Information Security Now – 35

The correct information at the time and place of need is what every manager desires. To this we need to add the requirement that the information complies with the statutory and regulatory framework. Every security manager quotes confidentiality, integrity and availability (CIA), but the compliance aspect is equally important. Indeed it may be argued that it is more so, because what is the point of having good CIA if you can go to prison for a breach of the law? As an example, one could design a secure image collection, storage and retrieval system which meets all necessary CIA criteria, but if the images are of a paedophilic nature, then the CIA aspects are trumped by the compliance criterion. Likewise, one could have really excellent CIA for government secrets only for these to be put into the public domain by someone who breaks the compliance (secrecy act) requirement. Even the collection of the raw data may be in breach of compliance requirements, as may encoding it and transmitting it in an encoded format. It just depends on where you are in the world and what the local regulations are. You can be arrested in the USA for processes run in in the UK, as the CEO of BetOnSports, the on-line gambling company, found to his detriment when he was hauled from an aircraft which was simply transiting through the USA. Although the bets were processed in the UK, the transactions passed through US networks and on-line gambling is an offence in the USA. Even ignoring the compliance aspects we may face major problems with data integrity due to the way the data is initially collected. Data entry, or garbage in-garbage out (GIGO) as it is better defined, needs far more attention than it currently receives. Simply eyeballing an entry and them pressing the Enter key canlead to a nearly two percent error rate. Even when coupled with instant validation of the entry the error rate is rarely reduced to zero. If the data quality rules allow a range, then anything within the range will be accepted regardless of its integrity. Even where only an absolute entry is allowed, such as gender, the resulting entry of M or F may still be incorrect, as we found from comparing gender with operation type in a patients' records system, where we found several males associated with hysterectomies! We know that we are not going to get absolute data integrity at the collection stage, it simply depends on how much additional care we are willing to put into those data items that really matter. We may decide that we can live with incorrect post codes, but not with incorrect account numbers. The risk analysis should determine what is acceptable and then we should design the controls to provide for that level of acceptability. Control design is both an art and a science and really should be done at the system design stage. Ideally we should generate a table of data quality rules for each data item. The challenge here is that the data may be one of four major classes: configuration, standing, derived, or transaction. Each of these has its relative level of importance. For example, configuration data may impact on the entire system, whereas standing data will only impact on the transactions to which it is applied. Derived data usually uses some standing and transaction data manipulated by some logic. So there is even more opportunity for the resulting information to be wrong. We once found a bug in a Unix compiler which resulted in a numeric one divided by a numeric one not equalling a numeric one, which made a real mess of the information being produced. Even if the compliance and integrity aspects are okay we still need to consider the availability and confidentiality aspects. The data may produce accurate information, but if that information is not available at time of need then

it is totally useless, as NATS found when it had to close a significant part of UK air space due to their air traffic control system failing. With real-time information systems the failure to deliver at time and place of need is immediately known to the customer, whereas an integrity problem may go unnoticed for yesrs. Which brings me to the confidentiality aspect of CIA. We spend vast amounts of money in trying to ensure that only authorised people have access to our data, but as I have argued previously, once you grant privileges, then your entire control framework is based on the trust you have in that individual and trust is not a control, It is a hope. I was taught to hope for the best, but plan for the worse. I am sure that Sony corporation wish that they had spent more time on the latter.

John Mitchell

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of BCS 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