losing sight of the whole purpose of your IT investment, namely supporting and growing your business. The traditional threats to the business still exist and, with a few exceptions are the ones that cause the biggest headaches. Unless the system in question operates in areas such as Government secrets, military or nuclear design information, or medical data, some level of security compromise has to be acceptable in order for users to get their work done. The challenge, as always, is to strike the correct balance.

Risk Assessment

The first step in any security audit is to identify the objectives of the business operation for the system being considered, i.e. what is of more importance and what is of less importance. The relative status of each individual component in a business IT structure will vary between different businesses and systems within any given business. For example, an online web catalogue site that becomes unavailable, or that has a compromised payment transaction process, will very quickly cease to exist. An in-house payroll system, however, could survive a system outage of several hours, or even days at certain times in the pay cycle, with all but the IT and payroll departments unaware that there had even been a problem. Each IT process requires its own unique risk assessment - the risks to each of them may be similar, but the impact most certainly will not be.

In order to conduct a risk assessment effectively, the system must be analysed to identify each component, and the risks to, and impacts of, that component must be documented. The components involved in a system are once again unique to each individual case, but a number of high level segments are common to most modern systems. These are the client layer, transport layer and server layer. These equate loosely to the PC (or browser device); the network and possibly the Internet; and the web, application and/or database servers. Each of these areas must be assessed separately and the results aggregated into the overall risk assessment.

Threat evaluation

Once the individual risks have been identified, the likelihood of the event occurring and the impact on the business if it did occur are estimated. Once this stage of the process is complete, an estimate can be made of the costs of mitigating any of the events. In reality of course, any business, even the Microsofts and IBMs of this world, will have an available budget for these issues and some sort of trade-off between cost and risk will need to be made. What is the point, for example, of securing the payroll system mentioned earlier against a power failure lasting more than around 10 – 15 minutes, or the time taken to ensure the system is shut down

in a secure manner to prevent file corruption?

Client side

Assuming that the business has effective network perimeter security in place, such as a firewall and anti-virus detection equipment, the biggest threats to the system on the client side are internal. Loss of power, telephone services etc, or flood or fire are likely to have a wide ranging impact that will not be confined to the IT client terminals. The threats vary from poor adherence to security policy, such as selection of easy-to-guess passwords or leaving passwords on post-it notes stuck to screens, to opening email attachments from unknown sources. Laptops are taken home and plugged into insecure broadband connections and portable devices lost. The increasing use of pocket devices containing sensitive information, including passwords, also brings additional threats to security. The best solution here is to ensure that adequate security policies exist and that staff understand the importance of following them. It is of course vital that any deliberate attacks by disgruntled employees are identified by system processes, where possible, and that good general management techniques are used to identify potential problem areas. A member of staff with a grudge has many areas where he or she can create mischief, not just in IT.

Transport layer

The risks here are dependent on the traffic being carried and who has access to the network at a low level. If you are a small company using a hosted web site, the only network traffic is accounting and stock information which is protected from transmission across the Internet by good network technologies. Where email and Internet usage is light and you do not use a wireless LAN, the risks from external threats at this level are small. If, however, you are a company dealing in financial transactions with clients' personal details being transmitted across the web, then ensuring this information is secure is not only critical to the business, but there will be legal implications if it is not.

Server layer

The risks that are most damaging to the business, and those most likely to happen, occur here. The risks of theft, power failure, fire and system breakdown still represent the biggest threat to the business and must be protected against – there is no choice.

The additional threats to systems security brought about by hackers and malicious software are also largely targeted at the server and the data contained within it. Solutions to the problems in this area include standby power supplies (Uninterruptible Power Supplies (UPS) or generator or both), fire detection and extinguishing equipment, intruder alarms and good physical security. If the risk merits the cost, then biometric security and security guards may also be justifiable.

Database security and, in particular, questions of access rights and audit requirements are of concern to everyone, but financial services organisations in particular have legal requirements for compliance.

At the next level, secondary utility and telecom services, backup firewalls and virus defence mechanisms are all required to ensure continuity of service for mission critical systems. A review of system security must be undertaken at regular intervals and must be monitored continually to ensure adherence to standards. It cannot be done once and forgotten.

Ensuring your system is secure

System security should be designed into the process with the all other functionality – it is

not an optional extra. It is possible to build in security later, and with new threats emerging and system requirements changing, it will be necessary to introduce additional software or physical or network level security at regular intervals. Security specialists exist, but how do you know that the one you engage really knows the solution until it is potentially too late? You could train or buy your own in-house security specialist, but what happens when he gets bored (it's not a full-time occupation in many organisations) and leaves! You could get someone to do the job alongside their normal responsibilities, but they will inevitably drop the security work when their normal duties become urgent. You could outsource at least the server side and many of the network issues by co-locating your servers into a data centre. All the physical security is provided, and because it is a shared centre, the costs are spread amongst many users. Perimeter data security is similarly taken care of with high quality duplicated devices configured and managed by skilled technicians whose sole purpose is to ensure that security remains intact. Power and telephone services should be duplicated and back-up power supplies in the form of large Uninterruptible Power Supplies and backup generators are normally part of the service.

The Application Service Provider (ASP)

A potentially cheaper alternative is to take advantage of an increasing number of utility computing providers, or ASPs, providing not only secure data centres, but software services with inbuilt security features. A good ASP service will not only ensure that the physical and environmental security is as good as possible, but the network and server level security will be up to the very latest standards. Firewalls should be updated with the latest protection constantly, not daily or hourly, but minute by minute. Sophisticated issues such as Denial of Service attacks will also be dealt with by the service provider. Data level security should similarly be world class, with the ASP ensuring that security encompassing link-level, end-to-end and application level encryption is applied as appropriate to ensure that information is kept secure at all times.

The use of an ASP does not absolve you from responsibility for security, it is merely a way of ensuring that the best available security techniques are applied to a substantial part of your IT infrastructure in a cost effective way.

As businesses become increasingly vulnerable to security breaches and more dependent on technology, it is important to take sensible precautions. The facilities at Shadow, a credit management company that depends on reliable high volume data transfer, are an example of such technically advanced facilities. Their ASP services are hosted in a brand new £90m data centre with multiple utility suppliers, uninterruptible power supplies and standby generators with sufficient capacity to run the centre at full capacity for an unlimited period. There are three layers of physical security, biometric pass security to server rooms and multilayered network protocol security with builtin redundancy. The hosting centre operator conforms to BS7799 (ISO17799). The option of duplicating services in a second data centre is also available for the ultimate in non-stop computing. Software development conforms to the latest standards in web and database security techniques.

No business can be sure that there will not be a security breach but, by deploying the best technology in a professional way, they can reduce the risk to the minimum.

Roger Wilkins is Technical Director for Shadow Credit Management