BDO NEWS

June 2020

www.bdo.com.hk

TECHNOLOGY UPDATES
June 2020 Issue

CONTENTS

Innovation and technology are drivers for organisation growth and the key to enhance competitiveness of different industries. Just as technology rapidly evolves, so does the sector. In every monthly issue of our 'Technology Updates', it will include the latest updates from cybersecurity, emerging technology & data privacy.

Suspicious mobile application (app) related to HK bank

On 20 May 2020, the Hong Kong Monetary Authority (HKMA) alerted members of the public on suspicious mobile application. The name of the app was very similar to the one released by a local bank in Hong Kong, however the download site was directing to a rogue website. The bank reminded their customers to download its mobile app via official App Store/Google Play and do not disclose their personal information, user credential to the suspicious website.

In recent years, phishing, malicious app and/or websites have become a mainstream. The rogue app or website are set up for malicious or criminal purposes. Hackers use malicious apps to gain access to confidential data. By downloading such an app, you are an opening door for anyone who wants to steal your data for malicious purposes.

How to recognise suspicious applications and improve mobile cybersecurity?

Whenever you download an app, it will ask you to give certain permissions so that the app can function correctly. For example, a video messaging app would require permission of using camera, which is completely normal. However, if you pay attention to the permissions you are being asked for, you can easily tell whether an application is legit or not. For example, if you are downloading a music player that asks for permission to access your call contacts, it might be a sign that you have come across a suspicious application. If the permissions do not match the app's original function, it is better to uninstall it right away.

As always, do not download apps outside the App Store and keep your data safe from untrusted website or sources. You may also consider hiring a working force to detect and monitor cybersecurity threats to your customers so that nearly real time notifications can be provided to end users.

Read more from the source:
https://www.fubonbank.com.hk/resources/common/pdf/pr_200520_e.pdf

China introduced measures to strengthen personal information protection

The fast-spreading coronavirus (Covid-19) has infected thousands of people in China and in over 20 other countries. In fighting against the outbreak of this new virus, Chinese authorities at all levels, in addition to providing emergency medical support to those affected by the virus, imposed quarantines and restricted travel to discourage outdoor activities. In order to control the outbreak and track the spread of the virus, Chinese health authorities and other stakeholders ranging from airlines, railway operators and property management companies, have collected a large amount of personal data, including data on individuals who have recently travelled to Wuhan or who have been in contact with those who have developed symptoms of infection. There have been several data breach incidents which have given rise to the concerns over privacy and potential discrimination against people from Wuhan and Hubei Province, eg the names, addresses, phone numbers and national ID numbers of more than 6,000 of people were circulated in social media.

In response to these concerns, the PRC Cyberspace Administration of China (CAC) (the key Chinese regulator on cybersecurity and data privacy) issued the 'Circular on Ensuring Effective Personal Information Protection and Utilisation of Big Data to Support Joint Efforts for Epidemic Prevention and Control' (CAC Circular) to provide detailed guidance on protecting personal data in the current circumstances.

How to prevent data breach or cybersecurity issues during critical moment or business disasters?

- Identification of critical systems and understand what systems and data are critical to operations will help prioritise contingency planning and minimise losses to the organisation
- Perform a risk analysis to identify the various risks, threats and its preventative measures to address potential disruption or harm to your operations and data

Read more from the source:
https://m.mp.oeeee.com/a/BAAFRD000020200127254378.html

Another airline suffered from data breach

A UK based budget airline admitted that they had been subjected to a 'highly sophisticated' cyber-attack and as a result, data from millions of customers were compromised. The email addresses and travel details of 9 million people had been leaked, and credit card details of 2,208 people were exposed as well.

The Europe's General Data Protection Regulation (GDPR) set a heavy maximum fine of €20 million (about £17.5 million) or 4% on annual global turnover for infringements of data protection issues. It is reckoned the airline would be fined under GDPR.

Which industries are more affected by data protection issues?

Any businesses processing customer information should take necessary measures to enforce high data protection and cybersecurity. For example, airlines, hotels, telecommunications, social media, online retail, digital banking, cloud computing, healthcare and IT system vendor.

What should you do after a data breach?

A business can prepare for cyber-attacks or data breaches by adopting a well-organised business continuity plan and a regularly drilled technology recovery plan (Figure 1). All stakeholders should be identified and trained to respond cyber-related disasters. After a cyber-incident, companies should analyse their systems in order to ascertain whether a privacy breach, confidentiality breach or cyber attack was occurred.

