

產業資安威脅議題攻略

議題2：資料安全保護

陳怡如 協理

邱品仁 副理

中華資安國際簡介

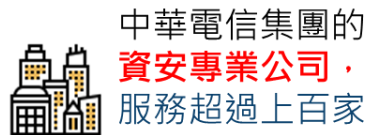
2017年成立 | 實收資本額3.09億 | 員工 200+人



領先業界之專業能力！



Abilities



中華電信集團的
資安專業公司，
服務超過上百家



具備**國家級資安**
專案建置能力與
實績



2003年開始經營資
安業務，於**北中南**
區有服務據點

Experiences



Quality

提供事前檢測、事中監控應變、事後事件調查的資安服務

- 上網資安防護服務**：ISP雲端的入侵防護服務、DDoS防護服務、防駭守門員、APT防護、新世代防火牆、WAF等
- 資安專業服務**：紅隊演練、滲透測試、IoT檢測、資安健診、金融安全評估、SOC監控、MDR、事故應變與鑑識調查、工控(ICS)資安
- 資安顧問**：ISMS/PIMS制度導入輔導、資訊安全評估、PKI建置規劃
- 資安管理平台規劃建置**：資安監控分析通報平台、弱掃管理平台、資安資訊分享與分析系統(ISAC)、網路威脅偵測與應變系統(SecuTex)
- 身分識別產品與應用**：安全晶片與PKI應用、加密安全通訊解決方案
- 企業資安整體解決方案**：資安、網路、雲端、軟硬體整體解決方案之規劃及建置

中華資安國際簡介

安全評估/紅隊演練/資安檢測/SOC/事件處理(IR)經驗豐富！

Abilities

Experiences

Quality



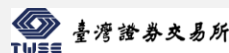
金融安全評估服務實績

通過ISO 17025認證之數位鑑識與資安檢測實驗室



滲透測試與紅隊演練服務實績

國內唯一通過ISO 20000之紅隊演練服務商



政府、金融、交通、科技、醫療業及跨國公司資安服務



華資安國際簡介

A級資安團隊 (2020)

