**MS Amlin**

* Most cases involving IT security breaches never get reported. This is to avoid reputational damage, regulatory investigations and lawsuits. Yahoo were found guilty of this, as they did not report the attack as soon as they had realised. This also might be the case as the media are not as interested in SMEs when compared to the larger global counterparts.
* According to last years’ Internet Security Report, 60% of all target attacks involved SMEs. Moreover, Ponemon Institute’s Cost of Data Breach Study revealed that in 2014 the average cost of attack for an SME with less than 100 employees was a massive $3.5 million.
* SMEs are targeted more often than others as they have a lack of resources invested in security, poor security technologies in place and very little training for employees to raise awareness. Cyrus Walker, CEO of Chicago-based Data Defenders says research shows approximately 80% of security-related incidents occur as a result of employee behaviour. It’s also been estimated by cyber-security firms that 71% of breaches go undetected.
* A report from McAfee found almost 90% of small- and medium-sized business in the US do not use data protection for company and customer information, and less than half secured company email to prevent phishing scams. Cybercrime costs the US economy $100bn a year and the global economy about $300bn annually, according to the Centre for Strategic and International Studies.
* Did look at the cyber-liability cover offered by Lloyd’s, which puts retail and finance ion the higher risk bracket. The risk associated is derived from the technology and regulation around privacy. These are both constantly changing, therefore the solutions provided via insurance need to be able to evolve.
* Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information.
* The 2016 Cost of Data Breach Study: United States carried out by Ponemon Institute LLC gains some valuable insights also. However, I don’t think it is accurate to draw conclusions from a study involving 64 companies.
* Although GDPR doesn’t affect the US, I thought I’d outline the fines associated. A two-tiered sanctions regime will apply. Breaches of some provisions by businesses, which law makers have deemed to be most important for data protection, could lead to fines of up to €20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater, being levied by data watchdogs. For other breaches, the authorities could impose fines on companies of up to €10m or 2% of global annual turnover, whichever is greater.
* A staggering amount, especially when coupled with the fact that 90% of large organisations reported breaches in 2015, up from 81% in 2014, while 74% of small organisations said they had been breached in 2015, up from 60% in 2014. PWC carried out an excellent piece work, being the 2015 Information security breaches survey, regarding the UK. I feel that this study is very credible as it is backed by the UK government and had 644 respondents.
* I believe that to help remedy this problem, SMEs should begin to:

1. Partner with a trusted firm to provide relevant advice related to their security infrastructure, including technical testing such as security audits and penetration testing to determine where the firm’s weaknesses lie and improve organisational readiness
2. Monitor networks for unusually high traffic volume
3. Work with their financial institution to implement multi-factor authentication and dual controls for financial transactions
4. Educate employees regarding good security habits including stronger administrative passwords, policies regarding email attachments, etc.