

Changing the hearts and minds

One of the most able administrators in the dying days of the British Empire was Gerald Templar who served as British High Commissioner in Malaya during the Emergency. He arrived in 1952 after his predecessor had been assassinated and with rising concerns that the country was drifting towards anarchy. Yet by the time he left in 1954 Malaya was well on its way to a peaceful independence. Templar achieved this by recognising that the best approach when dealing with alleged grievances was not through “pouring more troops into the jungle, but in the hearts and minds of the people”.

I suspect quite a few of today’s CIOs should take heed of Templar’s tactics when looking at how best to address their own security challenges. The task of securing the IT environment is certainly not getting any easier. Despite the economic downturn two independent global studies last year by Ernst and Young and PricewaterhouseCoopers revealed that around 50% of CIOs surveyed expected their investment in IT security to increase in 2009. As both reports highlight, in the integrated, globalised business world of today the integrity of an organisation’s information asset is an essential component for success.

Yet the evidence from both studies seems to be that CIO’s are ‘going through the motions’ in addressing IT security threats. They seem to be operating under a belief that because they have purchased new security solutions and because they have satisfied legislative compliance requirements they are somehow more secure. This was perhaps best illustrated for me by an example provided of Hannaford Supermarkets in the United States. This sizeable retail operation suffered from a significant theft of customer credit and debit card data over a three month period in early 2008. Yet, as this was happening, the company was trumpeting that it was compliant with the new Payment Card Industry Data Security Standard (PCI).

In fact the very thing that PCI was designed to prevent occurred in a high profile organisation that had made a significant commitment to complying with this standard. Clearly, as the Hannaford example demonstrates, compliance does not ensure security. Instead, the practices inherent within the security standard have to become part of the culture. Unfortunately, it would seem that in their approach to compliance requirements too many CIOs see the task at hand as one of being able to tick boxes. However, without living and breathing the controls within the compliance regulations there will be no real protection.

In a similar vein the same could be said about the escalating investment in IT security technology that both reports highlighted. The days are long gone when IT security was seen as virus protection and the use of firewalls. The use of more advanced security technologies like data encryption is growing around the world. Moreover, users have taken significant advances in securing their Web/Internet capabilities with large numbers of CIOs deploying the protection provided by secure web browsers, content filters and website certification. More are also using virtual private networks to safeguard remote access to their systems.

These responses are encouraging. I have no doubt that this functionality will assist in providing greater protection to IT environments. However, I very much doubt that this is all that is required. Unfortunately, it seems that too many CIOs are looking to technology to be some sort of silver bullet that will solve all their IT security hassles. In my mind that can be the only explanation of why a large number of CIOs are still not doing more work in establishing IT security plans and standards. The Ernst and Young analysis reported that only 30% of CIOs had implemented a

recognised IT security standard and that 29% had no documented information security strategy. The figures were even more troubling in the PricewaterhouseCoopers study which showed that only 59% of those surveyed had an overall information security strategy.

These low adoption rates for security standards and strategies are a concern. In the words of the PricewaterhouseCoopers report these approaches articulate “coherent, enforced and forward thinking security processes”. Embracing them is a recognition that effective IT security can only be provided through a change in corporate culture. Documented strategies and standards aim to do just this. Using technology to enhance security without an appreciation of the full change management task does not show much real resolve for the task at hand.

This weakness was further evidenced in a shocking ignorance that many respondents had to the number of security incidents that had taken place. 35% of respondents to the PricewaterhouseCoopers study were unsure how many security violations had occurred in the past year. Furthermore, 46% did not know the nature of these breaches and 42% had no insight in to the source of the incident. While it might be unreasonable to expect a CIO to have a handle on all these events this overlooks the fact that proper procedures were clearly not in place to document the security infringements that had taken place. Moreover, these findings also highlight the likely absence of a review process in many businesses which should provide the analysis to ensure that these security threats do not re-occur.

These drawbacks are compounded by the growing use of outsourcing in the provision of IT in business. Recent research by Ernst and Young in Europe showed over a third of organisations were planning to, or had, embraced IT outsourcing. Yet very few respondents seemed to attach any rigour to assessing the security capabilities of these third party suppliers and partners. 29% of respondents to the Ernst and Young study stated they performed no security reviews or assessments of how these third party organisations were protecting the information assets of the business. In many ways this security nonchalance can only be a matter of concern for these suppliers. They are likely to be blamed for any security incidents that occur. Yet they are obviously working for a client with a corporate culture of being lackadaisical in its approach to the challenges of dealing with IT security.

This then brings me back to the example of Gerald Templar. He recognised that in subduing the security threats confronting his administration he could not just deploy more and more resources. He saw that in the end the real challenge he faced was winning over the people affected. In a similar vein the same could be said about IT security. It is undoubtedly a good thing that business is prepared to invest more monies towards IT security. However, eventually they will want the assurance that these investments have been productive. If the IT department keeps getting more and more money but the problems of IT security keep escalating then the only real outcome will be a further blemishing of IT’s already tarnished business reputation. Instead CIOs need to demonstrate that only when IT security is owned by everyone in the business can the challenges around it be overcome. As Gerald Templar demonstrated back in Malaya in the 1950’s, this requires IT to win over the hearts and minds of the IT user community by showing them why supporting this task is in their best interests.