Focus on data security

Jason Connolly, of Next Generation IT, looks at how data security is intrinsically linked to the island's reputation

The Guernsey Financial Services Commission recently carried out a review of data security of local fiduciary companies. The aim was to measure current security practices and benchmark against industry best practices.

Maintaining confidence in the local fiduciary sector is paramount to its continuing success. Guernsey, like other offshore jurisdictions, is under intense scrutiny and needs to be seen to be whiter than white. In the past, the high profile thefts of customer data in the banking sector have caused some serious concerns, and the Commission believes that the same reputational risk applies to the trust sector.

The Commission benchmarked local businesses against industry best practice using ISO 27001 as a standard ISO 27001 covers all aspects of data security (although it is worth noting that this standard is not enacted in legislation and acts only as a guide). Local trust companies completed a self-assessment questionnaire comprising 79 questions. On-site visits to a representative sample of organisations followed.The compiled results were recently published on the Commission's website to outline current practices and areas for increased focus.

Key findings
Businesses were measured against a number of criteria. The highlights of the findings include:

Security policies and governance – These were found to be generally good, with 68% of organisations having a security policy that had been reviewed in the last 12 months. However, the majority were not placing enough focus on security matters in the boardroom.

Security awareness – Awareness of security risks among staff members throughout organisations was an area for improvement, with 64% of businesses providing less than an hour of security training per annum. Security awareness is the single most effective weapon against cyber-threats and data leakage.

Business continuity – Respondents ranked highly in this area, with 87% having a business continuity plan and 80% testing it in 2013/2014. The report author r ecommends that we build on that strength by carrying out further business impact analysis (BIA) which examines the full gamut of scenarios and risks, incorporating these additional security risks into the business continuity plan.

Remote access – 87% of businesses provide remote access for their staff, but only half of these secure their remote access with two factor authentication. This presents a significant security risk. Two factor authentication (using hard or soft security tokens to augment standard username and passwords) is viewed as a minimum standard of security for remote access.

Data leakage prevention – An area of particular concern to many businesses with the potential to harm reputation in the longer term, in addition to the immediate impact of the data loss. Organisations employ a wide variety of control measures to protect themselves, which is important because the mechanisms for data loss are myriad. For instance, 56% of respondents block webmail and 69% block USB ports and removable media. This is a fast developing area though, and businesses need to be continuously vigilant, adapting their security practices as new threats emerge.

Compliance and audit –Over 50% of organisations review their user privileges less often than annually; 54% only review data security risks annually. Whilst most organisations identified data security as a specific risk, the author reports a distinct lack of detail in risk assessments, and a focus on a few easily understood areas at the expense of others. The Commission encourages assessment of a broader scope of security risks, to address the weakest areas.

Conclusions
The Commission concluded that most organisations have adequate up-to-date security policies and generally business continuity plans are up-to-date and tested. It did outline several areas for improvement. Wider risk assessments; more thorough due diligence/vetting procedures for staff, temps and outsourced service providers; and also increasing awareness of security in the boardroom and throughout the organisation.

The Commission also highlighted the increasing focus on data security, and the recent high profile data leaks that have heightened the focus on safeguarding sensitive client information. Greater awareness is encouraged at board level, and vigilance to the threats is imperative across the entire organisation, and should form part of everyday practices, procedures and ongoing monitoring.

Protection of data security is a rapidly developing area. In the past a single line of defence behind a good firewall and desktop antivirus was all that was needed. But threats are evolving; IT systems are now very complex; and cloud computing, remote access and mobile devices mean that there is no longer a single line of defence. Phishing emails and social engineering attacks penetrate traditional edge protection measures.

Only a constant focus on security awareness and education throughout the organisation, coupled with regular proactive review and monitoring of security measures will protect against the ever evolving threats. This can be carried out in-house, or with the assistance of security specialists, such as Next Generation IT, who carry out one-off security audits, and also ongoing monitoring, penetration testing and health checks of IT systems on our clients' behalf.