PCI DSS Briefing Note Update & Corporate Exposure to Data Breach
March 2016

Our progress on the new Telephone-based Secure Payments Guidelines for Jeremy King and the PCI Standards Security Council have progressed well over the winter and a meeting with Jeremy w/c 11th April will begin to firm up on the publication date. These new Guidelines embracing all form of telephone payments from hotel reception desks to large contact centres, will form the basis for ongoing QSA certification as well as guidance to the acquiring bank community, so an early heads up for merchants and their TPSP's will be essential reading.

We anticipate being able to provide overviews in more detail once the publication date has been set.

Cyber security and data compromise has been a hot topic of discussion over the winter with several high profile data compromises covered by the press. What's been interesting is how others are responding to those data breaches, not just the FTSE 350 companies, for which the UK Government conduct the *Cyber Governance Health Check*, reporting on the extent to which company boards and committees understand and oversee risk management measures, but what the SME community are doing to proactively protect themselves.

There is lots of help available. The recent creation of the cyber security information sharing partnership *(CISP)* for example, provides a forum for Government and industry partners to exchange information on cyber threats and vulnerabilities. It's absolutely clear that the UK Government is emphasising the need for company boards and senior executives to take clear ownership and management of their cyber risks and deal with these in an overall corporate risk management regime. To support that the Government has created the *Cyber Essentials Scheme*, covering the very basic controls all organisations should implement to mitigate the most common cyber-attacks.

Whilst many organisations have become certified under the scheme including Vodafone, Barclays and Virgin Media, it was interesting that in the Information Security Breaches Survey 2015 revealed that almost half the companies that responded had certified themselves and being compliant with the scheme. So what are the risks to your company in the event of a cyber-attack, internal data security breach or a combination of both?

Risk to confidential and proprietary information which may be of significant value to the company or a competitor. For TPSP's having access to client systems holding personally identifiable information (PII) on customers a company could be faced with a claim for third party losses.

Reputational risk from brand damage and loss of reputation in the market place. For listed companies, there is a duty to disclose any breaches which constitute inside information (see later under disclosure obligations)

Litigation risk from 3rd parties or employees claiming that the company executives failed to take reasonable safety precautions resulting in possible negligence claims especially when dealing with payments, where their approach to take reasonable action to meet prevailing data security standards, resulted in lost revenue. Risk may also come from breach of express or implied contractual terms relating to data being stored securely.

Financial risk not only having significant impact on senior management time and BAU, but causing significant impact on customer (or client's customer) purchasing or renewal behaviour as we highlighted in or white paper published back in November which is still available to download from our website.

Sanctions from the ICO especially where it is shown that the board or individual executives wilfully failed to apply known data security standards (PCI DSS & DPA) that form part of a merchants (or their TPSP) contractual terms relating to their ability to store, process or transmit payment card data.
The ICO are known to be especially hard on companies where there is a risk of identity theft. The Data Protection Act 1998 (the DPA) requires organisations in control of personal data to take "appropriate technical and organisational

measures" against accidental loss, destruction of, or damage to personal data. Breaching the provisions of the DPA by failure to have appropriate cyber-security measures in place could result in ICO fines, enforcement notices and criminal prosecutions.

Risk of impact of attacks through supply chain especially where TPSP's have direct access to your own data systems whether that is through a company's external customer contact centre or contracted homeworkers, being threatened by organised crime to secure customer data as we have seen evidenced by UK police forces throughout the UK.

Directors of UK companies should give consideration to the need to disclose cyber security risks and actual or potential cyber security breaches in a number of areas:

- Listed companies may have a duty of care to disclose cyber security breaches to the market under the Disclosure and Transparency Rule, which provide that any issuer must notify a regulatory information service as soon as possible of any inside information which directly concerns the issuer unless an exception applies. Whether or not a breach constitutes inside information will depend on severity and the potential impact on shareholders.
- Directors of listed companies should also consider their reporting obligations under the UK Corporate Governance Code and Companies Act 2006, as well as in any Prospectus being issued by the company in relation to the issue of new shares. The annual report should also cover any data breaches or potential breaches during the period and the reporting of measures and controls to maintain shareholder value.
- An issuer that publishes (or dishonestly delays publishing) material that fails to adequately disclose cyber security events, minimises their impact or downplays their significance, may also face claims bought by investors under section 90A of the Financial Services and Markets Act 2000, as well as proceedings in tort.

What role should directors play in preventing attacks?

Company directors have various statutory duties under the Companies Act 2006, in addition to their fiduciary duties at common law. These include duties tom promote the success of the company and to exercise reasonable care, skill and diligence. Directors could have the potential liability where he or she is in breach of these duties and the breach relates to cyber security. However, directors of companies where it is believed that data is properly managed and there are governance and accountability structures in place, should be protected. However, directors should ensure that cyber security is on the risk register and that this register is reviewed regularly. It is also important that that a company does not simply put operational procedures in place (e.g. ISO standards or PCI DSS), but rather that these are actively followed, implemented and monitored.

Directors should also be aware of last year's amendments to the Computer Misuse Act 1990 bringing about substantial changes including:-

- introduction as an offence of unauthorised acts in relation to a computer that resulted in serious damage to any country, the economy, the environment, national security, human welfare or create significant risk of such damage; and
- extending existing offences to include obtaining tools like malicious software or unlawfully obtaining passwords to commit an offence e.g. unauthorised access to PII

Directors need to be aware of these new offences and should consider making all of their employees (office and home based) aware of the increased scope of these offences. Companies failing to that may be vicariously liable for actions of their employees where such offences are committed.

What can be done?

The key way for companies to minimise the risks of cyber-attack from internal staff or those external to the business is to comply with industry best practice, comply with industry and national data security standards, and do as much as possible to take sensitive personal data, be that PII or payment card data, out of your operational environment.

Taking risk off the table and 'devaluing' data is the most sensible and cost effective approach to protect your company, your shareholders, your customers and your employees from the significant downside of data breach.