2020

--- 行政院資安共同供應契約評鑑

序號	受評廠商	SOC 監控服務	資安健診服務	弱點掃描服務	滲透測試服務	社交工程 郵件測試服務
3	中華資安	A 級	A 級	A 級	A 級	A 級



Experiences

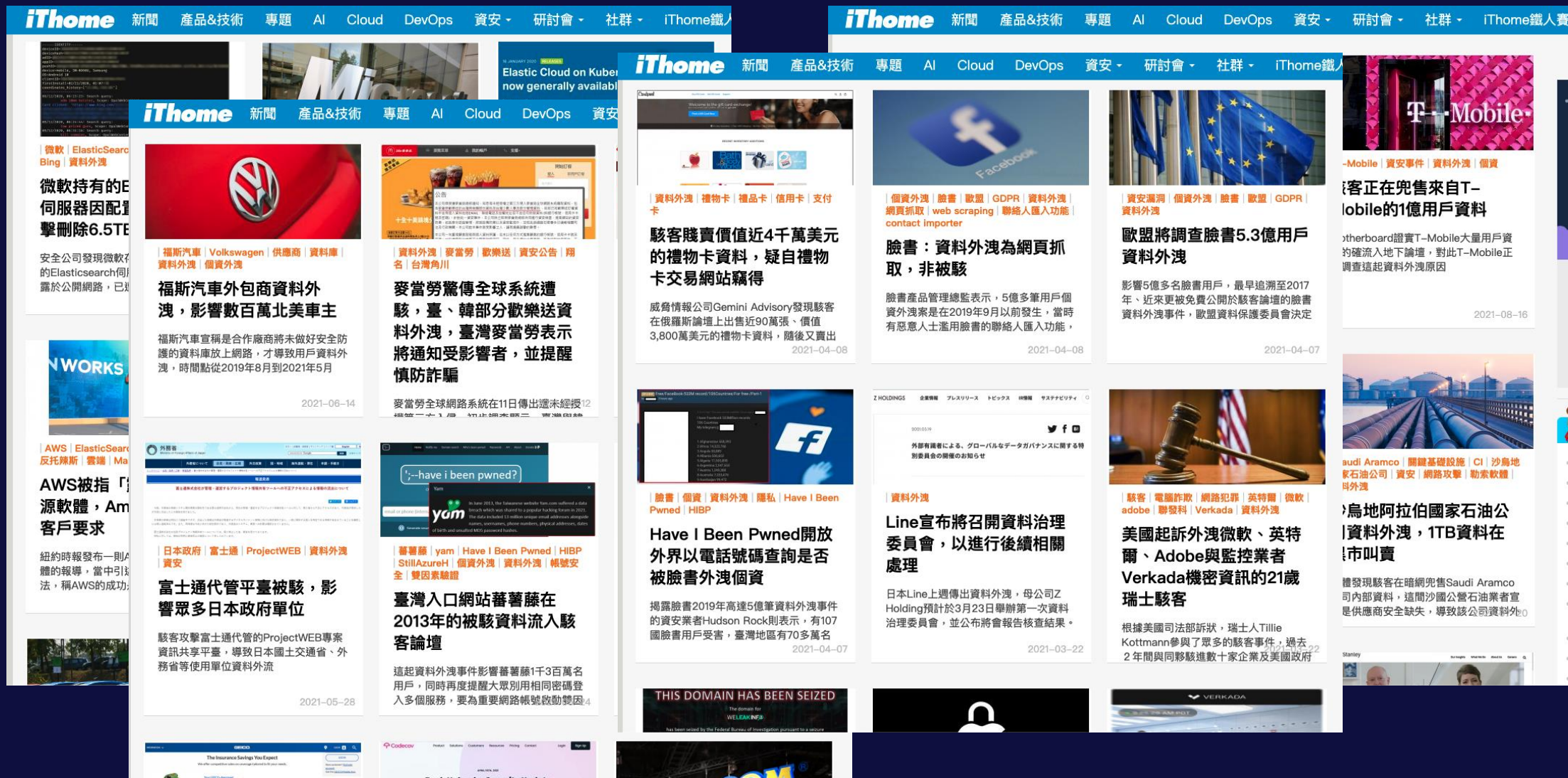


Quality



獲得最新行政院共契之評鑑「全項A級」廠商！
全國唯一連續三年獲此殊榮資安公司！

01 – 從資安事件看資料安全



資料外洩事件頻傳

iThome

新聞

產品&技術

專題

AI

Cloud

DevOps

資安

研討會

社群

iThome鐵人



美國財政部 | 勒索軟體 | 洗錢 | 加密貨幣
交易所 | Suex | 黑色產業鏈

美國制裁幫勒索軟體駭客
洗錢的加密貨幣交易所
Suex

根據美國政府以及華爾街日報的資訊，公
司及成員位於東歐的Suex，是墨西哥當
地知名的加密貨幣交易所，至少協助8
2021-09-22



New Cooperative | 農業 | 合作社 | 勒索軟
體 | BlackMatter | Darkside | 資安 | 網路攻
擊

美國穀物合作社New
Cooperative遭
BlackMatter攻擊，被勒
索590萬美元

美國愛荷華州的穀物合作社New
Cooperative遭到勒索軟體攻擊，犯案的
2021-09-21



Microsoft MSHTML 遠端執行程式碼漏洞
CVE-2021-40444
安全性影響
影響：2021/09/07 最後更新：2021/09/07
影響：CVE-2021-40444
CVSS 3.0 8.8 / 7.9

Windows MSHTML漏洞，勒索軟體 |
CVE-2021-40444 | 資安 | 修補 | Patch
Tuesday

微軟：Windows
MSHTML漏洞已有勒索軟
體開採


微軟在8月已經偵測到數個攻擊行動開採
MSHTML引擎中的CVE-2021-40444漏
洞，透過惡意Office文件散布勒索軟體9-17



Olympus | BlackMatter | 網路攻擊 | 資安
事件 | 勒索軟體 | 資安

相機大廠Olympus疑遭勒
索軟體BlackMatter攻擊


Olympus坦承在9月8日發生網路安全事
件，影響該公司位於東歐、中東及非洲
(EMEA) 據點的IT系統
2021-09-16



美國K-12學校 | 教育單位 | 網路攻擊 | 學生
個資 | 資料外洩 | 資安 | 勒索軟體

超過1,200所美國K-12學
校的學生資料曝露在暗網
中


NBC News指出，他們今年在暗網中看到
駭客張貼了超過1,200家K-12學校的檔
案，這些檔案充斥著學生的個資，包括名
2021-09-13



REvil | 勒索軟體 | 資安

勒索軟體REvil於暗網中再
現蹤跡

外界猜測源自俄羅斯的REvil勒索軟體集
團，在今年7月攻擊Kaseya VSA軟體用
戶後，因驚動白宮甚至俄國政府，選擇消
2021-09-09



資安 | 勒索軟體 | 零信任 | Zero Trust

駭客重金誘惑，內部員工
也必須零信任

iThome

新聞

產品&技術

專題

AI

Cloud

DevOps

資安

研討會

社群

iThome鐵人



THE AVERAGE COST OF RANSOMWARE-CAUSED
DOWNTIME PER INCIDENT
Ransom Payments by Quarter
2016 2017 2018 2019 2020 2021

資安 | 供應鏈 | 目標式攻擊 | 零信任 | 勒索
軟體 | iThome 2021臺灣資安年鑑

【資安教戰守則：因應雙
重勒索之道】目標式攻擊
瞄準供應鏈脆弱環節，該
如何因應？

發展已久的目標式攻擊，儼然讓駭客的勒
索敲詐行徑取得更有效且豐碩的成果，
而由於SolarWinds事件所引發出供應鏈
2021-05-28



conti | FBI | 攻擊指標 | 勒索軟體 | 勒索攻擊
醫療 | 政府 | 美國

FBI警告：美國占Conti全
球受害單位一半以上，公
布感染指標

FBI發現駭客對美國的行政、醫療與警消
單位頻繁發動Conti勒索軟體攻擊，當地
受害組織數更居全球之首，因此公布
2021-05-26



愛爾蘭健康服務管理署 | HSE | conti | 勒索
軟體 | 資安 | 雙重勒索

攻擊愛爾蘭健康服務管理
署的駭客要詐，給解密金
錢後仍威脅出售民眾個資

遭到勒索軟體攻擊的愛爾蘭健康服務管理
署 (HSE) 雖然獲得解密金鑰，但狡猾的
駭客仍然以盜走內部資料為要脅，試圖迫
2021-05-21



保險業者 | 安盛集團 | AXA | 勒索軟體 | 資
安

歐洲大型保險業者AXA遭
勒索軟體攻擊，亞洲營運
停擺

跨國保險業者安盛集團 (AXA) 淪為勒索
攻擊受害者，根據AXA的聲明，駭客鎖定
該公司的亞洲部門展開攻擊，影響了泰
2021-05-17



our health service
Appointment and service updates - HSE IT
system cyber attack

資安 | 勒索軟體 | 愛爾蘭健康服務管理署 |
Health Service Executive | HSE

愛爾蘭健康服務管理署遭
「重大」勒索軟體攻擊

愛爾蘭健康服務管理署 (Health Service
Executive, HSE) 因遭遇勒索攻擊，關
閉所有IT系統並切斷網路，有媒體指出，
2021-05-17



Cybersecurity & Infrastructure
Security Agency

資安 | 勒索軟體 | 零信任 | Zero Trust

駭客重金誘惑，內部員工
也必須零信任

勒索軟體盛行，產業哀鴻片野

SecuTex

中華資安國際
CHT Security

關於資料安全議題，我們面臨....

