Information Security Now – 31

Basically, data loss, or breach, may be caused by three things: accident, deliberate attack or negligence. The most common accident is sending an email message, often with an attachment, to a wrong address, or list of addresses. This is akin to the much older problem of sending a fax to a wrong number.   Deliberate theft by an external attacker is usually well covered by security mechanisms, but the negligence area has tended to be ignored. I define negligence as 'failure to take proper care over something'. So it is neither accident, nor deliberate, but rather an omission by someone who is responsible for a process to consider all aspects of a risk. Negligence may be a new consideration for security professionals, but as a self-styled control expert I consider it to be a significant challenge, simply because it seldom appears on any list of anticipated risks.

I facilitate the occasional risk workshop dealing with data loss and I am always surprised by the lack of clarity and imagination of the participants. This is often reflected in the subsequent risk register, which is the main outcome from the workshop. After all, if you fail to identify a risk, then you also fail to consider the relevant controls. Even where a risk is identified it is often the case that the associated controls do not adequately address it. Over the years I have developed a process which helps to tease out the generic risks, but I am still dependent on the delegate's local knowledge of their infrastructure, management structure, work flows and the like in order to develop a comprehensive risk register. The other challenge I have is the delegates' lack of appreciation of the prevention, detection, reaction sequence. In much of modern data processing, prevention is very difficult, especially where you have allocated privileges which allow a person to do something as part of their normal duties.

As an example, if you have allowed someone the privilege to view a record, then it is likely that they can also copy it. The copying may be from a simple screen shot, or by a comprehensive download, but either way there is an opportunity for a data breach. I prefer 'breach' to 'loss' because if something is copied it is not 'lost' in the accepted sense and this itself presents a problem. If something is 'lost' in the tangible sense, then you are likely to know that it is missing. With copying however, you still have the original, so may have no idea that a breach has occurred. An example. A NHS Trust was updating its patients' records database. It used temporary staff for this exercise and provided them with access, read and amend privileges to their secure patients' records system. They were also required to sign a non-disclosure agreement. One of the temps decided he would prefer to work from home so he downloaded sixty thousand patient records to the hard drive of his work station and then copied them to his smart device. He subsequently lost this on the way home. Had he not reported it the Trust would have been none the wiser of the security breach as nothing was 'lost' from their database. The non-disclosure clause in his contract was worthless.

So prevention is difficult, but detection may well be impossible. Of course, the fear of detection may itself act as a prevention mechanism and this is what many organisations rely on. There is some research to support this view along the lines that in any given population one quarter are honest, another quarter are dishonest and the remaining half are only as honest as the system under which they work require them to be. So if we can persuade the potential perpetrator that detection is certain, then we force this half into the honesty total, so we then only have to worry about the basically dishonest ones; which may still be a very big number. Which, as I pointed out to one organisation, who for a fee was eager to share your personal data with up to a third of a million people, meant that over eighty thousands of them were potential data thieves. Its prevention ‘control’ for unauthorised disclosure was the contract signed by the trusted partner - not the individual staff members. When I explained that this did nothing to prevent a member of staff from the trusted company disclosing the personal details to the press there was disbelief that anyone would break a contract. They could not conceive that the contract was neither a prevention, or detection mechanism. I see this in risk registers on a regular basis. The listed controls are often just processes which do nothing to address the risk.

On the detection side, it may be nice to have for damage limitation purposes, but it may well be far too late for reputation protection. It really depends on the nature of the breach and the response from the data custodian. A few years ago I was unimpressed by the response of one of the building societies to the loss of an unencrypted laptop containing six million customer records. They first refused to acknowledge the scale of the problem and subsequently refused to disclose what information had been stolen, although their subsequent reissue of every customer’s bank card provided a clue. On the other hand I was quite impressed when one of my credit card providers contacted me by SMS to alert me to the unauthorised use of my credit card. They hadn’t prevented it, but in this case their swift response gave me a comfortable feeling that they were looking after my interests. External attacks of this nature, which are really data creation rather than data loss, are far easier to identify than unauthorised copying by a privileged member of staff. So now we come the real nub of the problem. If you provide privileged access, then there is little you can do to stop unauthorised disclosure, or misuse of the accessed data. In my support I cite Edward Snowden. I bet that he too had a non-disclosure clause with his employer.

John Mitchell

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of Council and chair of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638