物聯網應用的資訊安全與資料保護：Verkada 物聯網資安事件分析

1136409 洪立恒

一、引言

1. 案例簡介

Verkada 是一家智慧監控系統的物聯網公司，提供雲端監控攝影機與管理平台的相關服務。2021 年 3 月，Verkada 發生了一起重大資安事件，駭客團體成功入侵 Verkada 的系統，取得了超過 15 萬台攝影機的即時影像與存檔影片。這些攝影機分布於全球各地，包括醫院、學校、企業、監獄等場域。駭客甚至能夠透過攝影機的管理後台，直接竊取使用者的個人資料、設備設定及其他重要數據。
這起事件暴露了物聯網應用中資訊安全與資料保護的嚴重挑戰，並引發了對物聯網設備管理與監控的廣泛關注。

2. 物聯網的發展與挑戰

- 物聯網技術（Internet of Things)
  物聯網（英語：Internet of Things，簡稱IoT）是一種計算裝置、機械、數位機器相互關聯的系統，具備通用唯一辨識碼（UUID），並具有通過網路傳輸數據的能力，無需人與人、或是人與裝置的互動。而該技術的目標是實現設備之間的數據交換與互動，從而實現智慧化的應用與服務。

- 物聯網核心概念

  A. 設備聯網
     透過網路將各種物理設備（如家電、車輛、醫療設備、工業機器等）連接起來，使它們能夠進行通信和協作。

  B. 環境感知
     透過感測器（如溫度、濕度、光線、GPS 等）收集環境數據，並傳輸到雲端或本地伺服器進行處理。

C. 數據分析

收集的數據經由人工智慧（AI）或大數據技術進行分析，以產生有價值的洞察或觸發自動化行動。

D. 自動化

設備根據處理後的數據進行自動化操作，例如智慧家居中的燈光自動調節或工廠設備的自動維護。

- 技術架構

物聯網架構一般來說有三層與四層架構之分，三層的架構從底層到頂層依序為感知、網路和應用，四層架構則是將應用層再拆分成「平台工具層」與「應用服務層」，對於軟體應用做更細緻的區分。

A. 感知層

物聯網的基礎即是要讓物理設備連接網路，但須給每一個物件分配標誌和位址。早期使用無線射頻辨識標籤，如今則使用網際網路進行連接。此外因目前主流的 IPv4 位址空間有限，因此物聯網傾向使用下一代網際網路協定 IPv6。

B. 網路層

物聯網有多種聯網技術可供選擇，依照有效傳輸距離可區分為短距離、中距離、長距離以及有線技術。

短距離：藍牙、無線射頻、Wi-Fi 或 NFC 等

中距離： LTE、5G 等

長距離：低軌衛星等

有線技術：乙太網路、電力線通訊等

C. 應用層

應用層可再細分為「平台工具層」與「應用服務層」。平台工具層為底層的軟體平台，作為應用服務層與網路層的介面，以支援各類的軟體應用；應用服務層針對不同的應用需求，直接呈現原始資料，或經過加值處理，藉由人機界面提供使用者，或是對應的硬體/軟體目標得到想要的資訊。