• 現今的挑戰

- 因應疫情，企業擁抱電子/數位化
- 為了資源有效運用與效益，企業開始了雲端化
- 萬物聯網時代來臨，企業的數位邊界逐漸擴大
- 法規的要求(GPDR、個資法..etc)對企業帶來資料處理上的新挑戰

• 讓我們試著問問自己

- 在我們的企業環境裡，資料都出現在哪裡？(Identify)
- 我們都如何保護資料與關鍵服務？(Protect)
- 我們如何進行異常偵測？(Detect)
- 我們如何在異常、事件發生時，作出回應？(Respond)
- 我們如何在事件中順利度過？(Recover)

當資料安全議題變成風險時

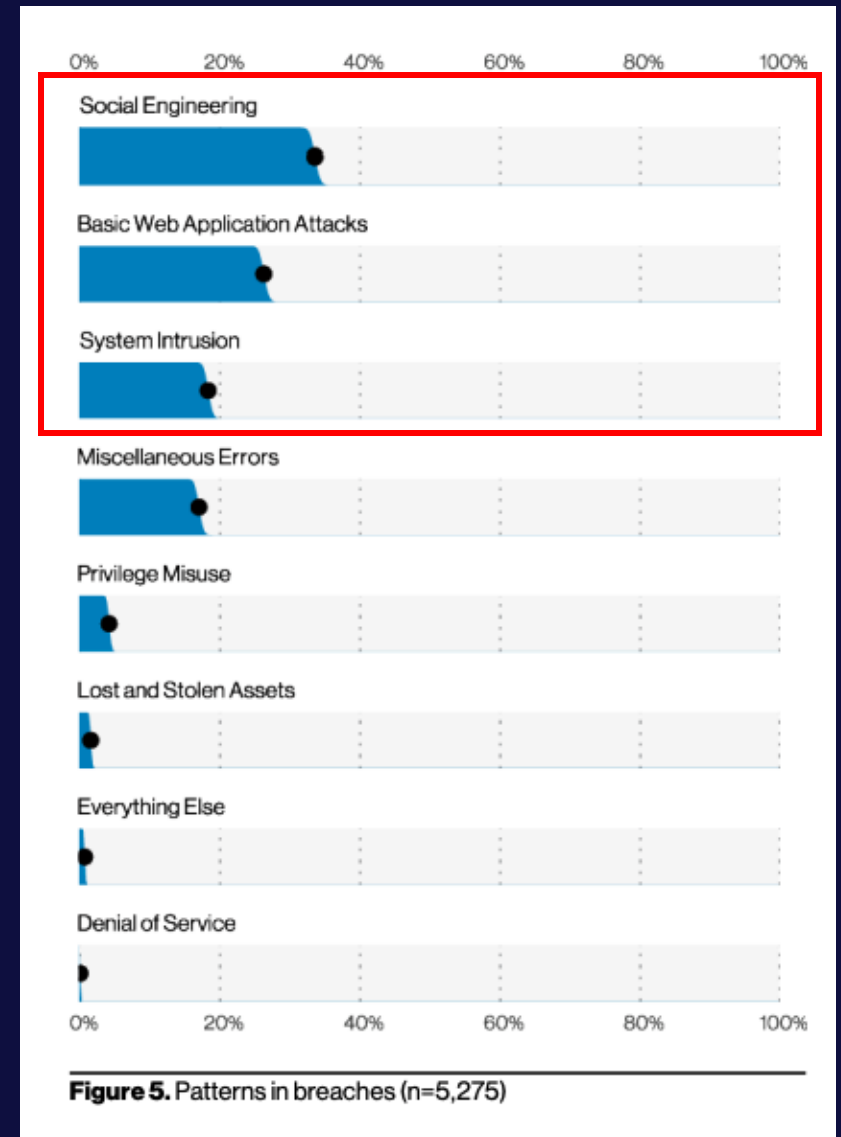
- 企業要面臨的是

- 法規遵循上的議題(GDPR、個資法、相關政策規範)
- 企業營運上的損失
 - 個資外洩所需面臨的賠償議題
 - 客戶信賴度的下降(Reputation)
 - 合作關係的毀損(涉及合作協議的資料外洩)
 - 勒索軟體議題
 - 支付贖金
 - 資料復原
 - 可能的營運中斷

