

Securing with Sapphire

There has been much news in the press of late surrounding high profile leaks of information, from organisations including the government and the military. Whether it is discs being lost in the post, hard drives or laptops being stolen, or information simply being left on trains, the security of information is becoming a major concern for many organisations. As a result, organisations are beginning to look at ways of ensuring they are meeting compliance standards and that confidential data is kept secure.

One organisation that is well ahead of this trend is the National Centre for Social Research (NatCen), the largest independent social research institute in Britain, which began implementing information security procedures more than two years ago. The organisation designs, carries out and analyses, research studies in the fields of social and public policy, including extensive research with members of the public.

Moving towards compliance

As Stuart Chapman, director of Facilities and IT at NatCen explains, “our initial move towards compliance was driven by customer demand. When we submitted tenders to clients such as government departments, they would ask if we complied with ISO27001, formerly known as BS7799, so as an organisation we began looking into whether we should be meeting with these standards, and how we would go about achieving this.”

From this starting point, NatCen began an informal tender process to find a partner to help them reach ISO27001 compliance and selected information security advisor Sapphire. The decision was based on the company’s method and approach to achieving compliance and its thoroughness.

Stuart Chapman explains, “The other company that we looked into said that they would effectively write our security policies and then present them to us, giving us very little input into the process, whereas Sapphire said that they would guide us through the process of writing and implementing new policies leaving us with a sense of ownership. In our opinion, their methods seemed very thorough and thought out.”

From this initial introduction to actually working with the company, it was only a short period of a couple of months. The first step in the move towards compliance was to carry out a GAP analysis to assess where the organisation was in terms of its culture and with respect to information security.



Policy Development

From this basis, Sapphire was then able to make recommendations as to which standards were applicable to NatCen and how they could go about developing these policies. The initial GAP analysis identified areas needing improvement. Sapphire worked closely with senior departmental representatives to agree policies and procedures and demonstrated how these would apply to their areas of responsibility.

As Stuart Chapman describes, "In the early days of the project, Sapphire provided excellent advice on how policies should look, they then discussed with us as a group how we should implement them. Formulating and implementing the new policies could take anything from a day to a year and a half, as you come to terms with the detailed practical implications of what implementing the policy will entail. Issues with policies will arise as each individual department implements them, meaning you have to amend and revise policies.

"This has been the real cultural challenge for us as we work through the practical implications of each policy for every member of staff affected. This is a huge task for any organisation and should not be understated," explains Stuart Chapman.

Another major change for NatCen was having to classify all of its information within security categories and ensuring that there were specific handling processes in place. As a research organisation whose primary product is information, implementing a classification process was a significant step as it affects all levels of the organisation in its day-to-day work.

The organisation recognised that although implementing these procedures was a significant step it was also a necessary one. "As our customers had been requesting that we conform to ISO27001 standards there was an acceptance within the company that this was something we needed to do," explains Stuart Chapman. "The only question we had regarding the whole process was one of value for money. Our main concern was to make sure that the costs of achieving this were realistic and working with Sapphire helped to ensure that this was the case." In terms of Sapphire's involvement with NatCen, it has gone above and beyond the ISO27001 certification project and has made itself available to the organisation to offer expert advice. Sapphire also attends a number of NatCen's Information Security policy meetings and has held a number of one-to-one briefings to ensure that everybody understands the process.

As the relationship between the two organisations has developed, it has moved towards a model where NatCen develops the policies and then call on Sapphire to provide expert advice and guidance. This has occurred gradually as NatCen as an organisation has matured and become more aware of the information security thanks to the support and guidance provided by Sapphire.



Moving Forward

More recently NatGen has begun looking at training and implementation, as Stuart Chapman explains, “We have now completed training every member of staff on the new procedures, having worked with Sapphire to develop a set of slides that have been used in the training.”

The final step for NatGen was its final audit to ascertain whether or not it had met with ISO27001 standards. Again this was a process in which Sapphire was instrumental. At the end of October 2008, Sapphire carried out a mock audit to ensure that all policies were correct and in place before the final audit, which was successfully completed at the end of November 2008.

Stuart Chapman confirms that in the future the organisation may consider taking the process one step further and becoming fully accredited. “Initially we made the decision not to become fully accredited in line with industry norms. However, if our customers were to request or we thought it was of benefit we would consider it.”

In terms of the organisations relationship with Sapphire, Stuart Chapman is nothing but complimentary, “Throughout every stage of this process we have been able to go to Sapphire and ask them for their expert advice. An example of the level of service they offer is that I am able to ring them up with queries outside of the ISO27001 compliance issue and get their opinion on what we should be doing as an organisation.”

With the furore surrounding information security set to continue, NatGen will continue to work closely with Sapphire to ensure that all of its client’s data remains safe and secure. “The biggest single benefit that working with Sapphire offers us is that we can adopt a position of confidence, not complacency,” concludes Stuart Chapman.