平台工具：區塊鏈、人工智慧、防毒軟體等。

應用服務：AR/VR、人機互動、永續發展等。

- 物聯網技術的應用

  當今已有大量物聯網技術存在於我們的生活之中，舉例如智慧家具、智慧城市、醫療健康等，皆旨在提升人類社會中的便利以及效率。

  A. 智慧家具：智慧音箱（如 Google Nest 或 Apple HomePod）可以控制燈光、冷氣或音樂等等，或是家用監視器提供使用者遠端監控家中狀況。

  B. 智慧城市：即時交通流量監測與信號燈控制，有效減少城市交通壅塞。

  C. 醫療健康：智慧手錶（如 Apple Watch 或 Garmin）可以監測心跳、步行數、血氧甚至是睡眠狀況，並適時提醒使用者該注意哪項數據。

  D. 車聯網（V2X）：近期熱門的自動駕駛（如 Tesla 的 FSD），透過車輛偵測結合邊緣運算功能實現自動駕駛，同時也能讓使用者隨時監控車輛狀況。

二、分析

物聯網技術在現代生活中迅速普及，帶來了極高的智能生活環境，但同時其「聯網」之特性也帶來了資安與資料保護的挑戰。由於其「分散性」，數量龐大且分佈廣泛，在終端上也出現了更廣的攻擊面，且基於大多數物聯網設備的硬體限制，無法做到強大可靠的加密或安全防護，並且在長時間使用的情況下缺乏定期更新機制，導致漏洞難以及時補救。還有資料敏感性的問題，對於處理有觸及隱私權部分的數據，一旦洩漏就可能造成種大筍師。

1. Verkada 事件的問題根源

- **弱密碼與憑證管理**：駭客能夠利用 Verkada 的管理者身份憑證取得授權，這表示 Verkada 本身的密碼管理與憑證保護存在嚴重的漏洞。根據報導，這些憑證來源都是 Verkada 內部員工的帳號，駭客透過網路釣魚以及洩漏的憑證取得帳號內容。

  根據 Yiping Cheng 的報告[4]指出，駭客經常利用漏洞掃描技術來識別弱密碼或

配置不當的設備，進而進行攻擊，例如 Mirai Botnet 就是利用這些漏洞來感染數百萬台物聯網設備[4]。

2022 年 Verizon 的資安調查報告[6]中也提及約 81% 的數據洩露事件與密碼攻擊相關。這些攻擊主要針對弱密碼、重複使用密碼或密碼遭竊的情況。

- **過度集中的管理系統**：Verkada 的系統採用集中化的雲端管理架構，所有攝影機與數據都透過單一平台進行管理，在該架構下會面臨的風險如同該次事件，一旦平台遭到攻擊，駭客就能夠存取所有的內容，且管理系統並沒有良好的分層權限管理，導致取得管理員帳號即是超級管理員的身份。

  許多物聯網平台採用集中化的雲端管理架構，所有設備和數據都由單一平台管理。這種架構的風險在於，一旦駭客取得管理員帳號，便可存取所有設備和數據[5]。

- **缺乏零信任裝置**：Verkada 系統並未採用零信任架構來限制用戶的訪問，在零信任的架構下，每一次請求都需要進行身份驗證與授權；相反地，Verkada 系統缺乏多因子驗證以及允許登入後可以無需再次驗證即可進行多次操作。

- **其他因素**：Verkada 的員工以及客戶在使用設備時並沒有接受充分的資安教育導致進一步降低系統的安全性。在法規與監管力度上的不足也是原因之一，物聯網設備缺乏安全監管，且針對設備製造商缺乏有效管制。

三、從法規、管理以及技術探討其改進方向

物聯網（IoT）技術的快速發展帶來便利，但也伴隨著嚴峻的資訊安全與資料保護挑戰。Verkada 資安事件突顯了物聯網應用的脆弱性。為了有效降低資安風險，並保障使用者數據安全與隱私，必須從宏觀的法規層面，向下推動企業的管理實踐，最終落實到具體的技術執行上。

1. 法規層面 - 法規先行

在法規層面，Verkada 事件揭示了物聯網設備 **缺乏統一的安全標準** 以及 **隱私保護與監管不足** 的問題。

現行法規在全球並沒有統一的標準，不同國家的物聯網法規在細節上存在差異（如美國 IoT Cybersecurity Improvement Act 和歐盟 Cyber Resilience Act），且各國缺乏專門的監管機構導致執法力度不足。此外，這些標準在具體要求（如身份驗證、加密方法、更新機制）上存在差異，導致企業難以同時滿足多個市場的規範。

雖然國際標準化組織（如 ISO、ITU）已針對 IoT 安全制定部分指導原則，但這些標準的落地實施存在不足，且未涵蓋所有安全需求。許多安全標準僅提供框架性建議，缺乏具體的實施細節。而許多製造商出於成本考量，選擇最低限度的安全措施，特別是在面對沒有強制性法規的市場，部分小型製造商對安全標準的理解和實施能力有限，進一步加劇了設備安全性的不一致。

