Companies Need To Build Cybersecurity Into Their Governance Systems
在企業管治系統中建網絡安全的重要性

Jolly C K Wong 黃振球

Management of publicly listed companies in every industry and across the globe are now treating cybersecurity as a top priority.

This is the result of a string of recent events, such as the WannaCry ransomware attack of May 2017, that have alerted management that their companies could fall victim to a global epidemic of cyberattacks [1]. Cybersecurity Ventures, a cyber economy researcher, has suggested cybercrimes cost USD6 trillion globally in 2021, and this cost will grow by 15% per year to reach USD10.5 trillion by 2025 [2].

Management and directors need to be more hands on with cybersecurity. The chief information officer (CIO) is typically in charge of cybersecurity, according to the Gartner 2020 Board of Directors Survey [3]. Oftentimes, however, the board and its various committees are unaware of the cybersecurity challenges the company might face and are, as a result, unconcerned.

And in 2020, only 60.5% of board directors surveyed by the US National Association of Corporate Directors (NACD) identified cybersecurity as a "very important" area for improvement over the next 12 months [4].

This needs to be rectified. Every board member must realize by now how big a risk cybersecurity threats are and should do everything possible to address them. Cybersecurity improvements must be a whole-of-company exercise, starting from the top.

At the same time, board members should also ensure that the executive team establishes a comprehensive risk management framework that addresses cybersecurity. This includes delegating people to take ownership of individual cybersecurity issues and set pre-agreed performance indicators so they can be reviewed regularly.

Boards should ensure a sole officer, the chief information

security officer (CISO) or equivalent, is accountable for overall information and data security and has authority to coordinate cyber-risk policies. This executive officer should encourage everyone else to consider cybersecurity when making decisions.

A 2020 survey of more than 400 global listed companies done by PwC, a consultancy, showed that 44% of board members believed that their organizations have made significant progress over the past three years in improving their cybersecurity [5].

This is good news but the increasing number of high-profile hacks should make leaders realize that there is much more to be done.

A third necessary step is to develop a strategy to adopt cyber risk management tools with plenty of mitigation.

A team should first devise a suite of cybersecurity policies that cover areas such as data protection, incident response and software application management. The team should then provide the board with an economic assessment of potential cyber-attacks versus the cost of prevention.

This analysis will help determine the appropriate risk-mitigation policy to take, such as insurance coverage on professional indemnity and public and product liability. The former covers all losses resulting from a claim for any civil liability related to the conduct of the company's IT services and products. The latter covers any legally liable claim for compensation for personal injury or property damages that result of an event related to the company's IT services and products.

But cybersecurity management is not just about normal day-to-day good practices. It is also important to think about potential vulnerabilities and prepare for the worst. This means mapping out possible worst-case scenarios and devising plans to respond to them.

This brings us to the final principle to remember: involve cybersecurity experts.

Boards should ensure adequate access to cybersecurity experts and have these experts regularly participate in board meetings.

Many existing board members lack cybersecurity skills. Inviting experts to attend meetings can facilitate cyber risk discussions and encourage members to ask the right questions.

In 2019, MIT researchers studied 3,200 listed companies in the United States with over USD1 billion in revenues [6]. They found that companies with three or more digitally savvy directors performed better, reported profit margins 7% higher and 38% higher revenue growth.

Ideally, every board member should have basic computing qualifications, such as the freely available Harvard Introduction to Computer Science course. Computer science is a thinking discipline essential to business, just as finance, law or management is.

Digital skills are essential in the digital age. Many companies are beginning to realize the benefits of including digitally skilled board members. By 2025, 40% of boards of directors will be expected to have a dedicated cybersecurity committee overseen by a qualified board member, up from less than 10% that reported such a committee for the Gartner 2020 survey.

The presence of a "digital director", alongside all the other important measures that should be taken, will help companies better address cybersecurity risks.

References

[1] The National Cybersecurity and Communications Integration Center (NCCIC), "WHAT IS WANNACRY/WANACRYPT0R?" https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

[2] S. Morgan, "Cybercrime to cost the world $10.5 trillion annually by 2025" Cybercrime Magazine, November 13, 2020 https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[3] Gartner 2020 Board of Directors Survey https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-#:~:text=According%20to%20the%20Gartner%202020,properly%20secured%20against%20a%20cyberattack.

[4] NACD, 2020–2021 NACD Trends and Priorities of the American Boardroom, pp. 15–20.