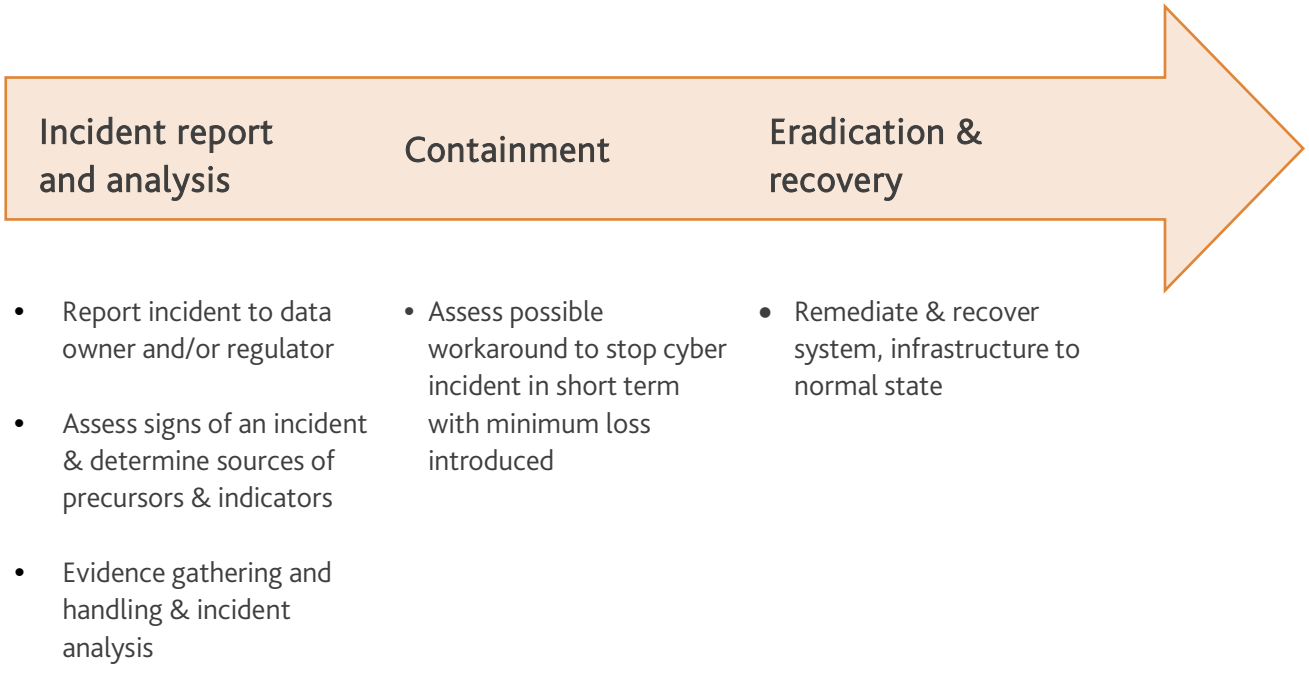
Meanwhile, it is always important to notify data owners and regulators as per agreement/regulation required. Next, company should look into the root cause and extent of the cyber-attack and provide immediate containment to address root cause. Eradication and recovery could be performed to resume system and infrastructure to normal state.

Read more from the source:
https://www.bbc.com/news/technology-52722626?intlink_from_url=https://www.bbc.com/news/topics/cz4pr2gd85qt/cyber-security&link_location=live-reporting-story

How can BDO help?

The BDO Risk Advisory Services (RAS) team is formed by a group of dedicated IT professionals. We are well equipped, qualified, experienced and well-prepared to assist your board or management to perform IT security assessments, data protection reviews, vulnerability assessments as well as penetration test or any other IT matters relating to regulatory requirements. Please do not hesitate to contact us and talk to our consultants. We are pleased to provide further insight or assistance, if needed.

Figure 1



BDO'S SUPPORT AND ASSISTANCE

25th Floor, Wing On Centre
111 Connaught Road Central
Hong Kong
Tel: +852 2218 8288
Fax: +852 2815 2239
info@bdo.com.hk

RICKY CHENG
Director and Head of Risk Advisory
Tel: +852 2218 8266
rickycheng@bdo.com.hk