"歸零射擊"零信任-資安三點與三險
(危險、風險與保險)

羅天一 博士

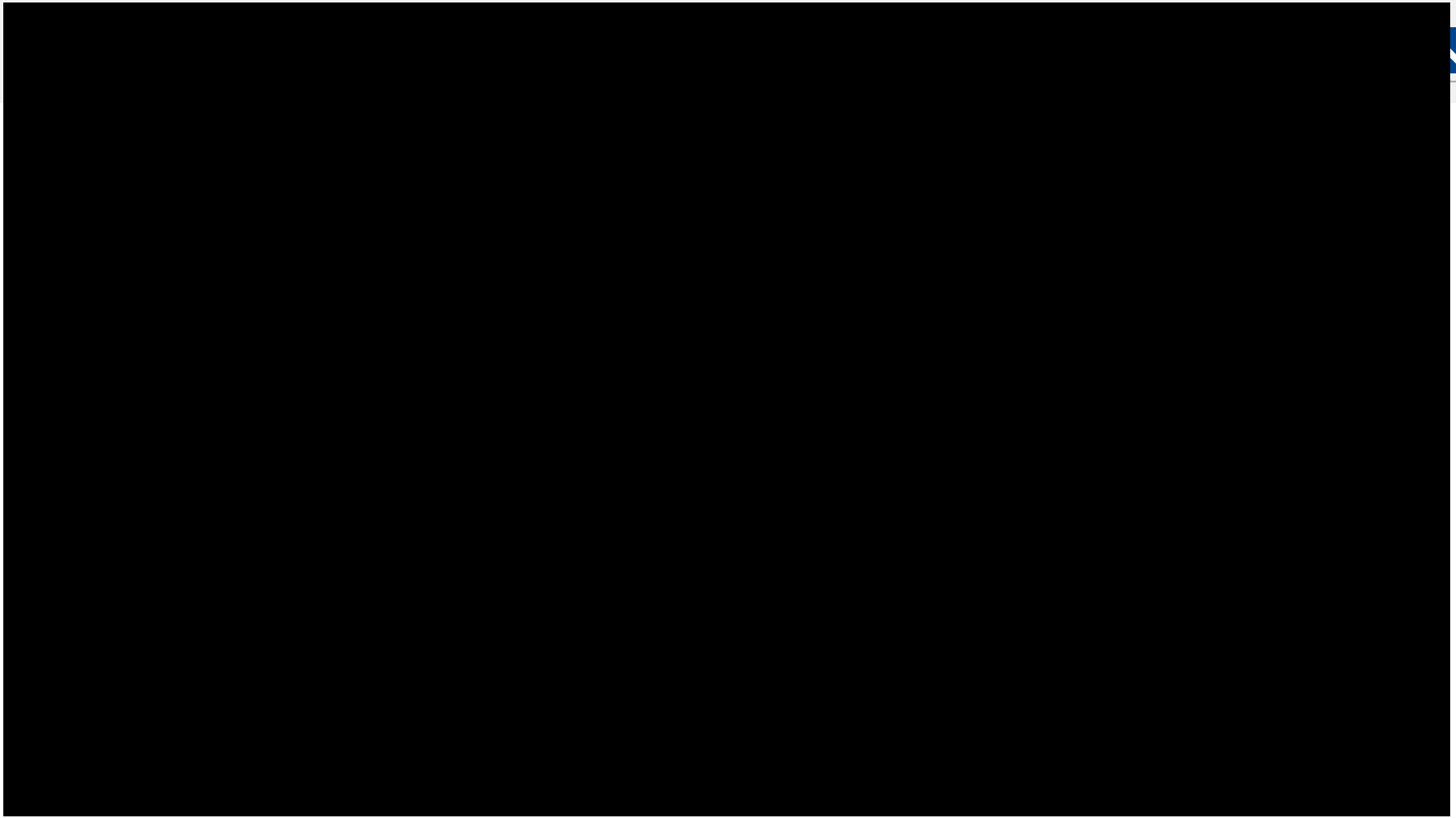
台灣科技大學 兼任副教授

2024

"歸零射擊"零信任-資安三點與三險
(危險、風險與保險)

目錄 CONTENTS

https://youtu.be/SWMF83gfG5o



第一部分

歸零射擊

1

歸零射擊

覘孔-看的見-危險

- 危及三生:生命、生活及生存:含生命、人格及財產
- 知識產權的損失、營運中斷及影響產品或服務品質等。

準星-看不見(瞄不準)-風險

目標:目標打不準-有保險

第二部分

零信任與資安

2

零信任與資安

3.零信任三階段

4.零信任的缺點

2.Zero Trust 原則的主要好處

5.零信任的未來是什麼?

6.零信任的挑戰

1.零信任架構-主要原則

7.零信任的誤解

零信任與資安-零信任架構-主要原則

運作原則是「從不信任，始終驗證」

持續監控和驗證

最低權限

裝置存取控制

微分段

防止橫向移動

多重要素驗證 (MFA)

零信任與資安- Zero Trust 原則的主要好處

透過微分段將漏洞限制在一個小區域，從而在攻擊確實發生時將損害降至最低，這也降低了復原成本。

透過驗證每個請求，Zero Trust 安全性降低了易受攻擊的裝置帶來的風險

有助於減少組織的攻擊面

多個驗證因素來減少使用者認證被盜和網路釣魚攻擊的影響。它有助於消除繞過傳統邊界型保護措施的威脅。

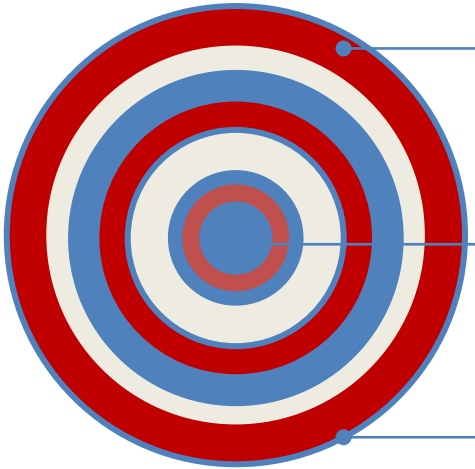
零信任與資安-零信任三階段

1) 風險評估和計劃

2) 實施必要的技術和政策

3) 持續監控、評估和調整。

零信任與資安-零信任的缺點



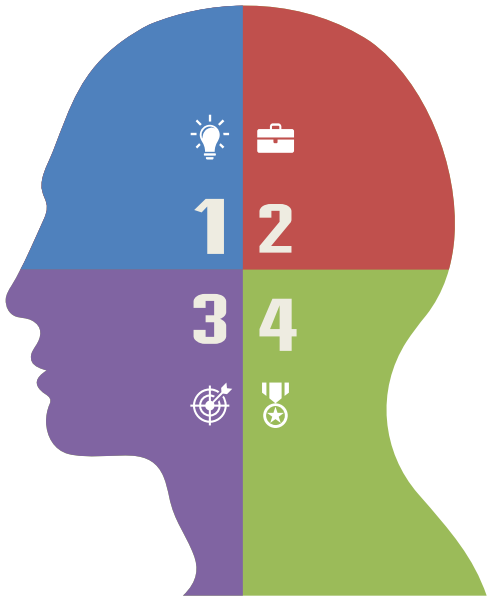
- 可能會增加復雜性和管理成本
- 大量的初始配置和維護工作
- 經常的身份驗證可能會降低使用效率

零信任與資安-零信任的未來是什麼?

