網絡安全行業

研究報告

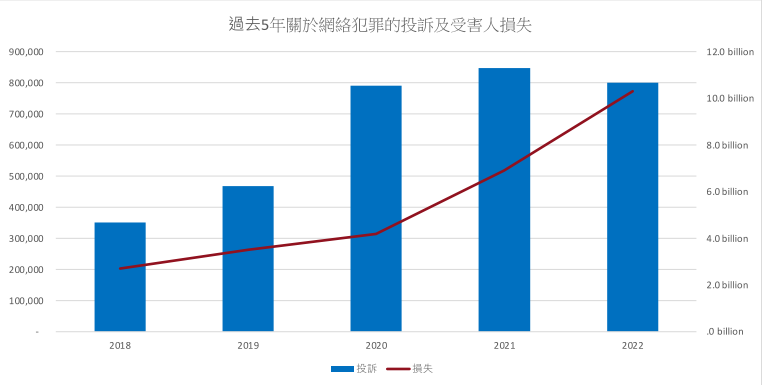
報告日期 2023 年 10 月 24 日

馬山資本研究團隊
info@masancapital.com

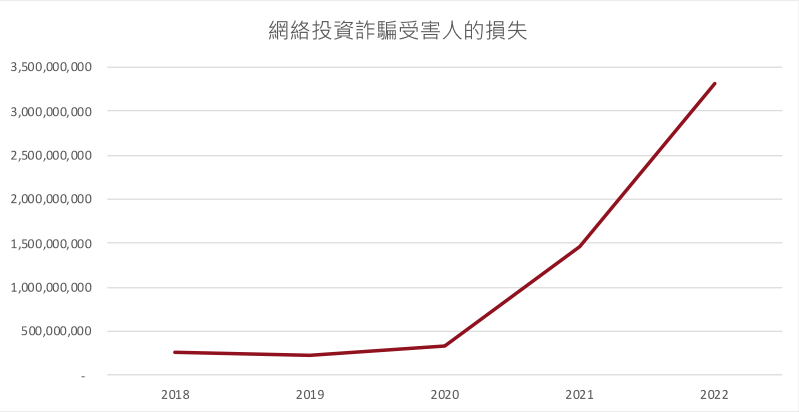
人工智能是今年股市備受追捧的概念，其發展也會對各行各業產生重大影響。而人工智能、物聯網以及人機交互（human-computer interaction）等科技的運用和發展必然會伴隨着更進一步的數碼化，令到網絡安全日益重要。根據 Acumen Research and Consulting，以人工智能為基礎的網絡安全方案的全球市場將會於 2030 年達致 1,338 億，由 2022 年到 2030 年的複合年均增長率（CAGR）高達 27.8%。我們接下來將會由需求以及供應兩方面評估人工智能時代對網絡安全的影響，以及哪一些上市公司值得留意。

網絡犯罪日益嚴重

根據聯邦調查局的《2022 網絡罪案報告》顯示，2018 年網絡犯罪導致的經濟損失為 27 億美元，而 2022 年則為 103 億美元，過去 5 年的 CAGR 為 30.7%。在這 103 億美元當中，有 33.1 億美元為投資詐騙，相較於 2021 年的 14.5 億美元，增長 127%。在這些投資騙案中，有 25.7 億美元為加密貨幣投資詐騙，而 2021 年僅有 9 億美元為加密貨幣投資詐騙，增長率達 183%。



