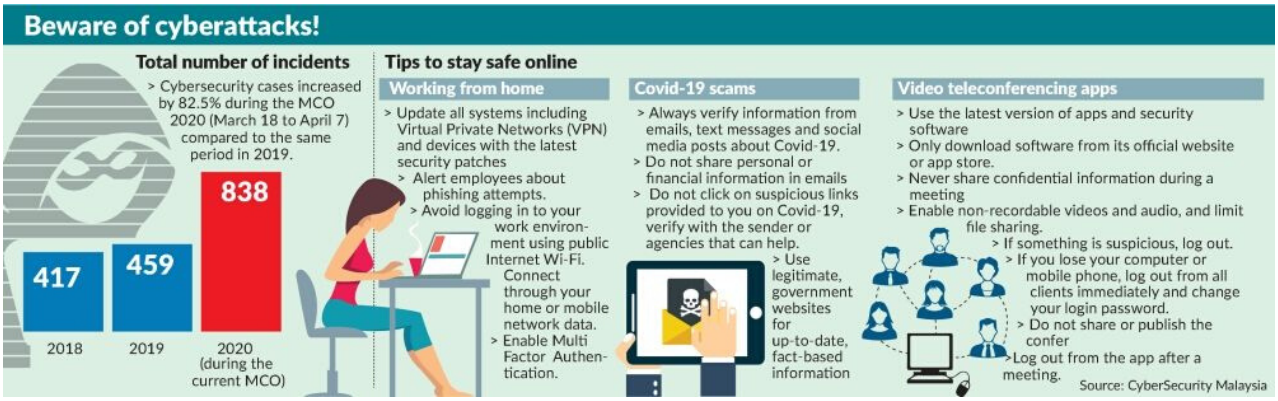
AZMI & ASSOCIATES
A member of TerraLex worldwide | advocates & solicitors
We care & share

VIDEO CONFERENCING:
DATA PROTECTION RISKS FOR COMPANIES



Introduction

In light of the coronavirus pandemic, millions of people around the globe had been forced to work from home. The use of video conferencing tools such as Zoom and Skype has increased significantly as both businesses and individuals relied on the platform to conduct meetings. In the past few months, the daily users of video conferencing tools such as Zoom surged from 10 million in December 2019 to 200 million in March 2020[1].

Nevertheless, the escalated use of such video conferencing tools has posed risks in data protection to corporates and individuals. For instance, it was reported that thousands of personal Zoom videos have been left viewable on the open Web; highlighting the data privacy risks to its users including businesses and individuals[2]. Aside from that, about 352 accounts on the video conferencing app Zoom were compromised on 8 April 2020, including a healthcare provider in the US and seven educational institutions. Details such as passwords, meeting IDs, host keys and names belonging to Zoom account users have been posted on the dark web, according to a report by Yahoo Finance[3]. Security issues such as 'Zoombombing' where unwanted users spam meetings with inappropriate images and offensive slurs. Fortunately, there has yet to be any report to Cyber999 on hacked Zoom accounts from Malaysia[4].

In light of the above incidents, companies have to be aware of the risks that it might be exposing their sensitive data including the data of its customers when its employee use video conferencing tools without precautions. It must take into consideration the fact that the data centre of the video conferencing tools is located outside of Malaysia render it difficult to control the leakage of the data.

Data Protection Law in Malaysia

In Malaysia, the primary legislation which governs data privacy is the Personal Data Protection Act 2010 ("**the Act**"). Under the Act, companies which process or have control over any personal data falls under the definition of a data user[5]. Data users in the industry such as banking, insurance, communications, real estate, utilities and others are required to be registered with the Department of Protection of Personal Data.

The Act enumerates the security principle as one of its data protection principles. Under this principle, the data user has to protect the personal data from any loss, misuse, modifications, unauthorized or accidental access or disclosure. Practical steps must be taken to ensure that the security measures are well in place to safeguard the personal data it processes.

As to what constitute practical steps, the Personal Data Protection Standard 2015 ("**the Standard**") which is formulated by the Department of Protection of Personal Data shall be referred to. The relevant provisions of the Standard are reproduced as below:

" *9. The transfer of personal data through removable media device and cloud computing service is not permitted unless with written consent by an officer authorized by the top management of the data user organization.*

10. Record any transfer of data through removable media device and cloud computing service.

11. Personal data transfer through cloud computing service must comply with the personal data protection principles in Malaysia, as well as with personal data protection laws of other countries.