事件中，Verkada 的內部員工帳號可以存取客戶攝影機影像，導致敏感數據遭到駭客利用，對於該權限設置很明顯違反了隱私法規中對數據存取的限制性要求，特別是對於 GDPR, CCPA [7][8]以及 IST IoT Cybersecurity Framework [7]的相關規定。

- GDPR (General Data Protection Regulation): 歐盟一般資料保護條例，是全球最嚴格的數據隱私保護法，適用於所有處理歐盟居民數據的企業，重點要球企業在數據處理過程中需要獲得用戶的明確同意。若發生數據洩漏問題，企業須在 72 小時內通知監管機構與受影響用戶。GDPR 還要求「最小化數據存取原則」，即只有必要人員才能存取敏感資訊，且需有明確的訪問紀錄。

- CCPA（California Consumer Privacy Act）：加州消費者隱私法，在法案中要求企業需提供用戶數據刪除權，並透明化數據洩漏事件的內容，此外，CCPA 也要求企業在收集用戶數據時提供充分的告知與選擇權[7]。

- NIST IoT Cybersecurity Framework：是**美國國家標準技術研究院（National Institute of Standards and Technology, NIST）**制定的指導框架，旨在幫助製造商，企業與政府機構提升物聯網設備的安全性。其中幾項重點包含：

  A. **安全設計原則**：需要有身份驗證、數據加密以及安全更新

  B. **風險管理**：威脅建模分析潛在安全風險、漏洞管理

  C. **資料保護**：數據最小化以及隱私保護

D. **系統架構與網路安全**：使用零信任架構與分層防禦

E. **供應鏈安全**：供應鏈中需維持透明化且需有第三方風險管理評估供應商的安全性

而 Verkada 並未對內部存取權限進行有效分層管理，導致員工可以濫用權限，也缺乏對數據存取行為與監控機制。此外 Verkada 並未在數據洩漏後及時通知受影響用戶，違反了上述相關的條例。

- 法規應該由誰進行管理？如何管理？

A. 國際層面

現有的有效組織主要有 ISO（國際標準化組織）以及 ITU（國際電信聯盟）可以透過這兩個組職建立有效的標準，以統一物聯網相關規範。

ISO 提供全球通用的物聯網安全標準並幫助各國制定本地化法規，參考標準如 ISO/IEC 27001 (訊息安全管理系統標準) 用於物聯網設備的安全管理，該系統標準幫助組織識別、管理和減少訊息安全風險，從而保護數位資產（如知識產權、財務數據和員工資訊），該標準採用了 **PDCA 循環（計劃-執行-檢查-改進）**，以確保系統的持續改進和有效性。

ISO/IEC 27400（物聯網專屬安全與隱私框架）涵蓋風險管理、數據保護和供應鏈安全，包含設計、開發、部署、運行和報廢，該標準的推行有助於統一 IT 和 OT（操作技術）在資訊與通訊安全方面的標準，這對於確保 IoT 系統的安全防護具有重要意義[9]，而 ISO 的標準通常都會被各國所採納並作為法規基礎，形成國際協作。

ITU 則是提供全球通訊標準，包含物聯網設備的操作性與網路安全，推動 IoT 通訊標準協議，確保設備兼容性，以及 5G 和 IoT 的安全應用。ITU 的 IoT 關鍵應用包括智慧製造、自駕車和智慧醫療等，這些應用與 5G 技術緊密結合，實現了更高效的物聯網串接和數據傳輸能力。通過其 IMT-2020 方案，為 5G 技術提供了標準化框架，並將其應用於 IoT 領域，確保網路的低延遲、高可靠性和大規模連接能力。此外，ITU 還針對 5G 的工業物聯網應用（如智慧城市）制定了相關技術建議，這些建議已被納入 ITU 的核心標準中[10]。

B. 國家層面

各國政府可以透過國際組織所提供的標準在針對特殊部分進行調整，並透過立法

機構建立更全面及符合國情的指導原則。以歐盟為例，歐盟制定了 Cyber Resilience Act (CRA) ，針對物聯網設備的安全設計與漏洞管理，並由 ENISA 負責監督、執行 CRA 並提供技術指導。