01. 可能包括更加自動化和智能化的安全解決方案，並逐漸成為組織標準

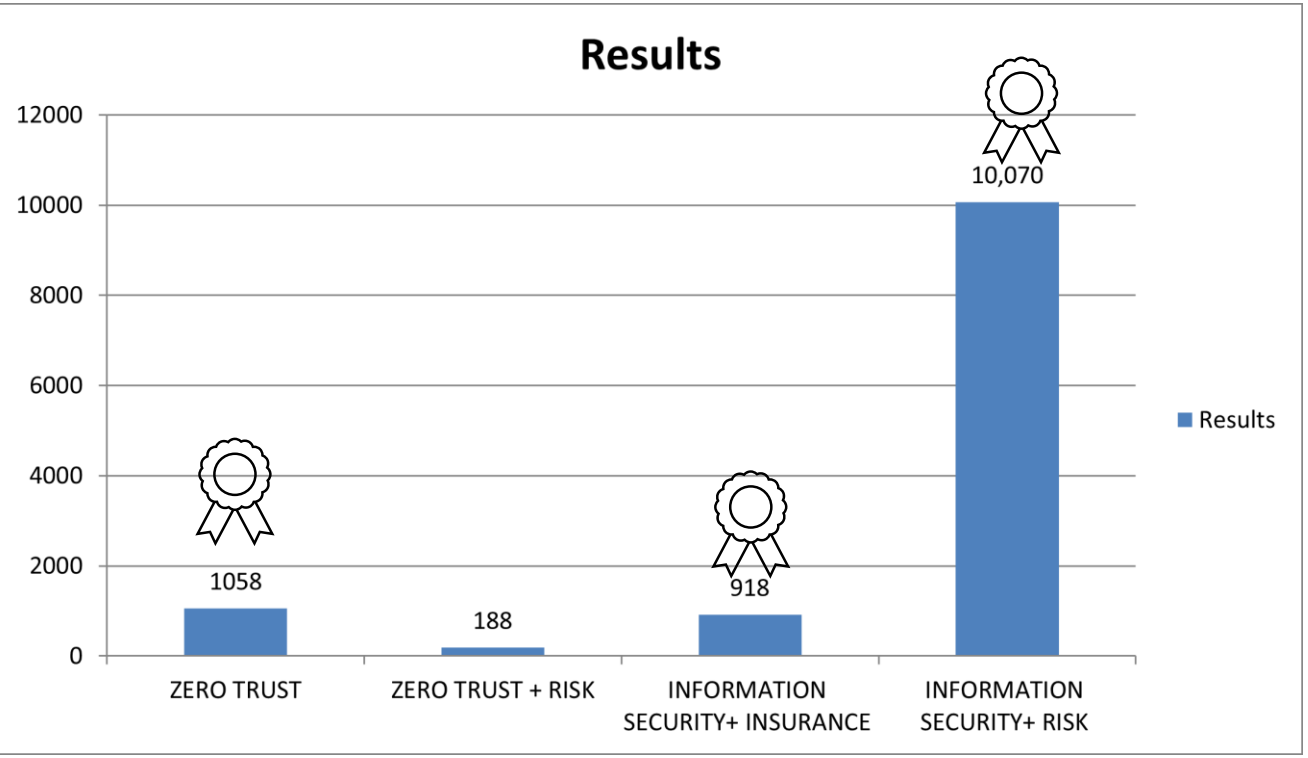
02. 參考統計數
- 產業
- 學術

03. 產業
- 2022-2023近兩年內，有 76% 的機構遭遇過勒索軟體攻擊
- 2023年內，63% 的機構經歷了資安漏洞的侵害
- 使用傳統技術偵測不正當通訊行為平均需時 212 天，而阻止這些行為則需 75 天
- 企業平均花費 37 天和 240 萬美元（中位數）來追蹤及恢復違規通訊
- Forrester Wave報告中的兩項領先技術，逐步被重視：微分段 (2022 年第一季度報告) 和零信任擴展生態系統平台供應商 (2020年第三季度報告)
- 有效降低違規通訊與有害資訊傳遞的風險，能在 10 分鐘內攔截勒索軟體，每年減少 5 次網路災害
- 較有餘力推動創新，每週節省 39 小時的工作時間，支持 14 個額外的數字轉型專案
- 降低成本，節省高達 2,000 萬美元的應用停機損失，並將平均故障恢復時間提高 68%

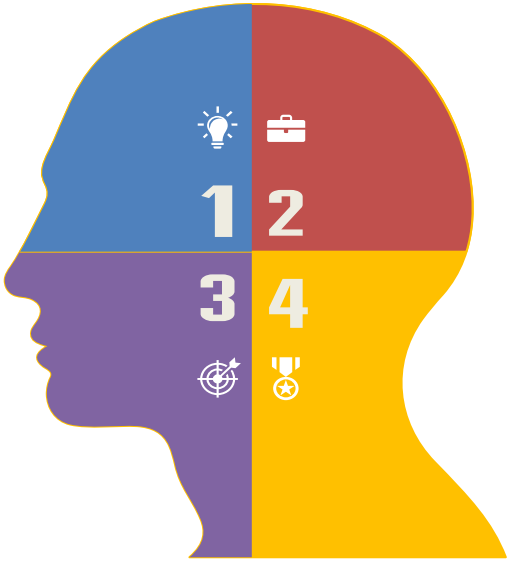


參考來源:
https://www.linkedin.com/pulse/%E8%A7%A3%E5%AF%86%E9%9B%B6%E4%BF%A1%E4%BB%BB-zero-trust%E5%9F%BA%E6%9C%AC%E5%8E%9F%E5%89%87%E8%88%87%E6%A0%B8%E5%BF%83%E6%A6%82%E5%BF%B5-tentenco-6advc/ December 16, 2023

