

Information Security Now – 32

The risk equation has two components; likelihood and consequence. The consequence is pretty much an absolute in that we can reasonably anticipate the outcome, but the likelihood is pretty much a guess. The biggest challenge in dealing with risk is uncertainty; will it happen, or not? So risk management is not a science. It is not even an art. Risk management is predominately witchcraft in which the necromancers (risk managers) recite their spells and incantations to anticipate the likelihood of something nasty happening. But ultimately it's all a guess. Now guesses are not necessarily bad and we know that a Delphic poll (see later) is likely to provide at least a consensus of the likelihood.

Some readers may be aware of my interest in the Search for Extra Terrestrial intelligence (SETI) project. My interest is not so much that the ultimate outcome will be important for mankind, but rather the sheer scope of the data mining exercise and the use of distributed processing. There are also the underlying assumptions to be debated such as is there anyone else out there, are they transmitting and are we scanning the right energy spectrum? Lots of guesses. Both the scope of the project and the correctness, or otherwise of the underlying principles, are of particular interest to me as a computer auditor. Let us start with the principles. The assumptions are that other intelligences will try to contact us by sending intelligible signals in the radio spectrum at frequencies that we can both detect and are listening to. These are huge assumptions. It may well be a very dangerous universe and advanced civilizations may well want to keep their existence secret. Even if this is not the case, then the secondary assumption, that the signals will be modulated in a way that we are familiar with and can decode is equally debatable. Let me provide an example. Most of our terrestrial radio signals currently transmit analogue information. In the near future analogue transmission may be replaced by digital. Therefore anyone listening on an analogue radio set will be unable to make sense of what they are receiving even though they are listening on the correct frequency. If off-world intelligences are broadcasting in some other medium, then the entire SETI project is a waste of time. On the subject of which frequencies to listen in on, the SETI assumption is that nature provides a nice way of establishing what these should be. The simplest 'stuff' of the universe, neutral hydrogen gas in interstellar space, emits radio signals at 1.42 GHz. Another molecule in space, the hydroxyl, or OH, emits at about 1.64 GHz. Now if you look at these two, H and OH, you would see that together they make up the compound of water HOH (or more commonly H₂O). Life as we know it requires water to evolve and exist. The frequency range between these two emissions, from 1.42 to 1.64 GHz, is therefore a region of the radio spectrum called the 'water hole'. Where would you expect water-based intelligent civilisations to meet? Around the water hole, of course! So is the assumption correct? Only time will tell. That aside it does have one of the prettiest screen savers that I have come across.

Applying this to my little world of assurance I have noticed that most of my important findings have been as a result of detecting something that I did not expect. In many cases this was as a result of data mining. As an example, I would not normally expect people of a male gender to have a hysterectomy, but I have found this interesting combination when data mining hospital patient

records. The fact that I found it was because I could understand the underlying data structures. Unlike the SETI participants I could be sure of the communication medium. Having found the strange combination of male+hysterectomy it was intuitive to examine the data quality rules on the assumption that the input validation routine was letting through an invalid combination. This was the case and my understanding of the data allowed me to detect a software anomaly. This is more difficult with SETI for two reasons. First we cannot be sure of the communication medium and secondly we do not know what the message should look like. I have had my share of data mining failures based on an incorrect understanding of the data. I once spent days trying to extract data from a file without success only to find that I was using an incorrect file layout description. My understanding of the signal was flawed. SETI could be in the same position.

The dribble of information from the Edward Snowden archives has revealed that America's National Security Agency is struggling in sending locally intercepted information back to America for data mining purposes. Not enough bandwidth. Perhaps it should adopt the SETI principle: break the data into chunks and get it analysed by local machines with only the important stuff then being sent home. They could dress it up with a fancy acronym, such as SETI (in this case Shared Exchange of Taxpayers Information) and provide a pretty screen saver too. I was once taught that one should never rely on secrecy as a control mechanism. Nation states do not seem to appreciate this.

If you are aware of the concept of a 'Delphic' poll you will know that if you ask a sufficiently aware and suitably large population it will intuitively predict the likely answer. This is important for estimating the likelihood component of the risk equation. Even if the answer is wrong it achieves a sort of consensus. On that basis the SETI survey predicts that we will detect the first ET signal within the next 90 or so years. To long for me, but if I see any little green men, or pink elephants for that matter, then they will probably be self-inflicted. My computers however, will continue their patient search with unflagging diligence. Assuming that the power stays on.

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