2021 年 5 月 10 日
討論文件

立法會資訊科技及廣播事務委員會

資訊保安的最新情況

目的

本文件向委員匯報本港資訊保安的最新情況和過去一年政府在資訊保安方面的工作。

背景

2. 創新及科技是推動經濟發展的重要元素，不但帶動社會進步，還可提升市民的生活質素。在過去一年，2019冠狀病毒病肆虐全球，大大改變了企業的營商模式和市民的生活習慣；遙距營商、在家工作、遙距學習和網上購物等成為「新常態」。在更廣泛應用資訊科技的同時，網絡攻擊的威脅亦不容忽視。因此，政府、企業和市民均須提高網絡安全的認知，以持續提升整體社會的防範意識和應對能力。

資訊及網絡安全的形勢

3. 在「新常態」下，企業一方面需要進行數碼轉型，另一方面亦須積極應對轉型所帶來的資訊保安挑戰。香港電腦保安事故協調中心（事故協調中心）在2020年共處理8 346宗保安事故，較2019年的9 458宗回落12%。當中最主要的資訊保安事故類別是殭屍網絡（4 154宗）和仿冒詐騙（3 483宗）。殭屍網絡事故宗數較2019年減少16%，但仿冒詐騙的宗數則較2019年上升35%，這與全球的網絡安全趨勢大致相同。仿冒詐騙大多利用市民對疫情的關注，發布虛假資訊或偽冒衞生組織要求捐款，誘騙受害人到訪惡意網站或披露敏感資料，甚或詐騙金錢。而惡意軟件（包括勒索軟件）的宗數則大幅下降85%至181宗，由於攻擊者轉以企業為主要目標，以致針對個人的惡意軟件事故宗數大減。此外，分散式阻斷服務攻擊（DDoS）的宗數雖少，只有53宗，但較2019年卻增

幅逾43%，估計是由於疫情下各行各業更普遍提供網上服務，因而「攻擊面」增大有關。在2021年首季，事故協調中心共處理2 004宗保安事故報告，當中仿冒詐騙（988宗）和殭屍網絡（864宗）仍為主要的事故類別。有關保安事故的分項統計數字載於附件一。

4. 香港警務處（警務處）在2020年共錄得12 916宗科技罪案，較2019年的8 322宗上升55%。每宗案件平均損失金額則有所減少，由2019年約35萬元減至約23萬元，相關損失的總金額約29億6,000萬元，與2019年相若。科技罪案數字上升主要是由於網上騙案（例如網上購物騙案或網上情緣騙案）有所增加，騙徒透過互聯網、社交媒體及電郵等科技媒介犯案。在2021年首兩個月，警務處錄得2 158宗科技罪案，損失金額約5億元。有關科技罪案的分項數字載於附件二。

社會層面的資訊保安措施

5. 政府致力為社會提供一個安全穩妥的網絡環境，包括提升公私營機構及公眾對網絡安全的認知和應對能力，和培育網絡安全專業人才。政府資訊科技總監辦公室（資科辦）與事故協調中心、警務處的網絡安全及科技罪案調查科（網罪科），以及香港互聯網註冊管理有限公司（HKIRC）一直保持緊密合作，向公眾提供適當支援。

(I) 提升本港企業（包括中小企）應對各種網絡攻擊的能力

監測和應對網絡威脅及攻擊

6. 事故協調中心一直為本港互聯網社群提供電腦保安資訊。由2020年至2021年首季，事故協調中心向業界和市民發布超過450項網絡安全資訊及保安建議，以及舉辦研討會和比賽，以推廣資訊保安的良好作業模式和提高公眾對網絡安全的認知。

7. 因應網絡安全對個別行業的重要性，事故協調中心聯同多個行業商會舉辦專題講座，進一步向業界推廣網絡安全意識。由2020年至2021年首季，事故協調中心舉辦了超過25次講座，吸引逾3 200名不同界別的從業員參與，涵蓋金融服務、保險、工業、教育、零售、餐飲及資訊科技等界別。事故協調中心會繼續與各