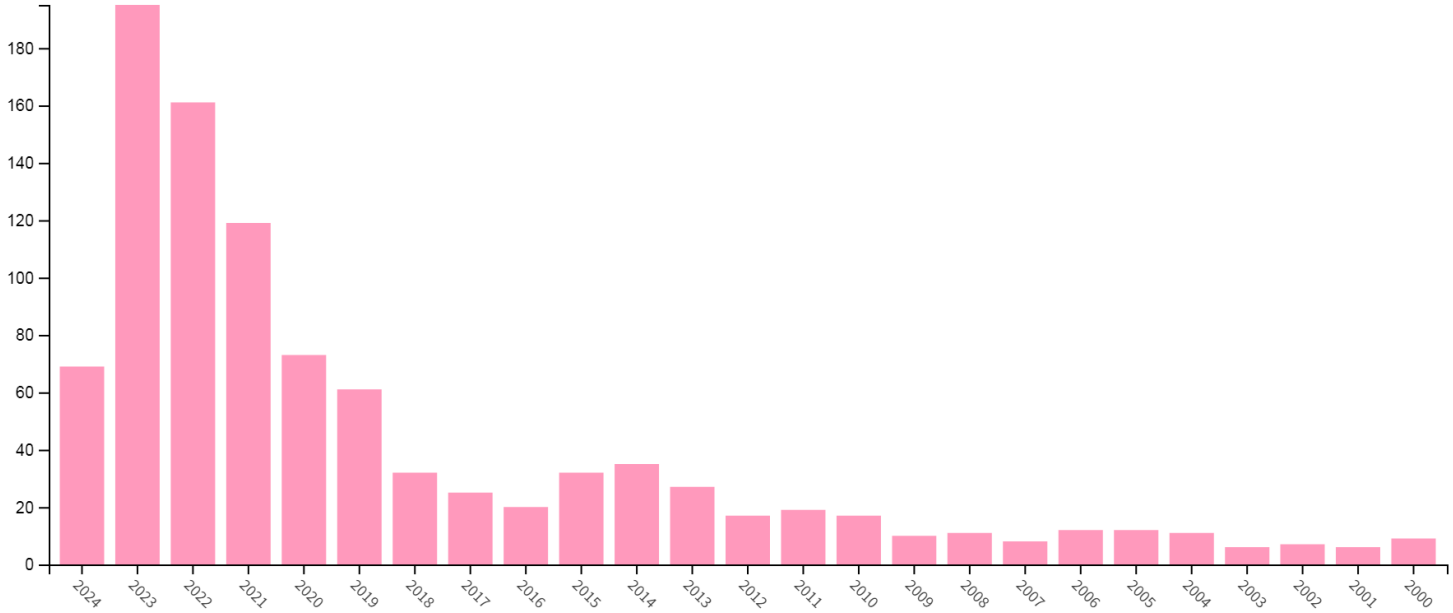
零信任與資安-零信任的未來是什麼？學術統計數

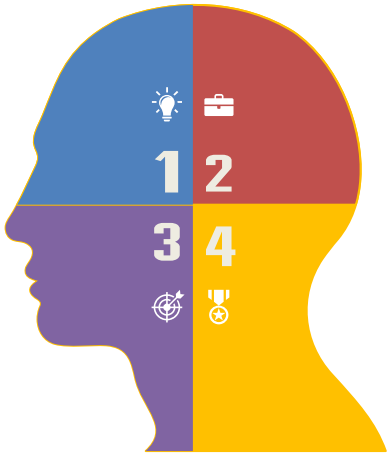


YEAR: 2000~2024



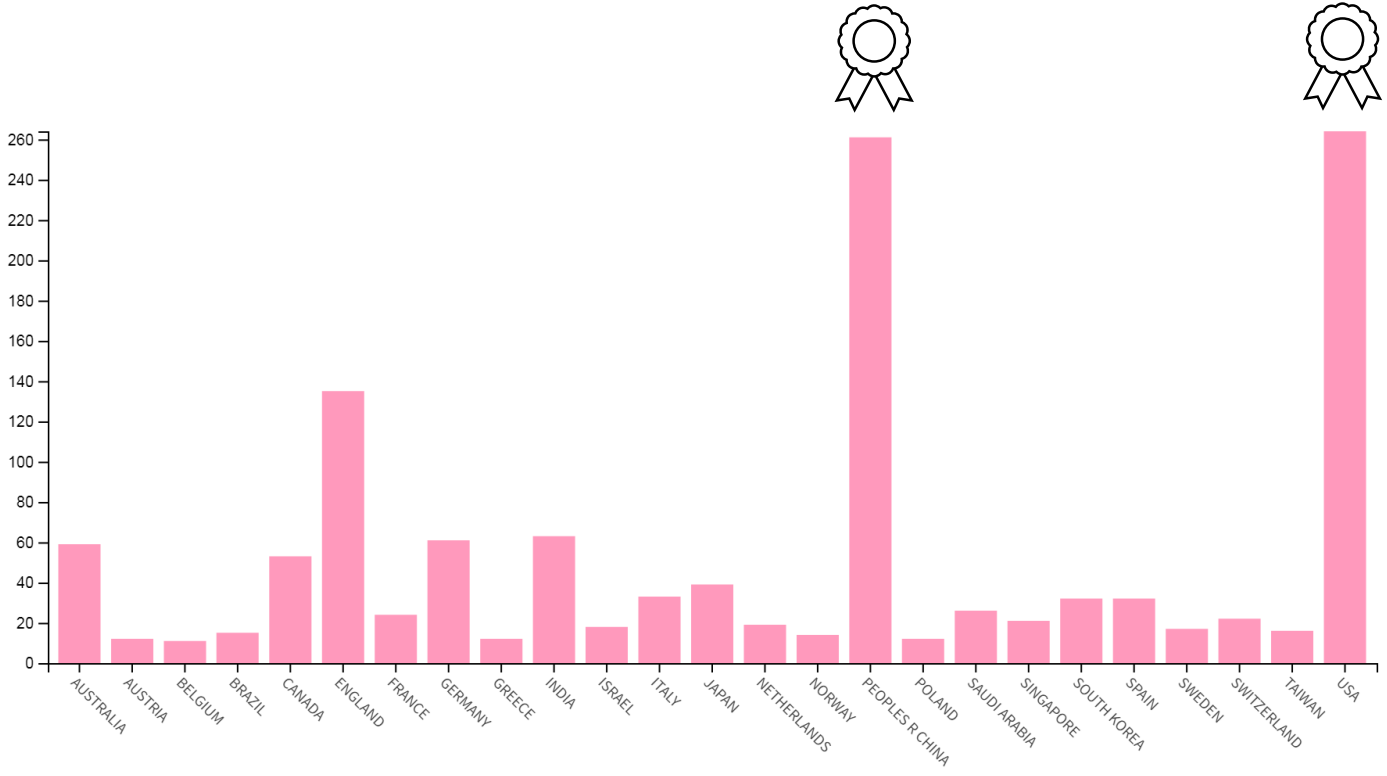
零信任與資安-零信任的未來是什麼? 學術統計數-ZERO TRUST

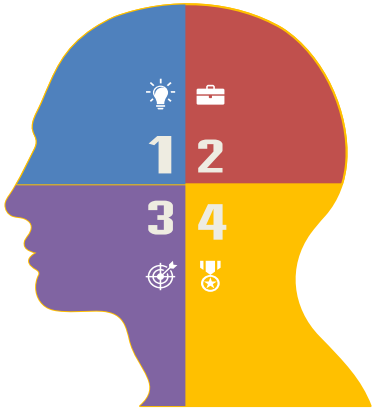




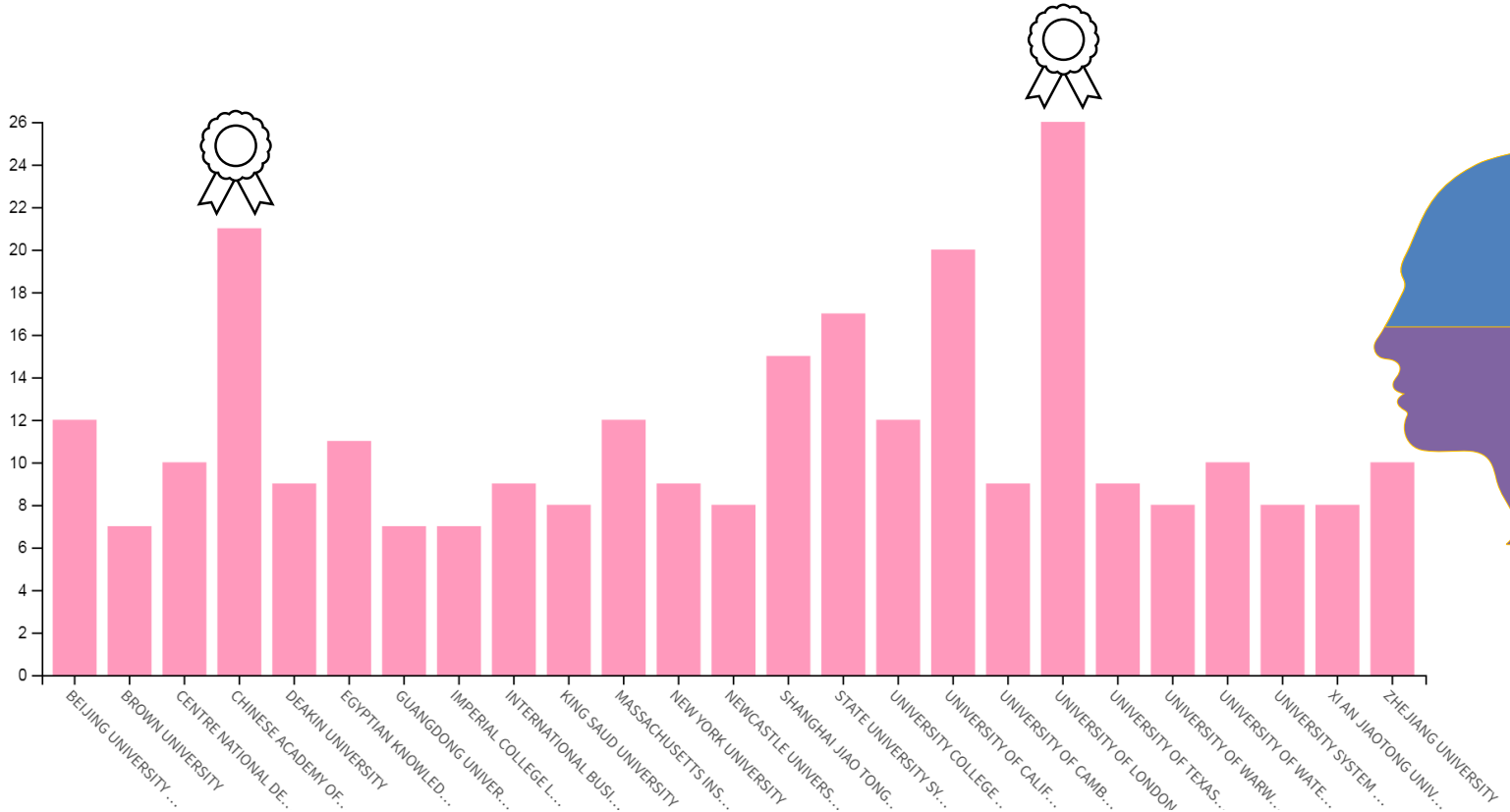
Final Publication Year

零信任與資安-零信任的未來是什麼? 學術統計數-ZERO TRUST

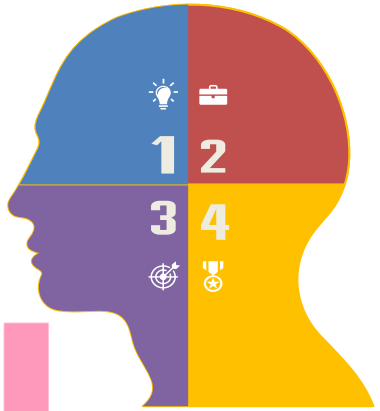




零信任與資安-零信任的未來是什麼? 學術統計數-ZERO TRUST

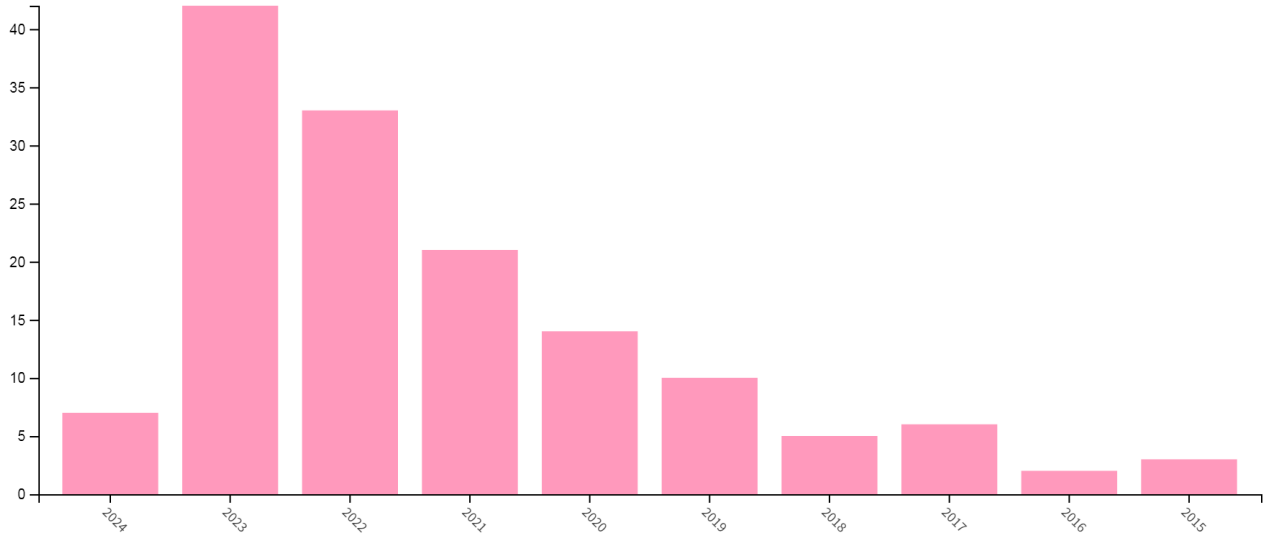


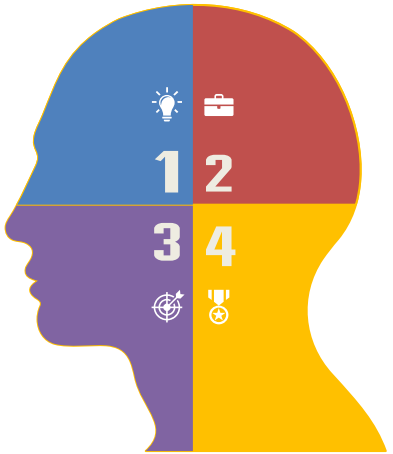
Affiliations



零信任與資安-零信任的未來是什麼？學術統計數-

ZERO TRUST+ RISK EVALUATION

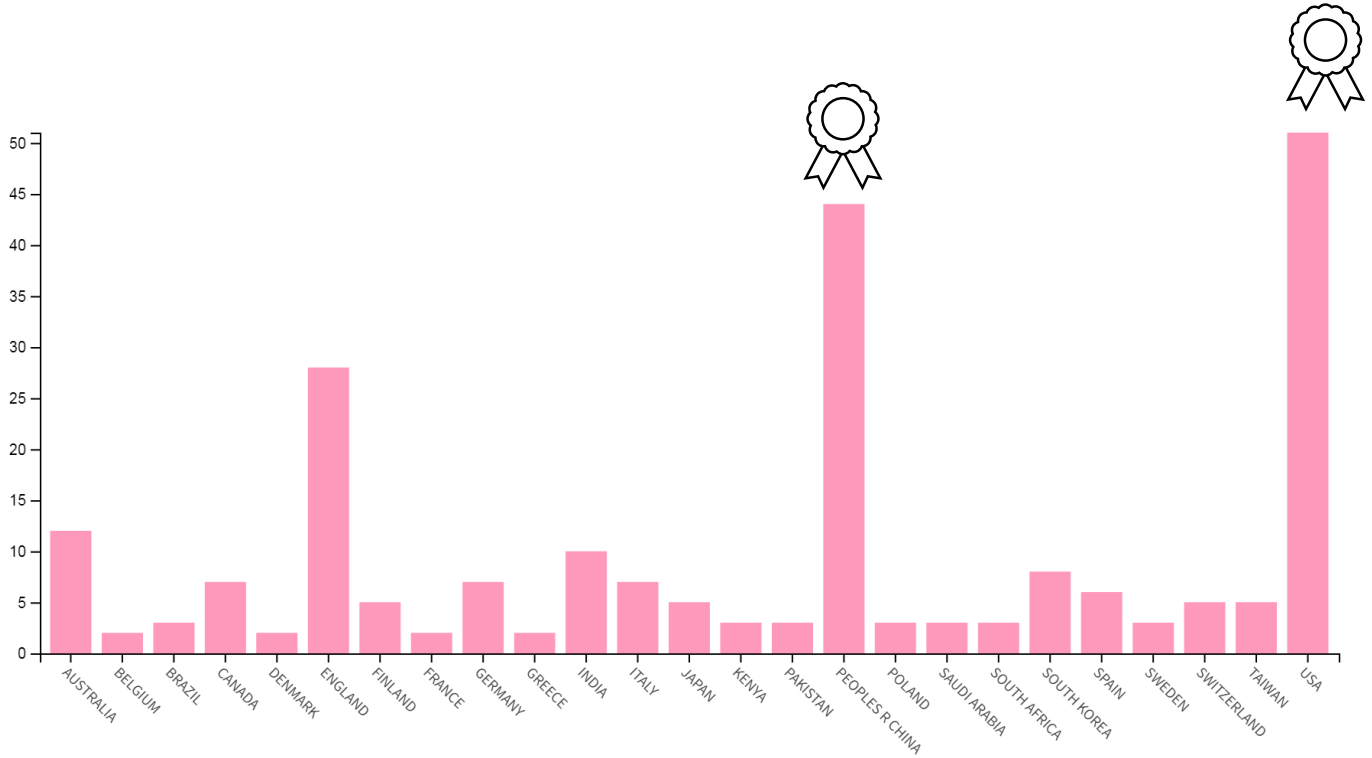


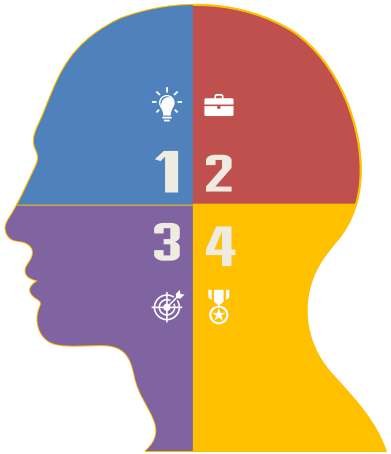


Final Publication Year

零信任與資安-零信任的未來是什麼? 學術統計數-

ZERO TRUST+ RISK EVALUATION

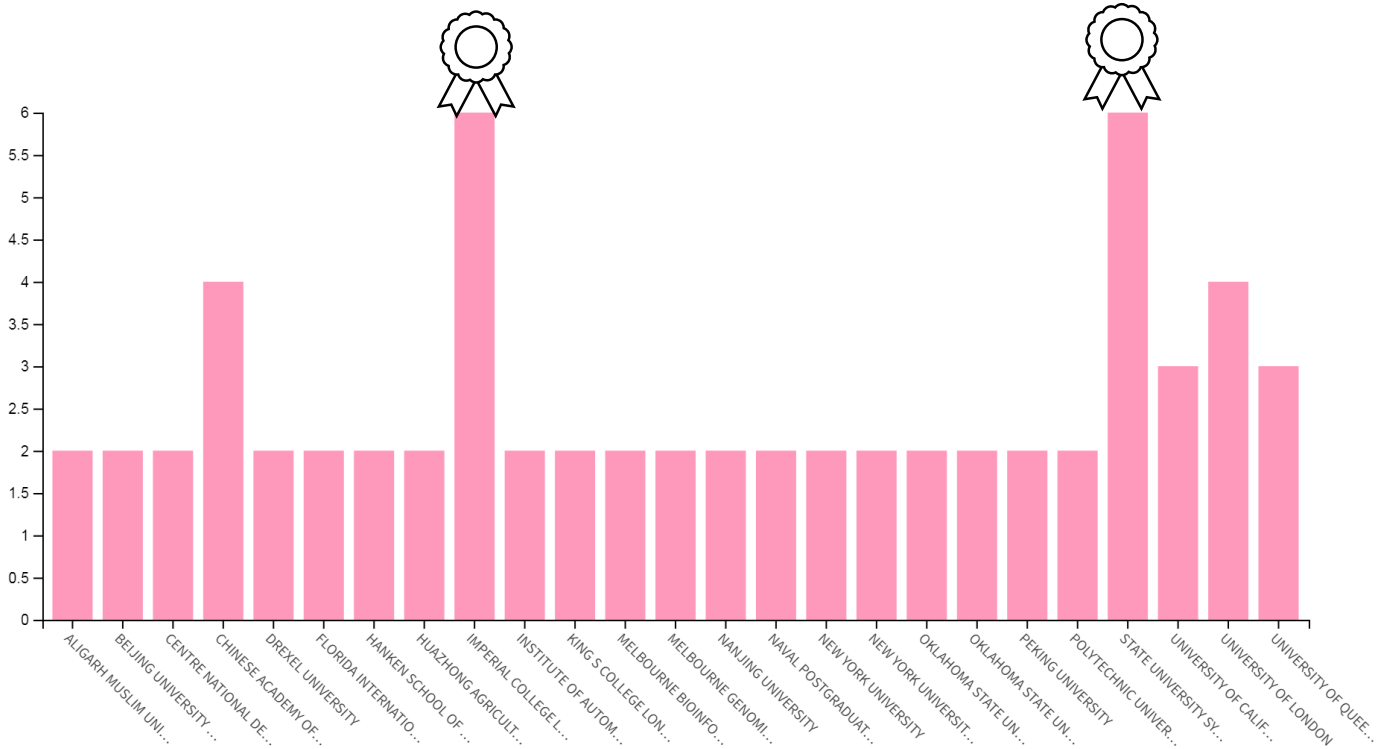


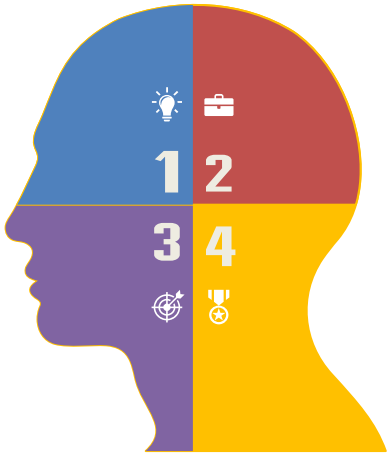


Countries Regions

零信任與資安-零信任的未來是什麼? 學術統計數-

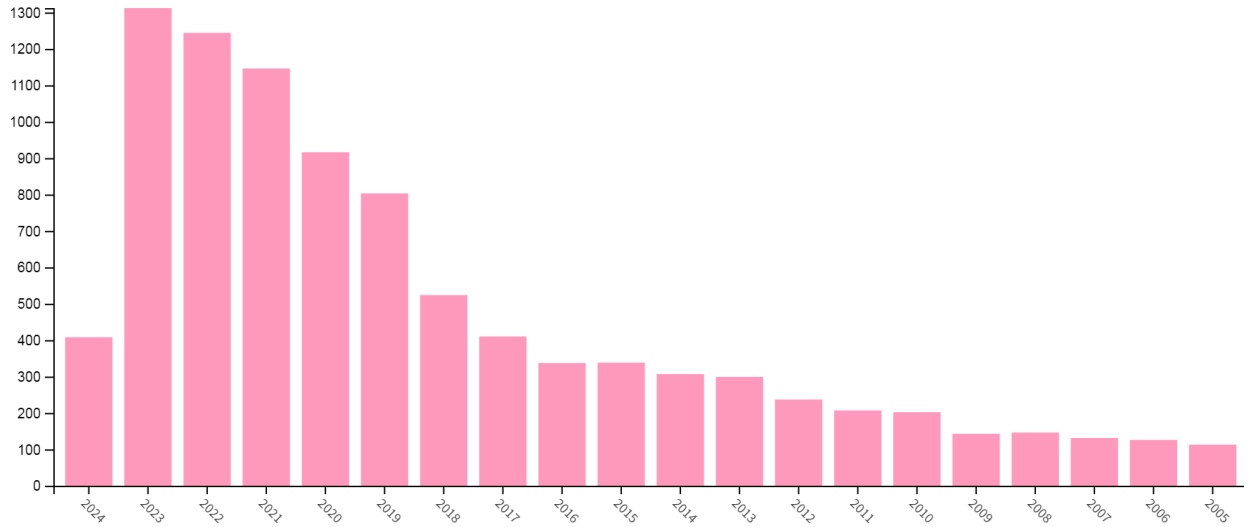
ZERO TRUST+ RISK EVALUATION

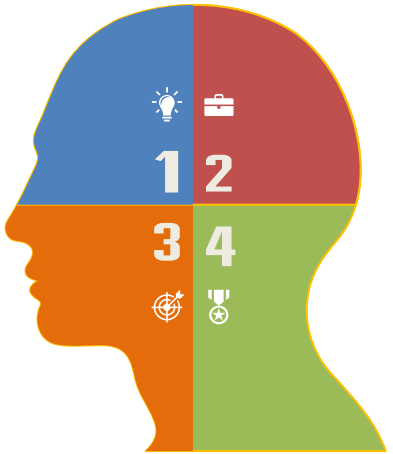




