FOCUS ON CYBER SECURITY

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

Last year the Guernsey Financial Services Commission carried out a review of data security of local fiduciary companies to measure current security practices and benchmark against industry best practices.

This year, the States of Guernsey is taking a wider remit and, in tandem with its digital focus on 'Smart Guernsey', is currently undertaking a cyber security review in Guernsey to better understand, and prepare, for the threat profile to islanders, business and government. The review is prompted by research published in the UK, which showed that 80% of large businesses and 60% of small businesses suffered a security breach in the last year.

This increase in focus is also prevalent across many local businesses. Local auditors are looking much more deeply into cyber security issues and are assessing local businesses against detailed security standards across the entire organisations. Cyber security is no longer just the responsibility of the IT department – it has become a board issue.

Maintaining confidence in the established local finance and fledgling fintech sectors is paramount to their continuing success. Guernsey, like other offshore jurisdictions, is under intense scrutiny, and we need to be seen to be whiter than white. In the past, high-profile thefts of customer data in the banking sector have caused serious concerns, and the GFSC believes that the same reputational risk applies to the trust sector.

To analyse current practices, the commission benchmarked local businesses against industry best practice. Using an internationally-recognised standard, it covers all aspects of data security.

The commission concluded that most organisations have adequate security policies and generally business continuity plans are up-to-date and tested. They outlined several areas for improvement, such as wider risk assessments, more thorough due diligence/vetting procedures for staff, temps and outsource providers, and increasing awareness of security in the boardroom and throughout the organisation.

The GFSC also highlighted the increasing focus on data security, particularly in the media, and 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 – it should form part of everyday practices, company procedures and on-going monitoring.

Cyber attacks are becoming ever more sophisticated and organised. Criminals and rogue governments with relatively little technical knowledge can access insecure systems, bring down websites or infect systems with viruses.

The most prevalent attack is phishing, where hackers penetrate the organisations' defences by sending a spam email enticing a staff member to click on a link to an external website, which then infects the network from within, bypassing firewalls and virus scanners. These emails can be very convincing, personalised to appear plausible, and often adding credibility by appearing to come from someone from within the organisation. It is so important that staff are careful when clicking on links within emails, especially if they are not totally sure they are genuine. Furthermore businesses must have robust procedures to verify instructions made via email. Whatever checks and balances exist in the real world should not be circumvented in the digital world.

DDOS (distributed denial of service) attacks have been in the news recently as criminals have attempted to extort local companies to avoid an attack. DDOS is where many infected systems are used to target and overwhelm a company's connection to the internet. Fortunately these attempts have been unsuccessful, but it highlights the need for a robust disaster recovery plan. In a recent statement Guernsey Police encouraged businesses to be vigilant and to consult with their local service provider if they were concerned.

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 fast evolving – IT systems are now very complex, and there is no longer a single line of defence. Attacks penetrate traditional edge protection measures, but a constant focus on security awareness and education throughout the organisation, coupled with regular proactive review and monitoring of security measures, will offer protection. 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, as well as ongoing monitoring, penetration testing and health checks of IT systems on our clients' behalf.