HERBERT SMITH FREEHILLS

CYBER SECURITY AND PAYMENT SERVICES

14 July 2015 | Africa, Australia, Bangkok, Beijing, Belfast, Berlin, Brisbane, Brussels, China, Doha, Dubai, Frankfurt, Germany, Hong Kong, India group, Israel group, Jakarta, Kazakhstan group, Latin America group, London, Madrid, Melbourne, Middle East, Moscow, New Yor
Legal Briefings – By **Yuban Moodley**

Cyber security is a major compliance issue for global payment services.

The technology advances in payment services and the use of online and mobile payments, electronic storage and global communications systems creates increased efficiencies in payment services, but with an increased risk from cyber security breaches. The recent 2014 Cost of Data Breach Study by the Ponemon Institute covering Australia and other countries highlighted that Australian companies in the financial services sector along with the retail sector are more likely to suffer a breach in contrast to other sectors of the economy.

Whilst companies can implement measures to prevent cyber-attacks from being successful, they cannot guarantee that those measures will be successful. Cyber security policies must cover not only prevention but post-breach mitigation.

WHAT ARE THE IMPACTS

Significant business impacts can flow from cyber security incidents. The most obvious are:

- reputational impacts resulting in loss of customers or revenue or both, or adverse impacts on share price,
- cost of containing and remedying the incident including the cost of remedying fraud,
- loss of intellectual property or confidential information which erodes competitive advantage or other commercial benefits, and

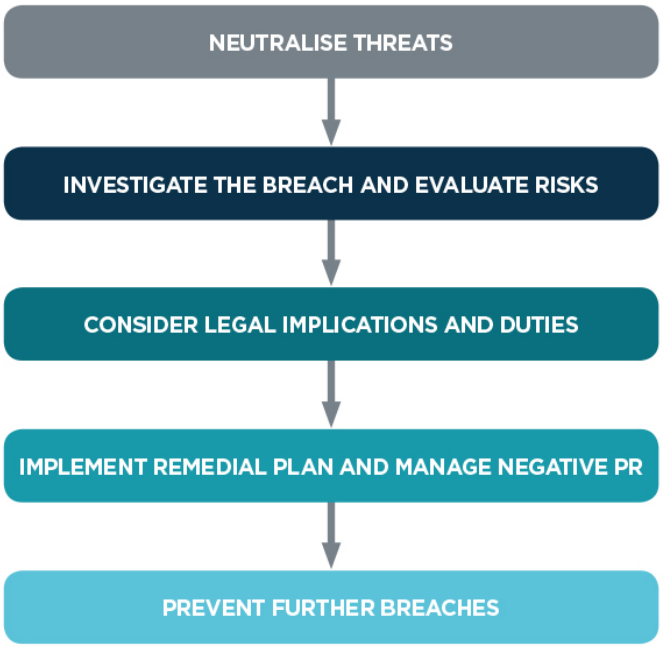
- loss of business continuity and revenue.

The financial impact of cyber security breaches is highlighted in the 2014 Cost of Data Breach Study by the Ponemon Institute. Taking Australia as an example, it notes the average cost of a data breach paid by a company in 2014 was AUD 2.8 million. Additionally, average churn rates have increased by 5% meaning more customers were terminating their customer relationship following a data breach.

Security breaches affecting payment services are likely to be more costly, than other breaches in particular as result of the cost of managing fraud. Perhaps the most widely known cyber security breach affecting payment services was in 2014 when 40 million credit card numbers and the personal information of 70 million individuals were reported to have been stolen from the US retail chain Target through the installation of malware in Target's security and payment system.

MANAGING THE RISK

In our experience, where a cyber security incident arises, several steps should be taken by the affected organisation to mitigate the impact on individuals, the organisation itself and other stakeholders.