CRA 是歐盟於 2024 年生效的一項法案，旨在提高數位產品的網路安全標準，涵蓋硬體設備、軟體應用及相關數位服務。該法案要求製造商需嚴格遵守安全規範並建立漏洞報告及管理機制，確保設備安全性，此外法案還規定了漏洞修復的時限與澤熱，以確保產品在整個生命週期中的安全性。

ENISA 在 2020 年發布了《物聯網安全準則－安全的物聯網供應鏈》，提供具體的技術指導並作為網路安全認證框架，幫助企業加強物聯網設備的安全性。並向歐盟各國政府提供政策建議，作為 CRA 監督機構， ENISA 也同時**負責培訓地方監管機構的專案人員**，並做足**威脅分析**，發佈年度威脅報告，針對新興網路攻擊模式提供預警功能，幫助企業了解最新的安全挑戰。

ENISA 還通過教育計劃和意識提升活動，發佈簡化的安全指南並舉辦網路安全研討會、培訓課程，不僅提升從業者的網路安全能力，也幫助公眾、企業了解網路安全的重要性。

ENISA 的監督工作不僅限於執行 CRA，還涵蓋了從標準制定到漏洞管理的全方位支持，以確保物聯網設備和數位產品的安全性。這些舉措為歐盟的數位生態系統提供了強有力的安全保障。

2. 管理層面 - 符合法規

事件中能看到 Verkada 公司的管理上，包含了權限管理以及員工安全意識、危機應對能力都有所不足。主要原因如權限管理不當、安全意識不足以及危機處理意識不足。Verkada 的內部員工擁有過多的訪問權限，可以隨意存取客戶的攝影機影像，這導致敏感數據的洩露風險增加。不論權限問題，在獲得如此高的存取權下，員工缺乏足夠的安全意識和相關培訓，導致對安全漏洞的識別和應對能力不足。且沒有持續的安全意識教育和培訓計劃，進而未能在日常工作中強化安全。Verkada 也缺乏有效的應急響應計劃，導致在事件發生後未能迅速採取行動，導致數據洩露影響擴大，此外也未能及時通知受影響的客戶和相關方，影響了客戶採取補救措施的能力。

- 權限管理

  管理權限上應符合法規所制定的**「最小權限原則」（Principle of Least Privilege）**，確保員工僅能存取工作所需的最小權限，並定期審核權限，移除多餘的或不再需要的權限，防止權限過度累積。且對於敏感資料（如攝影機影像）進行分級管理，僅授權特定角色或經過額外驗證的員工存取。此外，訪問日誌與監控也是十分重要，在該事件中雖然 Verkada 有做到訪問日誌的部分，但根據報導中表明該日誌形同虛設，日誌上會登載使用時間與使用目的，但並沒有任何人或系統會監控該日誌，導致沒有辦法及時發現異常行為[1]。

- 安全意識與員工培訓

  公司應定期配合或根據政府規範為員工提供網路安全相關的培訓課程，包括如何識別釣魚攻擊、弱密碼風險和數據保護的重要性。針對高風險崗位（如 IT 管理員）進行深入的安全專業知識培訓。並且應該遵照標準規範制定清晰的安全政策，涵蓋密碼管理、數據存取、設備使用等內容，確保員工能夠熟悉並遵守規範。

- 危機應對與事件管理

  建立完整的應急響應計劃（Incident Response Plan, IRP），包括事件檢測、應對、通知以及恢復的詳細流程是十分重要的，而在其中也應該根據法規要求，例如 GDPR 或 CRA，確保在規定時間內向監管機構報告數據洩露事件。

- 合規性與外部審計

  定期進行內部審核，確保公司在權限管理、安全意識和危機應對方面符合法規（如 GDPR、CRA）。聘請獨立的第三方進行安全審計，檢查系統漏洞、權限設置及應急計劃的有效性也是十分有建設性的做法，並且也應有部門或人員負責與法規保持同步，持續關注並更新公司政策以符合最新的法規要求，例如 CRA 對供應鏈安全和漏洞管理的規範。

