Information Security Now – 34

I have been re-reading Sun Tzu's *The Art of War*. 'Know thy enemy' is the mantra chanted at all military colleges, but it is only part of the quotation. The full reference reads, 'If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.' So, it's not just knowing your enemy's strengths, but also your own weaknesses. This implies that cyber defence requires, at a minimum, the identification of an adversary, knowing their capability and intent and comparing this against your capability to neutralise them.

So the first challenge is to identify your enemy. Is it a nation state, an organised group, or an individual? Will the attack be launched externally, or from within? Will it be against a specific asset, or against the network as a whole? Capability is not the same as intent, but if someone has the capability of conducting an attack, then it is prudent to assume that at some stage they may do so. The concept of mutually assured destruction (MAD) has prevented the use of atomic weapons by nation states for some seventy years, so there is a precedent for having a defensive capability based on hurting your adversary in the same way they may hurt you, but that philosophy assumes that you know the physical location of the enemy. Not so with cyber warfare, or even cybercrime. So perhaps we should begin by separating the former from the latter. Governments should assume responsibility for protecting its citizens from cyber warfare and for policing cybercrime. This does not negate the need for entities and individuals from taking proactive steps to protect themselves from attacks by groups, or by individuals. Akin to locking your door when you leave the house and perhaps setting your intruder detection system in case they are able to bypass your entry system. In fact, from a defensive point of view, perhaps we shouldn't bother to try to identify the enemy at all, but make it difficult for all potential enemies. Rather like our firewalls. We really couldn't care less who is 'pinging' us, or from where, providing we don't let them in. This type of passive defence may appear wimpish, but another quotation from Sun Tzu, ''the greatest victory is that which requires no battle' is supportive of this approach. If our defences are sufficiently strong, then our potential adversary will most likely expend their energies elsewhere, in much the same way that a burglar will more likely target a non-alarmed house.

The real challenge, however, comes from within. We give great privileges to highly intelligent people while knowing that in any given population we face the quandary that around one quarter are basically dishonest. I have previously dwelt on the conundrum of 'you have to trust someone'. Trust is not a control, it is a hope. Hoping that something won't happen is the negligence of the truly incompetent. I was taught to hope for the best, but plan for the worst. So on that basis, if I have the capability to conduct a denial of service offensive, then so does my enemy. If I have the capability to infiltrate a system and steal card details, then so does my enemy. If I can intercept and decode in-flight transactions, then so can my enemy. So, from any perspective we should anticipate the worse and plan for it. Breaches of confidentiality, breaches of both data and software integrity and service non-availability must be rigorously risk assessed and appropriate controls implemented. A rigorous and continuous risk analysis is essential. We really do need to think outside of the box, as is shown by the recent subversion of a Canon printer to run a video game. If a wireless networked printer can be subverted to run a game, then what else could it be used to do? I mentioned in my last column that many controls are ineffective in managing the risk that they are meant to be addressing. When challenged, the responsible management reveal their ignorance by stating that the crystallisation of the risk is unlikely anyway. Unlikely it may be, but what if it happens on their watch?

Control assurance for cyber systems can be far more reliable than for a manual system because the technology will behave as we predict. Not so those processes where the control element is a free-willed human being. It was Edward Snowden who stole those NSA secrets, not the devices on which the data resided. His theft was aided by the technology, but not conducted by it. Ultimately it was a betrayal of trust, which shows just how useless trust is as a control mechanism. We now have the ability to identify, classify and predict the effectiveness, or otherwise, of a particular control in a specific situation. We can run simulations to calculate the control effectiveness as a percentage of total control. We can identify our weaknesses and hopefully rectify them before the enemy finds them. Penetration Testing, or Intrusion Testing, as my more sensitive American colleagues call it, is a prime example of forewarned is forearmed, but I am constantly amazed as to how few organisations do this on a regular basis. ‘Too expensive’, I am often told by people who have apparently not done any form of cost-benefit analysis.

Not all cyber related threats are attack associated, but they can be just as deadly. As an example, one of my clients was found to be running £750,000 worth of unlicensed commercial software. Not due to any criminal intent on their part, but simply because of sloppy asset control. Another was fined £50,000 by HMRC because of incorrect VAT collection. Again, nothing intentional, but a result of poor change management. A third was fined £1.6 million by the FSA for poor spreadsheet control. Another has been unable to release a £90 million software development because they had not considered data protection at the design stage. The Home office cancelled a £347 million immigration system before it went live as being not fit for purpose. If organisations cannot get these things right, then what chance do they have they of countering deliberate attacks?

In the last two years we have had Edward Snowden steal an unknown number of secrets from the NSA, e-Bay has had nearly 150 million account details stolen and Home Depot has at last owned up to the loss of 60 million payment card details. What a shambles? I assume that each of these organisations had a Chief Security Officer backed by a host of professional security managers and administrators working to international security standards. They should be thoroughly ashamed of themselves. I conclude with a final quote from Sun Tzu. ‘‘Engage people with what they expect; it is what they are able to discern and confirms their projections. It settles them into predictable patterns of response, occupying their minds while you wait for the extraordinary moment — that which they cannot anticipate.’ Therein lies the challenge that we face.

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