- 資料安全已經是企業營運安全的重要一環

攻擊活動與資料安全議題的關聯

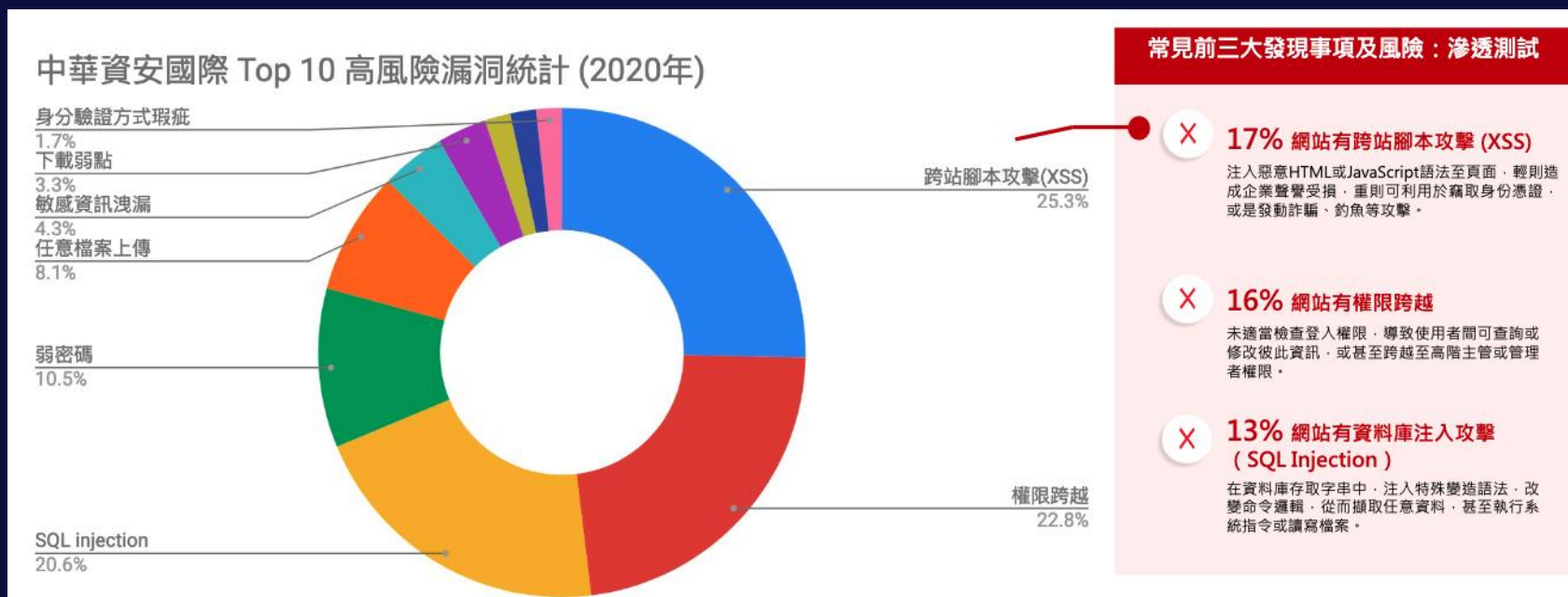
- 根據Verizon DBIR 2021報告指出
 - 社交工程攻擊、網頁入侵攻擊、系統入侵攻擊為前三大的資料安全事件關鍵原因



攻擊活動與資料安全議題的關聯(cont.d)

• 根據中華資安的觀察與歸納

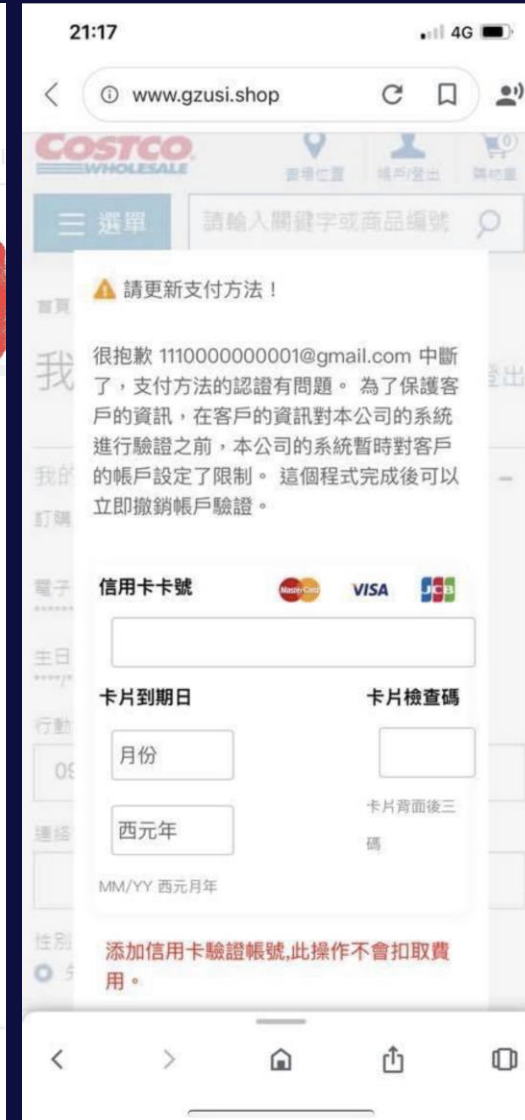
- 針對網頁系統攻擊的(Web Application Attacks) 途徑
 - 2020年的滲透測試統計，針對**150**個以上的企業，約**600**個系統，共發現了**3,600**個高度風險漏洞



攻擊活動與資料安全議題的關聯(cont.d)

• 根據中華資安的觀察與歸納

- 駭客入侵(Web Application Attacks) 又佔據了大宗
 - 2020年的滲透測試統計，針對150個以上的企業，約600個系統，共發現了3600個高度風險漏洞
- 以全球的趨勢來說，釣魚攻擊、變臉攻擊(BEC)與社交工程亦頻傳



02 – 面對資料安全的議題

今天的分享將針對..