通過以上措施，公司可以在權限管理、安全意識、危機應對及合規性方面取得全面改進，降低數據洩露風險，提升網路安全能力，並符合法規要求。

3. 技術層面 - 上行下效

- 密碼與憑證管理

  由於超級管理員憑證被駭客獲取，表示憑證存儲方式存在漏洞，導致駭客能夠直接提取密碼或密鑰。而事實也證明如此，駭客能夠進入後台的元因就是，因此 Verkada 應該在系統中加入「**多因子驗證（MFA）**」增加額外的驗證，並且對於密碼策略需要求高強度密碼，對憑證也需要進行加密，存放在安全的硬體模組中。而該憑證系統除透過管理層級進行審查、監控與自動化，也要符合法規要求如 ISO 27001 或根據國家再優化的標準確立管理流程與保護措施

- 集中化管理架構

  該架構使所有控制權集中於單一系統，一旦系統被攻破，駭客就能夠控制所有設備，因此應該對該架構進行重構，改為分散式架構，將控制權分散至多個特定區域，避免被集中控制；此外也要進行網路隔離與分段處理，避免被全盤影響。並且分散式架構也能夠符合數據最小化原則，若有需求也可以依照法令框架設立如 NIST 的 CSF 網路安全框架，建立更好的管理架構。

- 持續監控與異常偵測

  在事件中 Verkada 的系統並沒有即時偵測到駭客的異常行為，間接導致駭客能夠在系統中暢行無阻。因此應該在系統上部署行為分析系統以及即時警報機制，確保在發現異常時能夠有充裕的時間進行應對。此外，也應該導入零信任架構，對每一次操作都進行驗證。配合管理層級設立的應急響應計劃，訓練員工危機反應病能即時報告數據洩漏事件，快速的處理安全事件。

- 資料加密與隱私保護

  駭客能夠直接存取攝影機畫面以及存檔影片，不僅是集中話管理架構的缺點，同時也是資料保護上的不足，因此應該在資料安全上進行端到端加密，確保數據傳輸、存儲過程都能夠受到保護，並且應定期更新版本協議以應對新型攻擊。

  A. 資安防範理論的應用

  資安防範理論下，可以應用 CIA 模型、零信任架構以及密碼學三個部分進行補強。

  首先，CIA 三要素包含**機密性（Confidentiality）**、**完整性（Integrity）**、**可用**

性（Availability），機密性是指透過加密技術（如 AES、RSA）保護數據的存取權限，確保未經授權的用戶無法讀取敏感數據。完整性是利用數位簽章與雜湊函數（如 SHA-256）確保數據未被篡改。可用性則是透過冗餘設計與容錯機制，確保加密數據在合法需求下能被快速存取。

零信任裝置 (Zero Trust Device) 是「零信任架構 (Zero Trust Architecture)」的一部分，這是一種現代化的資安模型，核心理念是 **「永不信任，始終驗證」**。在傳統的網路安全模型中，內部網路的設備或用戶通常被預設為可信任的。然而，零信任裝置的概念打破了這種假設，即使是內部設備，也需要經過嚴格的驗證和授權才能獲得訪問權限。核心原則就是不預設信任、持續驗證與監控、最小權限原則、動態授權。

最後的密碼學概念則是**非對稱加密**（如 RSA）與**對稱加密**（如 AES）的特性去適配不同的數據並進行加密，非對稱加密耗時較久且較為複雜，因此適用於敏感數據以確保在公開網路中的安全性，但並不適合用於需要大量且快速傳輸的資料中，反之亦然。

- 技術層面挑戰與困難點

A. 加密技術的效能資源消耗

加密技術（特別是端到端加密與非對稱加密）會對系統效能產生較大影響，尤其是在處理高頻率的數據傳輸或大量數據存儲。此外，手機、物聯網（IoT）設備等資源受限的硬體平台，可能無法高效執行複雜的加密演算法。因此在效能與安全性之間的平衡仍然是挑戰，特別是在即時性要求高的應用場景（如即時影像傳輸）。

