MARSH JLT SPECIALTY

JULY 2020

Cyber Risk and Insurance Solutions

Risk in Focus – Digital Loyalty Programmes

MARSH

Contents

Introduction

Across different industries around the world, loyalty programmes have evolved from membership cards and mailing lists, to mobile applications and reward points systems that look to enhance the customer experience.

While many organisations are reaping the benefits from the convenience of innovative and streamlined technologies for their loyalty programmes, the associated cyber risks are commonly overlooked.

Digitised loyalty programmes can often contain a wealth of personal data and have the potential to cause harmful privacy issues if this information falls into the hands of malicious parties.

Digital Loyalty Programmes – In the Crosshairs

Digital loyalty programmes are an effective tool for organisations to create strong engagement and brand loyalty with their customer base. Many loyalty programmes effectively operate by encouraging customers to create individual accounts in order to access rewards and other benefits, such as exclusive membership discounts. Through innovations such as mobile applications, modern loyalty programmes provide transparency and convenience for the user, while simultaneously recording data which can be attributed to each individual's account.

Though they provide individuals with unique benefits and allow organisations to drive customer engagement, digital loyalty programmes can be prime targets for hackers as they hold a substantial amount of valuable customer information which can be manipulated to carry out more sophisticated and targeted attacks on individuals in the future, while rewards points also act as a kind of currency as they can be monetised.

Industries that optimise the use of digital loyalty programmes include:

- Airlines & Travel
- Retail
- Food and Hospitality
- Hotels and Accommodation

Although loyalty programmes are not limited to the above industries, they are most at risk given their large customer bases, and the nature of personal data that can be collected and stored.

Recent events highlight the growing consequences of cyber-attacks targeting digital loyalty programmes and respective customer databases:

- **British Airways, 2018** – Hackers specifically accessed the personal data of approximately 500,000 customers who used a payment card to make reward bookings. BA initially said compromised information involved included names, email addresses, and credit card information. The U.K. Information Commissioner's Office (ICO) fined British Airways 183 million pounds, the largest GDPR era fine to date, representing 1.5 percent of the airline's 2017 turnover. Airline reward programmes are such a lucrative target because they are both a kind of currency and replete with personal information on frequent flyers.[1]
- **Boots Pharmacy, 2020** – In March 2020, Boots temporarily suspended payments using loyalty points in shops and online after attempts to break into customers' accounts using stolen passwords. Boots said none of its own systems were compromised, but hackers had tried to access accounts using reused passwords from other sites in order to steal and spend rewards points for themselves.[2]
- **Dunkin Donuts, 2018-19** – Dunkin Donuts suffered two separate credential stuffing attacks in October 2018 and January 2019, where hackers take combinations of usernames and passwords leaked at other sites and use them to gain (illegal) access on accounts on the Dunkin Donut site. Hackers then put up the hacked accounts for sale on the darkweb, which are later bought by other third parties that use the reward points found in these accounts at Dunkin' Donuts shops to receive unearned discounts and free beverages.[3]
- **Marriot Hotel Group, 2020** – Hotel chain Marriott disclosed in March 2020 a security breach that impacted more than 5.2 million hotel guests who used the company's loyalty programme mobile app. Compromised personal data included guests identification details, loyalty points balances, partnership and affiliate information and also personal preferences.[4] It is the second major data breach, after they discovered in late 2018 that 383 million guests' details had been stolen by hacker groups.

1 Benjuya, D. (2020, March 19). Why Fraudsters Are Flying High on Airline Loyalty Programs. Retrieved from https://securityintelligence.com/why-fraudsters-are-flying-high-on-airline-loyalty-programs/

2 Molloy, D. (2020, March 4). Boots halts Advantage Card payments. Retrieved from https://www.bbc.com/news/technology-51742079

3 Cimpanu, C. (2019, February 12). Dunkin' Donuts accounts compromised in second credential stuffing attack in three months. Retrieved from https://www.zdnet.com/article/dunkin-donuts-accounts-compromised-in-second-credential-stuffing-attack-in-three-months/

4 Cimpanu, C. (2020, March 31). Marriott discloses new data breach impacting 5.2 million hotel guests. Retrieved from https://www.zdnet.com/article/marriott-discloses-new-data-breach-impacting-5-2-million-hotel-guests/

Cyber Exposures from Digital Loyalty Programmes

Personal Data

The potential loss of personally identifiable information is an obvious major exposure for any organisation offering digital loyalty programmes. A major data breach of a loyalty programme can incur significant first party losses including forensic investigation and data restoration costs, legal support, public relations costs and the time and additional costs to notify affected individuals and regulatory bodies. Additionally, third party liability claims could arise from class-actions in response to a major privacy breach from the loss of personal data.