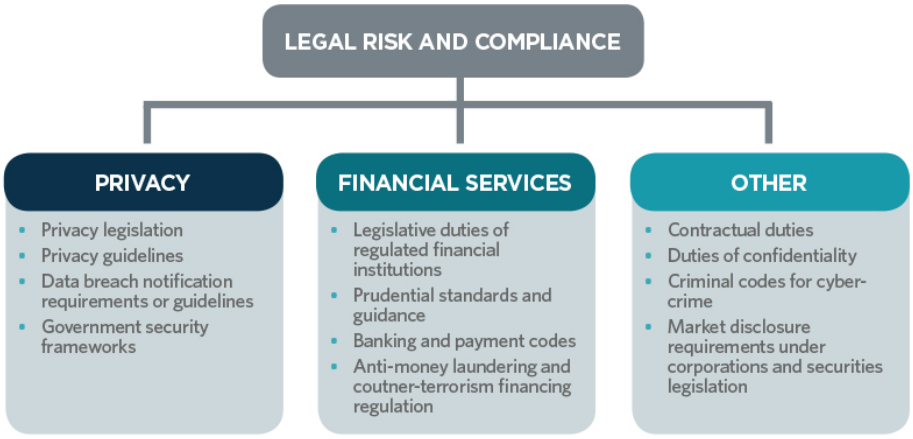


LEGAL RISK AND COMPLIANCE

There is no single piece of legislation or regulation that addresses cyber security holistically. In the payment services sector, relevant legislation covers a wide range from privacy legislation, financial services legislation, corporations and securities legislation to common law duties of confidentiality and cyber-crime offences under criminal codes.

The legislative framework is also heavily supplemented by guidance on recommended practice produced by privacy and financial services regulators. A key part of the legislative and regulatory framework relates not only to prevention, but also steps to be taken in the case of a breach.

In particular, data breach notification is a major legal and risk consideration, concerning duties or recommended practice to notify affected individuals, regulators, the market or crime enforcement agencies. The diagram below summaries the legislative landscape for cyber security.



CONSEQUENCES OF BREACH

- **Notification and market disclosure duties or recommended practice:** to affected individuals, privacy and financial services regulators, police and to the market.
- **Liability to affected individuals and third parties:** compensation for fraudulent activity under codes of conduct and contractual provisions, liability for breach of

legislation and regulation and under statutory compensation regimes, liability for breach of contract and duties of care, liability under indemnities, vicarious liability for fraudulent activity of employees.

- **Regulatory consequences:** enforcement action and liability to regulators (financial services, privacy and potentially corporations and securities regulators), determinations and orders by regulators enforceable undertakings and regulatory penalties.

- **Criminal liability:** for breaches of criminal codes for cyber-crime and for fraud.

MANAGING THE RISK

Organisations providing or receiving payment services clearly need to have systems and procedures to manage cyber security risk and the impact on their business, customers, and individuals. Key steps in any cyber security risk mitigation strategy include:

- **a review of the expertise and capability** of existing cyber security measures and personnel, and remedying any gaps or weaknesses,

- **establishment of clear procedures** and lines of authority for decisions regarding information security,

- **implementation of detailed policies and procedures** setting out cyber security requirements;

- **development of a response plan** specifically detailing actions to be taken if a cyber security breach occurs including a data breach notification plan and approvals required before communications are issued,

- incorporation of **cyber security as an agenda item** for senior audit and management committees to ensure that the issue is given the appropriate oversight, and

- **adoption mandated and best practice standards** regarding information security.

Cyber security is likely to remain a major risk management factor in the global payment services industry. Its relevance was highlighted in the last month, with the publication of the Cyber Resilience Health Check, Report 429, March 2015 by the Australian Securities and Investments Commission (**ASIC**). This report is aimed at assisting ASIC's regulated population improve their cyber resilience and is aimed at identifying how cyber security risks should be addressed as part of current legal and compliance obligations relevant to ASIC's jurisdiction. The report's publication is likely to increase the visibility of cyber security management at board level.

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.

© Herbert Smith Freehills 2021

SUBSCRIBE TO STAY UP-TO-DATE WITH INSIGHTS, LEGAL UPDATES, EVENTS, AND MORE
Close

© HERBERT SMITH FREEHILLS LLP 2021