B. 加密密鑰管理的複雜性

密鑰的生成、分發、存儲與輪替是加密系統的核心，但同時也是最容易出現漏洞的環節，密鑰的集中化管理可能成為單點失效風險，而分散式管理則會增加操作複雜性。而至目前為止尚未有完全自動化且無風險的密鑰管理方案，尤其是在大規模分布式系統中。

C. 資料加密與數據隱私的矛盾

加密技術保護了數據的機密性，但同時可能限制合法用戶的數據分析與應用，例如在醫療或金融領域，數據需要被解密後才能進行分析。同態加密

（Homomorphic Encryption）雖然能在不解密的情況下進行數據計算，但其運算效率極低，難以應用於實際場景。

同態加密是一種特殊的加密技術，允許在密文上直接進行數學運算，而不需要先將密文解密。因此經過加密的數據可以在不暴露其內容的情況下進行處理，最終的計算結果在解密後與對明文進行相同運算的結果一致。例如在金融交易與電子投票上，金融機構需要對交易數據進行運算，但也需要確保交易內容的保密性，同態加密就可以保護交易數據同時支援加密計算。

D. 法規與技術的協調

不同地區的法規（如 GDPR、CCPA）對數據加密與隱私保護的要求不一致，增加了技術實施的複雜性，法規要求數據可被刪除或匿名化，但加密數據的不可逆性可能與此相衝突。因此如何在遵守不同法規的同時，保持加密技術的有效性與一致性，仍需進一步探索。

四、總結

物聯網（IoT）技術的快速發展帶來了智慧化生活的極大便利，但其「聯網」的特性同時也帶來了嚴峻的資訊安全與資料保護挑戰。這起事件顯示了物聯網應用在資訊安全與資料保護上的脆弱性，並引發了對物聯網設備管理與監控的廣泛關注。為了有效降低資安風險，並保障使用者數據安全與隱私，必須建立一個由上而下、法規、管理與技術三者協同運作的防禦體系。而資訊洩漏往往發生在「人」與「物」互動或「人」管理「物」的過程中，當人為因素或憑證管理不當導致資訊從中洩漏，就有可能是如文中所示，技術層面中有漏洞，從漏洞可以進而向上找出管理層、法規層是否有缺失，應對此進行補強，避免同性質的事情發生。

對於物聯網系統中的資安改進是一項系統工程，需要從國際組織和國家層面的法規引導，到企業內部的管理政策落實，最終透過堅實的技術手段來實現防禦目標。使用者和員工的資安意識和良好習慣，則是這整個防禦體系中不可或缺的一環。

五、參考資料

1. https://www.verkada.com/security-update/report/?locale=zh_TW
2. https://www.ithome.com.tw/news/164825

3. https://zh.wikipedia.org/zh-tw/物联网

4. https://www.itc.ntnu.edu.tw/wp-content/uploads/2019/07/security-1080821.pdf?locale=zh_TW

5. https://www.checkpoint.com/tw/cyber-hub/network-security/what-is-iot-security/biggest-iot-security-challenges/?locale=zh_TW

6. https://www.charmingscitech.nat.gov.tw/post/sts10-password?locale=zh_TW

7. https://www.cpomagazine.com/cyber-security/verkada-data-breach-exposes-feeds-of-150000-security-cameras-targets-include-health-care-facilities-schools-police-stations-and-a-tesla-plant/?locale=zh_TW

8. https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-takes-action-against-security-camera-firm-verkada-over-charges-it-failed-secure-videos-other?locale=zh_TW

9. https://www.cio.com.tw/internet-of-things-to-set-up-security-standards-iso-27400/?locale=zh_TW

10. https://www.itu.int/zh/mediacentre/Pages/PR-2022-02-24-5G-Standards.aspx?locale=zh_TW

11. https://www.itbigtec.com/understanding-the-eu-cyber-resilience-act-and-achieve-product-cybersecurity-compliance/?locale=zh_TW