IBM 資安大預言
回顧2018 展望2019

The Top Cyber Security Trends in 2018
and Predictions for the Year Ahead

IBM Security

《經濟學人》尊稱為 "Security Guru"，著有 13 本資安書籍，享譽業界的知名大師：IBM Resilient 科技長暨 IBM Security 特別顧問布魯斯．施奈爾（Bruce Schneier），日前帶領其他四位專家發表線上對談，匯整 2018 資安重大趨勢發展與 2019 預測，本期《資安戰情室》為您摘要重點。

- *2018 年重要趨勢回顧*
- *2019 年值得觀察的趨勢發展*
- *2019 年給資安長的建言*
- *2019 年資安大預言*
- *給台灣企業的建議*

回首來時路：2018 年重要趨勢

■ IoT 物聯網安全威脅程度增高

IoT 擅長以自動化方式收集資料，在現今的業務流程中扮演關鍵角色，自然成為攻擊者虎視眈眈的新目標。許多企業的資安長 (CISO) 也被高層期待在負責網路安全 (cyber security) 之時，也同時扛起實體安全 (physical security) 的責任。然而隨著 IoT 的爆紅，許多公司積極投身這個新興產業，在進行 IoT 軟硬體開發之時容易求快而遺留下安全漏洞，為 IoT 的安全埋下隱憂。我們期待看到業界能推出一套 IoT 物聯網安全的完整架構，來解決這個問題。

■ 資安「平台」之戰日趨火熱

安全的領域分工太過精細，致使產品與解決方案的種類數量實在是汗牛充棟。尤其現在雲端與 IoT 應用更是方興未艾，企業難有足夠的自有資安人力，能同時精通所採用的環境與工具。但就像 IT 的運營一樣，資安的精髓並不在依賴個別工具的功能，而在於完整嚴密的流程。我們需要的是一套將安全功能內建在基礎架構的「平台」(platform)：能夠透過 open API 或 ecosystem 的設計，極大限度地包容各家產品，善用新的人工智慧與機器學習技術，提供底層共通的分析 (Analytics)、協調 (Orchestration) 與自動化 (Automation) 能力。企業則可將寶貴的自有安全團隊資源留給安全政策與流程的規劃與監督執行，然後透過專業的安全管理服務業者或系統整合業者的協助，挑選最適合該企業需求的安全運營模式、平台、並管理所採用的工具。

■ GDPR 之施行

號稱「史上最嚴格個資法」的歐盟《一般資料保護規範》(General Data Protection Regulation, GDPR) 在 2018 年 5 月上路了，目前尚未看到大規模的實際執法動作。資安長們期待能得到更多協助，讓對個資與隱私的保護不僅僅是列在紙上的規範與罰則，而能真正化為可運營、可執行的動作。那，就讓我們靜觀其發展吧！

> *2018 年重要趨勢*
>
> - IoT 物聯網安全威脅程度增高
> - 資安「平台」之戰日趨火熱
> - GDPR 之施行

2019 資安聚光燈：人工智慧、雲端資安、SOC 2.0

■ 人工智慧 AI 與機器學習 (Machine Learning, ML) 在資安的運用

人工智慧 AI 與機器學習 ML 擅長對大量資料進行規律性的蒐集、分類與分析研判。我們預見 AI 與 ML 技術應用在諸如弱點掃描 (Vulnerability Scanning)、滲透測試 (Penetration Test)、威脅偵測 (Threat Detection) 等安全領域將大有可為。事實上 AI 與 ML 的無窮潛力尚待挖掘，其重要性與威力甚至可比擬為 IT 世界裡的「曼哈頓計劃」（第二次世界大戰期間研發與製造核子武器的計劃）一般。

■ 我們需要完整的雲端資安架構

隨著雲端運算技術與環境的逐步普及，它已然一步步建立起信譽，成為機關與企業整體資訊架構中不可忽視的一環。資安當然也必須將雲端環境納入整體考量。許多資安廠商短期內著力於先將既有的產品功能「雲端化」，讓企業能在雲端環境使用現有資安工具的功能。但如果

未來越來越多的運算工作與資料儲存直接在雲端發生，長遠之計還是必須從雲端底層提供共通的安全防護架構，像是分析、協調與自動化能力等等。我們期待看到業界對雲端資安整體架構的設計有更大刀闊斧的新動作！

■ 資安監控中心 SOC 2.0 進化轉型

前面提到過許多資安長開始被高層期待同時扛起網路安全與實體安全 的「整體安全」責任。我們預見一些資安監控中心 SOC 也會開始啓動這一方面的進化轉型，將實體世界的安全防護工作一併納入 SOC 廣義的管理範疇（所以不只是「資安」，該改叫「安全」監控中心？）。未來的 SOC 應該要更積極配合企業業務需求，提供更直覺、視覺化的工具，作到更平順的運營管理。

2018 資安聚光燈

- 人工智慧 AI 與機器學習 (Machine Learning, ML) 在資安的運用
- 我們需要完整的雲端資安架構
- 資安監控中心 SOC 2.0 進化轉型

