

Bird & Bird ATMD

Cybersecurity & Singapore



The role of HR as gatekeeper

June 2019

*Cybersecurity involves more than just the 'technical' aspect of systems and processes involved in the digital landscape. Employees' actions (or inactions) also can have a significant impact on corporate liability. This second article in our **Cybersecurity & Singapore** series discusses the importance of the role of HR in preventing cybersecurity incidents.*

Onboarding

How often, and how well do employees know the Company's IT policies?

In many cases – not enough!

Data breaches occur either due to deliberate leaks or inadvertence; while IT systems are capable of detecting data breaches in both cases through monitoring, making sure that employees *understand* and *apply* IT policies adds another layer of protection.

IT policies should not be Company intranet literature; the onboarding process should involve a combination of training and familiarisation with IT policies.

Regular Training

Maintaining cybersecurity is a daily and ongoing process.

It is therefore not enough for companies to stop at disseminating guidelines and instructions to staff at the onboarding stage.

HR may adopt an active strategy e.g. regular maintenance and updating of policies and procedures to take into account changing circumstances, conduct regular training sessions

and staff exercises, with the objective of instilling in employees an understanding of the importance and requirements of their compliance with such policies and procedures.

Resource Management

HR is in the best position to determine and allocate resources towards cybersecurity issues. This ranges from provision of equipment to managing support coverage while an employee is away from work. HR's role in resource management is important because employers can be held liable for cybersecurity incidents that occur as a result of employees not being properly equipped or supported to handle their duties and responsibilities.

The effects of data breaches may be worse in certain working cultures. In a less open office culture, whistleblowing in relation to breaches may not be an attractive option. Data breaches in a workplace where deference to managers practised may not be easily detected. HR can help build a culture of openness and transparency which goes a long way in maintaining cybersecurity.

Crisis Management

HR is instrumental in formulating the internal response to a data breach. Conducting timely, effective and fair investigations upon detection of

an incident directly helps manage and contain the legal risks and reputational fallout.

It falls on HR to handle the "who-what-where-why" of an investigation with the other stakeholders, e.g. from making sure that the investigation yields the answers that are needed to manage employee relations, to meting out appropriate discipline measures.

Authors

Seow Hui Goh
Partner

Tel: +65 6428 9419
seowhui.goh@twobirds.com



Chye Shu Yi
Associate

Tel: +65 6428 9435
shuyi.chye@twobirds.com



Contact Us

For queries or more information, please do not hesitate to contact any member of the Employment team.

Seow Hui Goh
Partner

Tel: +65 6428 9419
seowhui.goh@twobirds.com



Jacqueline Tang
Senior Associate

Tel: +65 6428 9405
jacqueline.tang@twobirds.com



Chye Shu Yi
Associate

Tel: +65 6428 9435
shuyi.chye@twobirds.com



twobirds.com

Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses, which include Bird & Bird ATMD LLP as a Singapore law practice registered as a limited liability partnership in Singapore with registration number To8LLOO1K.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.