Cybercrime threat is very real for all

Jason Connolly, director at Next Generation IT, explains why cybercrime matters to all businesses and individuals and suggests what can be done about it

Q: We hear a lot these days about cybercrime, but how much of a real threat is it?

A: Cybercrime is growing at an alarming rate. According to a recent report by KPMG, the cost of cyber fraud in the UK increased by 1,266% in 2016 to £124m. Yahoo's recent disclosure is the biggest data breach in history, with more than a billion user accounts and personal details stolen. An incident like this really brings into focus organisations' responsibility to safeguard personal data, especially with General Data Protection Regulation sanctions not too far away. All businesses in the Channel Islands need to ensure they make themselves aware of the legislative changes which come into force in May next year, as they will have significant ramifications for the way that personal data is stored.

Q: Are we not a bit safer in the islands though?

A: No one is immune from attack and the Channel Islands' geographical location provides no protection. Recent widescale 'Smishing' (SMS phishing) and Vishing (Voice phishing), asking islanders to call them urgently, demonstrate the potential rich pickings, with many activists viewing the Channel Islands as a soft target. The most prevalent attack is phishing, where hackers penetrate 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 within the organisation.

Q: Why do companies' systems continue to be breached when we know hackers are out there?

A: There is widespread confusion and lack of understanding of what individuals and organisations can and should do to protect themselves and their data. This is coupled with the fast-paced development of the tactics used by hackers to evade detection by anti-viruses, firewalls and other security filtering systems employed by businesses.
A high stakes cyber arms race has developed between the hackers and cyber security providers. 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.

Q: Is there not one, simple, 'catch all' package to protect us?

A: There is no one silver bullet and a layered approach to protecting systems and data is essential. Businesses should employ a range of measures, including:

- constant patching of systems (to reduce vulnerabilities that can be exploited);
- up-to-date antivirus and anti-ransomware desktop software (to capture infections that get through);
- solid email, web and email filtering systems (to block phishing attempts);
- up-to-date firewalls and properly secured connections to the internet (to prevent hacking attempts);
- and, in case of infection, effective and reliable backups and SIEM (security information and event management) monitoring systems to quickly and effectively recover following a successful attack with minimal downtime, data loss and knowledge of the extent of the compromised data.

Most importantly, staff must be vigilant to avoid clicking on emailed links and documents unless they are absolutely sure they are from a reputable source. Regular security training is essential and robust processes and procedures around payments and other critical processes are absolutely crucial to avoid getting caught.

With the increasing complexity of IT systems, there is no longer a single line of defence against hackers.