Information Security Now – 40

John Mitchell

Most organisations focus their security efforts on preventing and containing external threats. This is their Achilles heel, because these defence mechanisms do little to prevent, or contain, a threat from one of their own staff, which research[1] has indicated as being a greater threat than external attacks. This in itself is not too surprising due to what I call the trust paradigm. Chief Information Officers believe that they have to trust someone and go apoplectic when asked why? I am sure that the NSA trusted Snowden until it was too late. That is the problem with trust. It is not a control mechanism, but a faith, which you only find has been broken when it is far too late. I have wasted the last thirty years of my life trying to persuade organisations that information security is a human, rather than a technical problem. The pro-argument is, I believe, pretty much self-evident. It is people who create the security infrastructure and it is people who break it. They may use technology to do so, but the starting position is the human. The Human Resources department initiate's the employment, regular assessment and termination processes, so perhaps the starting point for information security should be there; especially when one considers the insider threat?

Research has shown that for any given population twenty-five percent are basically honest, twenty-five percent are dishonest, with the remaining fifty-percent being only as honest as the system under which they operate requires them to be. So, if we have strong information security we only need to worry about the bad twenty-five percent, but if we have poor security that increases to a whopping seventy-five percent. Now, it is HR's job to help weed out the bad twenty-five percent by initiating good pre-employment practices such as reference confirmation and it is management's job to keep an eye on their staff through the regular appraisal process. However, even with these in place there is still the possibility of a disgruntled member of staff taking things into their own hands. Never mind the reason. Motive does not concern me; it is what they can do that counts. The problem then becomes one of privilege allocation. If it is a lowly clerk, then they will be constrained by their low privileges, although even this can cause problems as we will see later, but if it is an IT specialist with super-user privileges, then there is little that can be done to constrain them.

The lowly clerk with only read-only access may still be in a position to pinch your customer database, or release sensitive data into the public domain. This can be hugely damaging, but at least your IT is still functioning. The IT specialist can kill your IT and possibly your company. So the first lesson is that you cannot prevent people from using the privileges that you give them. The second lesson is how soon will you know that you have a problem employee? Are your detection mechanisms sufficiently fast and do they collect enough information to identify the perpetrator? When Edward Snowden stole that secret information from America's NSA the first they knew of it was when it appeared on Wiki-Leaks, which was hugely embarrassing. We now enter the

[1] Internal Vs. External Penetrations: A Computer Security Dilemma http://www.cameron.edu/~pdiaz-go/SAM3049.pdf

realms of whether, or not, even a robust detection and response process will act as a deterrent? If they do care about being caught, then your detection mechanism will act as a deterrent. One up to the good guys for keeping the fifty-percent honest. However, if they do not care about getting caught, then you are up the creek without the preverbal paddle. So what can be done about the insider threat?

First, you need to accept that the really bad thing will one day happen. So plan your response for the worst case scenario; just use your imagination and then some. Plan your reaction accordingly and be ready to scale up your media response ten-fold. You may think this a little negative, but I am just being realistic. You cannot stop the bad thing, because you have provided the privileges, so you had better have a good reaction plan. Having got that in place we can now go to the front-end to make it as difficult as possible for an individual to damage the company. It is for a reason that the firing trigger for a nuclear weapon needs two people to operate it. For really important things, require two, or even three people to run the killer app. One to authorise, one to initiate and one to release. Remember, this may relate to quite simple things such as copying a database, emailing sensitive files and allowing foreign flash drives into your USB ports. You need to do a proper risk assessment. Most organisation that I have dealt with are inherently insecure because of poor risk management based around he misplaced trust paradigm mentioned earlier. We assurance professionals have a mantra; ‘trust, but verify’. I spend a great deal of my time verifying control effectiveness by conducting control stress testing. This process takes the following steps. I first ask what is the control’s objective (what is it meant to achieve), then I ask how is the control meant to achieve it? Next what type of control is it (there are seven control types); how good is its design; has it been correctly implemented; how frequently is its operation monitored; how often is its effectiveness evaluated? Once I have gone through this process I find that most so called controls are not controls at all, but are simply processes and aren’t worth the paper they are printed on. This is really disappointing to the control’s designer and it becomes even more depressing for them when they tell me that it’s meant to prevent an insider threat …. and I tell them that it score’s zero on my control effectiveness scale. It’s not really their fault. Very few people have been trained in designing any controls, let alone effective ones. It’s one of those skill sets which seem to have gone the way of batch systems.

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of BCS Council, it’s Audit & Risk Committee 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