

Information security: who takes the rap?

Mike Gillespie offers risk managers tips on keeping company information secure

In the tough economic climate, security sits as a more important issue for business than ever. Risk managers are increasingly also responsible for migrating data leakages and security breaches. Helpfully however, there are a number of steps that can be taken to address physical security and information assurance issues, pushing the importance of getting the buy-in from board-level staff.

Following enactment of the Freedom of Information (FOI) Act in 2000, the media has profiled numerous high-level data-loss incidences, creating the perception that security breaches are on the increase. This is in fact, not the case. The problem has always been there but increased media attention has brought it to the fore. As such, varying figures within business are now responsible to guarantee information is more secure, both physically and logically. Perceptive readers may have noted that stories dominating headlines over the past two years are largely based on loss of laptops, sharing of protectively marked documents, encrypted memory sticks going awry, all of which concern the loss of confidential or sensitive data. The focus of these stories generally comes back to the technology that stores or shares the data, but rarely is the technology itself to blame. It is usually user error and carelessness, mainly due to lack of security awareness and policy training. Regardless of size, shape or purpose it is time for all organisations to take responsibility, by having the appropriate business processes in place instead of looking to IT for the answer.

As an independent protective security consultancy we come into contact with risk managers who suddenly find security now falling into their remit. As job roles merge during tough economic times and positions become blurred, risk managers are often unsure of their role within the organisation when it comes to security issues and how to address them.

Currently, the role of a risk manager runs much deeper than purely managing insurance responsibilities. They are now faced with the additional challenges and considerations for broader project, operational and enterprise risk management activities. We have noted over the years that these personnel come from all walks of life, including financial or health risk management backgrounds. Yet regardless of knowledge base they are in many cases, given the same high-level responsibilities,

Those taking up the risk management mantle have some of the most important and costly decisions in made throughout an entire organisation; however in most cases they are not given either board-level time nor consideration on the business agenda. Without the necessary backing from the chief executive figure, the risk manager is at a disadvantage when it comes to filtering security policies and procedures throughout an organisation.

Ultimately, the CEO is accountable for security, so gaining their buy-in as to how security is viewed by the organisation is crucial. By raising the security issue with each member of staff to understand its significance, companies can encourage them to take responsibility for their own actions. Those at the operational end will then start to see the value and make decisions based on this wider outlook, rather than relying on their own reasoning or instinct, which often can be misled. In one case we saw a CEO of an organisation adding an entry on their blog., outlining the fundamental importance of security. This one-liner in corporate materials or policies can really assist in gaining the buy-in from staff. While senior management disseminate the message down, risk managers can take effective action for security and information assurance on their behalf.

The task in preventing security breaches can seem an extremely intimidating one, especially as threats are often rife externally and from within. Foresight from the risk manager is key to assessing the true threats to a building, its contents and all information stored, rather than playing catch up after a threat has taken hold. Often, businesses only realise an item is missing when they come to use it. An effective way to combat this is to simply list all pieces of equipment and documents that are deemed 'essential' in an asset register. Each time a new worthy item is brought into that specific area it must be added to keep records updated. Only then can management understand what they are protecting and make best plans as to how to do this appropriately.

Once completed, the next step is to find ways to safeguard these assets. In some cases, it is deemed fit to

electronically 'tag' equipment. This is a useful but costly process to monitor assets and should be considered strategically before being implemented. As with all high-level decisions, any technology must be considered as part of the wider security strategy. Solutions do not work solely on their own, but as part of a 'layered' holistic approach whereby the environment and policies come together to form a robust and trusty business practice.

Another step risk managers can take is to conduct a quarterly threat assessment. Once all assets are established and recorded, a threat assessment enables businesses to understand their working environment with regards to risk. localised crime statistics, and detailing who requires access to certain parts of the building and why. This helps to address the 'opportunist' threat, where modus operandi might be harder to fathom – an independent view here often pays dividends. By establishing areas of concern, risk managers can look for measures to complement technology solutions they see fit for adoption. For example, the layout of furniture and walkways can be manufactured to direct people a certain way, slowed down for CCTV filming purposes or via a reception desk to ensure that visitors are directed to complement the wider security strategy.

Training for all employees is essential. As noted, breaches and data leakages are often instigated by the insider and not always of malicious intent. The most detrimental cases may be caused accidentally, whereby an employee fails to follow or is unaware of the preferred process. To address these incidences as part of the wider corporate risk strategy, risk assessments should be initiated. Treated with the same rigour as financial and health and safety assessments, the top 10 or 15 threats should also be analysed by using metrics and measurements, to ensure that the counter-measures put in place by a company continue to reduce the risk. Where possible, these assessments should be managed at a senior level, preferably by a SIRO (Senior Information Risk Officer), who will address information risks rather than IT risks. These often fall under the same umbrella, yet are very different entities. Again it is essential for this information to be fed into the board, thereby pushing the security issue up the management agenda.

Above all, technology should be seen as the enabler not the solution. With every technology, there is hardware, software and 'wetware'; the latter being the human element. The human unfortunately is the weakest security link. Every time a laptop containing critical data is stolen from an organisation, or a USB stick is left on a train, encryption is seen as the safety net. Although encryption slows down an intruder, it will not prevent them from hacking in and accessing the data. Ultimately it is the people element that causes the breach by leaving the USB behind or failing to lock the room containing the laptop.

Risk managers should always question why information was exposed to risk and whether it should have been stored on a USB, laptop or other media? By understanding the value of sensitive information and the 'five Ws'; the who, what, when, where and why, it may show that policies and procedures are what a business needs, rather than expensive technologies. Education is also essential and needs to be worked into each employee's training programme, if they are provided with a new piece of equipment to assist their daily working, not only do they need to learn about how to use the piece of kit, but also how to use it securely in hand with the company's agreed security policy.

Mike Gillespie, CIRM, is director at independent protective security consultancy Advent IM (www.advent-im.co.uk)

Risk Management Professional – September 2009