行業商會合作，推廣網絡安全的重要性，並支援個別行業做好保安措施。

網絡安全預防服務和資訊共享

8. 為協助本地中小企業以其有限資源應對日趨複雜的網絡保安威脅，政府在2019年年中聯同HKIRC推出中小企網站免費檢驗服務，包括檢查網站是否存在安全漏洞、講解掃描報告和提供緩解方案，以協助中小企及早識別潛在的保安漏洞。截至2021年首季，HKIRC已為接近2 000間本地中小企提供檢驗服務。

9. 此外，資科辦於2020年9月將跨行業的「網絡安全資訊共享夥伴計劃」（夥伴計劃）恆常化，並聯同HKIRC合作營運，推動更多公私營機構（尤其中小企）交流網絡安全資訊。計劃至今已有超過420間公私營機構參與，涵蓋的界別十分廣泛，包括金融與保險、公用事業、運輸、醫療、電訊、創新與科技、資訊保安和大專院校等。在金融界方面，在香港銀行公會支持下，至今已有超過120間銀行參與計劃。夥伴計劃設有協作平台讓參與成員交流網絡安全威脅、緩解方法和良好作業模式等，公眾亦可在平台內的公眾區域獲取專家提供的保安警報和建議。夥伴計劃積極深化關鍵行業（例如銀行業、醫療界等）內的交流，並舉辦特定行業研討會，為行業在協作平台上設立獨立群組分享資訊等。

10. 平台將於今年稍後從更多不同渠道（包括免費的公開來源及付費的商業來源）獲取網絡安全威脅情報，並增設應用程式介面促進不同資訊保安系統之間自動交換網絡威脅資訊，讓參與的成員能更迅速防禦網絡攻擊。我們會繼續加強推廣，鼓勵更多不同界別的機構加入夥伴計劃，積極推動共享網絡安全資訊。

(II) 疫情下應對資訊保安的挑戰

11. 政府一直透過財政資助以加強企業的資訊保安水平，包括資助本地非上市企業及機構使用科技服務和方案提高生產力或將業務流程升級轉型的「科技券」。企業可以利用資助提升系統及網絡安全措施，包括防禦網絡攻擊及運作復原方案。政府在2020年4月進一步優化「科技券」，將資助項目配對比例提升至3:1，每家企業的資助上限提高至60萬元，而可獲批項目的數目上限亦增

加至6個。由2016年至今，「科技券」計劃共資助超過330個涉及提升資訊系統及網絡安全的項目，相關的資助金額約4,500萬元。

12. 政府在「防疫抗疫基金」下推出「遙距營商計劃」，資助企業採用資訊科技方案開拓遙距業務，支援企業在疫情期間繼續營運。計劃涵蓋12個與遙距營商有關的資訊科技方案類別，當中亦包括網絡安全方案，加強防範網絡攻擊，提升企業資訊系統的安全。「遙距營商計劃」共批出3 000多個與網絡安全相關的資訊科技方案，涉及的資助金額約8,200萬元。

13. 事故協調中心於2020年亦不時提供適切的保安建議及指南，例如網絡會議安全的教育影片，遙距存取和企業虛擬私人網絡保安指南等，協助企業和市民安全地使用網上服務，並針對個別行業（如醫療界、物流業等），密切留意相關網絡攻擊，適時為企業提供有關保安威脅的資訊，例如提醒企業留意仿冒詐騙及DDoS攻擊等，做好相應防禦措施。個人資料私隱專員公署（私隱專員公署）亦就在家工作發布實用指引，為視像會議服務使用者提供建議，以加強資訊保安及個人資料私隱的保障。警務處持續加強宣傳教育，提高市民的防騙意識，以免墜入網絡陷阱。在2021年，警務處把加強網絡安全和打擊科技罪行列為首要行動項目之一，透過「反詐騙協調中心」繼續打擊和預防各類詐騙以減低受害人的損失。

(III)<u>公眾教育</u>

14. 因應本港的流動裝置使用率不斷上升，資科辦、警務處和事故協調中心在2020年舉辦了一系列主題為「安全使用流動裝置」的宣傳活動，以喚起公眾對流動裝置相關的資訊安全意識。資科辦亦聯同事故協調中心，以輕鬆易明的手法製作一系列的網絡保安動畫，透過社交媒體向公眾及中小企推廣。鑑於近期不時有社交媒體平台外洩用戶個人資料的事件，事故協調中心及私隱專員公署分別發布保安博錄及指引，提醒市民使用社交媒體及即時通訊軟件的保安及私隱風險，並提供減低風險和保障個人資料私隱的實用建議。

