Grant Thornton

An instinct for growth™

Cyber security concerns in the retail sector

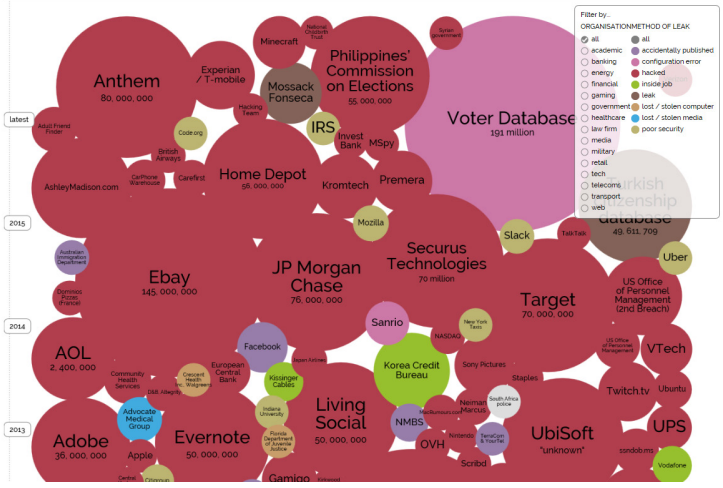
The statistics

One in eight retailers faced a cyber-attack over the past 12 months, according to data from Grant Thornton's International Business Report. Despite this, fewer than half of retail businesses have a cyber-strategy in place (46%) which is below the global average (52%) for all businesses.
With fierce competition and online customers less loyal to any particular retailer than those who visit in person, retailers need to make sure their digital presence is up to scratch. A slick interface and ease of payment are important but so too is security. Cyber-crime is on the rise, Grant Thornton research suggests the cost of cybercrime to the Irish economy is €630 million per year.

Problems – reputational damage

These estimates of direct financial impact do not include the long-term reputational damage (see Figure 1.0 below) and loss of trust that companies suffer when their systems are breached. If an online customer worries that their credit card details are not securely stored, they will almost certainly choose to shop somewhere else. Very few retailers are lucky enough to offer a product so unique that customers cannot find a substitute.

Figure 1.0 – World's Biggest Data Breaches



The threats

It is noteworthy that the majority of data breaches are the result of a hack or indeed extremely targeted cyber-attacks. The retail sector is no different in this regard.

Customer and corporate data is one of the most valuable assets that any organisation holds – the importance of securing this sensitive information is now widely accepted. As the business community continues to evolve, the security threats and vulnerabilities are increasing in complexity and are becoming increasingly difficult to address in a cost effective manner.

Attacks are not focused just on the online retailer, there have also been significant Point of Sale (POS) targeted attacks involving customised malicious software specifically written to ex-filtrate customer credit card data from the retailers' networks back to the cyber criminals both in the U.S. and Europe.

Tone at the top (at board level) is also a key issue for many retailers and is increasingly unacceptable for retail organisations to ignore the issue of cyber security, these issues need to be addressed by senior management and at board level in order to mitigate sufficiently against potential breaches. Cyber security and the prevention of cyber-crime is a key focus area for retailers in Ireland. Protecting customer's personal and financial data is now part of the cost of doing business. If retailers are not trusted to protect their customer's information they will go elsewhere.

Figure 2.0 – Retail security, types of attacker

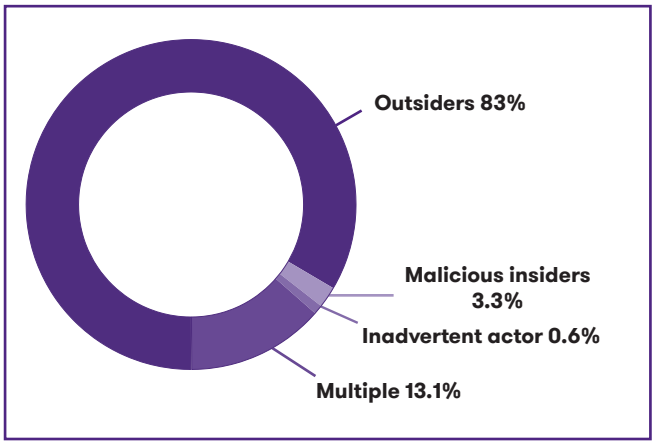
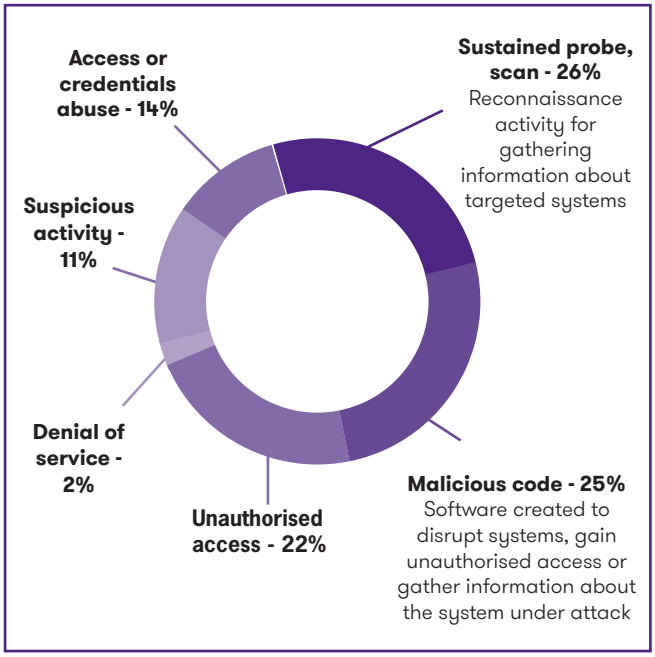


Figure 3.0 – Retail security, methods of attack



Risk mitigation

All retailers should at very minimum focus on the following areas in order to mitigate against their risk of a cyber-security incident:

- develop a cyber security strategy focusing on what needs to be protected;
- identify priorities for protection starting with a cyber security risk assessment and gap analysis;
- everyone be aware of the role that they have to play in making their company cyber-secure;
- effective policies embed cyber-security within the business; and
- incident response a detailed incident response plan should be put in place to contain and mitigate against any future attack.

Contact

Mike Harris
Partner, Cyber Security
E mike.harris@ie.gt.com
M +353 (0)86 855 6740

Tommy Maycock
Director, Cyber Security
E tommy.maycock@ie.gt.com
D +353 (0)1 500 8176

Over 1,000 people operating from offices in Dublin, Belfast, Cork, Galway, Kildare, Limerick and Longford.

www.grantthornton.ie

@GrantThorntonIE

Grant Thornton Ireland

Grant Thornton
An instinct for growth™