Affiliations

零信任與資安-零信任的未來是什麼? 學術統計數-
INFORMATION SECURITY+ RISK

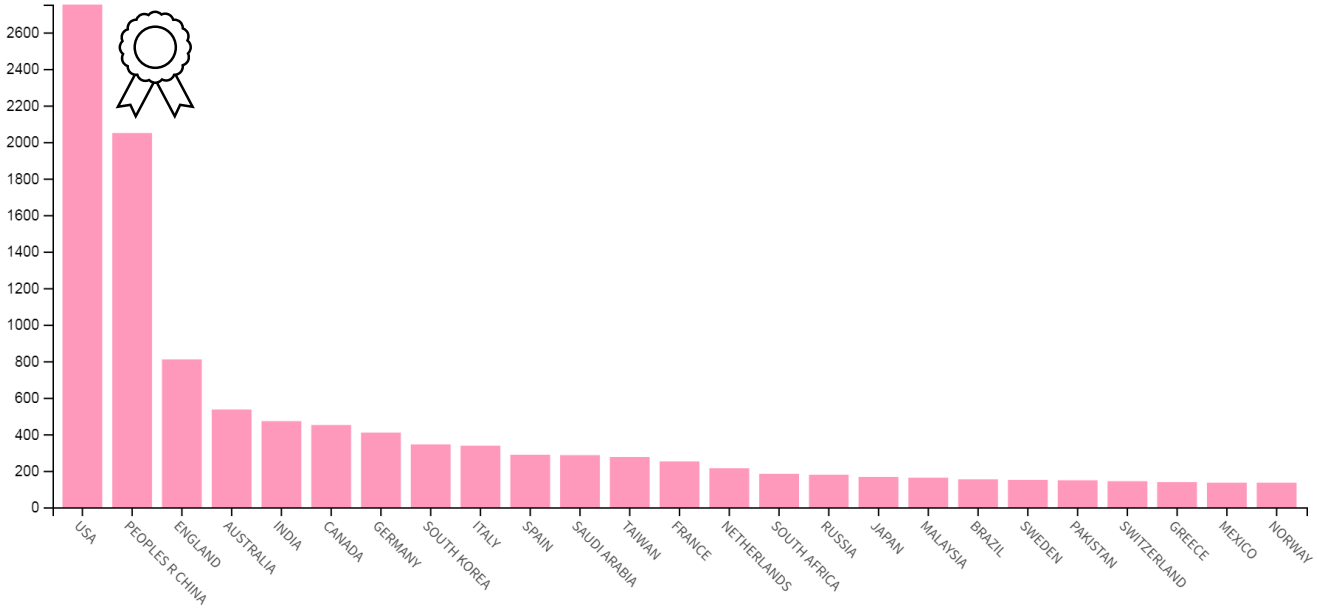


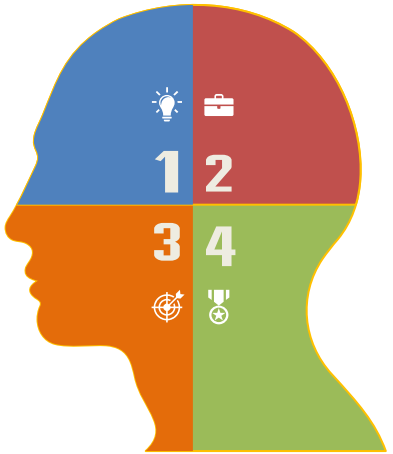


Final Publication Year

零信任與資安-零信任的未來是什麼? 學術統計數-

INFORMATION SECURITY+ RISK



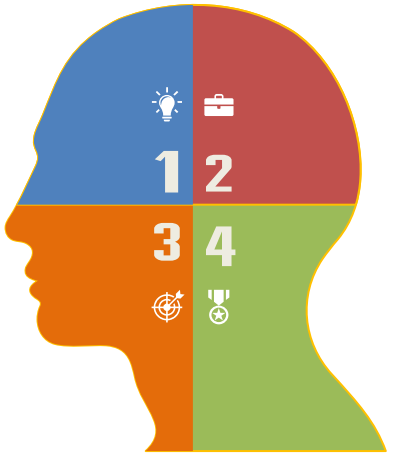


Countries Regions

零信任與資安-零信任的未來是什麼? 學術統計數-

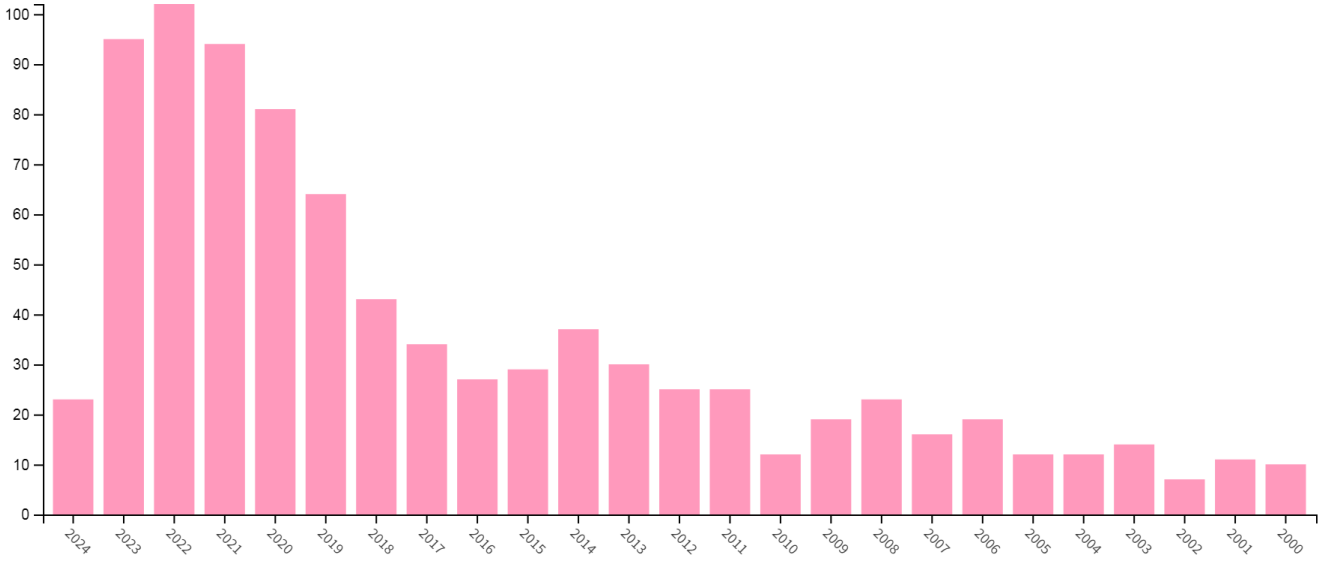
INFORMATION SECURITY+ RISK

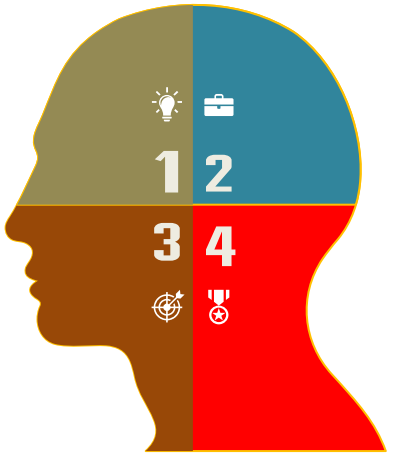
Affiliations



零信任與資安-零信任的未來是什麼? 學術統計數-

INFORMATION SECURITY+ INSURANCE

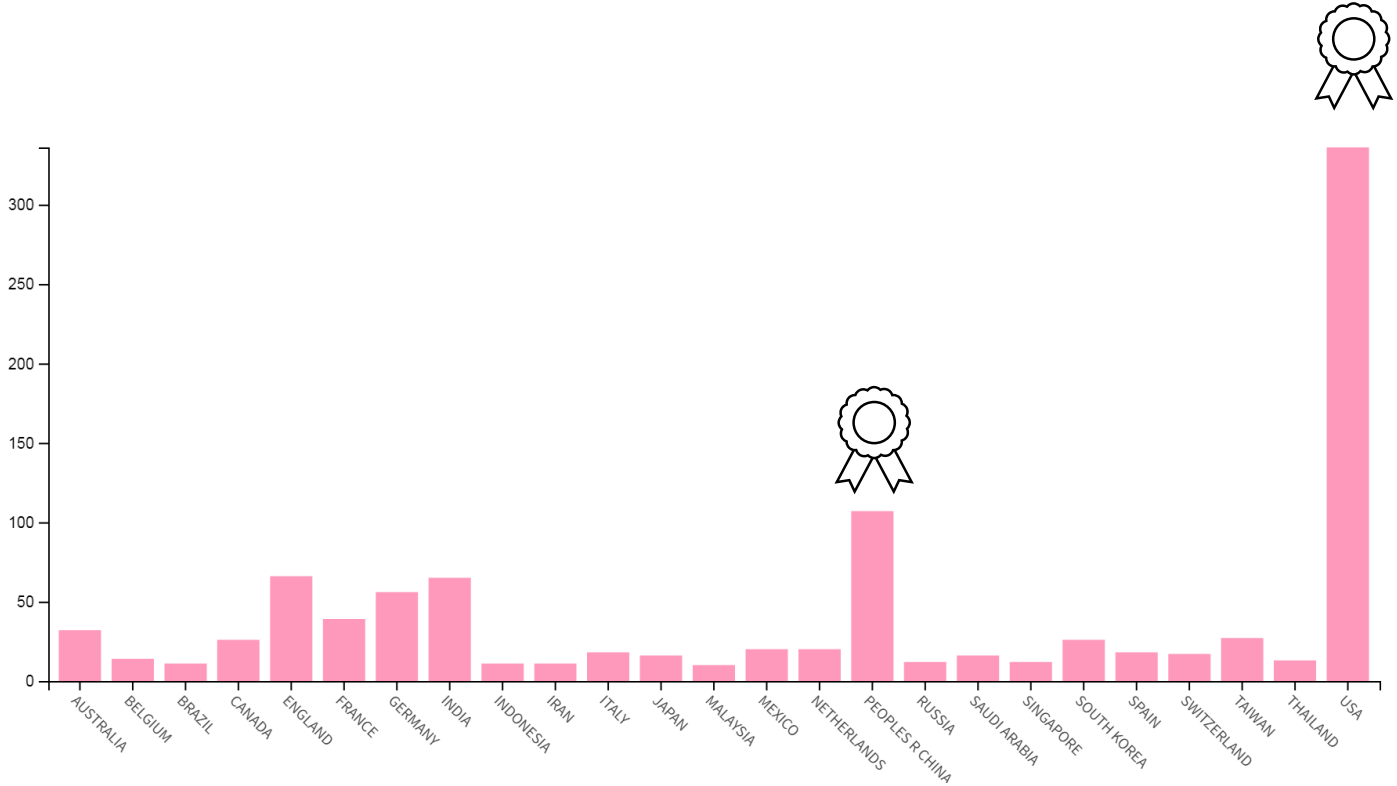




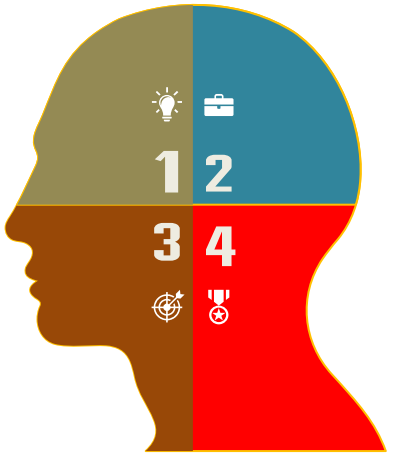
Final Publication Year

零信任與資安-零信任的未來是什麼? 學術統計數-

INFORMATION SECURITY+ INSURANCE

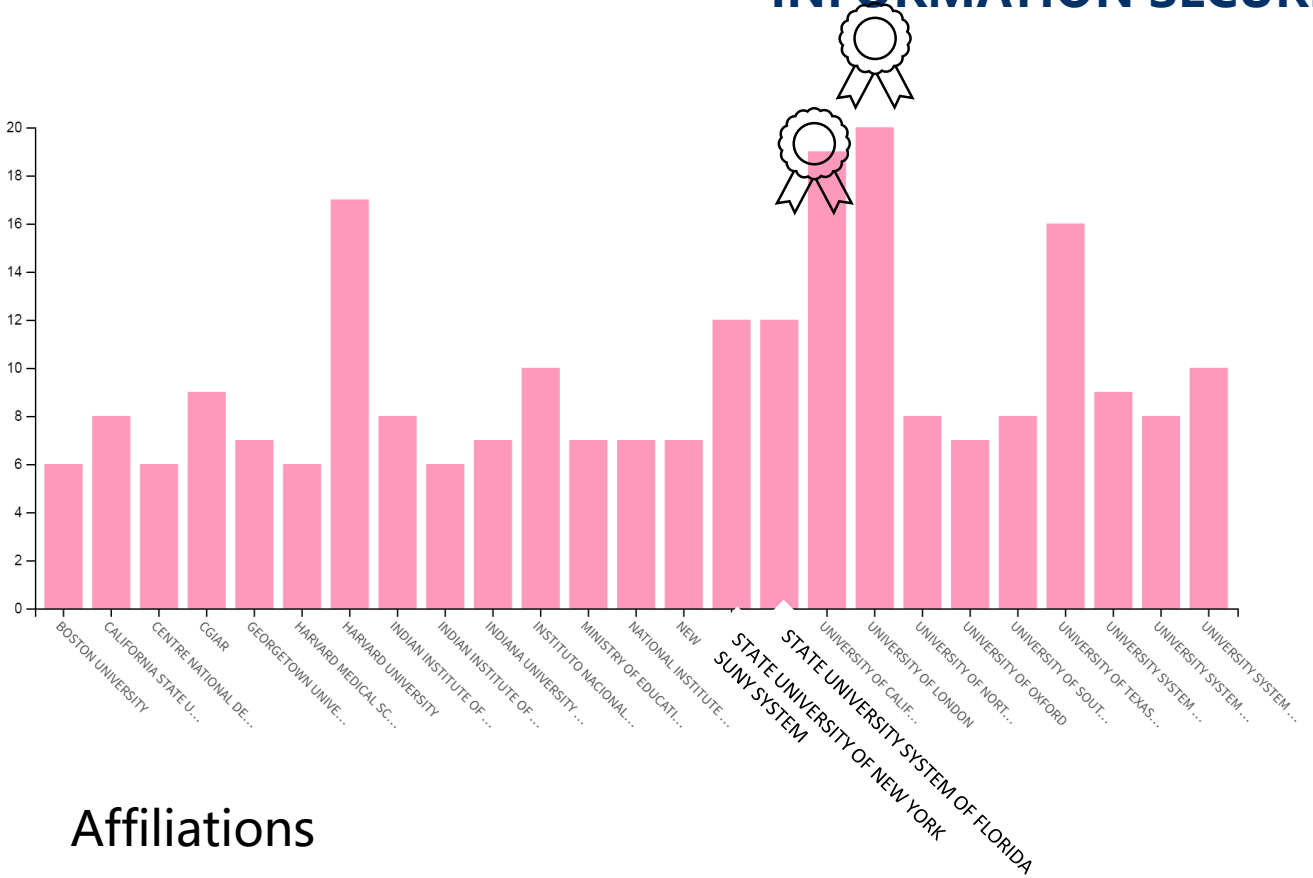


Countries Regions

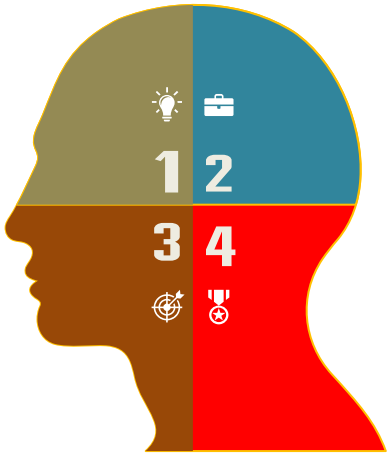


零信任與資安-零信任的未來是什麼? 學術統計數-

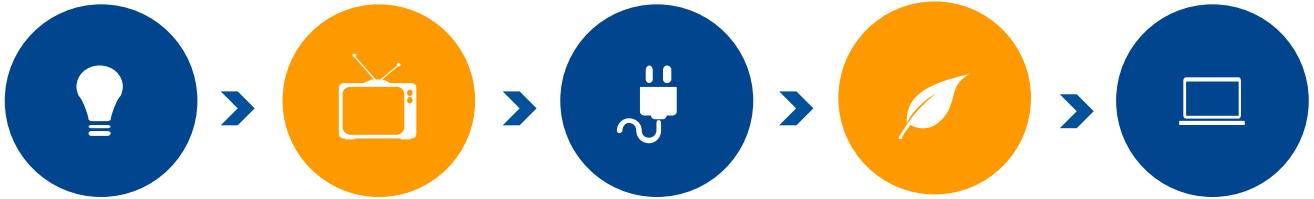
INFORMATION SECURITY+ INSURANCE



Affiliations



零信任與資安-挑戰



1.複雜的實施

零相信需要安全方法的根本轉變，涉及整合IAM-身分識別與存取管理、微分段和加密等各種技術。這種複雜性可能會使實施變得令人畏懼，尤其是對於擁有遺留系統的大型組織。