- 企業資安防護

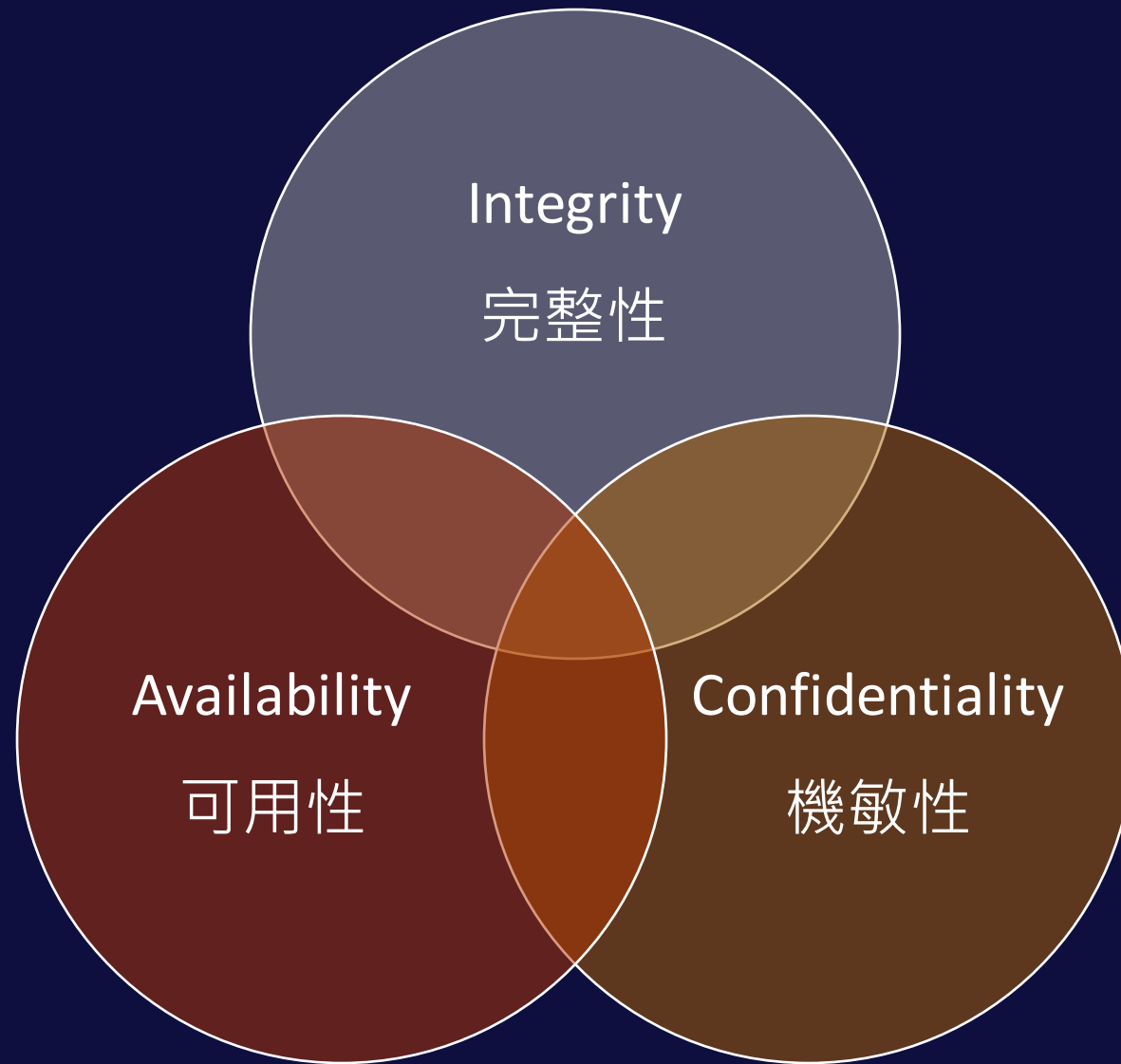
- 識別(Identify)

- 定義：Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
 - 沒有被識別、被妥善管理的資產、風險往往成為破口

- 保護(Protect)

- 定義：Develop and implement appropriate safeguards to ensure delivery of critical services
 - 針對「保護」機制的有效性量測往往沒有被有效量測、追蹤

資安基本功做得好，老闆晚上睡覺沒煩惱



如果只能選一個，您會選擇先守護哪一個？

找到好的方法

- NIST Cybersecurity Framework
- NIST NCCoE – Data Security
 - Data Integrity
 - Cybersecurity White Paper
 - Identifying and Protecting (SP 1800-25)
 - Detecting and Responding (SP 1800-26)
 - Recovering (SP 1800-11)
 - Data Confidentiality
 - Identifying and Protecting (SP 1800-28)
 - Detect, Respond, and Recover (SP 1800-29)

Data Security

Building Blocks

5G Security
Adversarial Machine Learning
Applied Cryptography
Data Classification
Data Security
Derived PIV Credentials
Internet of Things
Mobile Device Security
Patching the Enterprise
Supply Chain Assurance
Trusted Cloud
Zero Trust Architecture

Related News & Events

Virtual Workshop on Preventing and Recovering from Ransomware and Other Destructive Cyber Events
July 14, 2021

Wireless Roundup (July 2021)
July 01, 2021



Data security is the process of maintaining the confidentiality, integrity, and availability of an organization's data in a manner consistent with the organization's risk strategy. Preventing unauthorized access, data corruption, and denial of service attacks are all important tenets of data security and an essential aspect of IT for organizations of every size and type. Consistent, reliable, and secure access to database records, system files, user files, and customer data is necessary to prevent data from becoming vulnerable to attack. Before an incident begins, companies must have a security architecture and response plan in place. Once an incident occurs, they must be able to detect the event and respond accordingly. After the incident, the company must be able to effectively and efficiently recover.

