Yui Kee Computing Ltd.

Newsletter

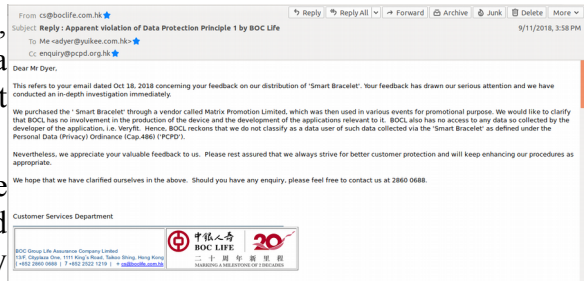
November 2018

Contents

BOC Life Denies Responsibility

<web-link for this article>

In an email reply to Yui Kee's Chief Consultant, Allan Dyer, BOC Life has claimed they are not a data user for data collected via the 'Smart Bracelet'.



Email reply from BOC Life

As **reported in this newsletter, last month**, the 'Smart Bracelet' is a device with an associated app that was distributed as a promotional gift by BOC Life. The User Agreement for the app, which could be accepted without reading, appeared to allow collection of excessive personal data, apparently in violation of Data Protection Principle 1.

According to their email, BOC Life purchased the device from 'Matrix Promotion Limited'. BOC Life had no involvement in the production of the device and the development of the app, and no access to any data collected by the device. Therefore, BOC Life concludes that they are not the data user for data collected by the device.

Allan Dyer commented, "Does a company have a responsibility to ensure the gifts they give out are safe? In their promotion, did BOC Life make it clear to people that the gift they were being given in return for their personal data would, itself, collect further personal data on behalf of a third party they had not heard of?"

More Information

- **Privacy: Who Cares? A Quick Look at the BOC Smart Bracelet**

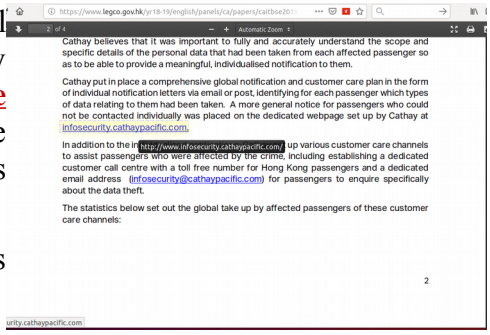
Cathay Pacific to Face LegCo Panel on Data Leak

<web-link for this article>

Hong Kong's Legislative Council (LegCo) has requested Cathay Pacific Airways Limited (Cathay) to attend a joint meeting of the Panel on Constitutional Affairs, Panel on Information Technology and Broadcasting and the Panel on Security on Wednesday, 14 November, 2018 to face questions about the **leak of personal data revealed last month**.

The **written paper submitted in advance** of the Panel contains few details of the incident that have not already been revealed in the press and on **Cathay's website dedicated to the incident**. Unfortunately, the link to the dedicated website provided in the submission is incorrect, having an extra 'www' at the beginning.

The submission does give statistics on the effectiveness of Cathay's efforts to warn their customers:


Cathay believes that it was important to fully and accurately understand the scope and specific details of the personal data that had been taken from each affected passenger so as to be able to provide a meaningful, individualised notification to them.

Cathay put in place a comprehensive global notification and customer care plan in the form of individual notification letters via email or post, identifying for each passenger which types of data relating to them had been taken. A more general notice for passengers who could not be contacted individually was placed on the dedicated webpage set up by Cathay at infosecurity.cathaypacific.com.

In addition to the in http://www.infosecurity.cathaypacific.com up various customer care channels to assist passengers who were affected by the crime, including establishing a dedicated customer call centre with a toll free number for Hong Kong passengers and a dedicated email address (infosecurity@cathaypacific.com) for passengers to enquire specifically about the data theft.

The statistics below set out the global take up by affected passengers of these customer care channels:

2

urity.cathaypacific.com

Cathay's Submission to LegCo, showing incorrect link

Channel	Statistics to midnight 12 November 2018
Website	181,700 page views
Call centre enquiries	5,031 calls received
Enquiry mechanism on the Website	19,005 enquiries received
Emails received by infosecurity@cathaypacific.com	5,622 emails received
Free ID monitoring service	50,271 passengers enrolled

Therefore, as of midnight 12 November 2018, over 97% of the 9.4 million people affected by the leak have taken no known action to find out more or protect themselves.