2.持續監控和管理

零通道模型中持續監控和動態策略執行需要大量資源和複雜的工具，而這對於有效管理來說可能具有挑戰性。

3.使用者體驗

更嚴格的存取控制和頻繁的身份驗證請求可能會導致使用者摩擦，從而對使用者體驗產生負面影響。

4.成本和資源強度

零信任架構的初始設定、持續管理和維護可能會佔用大量資源且成本高昂，尤其是對於小型組織而言。

5.與現有系統整合

將零信任原則與現有安全系統和協定整合可能具有挑戰性，需要仔細規劃和執行。

零信任與資安-誤解

完全消除威脅：一個常見的誤解是零信任可以消除安全威脅。雖然它大大降低了風險，但沒有任何系統可以保證絕對安全。

John Kindervag

僅適用於大型企業：人們認為零信任只適合大型組織。各種規模的企業都可以從其根據其特定需求和能力量身定制的原則中受益。

立即結果：有些人期望實施後立即得到結果。然而，零信任是一種隨著時間的推移而發展和成熟的策略方法。

一刀切的解：零信任不是一刀切的解。它需要根據每個組織的具體需求和架構進行客製化。

完全基於技術的解決方案：雖然技術是關鍵組成部分，但零信任還需要改變組織內的政策、文化和安全方法。

零信任與資安-誤解: John Kindervag

John Kindervag

No More Chewy Centers

illumio

For Security & Risk Professionals

2010

September 14, 2010 | Updated: September 17, 2010

No More Chewy Centers: Introducing The Zero Trust Model Of Information Security

by John Kindervag
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For a generation of information security professionals, this was the motto we grew up with. It was a motto based on trust and the assumption that malicious individuals wouldn't get past the "hard crunchy outside." In today's new threat landscape, this is no longer an effective way of enforcing security. Once an attacker gets past the shell, he has access to all the resources in our network. We've built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that easily pierce our current security protections. To confront these new threats, information security professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. To help security professionals do this effectively, Forrester has developed a new model for information security, called Zero Trust. This report, the first in a series, will introduce the necessity and key concepts of the Zero Trust Model.

https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

Strategy

ZERO TRUST

EXFILL

A strategy designed to stop data breaches and prevent other cyber-attacks from being successful by eliminating trust from digital systems.