12. Ensure that all employees involved in processing personal data always protect the confidentiality of the data subject's personal data."

Recommendations

In light of the above, companies should be aware of the data privacy risks that might arise and take steps to mitigate the risk to ensure compliance with the Standard.

The Data Protection Commission in the European Union has published an article which set out data protection tips for video conferencing[6]. We reproduce the relevant excerpts of the article as below:

1. Employees should be using your contracted service providers for work related communications. Ensure you are happy with the privacy and security features of the services you ask them to use. Ad-hoc use of apps or services by individuals should not be encouraged.

2. Try to ensure that employees use work accounts, email addresses, phone numbers, etc., where possible, for work-related video-conferencing, to avoid the unnecessary collection of their personal contact or social media details.

3. Make sure that clear, understandable, and up-to-date organisational policies and guidelines are provided to those using video conferencing, so they know what rules to follow and steps to take to minimise data protection risks. This should include information on the controls the services provide and that are available to them to protect their security, data, and communications.

4. Implement, and/or advise employees to implement, appropriate security controls such as access controls (such as multi-factor authentication and strong unique passwords) and limit use and data sharing to what is necessary.

5. Where video conferencing services need to be used for organisational reasons, have a consistent policy regarding which services are used and how, and offer through VPN or remote network access where possible.

6. Avoid sharing of company data, document locations or hyperlinks in any shared 'chat' facility that may be public as these may be processed by the service or device in unsafe ways.

7. Read our guidance on Protecting Personal Data When Working Remotely and our guidance on data security and make sure the points contained within are made clear to employees.

The Malaysia Computer Emergency Response Team (**MyCert**) has also issued an advisory[7] on the use of video conferencing applications like Zoom. MyCert said that users have a responsibility to choose a "secure and safe VTC (video teleconferencing) platform for web conferencing". It shared some security guidelines such as asking users to only download VTC software from official websites or app stores, never share confidential information during a meeting, enable non-recordable videos/audio function and urge hosts to utilise the 'waiting room' feature to monitor participants joining the meeting.

Conclusion

In conclusion, companies should be aware of their duty as data users and take the necessary precautions as suggested by the Data Protection Commission in European

Union and MyCert to prevent any possible data leakage when using video conferencing tools.

---

1 Retrieved from https://www.channelnewsasia.com/news/business/video-app-zoom-rockets-to-fame-some-hiccups-covid-19-12609518
2 Retrieved from https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/
3 Retrieved from https://www.thestar.com.my/tech/tech-news/2020/04/08/hackers-post-hundreds-of-verified-zoom-accounts-on-dark-web
4 Statement by CyberSecurity Malaysia chief executive officer Datuk Dr Amirudin Abdul Wahab to the Star Retrieved from https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825
5 Section 2 Personal Data Protection Act 2010
"data user" means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor
6 Data Protection Commission. (2020, April 3). Data Protection Tips for Video-Conferencing. Retrieved from https://www.dataprotection.ie/en/news-media/blogs/data-protection-tips-video-conferencing
7 Malaysia Computer Emergency Response Team. (2020, April 7). Online Video Tele-conferencing (VTC) Application Security Guidelines. Retrieved from https://www.mycert.org.my/portal/details?menu=431fab9c-d24c-4a27-ba93-e92edafdefa5&id=747f10c3-7c8b-4606-bcbd-f20aec96b918

Important Information

Azmi & Associates has set up Azmilaw Task Force to look into all issues arising from COVID-19 and MCO. Clients are welcomed to contact their usual Partner who will bring their issues to Azmilaw Task Force for our further action.

Prepared by:

Omar Saifuddin Abdul Aziz
Senior Associate 1
DL: +603 2118 5030
E: omar.saifuddin@azmilaw.com

Liana Lim Xi Ci
Associate
DL: +603 2118 5076
E: liana.lim@azmilaw.com

We hope the above discussion is of assistance to you and your company. If your company's operations or contractual obligations are affected by the COVID-19 outbreak, we are ready to assist you on any queries you have.

Corporate Communication
Azmi & Associates
15 April 2020