資源來源：聯邦調查局、馬山資本

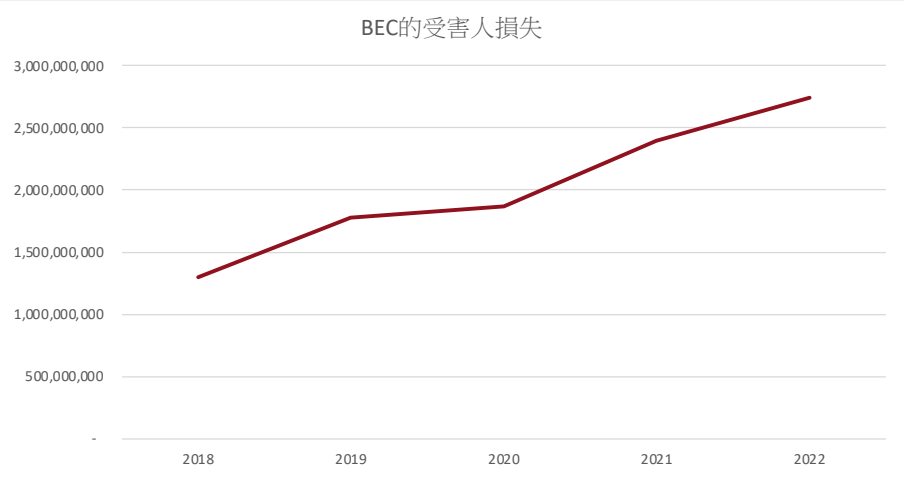


資源來源：聯邦調查局、馬山資本

近年騙案導致的經濟損失的增長，除了因為駭客以及騙徒的手法因為科技的進步而越發高明之外，亦因為人們重度依賴網絡，而增加了受到網絡攻擊或詐騙的風險。因此，我們將會從「人工智能如何增加網絡攻擊或詐騙的效率」以及「人工智能、物聯網以及人機交互等科技發展及運用如何增加人們對於網絡攻擊或詐騙的脆弱性（vulnerability）」這兩個角度來分析對網絡安全的需求。

人工智能時代的社交工程

社交工程（social engineering）一直是網絡安全的重要一環，因為哪怕安全系統設計得天衣無縫，執行人或用家仍然是有弱點的，讓駭客或者騙徒有機可乘。人工智能可以讓罪犯把社交工程進一步應用於網絡陷阱上，例如現時的釣魚訊息和電郵普遍而言都是通用的，缺乏針對性。而人工智能的應用則可以生成大量更加個人化和複雜的訊息內容，以及令被害人更難發現對方是騙徒。事實上，現時已經有這樣的人工智能出現，那就是 FraudGPT 以及 WormGPT。它們都是在暗網上售賣的人工智能產品，FraudGPT 每個月只需要付 200 元美金（一年則只需要 1700 元美金）就可以使用。不同於 ChatGPT，這些人工智能沒有內置限制，可以生成欺騙內容例如釣魚電郵以及提供資料協助駭客攻擊。這些人工智能的另一項用處則是幫助網絡罪犯跨越語言障礙，令他們可以詐騙說其他語言的人。而社交工程是商務電郵入侵（business email compromise，簡稱 BEC）的重要一環，它們利用電郵模仿他人來讓受害人轉錢。BEC 佔網絡犯罪相當大的部分，在 2022 年導致了約 27 億美金的損失。



資源來源：聯邦調查局、馬山資本

人工智能生成的虛假內容

除了大型語模型（large language model）的人工智能可以幫助網絡罪犯，其他如 DeepFake 以及生成語音內容的人工智能都可以對人們產生威脅。因為這些網絡罪犯可以利用這些工具模仿受害人熟識或信服的人，並誘騙他們以達成自己的目的。例如現時社交媒體已經出現大量假扮名人傳授投資秘訣的詐騙廣告。一旦這些網絡罪犯成熟地使用這些工具製作短片廣告，將會更有說服力，令更多人受害。事實上，這種新型騙案已經出現。早前在 TikTok 上，已經有騙徒利用 DeepFake 假扮 Mr.Beast（一位以經常派發獎品和獎金而出名的 YouTuber，也是現時最多訂閱人數的 YouTuber），聲稱觀眾可以以 2 元美金購買新的 iPhone。也有人假扮英國廣播電台（BBC）的新聞主播詐騙。這些令人防不勝防的詐騙

手段，將會令市場對人工智能網絡安全服務的需求大增，例如以人工智能檢測影片是否有 DeepFake 的痕跡，某一封電郵是否為寄件者利用人工智能生成的釣魚電郵等。

資料下毒對人工智能的威脅

除了人工智能會令網絡犯罪更防不勝防，令市場對於先進的網絡安全方案有更高的需求外，人們越來越依賴數碼、網絡工具，也令他們暴露於網絡攻擊的風險增加。例如針對人工智能的資料下毒（data poisoning）以及針對物聯網、無人駕駛和人機交互的駭客攻擊也會對人們造成更大的傷害。