Updated: 23rd November 2018

Legislative Councillor for Information Technology Hon Charles Mok submitted written questions to Cathay Pacific in advance of the LegCo Panel meeting. He has now released **his questions and Cathay Pacific's answers**.

The answers reveal that Cathay Pacific in March 2018 initially detected brute force attacks on user account and launched an investigation with an outside cybersecurity firm. The attacks continued, being most intense in March, April and May. Early in May, the investigation revealed forensic evidence of unauthorised access and data exfiltration. The second phase of the investigation, which took until August, focussed on identifying which passenger data had been accessed and whether it could be reconstructed in a readable format outside of Cathay's systems. The third phase, which was not completed until 24 October 2018, focussed on identifying the compromised data types for each passenger. Cathay's databases and database servers have logging capabilities enabled at the OS and database level, which allowed the investigation to identify the activities of the attacker.

The investigation revealed that the attacker used previously unknown malware and utilities in the attack, which Cathay's up-to-date anti-virus system did not detect. Cathay has had in place detection and monitoring systems to detect APTs, and in March 2018 they also implemented an advanced endpoint detection and response system.

Cathay took both tactical and strategic remediation steps from the beginning of the investigation, improving their already robust security program.

It is interesting that the incident started with brute force attacks on user accounts, and no other unauthorised access method is mentioned, but there is no mention in the remediation measures of strengthening authentication systems, for example, by moving to 2 factor authentication or public key authentication.

More Information

- **Cathay Pacific written submission LC Paper No. CB(2) 222 /1 8 -1 9 (0 2)**

- **The Abysmal State of Personal Data Protection**
- **Dedicated webpage about the data leak set up by Cathay**
- **Cathay Pacific hack: Airline admits techies fought off cyber-siege for months**
- **Charles Mok's Follow-up on the Cathay Pacific data breach**

AVAR Conference Illuminates Malware Development

<web-link for this article>

(Left to right) Mr Keseven, Mr Dyer, Dr Sanjay Bahl, Mrs Rama Vedashree and Mrs Sheba Grace at the Lighting of the Lamp

The 21st AVAR Conference opened with a traditional Indian Lamp Lighting Ceremony. K7 Computing Private Limited, an Indian cybersecurity industry leader, hosted The Association of Anti-Virus Asia Researchers International Conference (AVAR) in association with Indian Computer Emergency Response Team (Cert-In). The conference was held at Holiday Inn resort, Goa from the 29th to 30th of November, 2018. The gathering of more than 400 participants along with 67 speakers from 25 different international security companies addressed and discussed the significant and acute aspects of cybersecurity. The theme of the conference was "The Dynamic Security Ecosystem."

The International security conference in its 21st year saw one of the largest gathering of cybersecurity experts, researchers, product developers and eminent speakers from around the world, engaging in panel discussions and paper presentations.

K7 Computing previously hosted the conference in Chennai, in 2013. Hosting the event for the second time and bringing the event back to India for the third time, J Kesavardhanan, MD & CEO, K7 Computing said; "Since its inception, AVAR has witnessed increasing participation from leading cybersecurity players from around the world. It has also evolved as a platform to discuss on the latest trends, innovations and disruptions impacting the cybersecurity industry. This year we had participation from more than 25 leading cybersecurity players from across the globe."

He further added; "It is our privilege to be associated with AVAR and to host it again in India. We are very happy with the success of AVAR 2018. With initiations like these, we aim to further our cybersecurity mandate of bringing the industry together to discuss and develop an advanced roadmap to curb cyber threats."

Commenting on AVAR 2018, Mr. Allan Dyer, Chairman, AVAR said, "We are very glad to have held the 21st edition of AVAR in India in association with K7 Computing; for the second time. Considering the expanding digitalization, India is one of those nations where the need for cybersecurity solutions and awareness on cyber threats is immensely required. Therefore, forums like AVAR, play a pivotal role in bringing the cybersecurity industry together to brainstorm on the complexities of the threat landscape and discuss the way forward to deal with these."

He further added; "It is very satisfying to see the increasing participation at AVAR every year. We congratulate K7 Computing on the successful completion of AVAR and on taking this initiative further, the second time."

More Information

- **AVAR**

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/