In accordance with this methodology, the Data Security program at the NCCoE has produced guidance for both data integrity and data confidentiality. Each will consist of a series of publications that work together to identify, protect, detect, respond to and recover from critical events.

If you have questions or would like to join our Community of Interest, please email the project team at ds-nccoe@nist.gov.

Also, if you would like to get involved in our ransomware guidance, please contact us with any comments, questions or suggestions at ransomware@nist.gov, view the recording of our recent [workshop](#), and review our recently released draft [NISTIR 8374: Cybersecurity Framework Profile for Ransomware Risk Management](#).

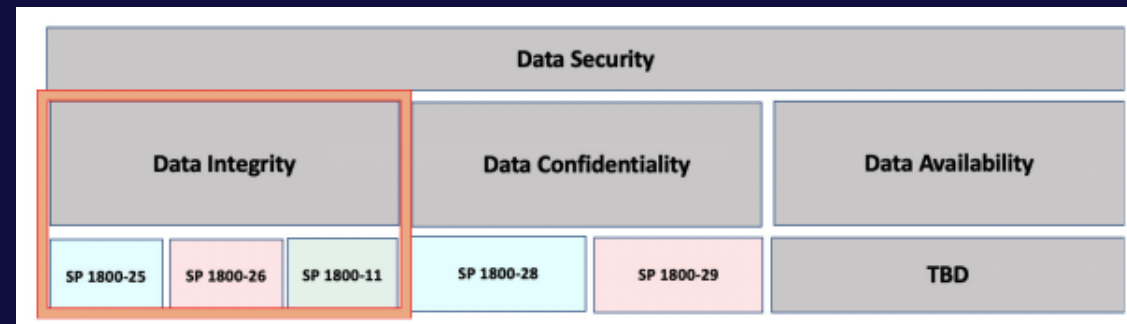
Data Integrity: Cybersecurity White Paper

Providing an overview of the three Data Integrity projects and how they align with the NIST Cybersecurity Framework. [Download the paper](#) here.

Data Integrity: Identifying and Protecting

Exploring methods to effectively identify and protect assets against data integrity attacks. [Learn more about this project and download the NIST Cybersecurity Practice Guide 1800-25.](#)

