

Driving down information risk

Whilst some areas of risk management such as credit and safety risk are well established and seen as an essential part of running a successful and responsible organisation, few can claim a sound method of measuring and managing information risk

This is a surprising fact when you consider that that most organisations - whatever size - are more than ever acutely aware of the potential threats to their mission-critical IT systems and the impact of losing or losing access to essential or sensitive data. As a result, tackling information risk is now rapidly rising up the 'must do' list of IT directors and poised to be one the largest and fastest growing areas of risk management and IT security.

In the latest biennial Information Security Status Survey, The Information Security Forum (ISF) - an independent not-for-profit global association of large organisations that recognise the importance of protecting their business information - found that a business critical information resource will, on average, suffer some kind of information incident 260 times a year. This amounts to an incident every working day. And while many of these incidents may be minor, collectively they erode efficiency, prevent the attainment of business targets and increase costs. Information incidents include not only virus and hacker attacks but also software malfunctions and system response or availability problems. Surprisingly, or maybe not, human error still accounts for the largest proportion of incidents.

Worse still, every business critical information resource has more than a 60% chance of suffering a major incident with loss of vital information over the course of a year. For example, this might be reputation-damaging IT security breaches, natural disasters or acts of terrorism and serious fraud. The average cost of these incidents based on real data from the ISF is surprisingly high - \$500k.

These are certainly compelling figures for IT managers and their Boards, but if this is the case, why isn't more being done to understand and cut down the potential

risks? It is not due to a lack of general awareness of the need to protect information resources, but unlike other types of risk to an organisation, information risk and its consequences are rarely understood and analysed in any detail.

So with tough financial constraints on any form of expenditure these days, it's difficult for IT management to go to the Board and ask for investment to plug a security gap and reduce information risk without any facts and figures to prove the need. In particular, quantifiable financial implications are usually needed to convince the financial director to spend money. Unfortunately it's often not until the proverbial 'horse has bolted' that senior management respond to close the gate too late.

Not only does good information risk management make solid business sense, it is also a key requirement of a growing number of corporate governance initiatives. So how can these challenges be resolved? Managing information risk starts with measuring the chance and potential cost of an enterprise suffering harm as a result of losing the confidentiality, integrity or availability of data processed by IT systems. But it also involves understanding that business is all about taking calculated risks. Therefore organisations need to decide what constitutes acceptable risk and at what point action is needed.

By being in a position to identify, measure and quantify levels of risk it is possible to make these judgements and put forward a case for getting necessary controls in place. There is a clear correlation between the status of controls and the likelihood of a major incident. According to ISF research, information resources with controls in good all-round condition are four times less likely to suffer a major incident than those that do not.

One way to measure and bring infor-

mation risk under control is to use FIRM, the Fundamental Information Risk Management methodology developed by the ISF to provide an informed and consistent way to measure and manage information risk across enterprises. Its development is based on over ten years' of statistical research into what makes business-critical information systems go wrong in real organisations. FIRM works by measuring the factors including level of threat, system criticality and control weakness which help determine the true level of information risk.

Armed with this information, IT, security and risk managers can identify and focus their attention on areas where information risk is unacceptably high. And importantly, they can now go to the Board and present strong and well-supported cases to target and maximise new expenditure on security controls to reduce risk and achieve corporate governance objectives.

In the information age, Board directors and executive management have a duty to protect the information resources of their enterprises, customers and partners. Only with a systematic and proven methodology that highlights the quantifiable and sustainable financial benefits of driving down information risk will senior management buy-in be achieved and information risk reduced. Companies for the first time can take control of their information risk.

Further information:

Citicus

Tel: +44 (0) 207 203 8405

Web: www.citicus.com