[5] PricewaterhouseCoopers, Global Digital Trust Insights Survey 2021 https://www.pwc.ch/en/publications/2020/ch-Digital-Trust-Insights-Survey-2021-report.pdf

[6] P. Weill, T. Apel, S. L. Woerner, and J. S. Banner, "Assessing the Impact of a Digitally Savvy Board on Company Performance," MIT Sloan CISR Working Paper No. 433, January 2019. https://cisr.mit.edu/publication/2019_0101_DigitallySavvyBoards_WeillWoernerApelBanner

PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Join the PCPD Professional Workshops to Enhance Your Organisations' Competitiveness

參加私隱公署專業研習班 提升業務競爭力

A sound Personal Data Privacy Management Programme (PMP) requires all members of an organisation to be aware of, and be ready to act on personal data protection responsibilities. Organisations should provide employees with up-to-date data protection training tailored to their specific needs.

To this end, the PCPD has developed a series of Professional Workshops on Data Protection catered to the needs of specific industries and sectors. **Professional Workshops in February and March are now open for enrolment! HKIoD members can enjoy the discounted fee.**

健全的個人資料私隱管理系統有賴機構內各個員工知悉其保障個人資料的責任，並付諸實行。機構應針對相關員工的特定需要而提供培訓及教育，並傳達最新資訊。

就此，私隱公署設計了一系列有關保障個人資料的專業研習班，以配合在不同工作範疇處理個人資料的人士的需要。**二至三月的專業研習班現已接受報名，香港董事學會的會員可以優惠價參加。**

	Date 日期	Time 時間	Course (Online workshop) 課程名稱 (網上進行)	Course Fee* (HK$) 課程費用（港幣$）
2022 / 02	17/2	2:15pm - 5:15pm	Data Protection in Insurance 保險業的資料保障	$750/ $600*
	24/2	2:15pm - 5:15pm	Data Protection in Direct Marketing Activities 直接促銷活動的資料保障	$750/ $600*
2022 / 03	17/3	2:15pm - 5:15pm	Recent Court and Administrative Appeals Board Decisions 法院及行政上訴委員會近期的案例	$950/ $760*
	24/3	2:15pm - 4:15pm	Personal Data Privacy Management Programme 個人資料私隱管理系統	$750/ $600*
	31/3	2:15pm - 5:15pm	Data Protection in Human Resource Management 人力資源管理的資料保障	$750/ $600*

* Applicable to members of PCPD's Data Protection Officers' Club ("DPOC") and the supporting organisations (including HKIoD) only.
* 只適用於私隱公署之保障資料主任聯會會員或支持機構（包括香港董事學會）的成員。

Above courses will be conducted in Cantonese with courses materials in English. For more details, please visit below website or scan the QR code for further information and registration.

以上課程將以粵語授課並提供英文課程教材。詳情請參閱以下網站或掃瞄二維碼以獲取更多有關課程的資訊及報名方法。

Register NOW! 請即參加！

https://www.pcpd.org.hk/english/education_training/organisations/workshops/workshop.php

For enquiry, please contact Communications and Education Section of PCPD at 2877 7169 or 3423 6654 or training@pcpd.org.hk.

如有查詢，歡迎致電2877 7169 / 3423 6654 或電郵 training@pcpd.org.hk 聯絡私隱公署傳訊及教育組。

今天，全球各行業的上市公司正在將網絡安全視為其首要事項之一。

這是近年發生的多宗網絡安全事件導致的結果，例如發生在2017年5月的「想哭WannaCry」勒索軟件攻擊事件，該軟件已經向全球發出警告，所有公司都有可能會成為全球流行病式的網絡攻擊的受害者[1]。

網絡經濟研究機構網絡安全風險投資（Cybersecurity Ventures）表示，2021年全球網絡犯罪引發的經濟成本為6萬億美元，以每年增長15%估算，到2025年該成本將達到10.5萬億美元[2]。

美國資訊科技顧問公司高德納 （Gartner） 2020年董事會調查[3] 表示，公司董事相信首席信息官 （CIO）有能力並將會處理網絡安全問題。因此，董事會及委員會的成員並未完全意識到網絡安全風險的嚴重程度，故並無參與任何實質工作。在網絡安全問題上，董事會及委員會成員應該更加親力親為。

在2020年美國國家企業管理協會（NACD）調查中，只有60.5%受訪的董事會成員將網絡安全確定為未來12個月的「非常重要」改進領域[4]。

這說明網絡安全問題需要得到修正。 每名公司董事都必須意識到當下風險網絡安全威脅的嚴重程度，並應採取一切適切的措施解決。公司必須從上到下採取共同行動改進網絡安全。

同時，董事會成員應確保執行團隊建立全面的風險管理框架，徹底解決網絡安全問題。

這個框架將包括重視個人網絡安全問題，並設定商定的績效指標，作定期檢討。

董事會應確保高層行政人員中有專職人員，例如首席信息安全官（CISO）對公司整體信息和數據安全負責，並有權協調網絡風險政策。該行政人員應積極鼓勵公司上下員工在作出決策時考慮網絡安全因素。

