Safe in their hands (Jan 06)

IT security is now more important than ever for BA. Which is why the airline is professionalising its central security team, reports Ron Condon

Even the most hardened air traveller feels a wave of relief when they see the pilot and crew come wafting through the airport lounge in their smart uniforms, and caps covered in gold braid. The smart appearance, and that reassuring sound of ‘This is your Captain speaking’ when you get on board, all help you to feel safe and secure, and in the hands of professionals who know what they’re doing.

But the perception of safety has to be backed up by the right knowledge, skills and procedures. And it needs to apply throughout the organisation, including its IT systems. British Airways, for one, is well aware that with IT systems supporting everything it does – from taking bookings to managing the plane fleet – the safety of IT systems is just as vital as any other part of the business.

And so over the past few months, the company has embarked on a project to ensure it has the same level of professionalism in IT security that it has in other parts of the organisation. The transformation programme has included intensive training for the central team in charge of IT security, with a recognised certificate at the end of it.

The man leading the project is Bob Fletcher, chief information security officer at BA and a veteran of the IT security field. ‘We are in the process of transforming the old IT security approach into more of a strategic information assurance function,’ he says. ‘I’m raising the game of many of the people engaged in the process.’

The team that was being trained consists of a group of some 30 people who set security policies and standards for the whole of the airline, and get involved in ensuring the policies are adopted across the company. As part of the overall project, Fletcher is restructuring processes, reappraising the security technology used to protect BA’s networks and data, and looking at how people use the systems.

The task of the central security team is huge and complex. BA employs almost 50,000 people around the world, and most of them have access to information systems. The team setting policy therefore needs to spread good practice and ensure proper usage of IT across the organisation.

Although many of them had been doing the job for several years, some team members had come into the department from other parts of BA and had picked up the job as they went along. The new training programme was intended to provide some formal training and set a formal baseline of expertise.

‘We have a quite deliberate programme of getting as many people as want to do it through the appropriate level of professional external accreditation,’ says Fletcher. ‘One of the reasons for that is to raise the level of prestige and self-esteem among the group. So there is a morale-boosting element here, and a recognition that the airline takes this very seriously and is sponsoring the training, at not insignificant cost.’

Intensive training
The training has been carried out by an external company, Ultima Risk Management, with classes taking place at BA’s headquarters near Heathrow. The course is an intensive five-day foundation course in information security, accredited by the Information Systems Examination Board (ISEB) of the British Computer Society, that leads to the Certificate in Information Security Management Principles (CISSP).
It is a wide-ranging curriculum, which starts with the basic risk management principles – identifying the most important areas to protect – and then covers the main techniques and technologies used to protect systems and networks. The course also examines current legislation and regulations that affect information security, as well as standards (BS 7799) and frameworks that facilitate best practice. So it packs quite a lot into just five days.

However, Fletcher feels it is a useful first step. ‘My team is more business focused than technology focused. We have extensive technology skills elsewhere in the airline, and some heavyweight experts in my team. But in the main we function as a bridge between strategy, the regulatory environment and the IT environment.’

Not everyone managed to get through the course first time, although Fletcher insists that this was more because the individuals involved found it difficult to take exams rather because they lacked the required knowledge. ‘We had a couple of people who were good at the subject but were not good at passing exams. I think it was like driving-test nerves,’ he says. ‘Those who got distinction are on cloud nine.’

The shape of things to come
As a seasoned security professional, Fletcher sees the CISMP as ‘a stepping-stone – the equivalent of the cycling proficiency badge. But it is a jolly good start’. And it will provide the team with a baseline of expertise that can now be supplemented by other courses, such as specialist technology courses for some, or for others moving on to the most widely recognised security qualification, the CISSP (the Certified Information Systems Security Professional, run by the US-based (ISC)² (The International Information Systems Security Certification Consortium)

But Fletcher sees qualifications as a question of horses for courses. ‘We have no plans to move everyone to CISSP – not everyone could do it, not everyone needs to do it, and the costs would be prohibitive.’ Nevertheless, he adds, there is a strong incentive to professionalise the security practice, as senior management within BA is constantly looking to streamline operations, and technology has a huge part to play in that. For example the BA website already allows customers to book online and, in time, it will give customers greater ability to do remote check-in and choose their seats. For that to work in a world beset by terrorist threats, authentication of customers and general security of systems need to be highly developed.

As Fletcher puts it: ‘The airline industry is a global business and operates in a very hostile threat environment. The business model, with lots of joint ventures, makes the control of information quite interesting. It is not easy. There is also a lot of regulatory pressure.’

Certificate in Information Security Management Principles
The CISMP is designed to provide the foundation of knowledge necessary for individuals who have security responsibility as part of their day-to-day role, or who are thinking of moving into a security-related function. It also provides the opportunity for those already in these roles to enhance or refresh their knowledge and in the process gain a recognised qualification.

The qualification indicates the holder has a good knowledge and basic understanding of the subject areas that make up information security management. The course covers:

- Concepts relating to information security management (confidentiality, integrity, threats, vulnerability, risks and countermeasures etc.)
- Current UK legislation and regulations that have an impact on information security management
- Current national and international standards, frameworks and organisations that facilitate the management of information security
- The current business and technical environments in which information security management takes place (security products, malicious software, relevant technology etc.)
- The categorisation, operation and effectiveness of safeguards.
The student’s view

Rob Hadfield is a long-serving employee of BA who moved into IT seven years ago, later focusing on IT security. As well as attending the ISEB course, he helped organise it and knows only too well the task of selling security to the rest of the company.

“We have lots of different challenges,” he says. “For instance, we have 20,000 air crew who turn up for work for an hour and then disappear for long periods, so it’s quite a challenge making contact with them. And they deal with fairly important information.”

He says the CISMP has been a useful exercise. “The course is ideal for people who are quite new into the IT security arena,” he says. “If you’ve just joined the department and have only been involved in a few aspects of the subject, then it is a good, broad training.”

The programme covers just about every aspect of information security at a fairly high level, he says, but does not go into a great deal of detail.

“It starts off with the risk analysis approach, and then looks at what you need to do to manage the risk. It gives a structured and logical approach.

It then works down to the things you can do to mitigate the risks — some of them technical, and others procedural or managerial,” Hadfield explains.

He admits that much of the content was quite basic, given his three years’ experience in the department, but insists the structure of the content has helped to put a lot of things in context.

The CISMP certificate, he says, is “not massively important to me. It’s not something I put a huge value on. But as an organisation it makes sense to have people in the role who are professionally qualified, just as we have professionally trained accountants and engineers.”

“IT security is a relatively immature area, but it does make sense to define a level of competence within the organisation. Other members of the team put a higher value on the certificate.”

For Hadfield himself, the CISMP has whetted his appetite for more training. When we spoke to him in November, he was due to do the CISSP course, again in a one-week accelerated learning programme.

“The studying for the CISSP is, let’s say, challenging. There is an awful lot of material. We are running it in-house. A week is not a long time to get it done,” he says.

© Haymarket Professional Publications Ltd