Data Integrity: Detecting and Responding

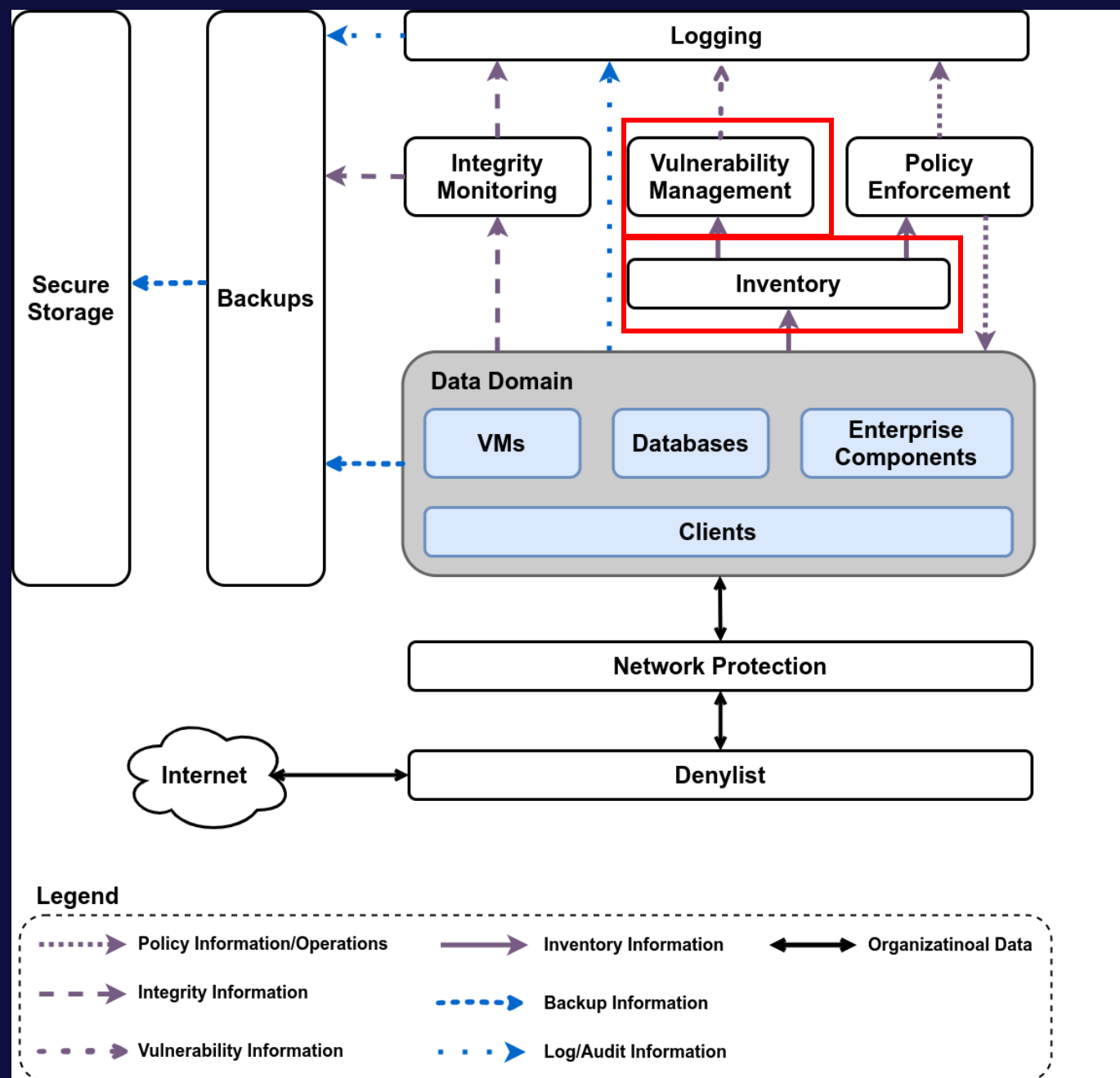


了解自己 - Identify

• 有效率的盤點

- 找出數位邊界盲點
 - Asset Discovery
 - Asset Inventory
- 找出曝險區域
 - 弱點檢測
 - 弱點管理
- 找出資料在哪裡
 - 資料處理流程
 - 政策、制度的制定與導入

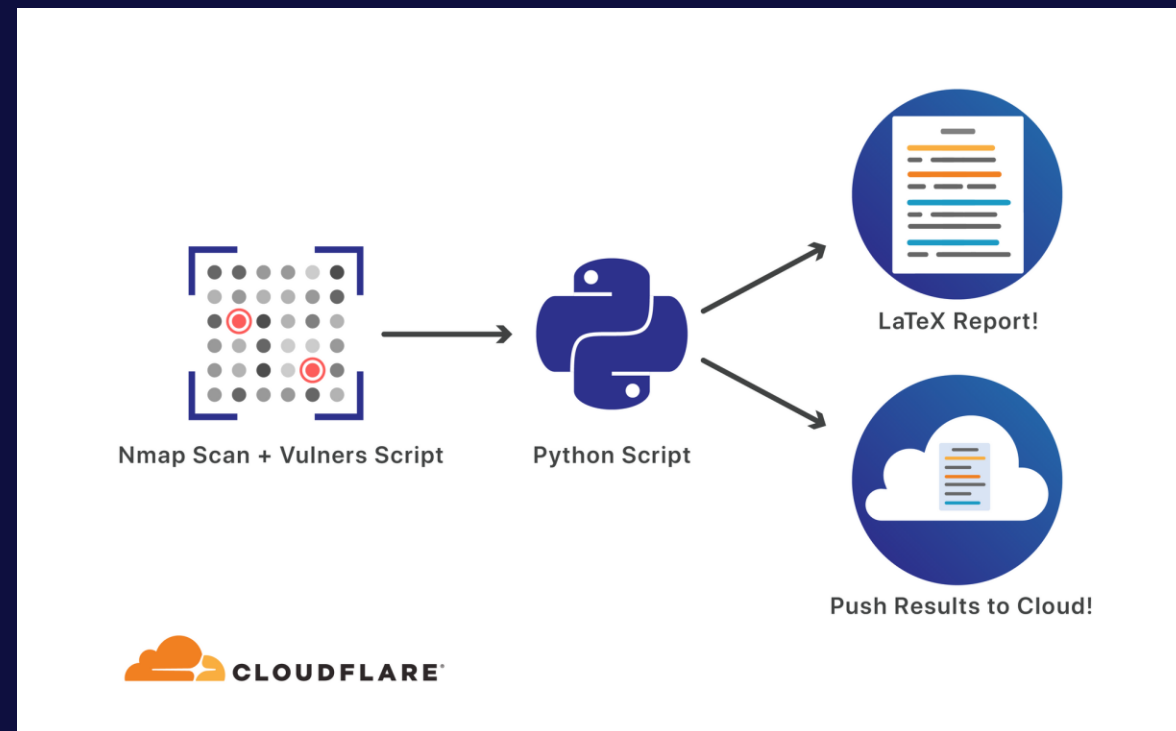
• 唯有知己(Enterprise)知彼(Vulnerability, Risk), 才能降低風險(Risk, Damage)



如何有效的找出數位邊界？

• 資產的探勘與管理

- 資產系統的建置導入(Inventory)
- 資產數位足跡的挖掘與勾稽
 - 從已知找出未知
- 幾個自我評核的情境
 - 企業多久做一次資產清冊更新？
 - 資產清冊更新的流程與做法？
 - 是否系統化、**自動化**？
 - 是否為有效盤點？
- 分享開源的做法：Cloudflare Flan Scan
 - <https://blog.cloudflare.com/introducing-flan-scan/>
- 獲取更多的外部視野，從駭客的角度看企業網路邊界
 - Shodan: <https://www.shodan.io>
 - Censys: search.censys.io
 - Zoomeye: www.zoomeye.org



你的資料在哪裡？如何管理？

- 找到資產，你才有可能知道你的資料會在哪裡？

- 定義出資料中心(Data Zone, Data Domain)
- 檢視與修訂出資料處理相關辦法
 - 資料生命週期
 - 資料存取管控機制
 - 資料保護政策
 - 資料隱碼
 - 資料備份、復原
- 導入對應的防護機制
 - 木桶理論延展：你的資料安全議題，其實還是取決於企業對於圍繞在資料周邊的系統之防護基礎的成熟度、落實度而定
- 定時的演練與量測
 - 有沒有效只有試了才知道，Make it real.