15. 此外，資科辦聯同HKIRC在2021年3月舉辦了「網絡世界的保安與法律」網絡研討會，除了提高參與者的網絡安全知識外，

也提醒他們網絡世界同樣受到現行法律的規管，加強他們進行網上活動時的守法意識。

16. 在2019/20及2020/21（截至2021年首季）兩學年內，資科辦與專業團體共合辦了超過20次實體或遙距模式的學校探訪，向超過5 100名師生傳遞資訊保安的訊息。此外，針對長者使用資訊科技越趨普及，資科辦通過實體或遙距模式到長者服務中心舉行網絡安全講座，以提高他們的保安意識。

17. 在2020年，資科辦優化了一站式資訊保安入門網站「資訊安全網」，讓市民大眾更方便取得各類與資訊保安有關的資訊。網站根據不同主題作出分類，方便不同人士瀏覽。資科辦繼續與不同機構協作並通過不同渠道，包括網站、社交媒體、文字媒介等擴大接觸面，加強向公眾發放不同種類的網絡安全資訊。

(IV) 支持國家安全教育

18. 資科辦聯同警務處就2021年4月舉辦的「全民國家安全教育日」提供與網絡安全相關的資料作公眾教育展覽，加強市民認識網絡安全對國家安全的重要性。配合國家將於9月舉行的「國家網絡安全宣傳周」，資科辦會繼續聯同警務處和事故協調中心舉辦年度「共建安全網絡」資訊保安推廣活動，加強機構及公眾對網絡安全與國家安全的認識，並提醒他們須採取穩妥的網上行為，共同維護網絡安全，避免落入網絡陷阱，甚至誤墮法網。

資訊保安人力資源發展

19. 政府於2020年1月優化「科技人才入境計劃」，把適用範圍擴大至全港進行指定科技範疇研發活動的企業（包括網絡安全），讓更多企業可受惠於計劃和簡化手續，從而加快吸納世界各地的網絡安全科技人才來港。

20. 香港生產力促進局和事故協調中心於2020年11月合辦首屆「香港網絡保安新生代奪旗挑戰賽2020」，以培育更多有志投身資訊保安行業的人才，並提升本港大專及中學生對網絡安全的興趣。學界反應十分踴躍，接近540名來自37間中學和19間大專院校的學生，分別組成合共156支隊伍參賽。比賽將在2021年繼續舉行。

政府內部應對網絡安全威脅的措施

(I) 檢討政府資訊保安政策

21. 面對科技高速發展和新興保安威脅，資科辦在2021年3月完成《政府資訊保安政策及指引》的全面檢討工作，並頒布了經修訂和更新的版本。檢討工作參照了最新國際標準和業界的良好作業模式，並在個別保安範疇加強要求，例如參照《ISO 27701私隱資訊管理》優化對個人資料保護的管理要求、強化應用物聯網和公共雲端服務的風險管理、提升資訊系統的軟件管理及測試等要求。因應疫情期間部門對在家工作的需要，經修訂和更新的版本亦同時加強遙距接達部門網絡和資訊系統的保護。最新的《政府資訊保安政策及指引》已上載資科辦網站供公眾參閱。

(II) 推動智慧城市建設的保安

22. 政府在2020年發布《香港智慧城市藍圖2.0》，致力透過更廣泛使用科技改善市民的生活和協助抗疫工作，如「智方便」平台、「居安抗疫」檢疫系統、「安心出行」感染風險通知系統、新一代政府雲端基礎設施及大數據分析平台等。在開發相關系統及基礎設施時，政府一直嚴格遵守《政府資訊科技保安政策及指引》和《個人資料（私隱）條例》的規定，並在推行項目的不同階段時，聘用獨立第三方進行私隱及資訊保安風險評估及審計，以確保系統及數據的安全和市民的私隱得到穩妥的保障。

(III)資訊分享及威脅警報

23. 過去一年，資科辦利用大數據分析收集和分析不同來源的網絡安全威脅資訊，進行整理及評估，加強發布網絡威脅及預警能力，並提醒部門盡快修正保安漏洞。資科辦在2020年至2021年首季共發出超過120次關於電腦系統或軟件漏洞的保安警報，並要求各局和部門迅速採取適切的防禦措施，確保政府的資訊系統和數據資產安全。