Reward Points Theft

Theft and misuse of rewards points as a form of currency can incur several additional costs for an organisation. This may require compensation to affected individuals in the form of account credit or goodwill coupons, especially to mitigate further reputational harm and loss of customers.

Reputational Harm and Brand Damage

Brand and reputational damage from a loyalty programme breach can be very detrimental to an organisation, as affected customers and the wider public can easily lose trust in a brand overnight, especially from reporting in the media. Customers will often seek out more secure competitors in the event of a breach, causing a direct loss of customers and revenue. Data breaches should be handled with strategic care and with support from expert breach counsel.

Digital Supply Chain

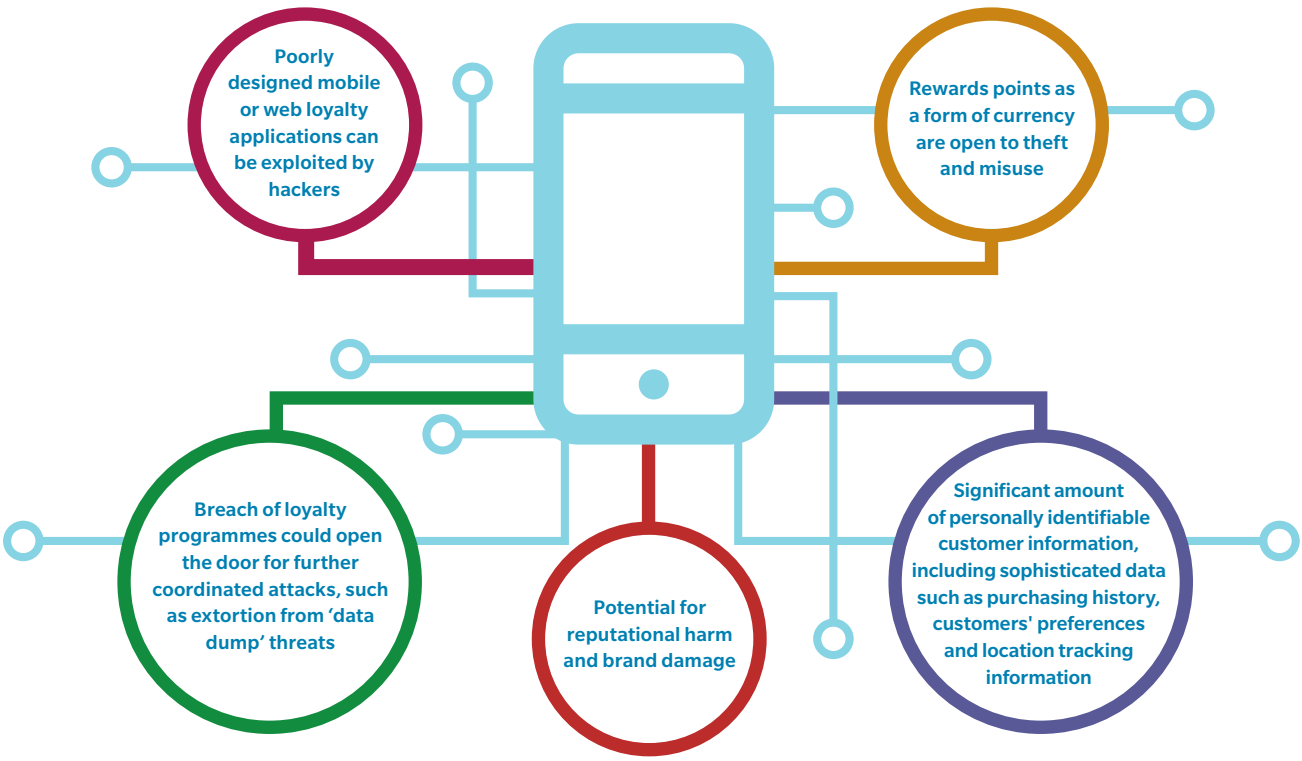
Given the reliance on external vendors to develop or host digital loyalty programmes on behalf of organisations, breaches of personal data or the sudden unavailability of loyalty apps can be outside the control of an organisation but still result in significant unanticipated financial costs. This could be not only from privacy liability claims from any breach of personal data, but also from contingent business interruption if loyalty programme functionality is impacted by a vendor.

Global Privacy Regulations

Organisations with large loyalty programmes and international customer bases may also face exposure to third party claims and regulatory actions for privacy breaches on a mass scale from multiple jurisdictions. In the event of a breach of customer personal information, companies could find themselves subject to class action lawsuits or onerous international privacy legislation from multiple jurisdictions. The European Union's GDPR (General Data Protection Regulation) which was introduced back in 2018 has become a regulatory model, which is being closely observed by other territories around the world as a potential framework to adopt, including Australia and New Zealand.[5]

5 Benady, D. (2018). *GDPR has established Europe as leaders in data protection.* [online] Raconteur. Available at: https://www.raconteur.net/hr/gdpr-europe-lead-data-protection [Accessed 17 Oct. 2019].