03 - CIA準則於資料安全的應用

CIA - 機敏性(Confidentiality)的保護

- 常見的威脅與解決之道

- 駭客入侵/裝置受駭

- 針對邊界的防護，導入IPS與WAF的防護機制
 - 針對端點的防護，應導入端點防護機制、DLP..等

- 未妥善設定而暴露於網路上

- 落實資產盤點(Identify)
 - 定時的進行資產Discovery(外到內的視野也應該建立)
 - 導入設定變更管理措施

- 內部威脅(Insider)

- 落實存取管控機制(定義資料分級與存取管控機制)
 - 針對關鍵資料的存取
 - 落實存取行為的監控與紀錄
 - 導入DLP防護方案

CIA - 完整性(Integrity)的保護

- 常見的威脅與解決之道

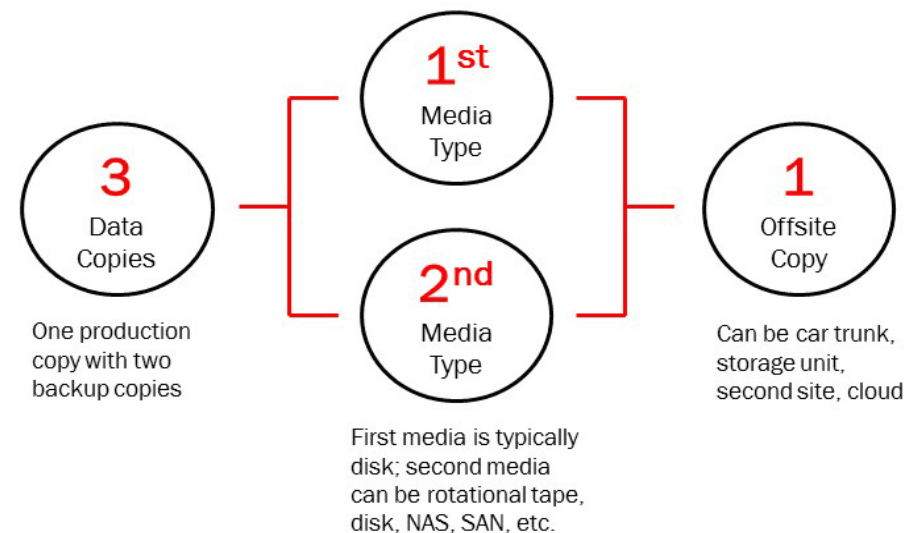
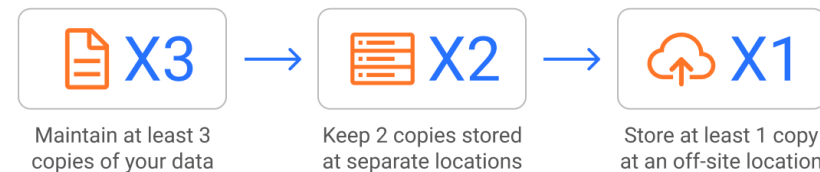
- 駭客入侵/裝置受駭
 - 針對資料存取的軌跡進行記錄與監控(例如：DB Auditing)
- 異常的存取
 - 需落實權限的控管(讀/寫分離)
 - 需落實網路層次、Application層次的存取管控
 - 針對資料存取的軌跡進行記錄與監控
- 軟體、硬體故障
 - 針對關鍵的資料處理單位應該要建立好完整的架構設計
 - 備份機制的確立
- 勒索軟體攻擊
 - 針對網路、端點的防護機制建立(MDR、白名單管控..等)
 - 備份機制的確立

CIA - 可用性(Availability)的保護

• 常見的威脅與解決之道

- 駭客入侵/裝置受駭
 - 針對邊界的防護，導入IPS與WAF的防護機制
 - 針對端點的防護，應導入端點防護機制、DLP..等
- 軟體、硬體故障
 - 針對關鍵的資料處理單位應該要建立好完整的架構設計
 - 備份機制的確立
- 勒索軟體攻擊
 - 針對網路、端點的防護機制建立(MDR、白名單管控..等)
 - 備份機制的確立

3-2-1 Backup Rule



圖片來源:

1. <https://www.msp360.com/resources/blog/following-3-2-1-backup-strategy/>
2. <https://www.unitrends.com/blog/3-2-1-backup-sucks>

今日總結

- 企業對於資料的掌握程度應落實
 - 盤點
 - 識別
 - 分級
- 針對資料安全的需求與風險進行排序
- 導入適切的資料安全防護方案
 - 除了產品的導入，方法與**流程**應該要同時規劃
 - NIST NCCoE – Data Security
 - 應針對防護機制進行有效性量測，並進行演練
- 準備好面對資料安全事件時的對應方案

讓我們付諸實行

- 在聽完演講的一週後，你將
 - 完整檢視企業/組織的資安防護能量，尤其是針對資產與資料的識別
 - 下載與閱讀NIST NCCoE Data Security的參考資料
- 在三個月內，你應該要完成
 - 全面的資產與資料盤點
 - 規劃與建立你的資料處理流程、中心(Define your Data Zone/Domain)
 - 檢視針對Data Domain的防護架構是否完善，並制定對應的優化方案
- 在半年內，你應該正在進行甚至完成
 - 導入針對資料的防護機制，例如：WAF、Network Protection、Access Control、Log monitoring與紅隊演練
 - 制定與完成針對資料安全的相關應變方案，例如：
 - 如何處理資料外洩通報？對應的SOP與應變團隊？
 - 如何處理勒索軟體攻擊？是否有合適的資安監測、防護與應變機制？

謝謝您的聆聽