(IV) 員工培訓及技術支援

24. 資科辦聯同警務處於2021年1月舉辦第五屆「跨部門網絡安全演習」，通過演習和工作坊模擬多個網絡攻擊情境，讓各部門

人員了解與遙距工作相關的網絡攻擊手法和實習事故處理程序，提高政府部門防禦和應對網絡安全事故的能力。

25. 在2020年，資科辦舉辦了多個網上研討會及解決方案展示會，以提升政府人員的資訊保安知識。在2020年至2021年首季，約2 000名政府人員藉此認識最新的網絡安全趨勢及在家工作的資訊保安預防措施。資科辦亦舉辦了「全政府防範仿冒詐騙演習運動」，並鼓勵員工考取國際認可的資訊保安證書，以鞏固和提升專業知識。

26. 資科辦繼續強化網絡及系統檢測平台的功能，協助各局和部門為其網上系統及網頁進行安全檢測及滲透測試，及早找出潛在漏洞並進行修補。在2020年至2021年首季，該檢測平台為超過830個政府網站和各個與抗疫相關的緊急系統提供適時和便捷的安全檢測服務。

(V) 遵行審計

27. 資科辦定期為局和部門進行獨立的資訊保安遵行審計，確保他們嚴格執行政府的保安規定，並提供建議協助他們持續改善保安管理系統，以應對新興資訊保安威脅。遵行審計的報告會直接呈交部門首長作參考和跟進。截至2021年首季，資科辦為21個局和部門完成新一輪審計工作，並預期於2022年首季內為所有局和部門完成審計。

展望

28. 除了繼續與不同界別的企業和機構合作提高社會各界對網絡安全的認知和能力外，政府會繼續加強本地網絡安全人才的培訓、推廣資訊安全的良好作業模式、透過不同措施提升企業網絡的安全，以及與國際及內地合作和分享資訊保安情報，構建香港成為一個安全穩妥的智慧城市。

徵詢意見

29. 請委員備悉文件內容。

創新及科技局
政府資訊科技總監辦公室
2021 年 5 月

附件一

香港電腦保安事故協調中心
處理的保安事故分項統計數字

事故類別	**2019** 年		**2020** 年			**2021** 年 **(**截至 **3** 月**)**	
	宗數	百分比	宗數	百分比	與 **2019** 年比較 **(**百分比**)**	宗數	百分比
殭屍網絡	4 922	*52*	4 154	*50*	*-16*	864	*43*
仿冒詐騙（包括釣魚電郵及網站）	2 587	*27*	3 483	*42*	*+35*	988	*49*
惡意軟件（包括勒索軟件）	1 219	*13*	181	*2*	*-85*	23	*1*
分散式阻斷服務攻擊	37	*<1*	53	*<1*	*+43*	5	*<1*
黑客入侵／網頁塗改	48	*<1*	36	*<1*	*-25*	4	*<1*
其他[1]	645	*7*	439	*5*	*-32*	120	*6*
總計：	**9 458**	***100***	**8 346**	***100***	***-12***	**2 004**	***100***

[1] 包括身分盜竊、資料外泄等

附件二

香港警務處處理
有關科技罪案宗數及其導致的財政損失的統計數字

	2019 年	**2020 年**		**2021 年 (截至 2 月)**
案件性質	**宗數**	**宗數**	**與 2019 年比較 (百分比)**	**宗數**
網上騙案	5 157	10 716	*+108*	1 921
（i）網上商業騙案	*2 317*	*6 941*		1 040
（ii）電郵騙案	*816*	*767*		93
（iii）網上銀行騙案	*3*	*0*		0
（iv）社交媒體騙案	*1 678*	*1 988*		476
（v）網上雜項騙案	*343*	*1 020*		312
網上勒索	300	1 144	*+281*	142
（i）裸聊	*171*	*1 009*		119
（ii）其他網上勒索	*129*	*135*		23
盜用電腦[2]	71	111	*+56*	14
其他性質	2 794	945	*-66*	81
總計（宗數）：	**8 322**	**12 916**	***+55***	**2 158**
財政損失（百萬元）：	**2,907**	**2,964**	***+2***	**511**

[2] 包括網上戶口盜用、入侵系統活動和分散式阻斷服務攻擊