資料下毒是一個在人工智能時代的新威脅。人工智能向來有「垃圾進，垃圾出（garbage in, garbage out）」之說，因為模型的準確性和效率高度取決於資料的質量。而資料下毒則是針對人工智能訓練用的數據集的攻擊。駭客可以透過改變數據集的部分數據或注入某些數據，來 1）降低該人工智能模型的準確性，或；2）加入「後門」。前者很易理解，而後者可以舉一個例子來解釋。假如政府為某一個地區安裝攝像頭，並且利用人工智能跟蹤該地區的行人的去向，但是有駭客資料下毒，使得只要戴紅帽子，人工智能就會不能辨別他是行人，從而令人工智能對戴紅帽子的人失去作用。相比第一種攻擊，第二種攻擊隱蔽得多，因為在前設條件未滿足時，模型仍然是運作正常的，只有滿足條件後，才會觸發駭客想要的結果，因此潛在傷害也大得多。

物聯網時代的勒索病毒

物聯網是一種高度依賴數據傳輸科技的系統，因為涉及的裝置繁多，也令它更容易成為攻擊的目標，而一旦被攻擊成功，將會造成嚴重的後果，因為駭客將會可以癱瘓整個系統。事實上，在 2023 年上半年，美國就有 220 宗以上針對醫療系統的勒索病毒（ransomware）攻擊，超過 3,600 萬人受到影響，反映網絡攻擊對於物聯網時代可以造成的嚴重後果。可以預想當無人駕駛技術獲得大規模應用時，一旦有駭客成功攻擊，造成的損失不會比這些攻擊少。

人機交互技術有很多種，有傳統的圖形使用者介面（Graphical User Interface，GUI），智能管家例如 Alexa，或者研發當中的腦機交互技術。但是隨着人機交互技術的發展，人們的現實生活必然會進一步數據化及數碼化，資料洩漏的風險將會進一步增加。

監管的進一步加強

網絡攻擊的風險增加，除了會令人們以及企業更加重視網絡安全外，政府以及監管部門也會推出不同的規例，要求企業遵從一些網絡安全的標準。例如美國聯邦政府在今年年初就發佈了「National Cybersecurity Strategy 2023」，在第三支柱中重點強調私人市場的重要性，包括保存國民資料的公司需要為其安保負責、需要推動安全的物聯網設備的發展、私人企業必須要為自己產品的網絡安全性負責以及聯邦政府將會資助私人企業並與它們合作去建立安全的數碼生態系統等。預計美國政府將會收緊網絡安全的規例，屆時大量企業將會為了合規而提高其服務及產品的網絡安全標準。

人工智能在網絡安全行業將會擔當的重要角色

在供應方面，人工智能的發展將會為網絡安全帶來各種好處，但是從生意角度，人工智能帶來的效益主要是：1）進一步提升網絡安全方案的成本效益，利用人工智能為客戶分析客戶的行業和公司特點，甚至以人工智能作為安全顧問，結

合實時數據提供最合適的方案；2）模擬社交工程攻擊，幫助企業偵測出潛在的漏洞，也可以以此為員工提供更擬真的網絡安全教育。

前者可以以更低的成本為中小企提供專業的服務，而中小企正是最缺乏網絡安全措施的一群。根據歐盟網絡安全局於 2021 年的調查顯示，中小企面對網絡攻擊的最大挑戰是：1）缺乏網絡安全意識；2）預算問題，尤其中小企只能負擔最基本的網絡安全服務，例如防火牆和防毒軟件等，而更先進的服務往往是為大型企業設計的方案中的一部分。因此，當人工智能安全顧問獲得大量應用時，將會可以滿足中小企對於網絡安全的需求，成為整體市場規模增加的關鍵點。