為全球超過400家上市公司提供顧問服務的公司普華永道（PwC）進行的一項調查顯示，44%的董事會成員認為，他們部門過去三年在改善網絡安全方面取得重大進展[5]。

這確實是個好消息，但隨着高調的黑客攻擊數量的增加，企業領導應該意識到他們應該做的還有很多。

第三步就是制定網絡風險管理工具的策略，並提供充足的緩解措施。

管理團隊應首先制定一套針對數據保護、事件應對及軟件應用管理網絡安全政策。然後，他們應該向董事會提供與潛在的網絡攻擊風險相對應的預防成本及經濟損失評估。

這些分析將有助釐定適當的風險緩解政策，例如考慮專業責任保險以及公共及產品責任保險。

前者將涵蓋與公司信息服務和產品的操作有關的任何民事責任的索償而產生的所有損失。後者涵蓋與公司信息服務和產品有關的事件導致的人身傷害或財產損害的法律責任賠償。

但網絡安全管理不止於日常的良好操作。我們亦應考慮系統潛在的弱點，為最壞的情況做好準備。這意味著計算出可能出現的最壞情況，並制定應對計劃。

我們必須謹記：公司要聘用網絡安全專家。

董事會應確保公司高層行政人員擁有足夠的網絡安全專業知識，讓專家定期參加董事會會議。

由於許多公司現有董事會成員缺乏網絡安全技能。參加董事會議的專家可以促進網絡風險討論，並鼓勵董事會成員提出適當問題。

2019年，MIT研究員在美國研究了收入超過10億美元的3,200 家上市公司[6]。他們發現，擁有三名或以上具備數碼技術知識的董事的公司表現較佳；他們的利潤率和收入增長分別高於其他公司達7%和38%。

誠然，最理想的情況就是每名董事會成員都具備基本的電腦計算資格，例如學習哈佛大學推出的電腦科學公開課程。電腦計算是商業不可或缺的思維方式，與金融、法律或管理同樣重要。

數碼技能對數碼時代至關重要。許多公司開始意識到有董事會成員熟悉資訊科技的好處。根據此前提及的高德納2020年的調查，到2025年，預計40%的公司董事會將會擁有一個由合資格董事會成員監督的專門網絡安全委員會，而現今這一比例不足10%。

設立公司「數碼董事」，加上其他重要措施，將有效打擊數碼時代網絡安全風險。

Dr Jolly Wong is the Policy Fellow, Centre for Science and Policy, University of Cambridge.
黃振球博士是劍橋大學科學與政策中心政策研究員。

The 21st Century DIRECTOR 廿一世紀董事

Sponsored by 贊助機構：
Corporate Governance Development Foundation Fund
企業管治發展基金

Publisher 出版機構
The Hong Kong Institute of Directors 香港董事學會

Sponsor 贊助機構
Corporate Governance Development Foundation Fund 企業管治發展基金

Publishing Board 出版委員會
Mr Stanley Mok (Chairman) 莫兆光先生（主席）
Ms Bonnie S Y Chan 陳心愉女士
Ms Agnes K Y Tai 戴潔瑩女士
Mr Richard Tsang 曾立基先生
Dr Carlye Tsui 徐尉玲博士

Project Management 項目統籌
Executive Office, The Hong Kong Institute of Directors
香港董事學會行政處

For enquiries about circulation and advertisement, please contact:
有關發行及廣告查詢，請聯絡：
Chief Business Officer: Ms Miriam Yee
業務總監：余海恩小姐

For editorial enquiries, please contact:
有關編輯上的查詢，請聯絡：
Associate Manager, Communication & Projects: Ms Joanne Yam
傳訊及項目副經理：任綺欣小姐

Tel 電話： +852 2889 1414
Fax 傳真： +852 2889 9982
Email 電郵： magazine@hkiod.com

《廿一世紀董事》同時可於網上閱覽
The 21st Century Director is also available at
http://www.hkiod.com/21century.html

ISSN 1996-9619

The Hong Kong Institute of Directors 香港董事學會

Patron 贊助人
The Hon Mrs Carrie Lam Cheng Yuet-ngor GBM GBS 林鄭月娥行政長官

Hon President & Founding Chairman 榮譽會長兼創會主席
Dr the Hon Moses Cheng GBM GBS OBE JP 鄭慕智博士

Past Chairmen 前任主席
Dr Herbert H M Hui JP (Deceased) 許浩明博士(已故)
Mr Peter S H Wong MBA 黃紹開先生
Dr Kelvin Wong SBS JP DBA 黃天祐博士
Mr Henry Lai 賴顯榮律師