illumio

- 目的:防止因網路攻擊所造成的資料外洩
- 策略:最低的信任以建立該有的防護

零信任與資安-誤解: John Kindervag

False

Some Zero Trust Misconceptions

Zero Trust means making a system trusted

Zero Trust is about identity

There are Zero Trust products

Zero Trust is complicated

illumio

第三部分

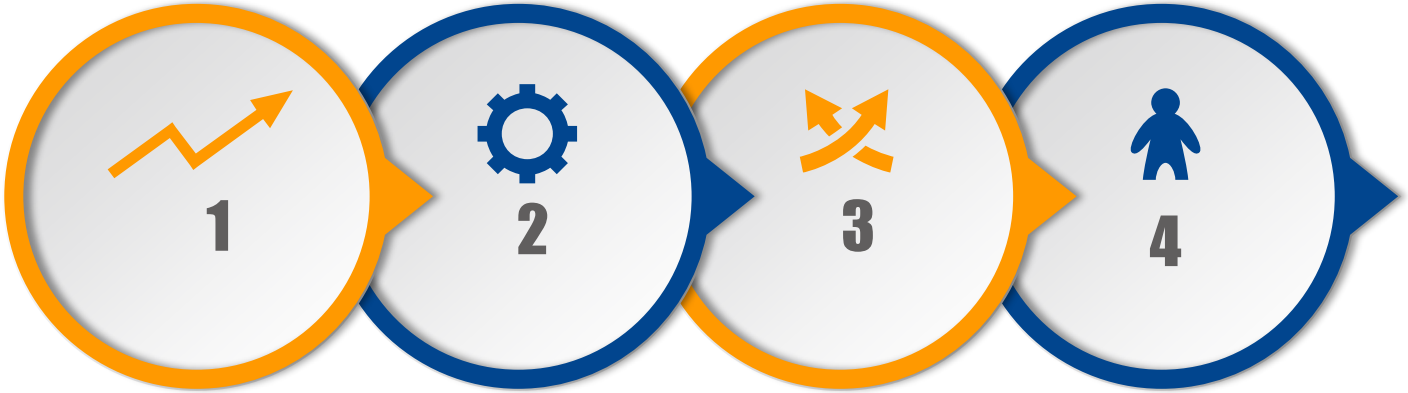
三點與三險，危險、風險與保險

3

三點與三險，危險、風險與保險

資訊安全的保險評估

零信任與資訊安全保險



資訊安全的風險評估

零信任與資訊安全風險評估

三點與三險，危險、風險與保險-資訊安全的風險評估

資料外洩對財務及信譽都可能造成嚴重的影響。根據 IBM 2022年的資料外洩損失成本報告，資料外洩事件在全球造成的平均損失成本為435萬美元，其中美國的平均損失成本超過944萬美元。
與資料外洩相關的損失成本包括(1)、業務損失、收入損失和客戶損失，平均為142萬美元。(2)、檢測和控制外洩的成本稍高一些，平均為144萬美元。(3)、外洩事件後的處理費用（如罰款、和解、法律費用、報告費用以及為受影響客戶提供免費信用監控的費用）平均為149萬美元。

三點與三險，危險、風險與保險-資訊安全的風險評估

1.識別資產：首先需要識別出組織中所有重要的資訊資產，如數據、硬體、軟件、通訊系統等。

2.識別威脅和脆弱性：確定哪些威脅可能影響這些資產，包括內部和外部的威脅。同時，識別這些資產的脆弱性，即攻擊者可以利用哪些弱點。

3.評估影響和可能性：評估如果這些威脅變為現實，可能對組織造成的影響程度，以及這些威脅發生的可能性。

4.風險評估：使用影響和可能性的評估結果來確定風險的等級。通常風險可以分為高、中、低三個等級。

5.風險處理：根據風險的等級，決定如何處理這些風險。風險處理策略可能包括風險的避免、減輕、轉移（例如通過保險）或接受。

6.制定措施並實施：為每個識別和評估的風險制定合適的安全措施，並將這些措施實施到相應的資訊系統和流程中。

7.監控和審查：風險評估是一個持續的過程，需要定期審查和更新，以應對新出現的威脅和脆弱性。

三點與三險，危險、風險與保險-資訊安全的風險評估

關於ISRM的文獻強調了資訊安全風險三種缺陷：

不足1：資訊安全風險識別**普遍敷衍**

不足2：資訊安全風險的估計通常**很少參考組織的實際情**況

不足3：資訊安全風險評估通常**是間歇性的、非歷史的**

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Computers & Security 44, 1–15. https://doi.org/10.1016/j.cose.2014.04.005

三點與三險，危險、風險與保險-資訊安全的風險評估

- 模型四階段:環境、理解、決策與行動
- **風險管理的理解模型:認知、了解及投射**
- 二因子變數:
  - ■不可拆分的系統因子:任務性/整合性
  - ■可拆分的因子:個人、軟硬體及目標管理等

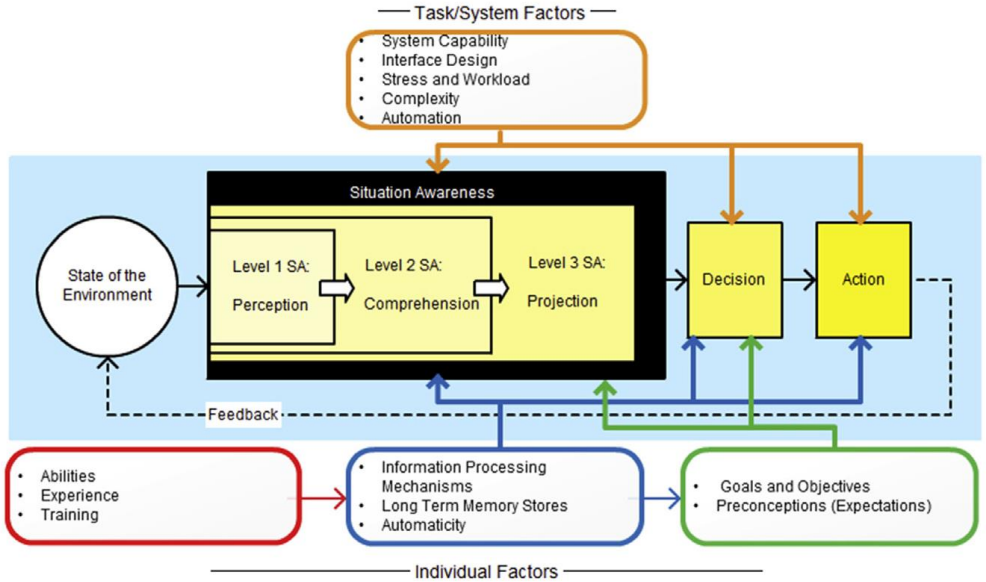


Fig. 1 – Endsley's SA model (adapted from Endsley, 1995).

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Computers & Security 44, 1–15. https://doi.org/10.1016/j.cose.2014.04.005

三點與三險，危險、風險與保險-資訊安全的風險評估

情報循環-
(Intelligence cycle) 12階段

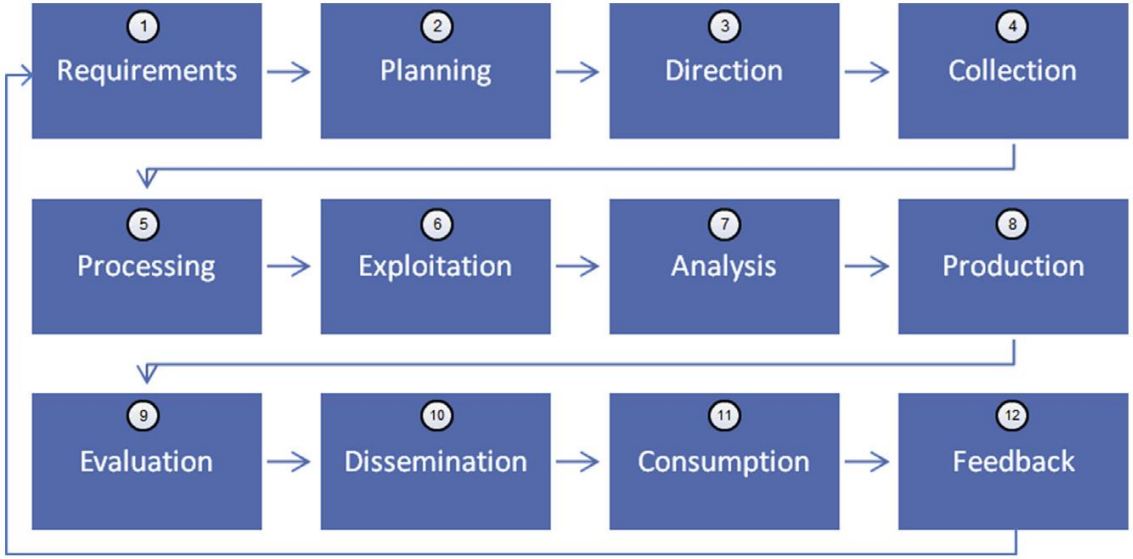


Fig. 2 – The intelligence cycle in 12 phases.