根據 Global Market Estimate 的預測，全球網絡安全意識練訓的市場將會由 2022 年的 18.5 億美金增長至 2027 年的 121.4 億美元，CAGR 達 45.6%。而 AI 在這些教育當中將會扮演重要的角色。社交工程攻擊是利用企業員工和管理層的人性漏洞來進行攻擊，但是這類型的攻擊往往因為 1）一般的講座或者課程終究只是紙上談兵，以及；2）因為受訓人覺得自己不會中這些社交工程陷阱，而令到針對社交工程攻擊的訓練難以收效。因此一些大型企業會聘請團隊來模擬社交工程攻擊，一來提高員工的安保意識，二來也是檢查安保系統有沒有漏洞。但是這種方式往往只能夠用於少數管理層或員工身上，因為成本太高。但是有了人工智能後，這種模擬的成本將會降低，並且可以大量應用，甚至日常化，令員工保持網絡安全意識。同時，也可以讓中小企也使用這種服務。

值得關注的公司

(百萬美元)						
CrowdStrike	2021	2022	2023	Q1	Q2	
收益	874.4	1,451.6	2,241.2	692.6	731.6	
銷售及市場推廣開支	401.3	616.5	904.4	281.1	282.9	
銷售及市場推廣開支佔收益比	45.89%	42.47%	40.35%	40.59%	38.67%	
研發開支	214.7	371.3	608.4	179.1	179.4	
研發開支佔收益比	24.55%	25.58%	27.14%	25.85%	24.52%	
CloudFlare	2020	2021	2022	Q1	Q2	
收益	330.0	509.3	742.6	290.2	308.5	
銷售及市場推廣開支	217.9	328.1	465.8	137.0	146.7	
銷售及市場推廣開支佔收益比	66.02%	64.42%	62.72%	47.21%	47.55%	
研發開支	127.1	189.4	298.3	81.5	89.6	
研發開支佔收益比	38.53%	37.19%	40.17%	28.10%	29.05%	
Palo Alto Networds	2020	2021	2022	Q1	Q2	Q3
收益	4256.1	5501.5	6892700	1563.4	1655.1	1720.9
銷售及市場推廣開支	1753.8	2148.9	2544	615	625.5	639.5
銷售及市場推廣開支佔收益比	41.21%	39.06%	0.04%	39.34%	37.79%	37.16%
研發開支	1140.4	1417.7	1604	371.8	404.1	413.7
研發開支佔收益比	26.79%	25.77%	0.02%	23.78%	24.42%	24.04%
CheckPoint	2020	2021	2022	Q1	Q2	
收益	2064.9	2166.8	2329.9	566.2	588.7	
銷售及市場推廣開支	569.9	597.8	675.2	177.7	185.6	
銷售及市場推廣開支佔收益比	27.60%	27.59%	28.98%	31.38%	31.53%	
研發開支	252.8	292.7	349.9	91.5	87.4	
研發開支佔收益比	12.24%	13.51%	15.02%	16.16%	14.85%	
Fortinet	2020	2021	2022	Q1	Q2	
收益	2594.4	3342.2	4417.4	1262.3	1292.8	
銷售及市場推廣開支	1071.9	1345.7	1686.1	478.3	515.9	
銷售及市場推廣開支佔收益比	41.32%	40.26%	38.17%	37.89%	39.91%	
研發開支	341.4	424.2	512.4	151.1	153.3	
研發開支佔收益比	13.16%	12.69%	11.60%	11.97%	11.86%	

資料來源：公司資料、馬山資本

以上為 5 間具代表性的網絡安全公司，我們可以從它們中發現這個行業的成本結構有甚麼特點。從上圖可見，網絡安全公司普遍而言銷售及市場推廣開支高，是其所有開支中最高的一項，甚至比研發開支更高。這是因為網絡安全行業競爭激烈，而且網絡安全是一個複雜的範疇，行外人難以理解當中的原理，更遑論其重要性。因此，市場推廣開支高企，也有部分原因在於教育客人的成本。但是，在人工智能可以擔當網絡安全顧問之後，將會可以令網絡安全公司更有效地科普網絡安全的重要性，以及告知潛在客人其面對的潛在網絡安全威脅，從而減省網絡安全公司的教育成本。