2019 年對資安長的建言

■ 選定資安標準

為了符合法律規定，以及跟企業高階管理團隊以及企業的股東 / 客戶有效溝通，資安長應該遵循一套明確的資訊安全標準（譬如像 ISO 27000 系列、NIST 網路安全框架（NCF），或是其他標準），並能清楚說明涵蓋的範圍。當遇到董事會或客戶質疑安全事項的時候，資安長若只是一味強調：「我們有做事，我們有設置一座 SOC 中心耶」，卻沒辦法明確解釋作到甚麼程度，是不及格的喔！

■ 以明確的資安指標與高階主管溝通

面對新攻擊手法層出不窮，新防禦科技蓬勃發展，資安長必須能將技術語言轉化成商業語言，以更簡單明瞭的績效指標，讓企業的董事會與高階主管理解資安長的工作成效，這對資安長的職涯發展更是有正面的助力！

■ 增強技術組合的管理能力

就像理財的投資組合 (portfolio) 一樣，資安長掌管了安全技術與解決方案的投資組合。但企業不可能有無限的資源，每樣技術都專精熟練。資安長必須盱衡全局：在有限的資源條件之下，那些核心技能必須由自家安全團隊牢牢掌握？哪些領域的運營必須自己操刀？那些工作可以尋求外部資源的協助？如何對外部的安全供應商（譬如像安全管理服務廠商，或是系統整合廠商）作有效的評估與管理…。

2019 年我們建議資安長：

- 選定資安標準
- 以明確的資安指標與高階主管溝通
- 增強技術組合的管理能力

2019 資安大預言

■ IoT 安全災難爆發？

IoT 物聯網設備的興起肯定存在許多風險和漏洞。無論是否即將發生重大攻擊，IoT 物聯網安全都需要成為 2019 年安全團隊的首要任務。

■ 持續的風險管理將幫助企業更好地理解風險

今天，風險評估和漏洞掃描為機關與企業提供了某一時間點的安全狀況和威脅形勢。但在 2019 年，這還不夠。安全團隊，以及董事會成員與高階主管們，需要有關的實時資訊來理解所面臨的風險，以及需要採取哪些措施來減低風險。建立持續風險管理系統將有助於安全團隊滿足這一需求。

■ 資安自動化 (Security Automation) 將產生意想不到的負面後果

安全事件回應自動化和協調是一種越來越流行的方式，資安團隊可以簡化重複流程並提高分析人員的效率。但貿然將定義不明確的流程自動化可能會產生更大的問題，就像在 IT 領域中，我們常見到某些自動化流程意外將系統關閉的例子一般。在 2019 年，我們將看到安全自動化以不可預見的方式傷害企業的例子。為避免這種情況，企業需要考慮在編排事件回應流程時專注於協調人員、流程和技術，並有條不紊地採用自動化來進一步增強其安全團隊的能力。

■ 新法律將為合規的機關企業提供安全庇護

美國俄亥俄州的一項待定法律有望成為美國第一個數據隱私法規：為符合安全法規的機關與企業提供侵權索賠的安全港。換句話說，如果一個機關或企業已經遵守其監管義務，卻仍發生數據洩露事件，它將受到保護，免受與該違規行為相關的訴訟。我們預期各國也會開始推動類似的法案。

給台灣企業的建議

人工智慧 AI 的發展突飛猛進，我們自然不應忽略這項利器。但是運用 AI 不代表企業要自己去鑽研 AI 的技術，而是應該善用全球夥伴協作的力量，選用已經具有 AI 能力為後盾的解決方案與服務，這樣不僅節省企業的資源投入，也能馬上享受到全球最先進的安全防禦功能。

預測 2019 年資安態勢

- IoT 安全災難爆發？
- 持續的風險管理將幫助企業更好地理解風險
- 資安自動化 (Security Automation) 將產生意想不到的負面後果
- 新法律將為合規的機關企業提供安全庇護

此外，去年發生了知名高科技企業的資安事件，想必大家記憶猶新。連世界級的模範生都難逃安全事件的考驗，期待絕不出事看來也只能是夢想！台灣的機關企業在持續加強防禦之時，應該也要正視「事件應變」的重要性，定義好事件應變流程 SOP，並結合自動化與協調的能力，來降低與管控傷害。

最後，因應台灣的「資通安全管理法」已經在 2018 年 5 月經立法院三讀通過，接下來的挑戰就是施行細則與如何遵循。許多公務機關與關鍵基礎設施提供者（企業）都將受其規範。機關或企業的資安長應該掌握時機，選定明確的資安標準，以此為本去推動落實，檢視防禦的成效，才能符合法規的要求、滿足主管機關或董事會的期待、以及對股東與客戶的有效溝通。

聆聽完整線上會議內容

想詳細聆聽 IBM Resilient 的年終線上會議內容嗎？**點此聆聽完整線上論壇**。

與我們連繫

若您有任何與 IBM 資安情報、資安產品或資安服務等疑問，歡迎來電 0800-016-888 按 1，或前往 **https://www.ibm.com/tw-zh/security** 與線上業務代表互動。