Council 理事會 (2021-2022)

Chairman 主席:
Dr Christopher To 陶榮博士

Deputy Chairmen 副主席:
Ir Edmund K H Leung SBS OBE JP 梁廣灝工程師
Ms Bonnie S Y Chan 陳心愉女士
Mr Richard Tsang 曾立基先生
Mr William Lo 羅志聰先生

Treasurer 司庫:
Mr Man Mo Leung 文暮良先生

Immediate Past Chairman 卸任主席:
Mr Henry Lai 賴顯榮律師

Chief Executive Officer 行政總裁:
Dr Carlye Tsui BBS MBE JP 徐尉玲博士

Council Members 理事會成員:
Dr Leonard S K Chan 陳新國博士
Mr Vincent Chan 陳永誠先生
Dr Chen Linlong Mike 陳林龍博士
Mr Hamilton Cheng 鄭炳熙先生
Dr Charles Cheung JP MBA DBA (Hon) 張惠彬博士
Dr Justin K H Chiu 趙國雄博士
Mr Richard Ho 何麗康先生
Mr Randy Hung 孔敬權先生
Mr Ip Shing Hing JP 葉成慶律師
Mrs Margaret S Leung 梁甘秀玲女士
Mr Ka-Yin Li 李家彥先生
Mr Jeffrey Mak 麥振興律師
Ir Prof John Mok 莫建鄰教授
Mr Stanley Mok 莫兆光先生
Ms Agnes K Y Tai 戴潔瑩女士
Ms Cynthia Y S Tang 鄧宛舜女士
Mr Jim Wardell 詹華達先生
Mr Stephen Weatherseed 韋大象先生
Mr Andrew Weir 韋安祖先生
Mr Huen Wong BBS JP 王桂壎律師
Mr Kenneth Wong 黃永恩律師
Ms Alice Yip 葉嘉明女士

The 21st Century Director is the official magazine of The Hong Kong Institute of Directors. All rights reserved. No part of this magazine may be reproduced or stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written permission of the publisher and/or the copyright owner of this magazine. Quotation of short passages of the magazine for the purposes of review and education is allowed provided that it is made with explicit reference to the source and publisher. Neither the magazine nor the publisher accepts liability for any views, opinions or advice expressed by writers and interviewees of articles. The contents of the magazine do not necessarily reflect the views or opinions of The Hong Kong Institute of Directors or the members of the Institute and no liability is accepted in relation thereto. This magazine includes articles that have been invited from or contributed by authors. While such articles present the views of the respective authors, these articles may not necessarily represent the views of the Publishing Board of the magazine or The Hong Kong Institute of Directors. It is the intention of the Institute to present views from various perspectives, which may inspire thinking and generate constructive discussions.
《廿一世紀董事》是香港董事學會的官方雜誌。本雜誌所有出版內容的版權為香港董事學會所有。未經出版人及 / 或版權擁有人書面同意，本雜誌所有內容一律不得以任何形式或以任何工具 (電子、機械、影印、錄製或其它工具) 翻印、儲存或引進於檢索系統或傳送。本雜誌內容可供摘要引述以作研討或教育用途，但必須註明出處或出版人。本雜誌及出版機構不會為雜誌內作者及被訪者所表達的觀點、意見或建議負上責任。雜誌的內容並不一定反映香港董事學會或學會會員的觀點及意見，學會與會員均不因此而負上任何責任。本雜誌收錄邀約作者及供稿作者的文章，然而這些文章表達了其作者的觀點，卻不一定代表雜誌出版委員會或香港董事學會的觀點。學會的用意是容納多角度的意見，這或可啟發思考及產生具建設性的討論。

© The Hong Kong Institute of Directors 香港董事學會 © 版權所有

The Hong Kong Institute of Directors is Hong Kong's premier body representing directors to foster the long-term success of companies through advocacy and standards-setting in corporate governance and professional development for directors.
香港董事學會為香港代表專業董事的首要組織，其宗旨是促進所有公司的持久成就；為達成使命，
學會致力提倡優秀企業管治與釐訂相關標準，以及協助董事的專業發展。

The Hong Kong Institute of Directors Executive Office 香港董事學會行政處
2104 Shanghai Industrial Investment Building, 48 Hennessy Road, Wan Chai, Hong Kong 香港灣仔軒尼詩道48號上海實業大廈2104
Tel 電話 : (852) 2889 9986 Fax 傳真 : (852) 2889 9982 E-mail 電郵 : executive@hkiod.com
The Hong Kong Institute of Directors 香港董事學會 The Hong Kong Institute of Directors