Digital Loyalty Programmes – Cyber Risk Profile



Filling the Insurance Gap

Cyber insurance can provide critical protection for direct loss and liability arising out of the use of technology and data in day-to-day operations, assisting retail companies to mitigate their exposure to cyber risk and successfully recover from a cyber-incident.

Cyber 1st Party Coverages

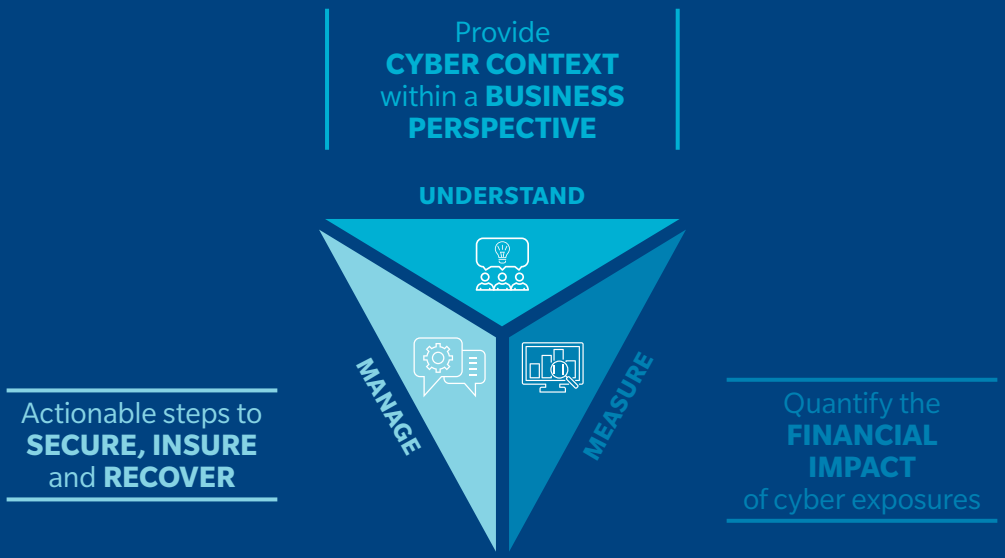
- **Incident Response Costs** – Immediate access to specialist vendors to minimise the potential financial, regulatory and reputational impact following a cyber-event. This includes the appointment of forensic IT experts, public relations consultants and legal firms.
- **Business Interruption/Extra Expense** – Reimbursement for lost profit, including extra expense resulting from a technology failure, computer system outage or cyber-attack. Coverage can be expanded to include contingent business interruption arising out of a cyber-event impacting a critical supplier.
- **Information Asset Protection** – Costs incurred to recreate, restore or recollect data damaged, stolen or corrupted.
- **Privacy notification and credit monitoring** – Provision for costs to comply with privacy breach notification statutes, as well as the provision of credit monitoring protection for affected customers.
- **Extortion** – costs to negotiate a ransom demand, as well as coverage for an extortion payment.

Cyber 3rd Party Coverages

- **Privacy Liability** – Liability for failure to prevent unauthorised access, disclosure or collection of confidential personal information, or to properly notify a privacy breach.
- **Media Liability** – Defence and liability costs for online libel, slander, plagiarism or copyright infringement.
- **Regulatory Defence** – Defence of regulatory actions, including affirmative coverage for certain assessed fines and penalties where permitted by law.

Marsh Cyber Services

Cyber risk can be effectively managed through a programme of continuous improvement and vigilance that combines technology with risk transfer. Cyber risks are not technical problems that firewalls and patches (though important) can solve alone. Marsh delivers risk solutions to help you protect your hospitality and tourism business and enable confident risk taking. Marsh's approach to cyber risk management is comprehensive and employs techniques that **Understand, Manage** and **Quantify** the unique cyber risks affecting retailers.



Connect with us

To further understand your organisation's cyber and technology liability exposures and which potential risk management or insurance solutions may assist, please contact your Marsh representative, or speak to one of our cyber risk and insurance specialists.

KELLY BUTLER
Cyber Practice Leader – Pacific
+61 3 9603 2194
kelly.butler@marsh.com

NICOLE PALLAVICINI
Principal
+61 2 8864 8323
nicole.pallavicini@marsh.com

JONO SOO
Head of Cyber Specialty – New Zealand
+64 9 928 3092
jono.soo@marsh.com

KRISTINE SALGADO
Managing Principal
+61 3 9603 2871
kristine.salgado@marsh.com

SAMUEL ROGERS
Managing Principal
+61 3 9603 2381
samuel.rogers@marsh.com

GEORGIA O'GRADY
Principal
georgia.ogrady@marsh.com