因為一般的大型企業都有專門負責網絡安全系統的人材，甚至設有首席安全官（chief security officer）的職位，所以人工智能顧問只能夠起到輔助的作用，因為這些人已經是網絡安全專家，清楚自己的需求以及市場上有哪些方案提供。相反，中小企一般缺乏這方面的人力資源，而人工智能顧問將會可以幫助網絡安全公司開拓這一片藍海。因此，我們將會從 1）產品特點是否符合中小企的需求、2）其對人工智能的應用這兩方面入手選出值得留意的網絡安全公司。

CrowdStrike（Nasdaq: CRWD）是一間專門提供端點保護的網絡安全公司。端點是指透過網絡（無論是互聯網還是內聯網）溝通的設備，可以是電腦、手機、伺服器甚至物聯網中的智能設備。而端點保護則是指針對這些設備的保護，讓它們免於網絡攻擊。電郵伺服器、公司的路由器、公司內部儲存檔案及資料的伺服器都是端點。而針對端點的網絡攻擊的其中一個特性就是只要有其中一個端點的攻擊成功，就有可能獲得對網絡中其他端點的訪問權限，令到其他端點也受到

攻擊。例如一個員工的電腦被攻擊成功，從而令到公司伺服器也被攻擊成功。因此端點保護也越發重要。而 CrowdStrike 專門提供端點保護，其 Falcon 平台讓客人可以以模組的方式訂閱不同的保護方案，具備靈活性之餘，其專門提供端點保護服務也令其服務的複雜性降低，讓客人更容易部署（deploy）。更重要的是，CrowdStrike 除了在其網絡安全方案中有利用人工智能外，今年亦推出 Charlotte AI，這是一個基於大型語言模型、可以作為顧問的人工智能，解決中小企缺乏網絡安全專家的難題。它可以檢查一次客人的網絡系統，並且指出有甚麼潛在威脅以及風險，並且解答客人對於網絡安全的疑問。

Cloudflare（NYSE: NET）是一間專門提供網站相關的網絡安全服務公司，其提供包括內容傳遞網路（content distribution network）、DDoS 保護、網頁應用程式防火牆（web application firewall）等。其客戶群主要是一些有網頁的公司，尤其是電子商務、網上媒體內容的公司。因為它們網站的流量大、涉及敏感資料（例如登入資料以及信用卡資料），因此特別容易成為攻擊對像。而且，網站的安全漏洞也可能令其伺服器成為其中一個可被攻擊的端點，從而令公司的內部資料有外洩的風險。跟 CrowdStrike 一樣，Cloudflare 因為專攻網站安全這一個範疇，令到其產品服務有容易部署的優勢。不過其對於人工智能的應用暫時僅限於提升其網絡安全系統上，未有任何利用人工智能作為顧問的消息。

Palo Alto Network （Nasdaq: PANW）、Check Point（Nasdaq: CHKP）以及 Fortinet（Nasdaq: FTNT）相較於 CrowdStrike 和 Cloudflare 的優勢在於它們更全面的網絡安全方案，既有端點保護及網站安全方案，也有次世代防火牆、雲端安保等服務，除了軟件產品外，亦有硬件產品。簡而言之，因為其產品矩陣的全面性及多樣性，讓其可以為不同的客人客製化不同的一站式網絡安全方案。但是亦因為其方案涉及多種不同的工具，令其方案部署難度增加。而日常的使用和管理，也需要客人內部有網絡安全的專家才行。而且這三間公司也暫時未有人工智能顧問的消息，因此其使用門檻令其不易受中小企的青睞。

綜上所述，CrowdStrike 是比較值得留意的網絡安全公司，因為其有產品簡單明瞭的特點，也有利用人工智能為其客人提供顧問服務，更容易開拓中小企這個藍海市場。而 Cloudflare 的產品定位與 CrowdStrike 不同，但是同樣具備專門性，而且容易入手的特點。至於 Palo Alto Network、Check Point 以及 Fortinet 則要留意其後續有沒有降低產品入門門檻的手段。

CONTACT INFORMATION

☏ +852 3905 4615
✉ info@masancapital.com
🌐 www.masancapital.com

8/F, Aubin House, 171-172 Gloucester Road, Wan Chai, Hong Kong
香港灣仔告士打道 171-172 號安邦商業大廈 8 樓