Information Security Now – 9

John Mitchell

My various internet financial services companies range from banks to ISA providers and I regularly buy things over the web using my various credit cards. The banking sites now require three factor authentication and I feel fairly safe in dealing with them on the basis that it is so difficult for me to make a payment that any thief will die of boredom before he can emulate my card details, letters from my special word and the card itself. Not so with the average ISA provider or retailer who in some cases kindly ask me if they can keep my credit card details to make subsequent purchases easier for me to complete. Now I know a great deal about the PCI security requirements and just how far most companies have got in matching these and I know a reasonable amount about human nature. We can control the technology, but can only manage people, until the government gets us chipped at birth that is. We manage people through policies, standards and procedures. The problem is that people are notoriously unreliable. They are also subject to pressures that the technology is not. Over worked, underfunded, emotionally unstable, in love, out of love, the list is pretty much endless. We can see inside the technology. Us auditors have tools which makes the invisible visible, but we cannot see inside people's minds and neither can anyone else.

The technology does not defraud you, it is the people. Us auditors believe in division of duties. The more people you involve in the process the less chance there is that they will all be crooked at the same time. This is very much like two/three/four factor authentication. So here is my solution for protecting sensitive data:

1) Split the individual elements of key items between three databases. so that no single database has sufficient useful data in one place (so sort code, but not account number);
2) Any individual database administrator is only allowed access to a single database;
3) Any requirement to combine the elements to provide useful information will require the authorization of all three administrators.

The three databases will be in geographically separated locations, preferably on different continents, so that the administrators cannot meet All databases will be encrypted as will any other storage device. All data transfer will use strong encryption and the data will only be provided in clear for a specific purpose and a limited time, after which it will be destroyed.

So if I agreed that they could hold my card number it would be split between the databases, with the CSV and other authentication information also split. Nine times out ten the reassembled information will not need to be available in clear.

We should never rely on secrecy as the *control mechanism*. Rather we should put multiple controls in place to preserve the secrecy of the data.

The actual control mechanism will *always* get into the public domain, but the strength of the control should be capable of defeating any attack. In-depth control is initially expensive to implement, but as Gordon and Loeb have shown in their "Economics of Security Investment" the incremental cost is low in comparison to the protection provided by doing so.

We auditors have techniques for assessing control strength and these have shown that a single control is seldom more than sixty percent effective in mitigating a particular risk. As the risk equation has two sides (likelihood and consequence), then we need a minimum of two controls to manage a particular risk. If however, a single control is only 60% effective, then it stands to reason that we need a minimum of two controls on each side, a total of four, to deal with a specific threat. This is what I mean by control in depth. Every security mechanism that I have evaluated comes out very poorly on total effectiveness.

When I was a member of the BCS Security Committee, I evaluated several electronic voting pilots. In every case there was no protection from authorized staff meddling with the results. The protection mechanism was always focused on an external threat whereas my risk analysis showed quite clearly that the real threat was from the inside. IS security is currently being conducted in the same way that the drunk looks for his keys under the light of a lamppost. When asked where the keys were lost, the drunk replies up the street, but the light is so much better here. We are looking in the wrong places because it is often easier to do so than looking in the dark places.

The old adage that hope is not a strategy applies to security. Hope for the best, but prepare for the worse.

John is editor of BCS IRMA's award winning *Journal* and Managing Director of LHS Business Control, a corporate governance consultancy that he founded in 1988. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or +44 (0)1707 851454.