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Computers & Security 44, 1–15. https://doi.org/10.1016/j.cose.2014.04.005

三點與三險，危險、風險與保險-資訊安全的風險評估

理解的發展

理解的綜整合成

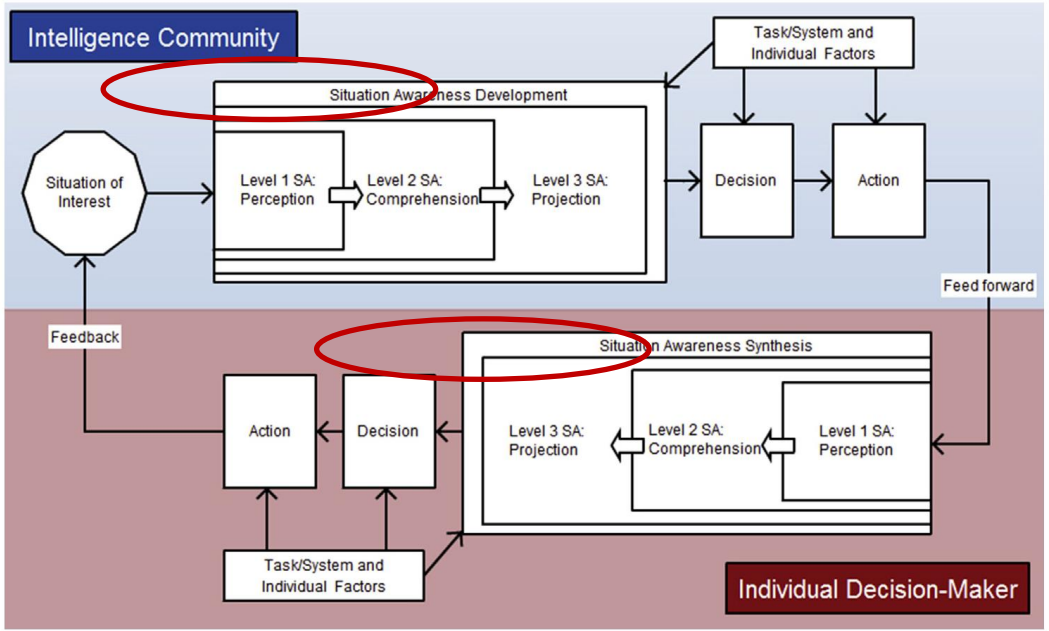


Fig. 3 – Our initial adaptation of Endsley's model to describe the USNSIE.

美國國家安全情報企業USNSIE） 案例研究結果

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Computers & Security 44, 1–15. https://doi.org/10.1016/j.cose.2014.04.005

三點與三險，危險、風險與保險-資訊安全的風險評估

- 配合情報循環- (Intelligence cycle) 12階段
- 結合目標管理

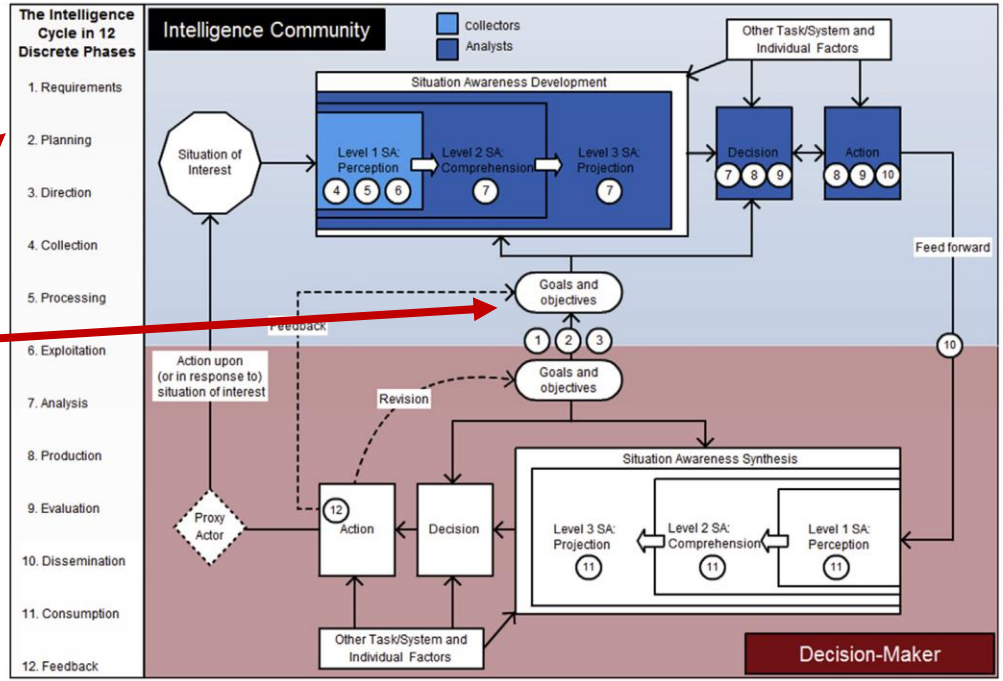


Fig. 4 – The USNSIE model.

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Computers & Security 44, 1–15. https://doi.org/10.1016/j.cose.2014.04.005

三點與三險，危險、風險與保險-資訊安全的風險評估

任務角色

- 風管團隊
- 風管經理

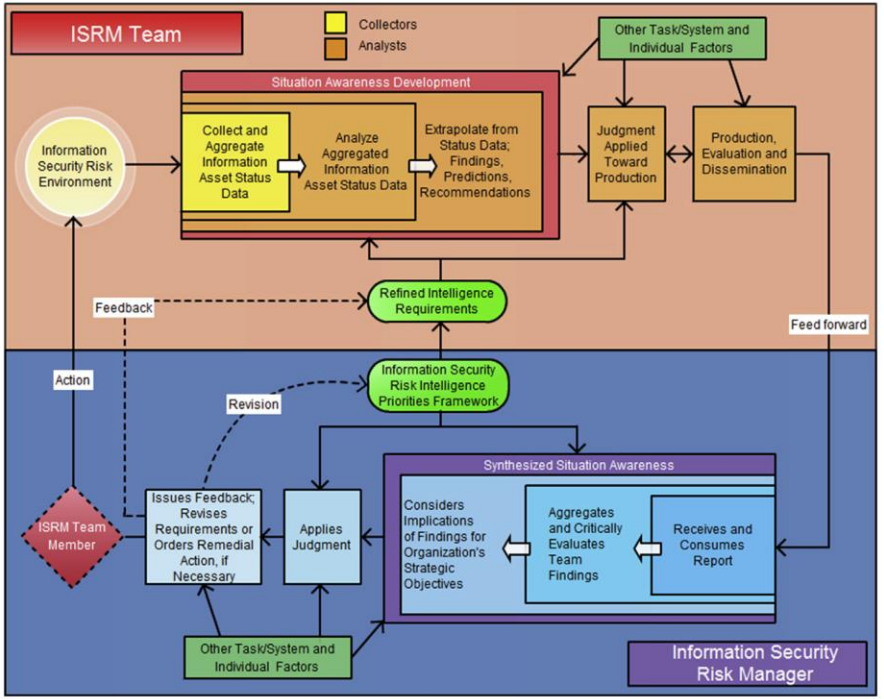


Fig. 5 – The SA model for use in ISRM (SA-ISRM).

組織美國國家安全情報企業 US national security intelligence enterprise（USNSIE） 案例研究結果

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Computers & Security 44, 1–15. https://doi.org/10.1016/j.cose.2014.04.005

三點與三險，危險、風險與保險-資訊安全的風險評估

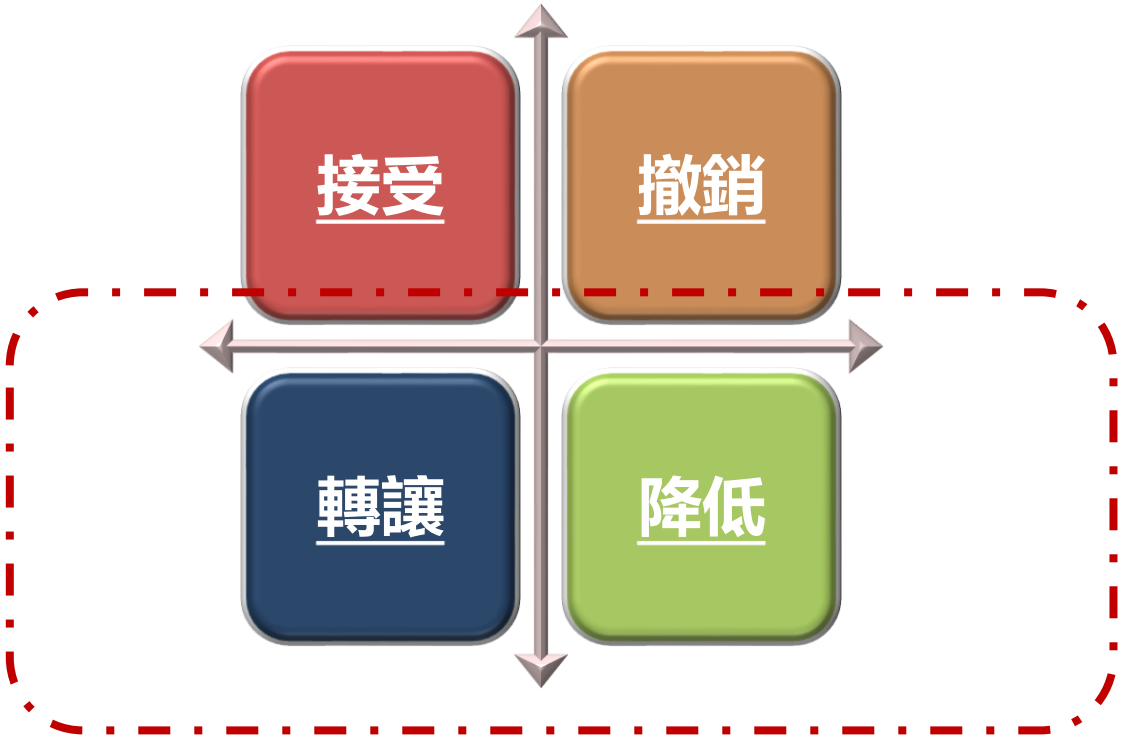
SA-ISRM 模型的情報驅動的 ISRM 流程活動

1. 具體的情報要求
2. 正式的數據收集和分析的規劃
3. ISRM 收集和分析工作的方向由ISRM負責人協調和集中管理。
4. ISRM 負責人負責在必要時協調和解決相互衝突的收集工作。
5. 在可能的情況下，處理是自動進行的
6. 在可能的情況下，開發是自動進行的
7. 分析可以由系統輔助，但主要由人類分析師進行
8. 資訊產生可能是電腦輔助的，但主要由人工分析師進行。
9. 在**風險評估發出**前進行評估，以確保ISRM情報產品符合發佈的要求並遵守產生標準。
10. 通過預先確定的溝通管道提供風險管理決策者;按照預先制定的準則，向機構或資料庫進行發布。
11. **風險評估報告**必須產生，否則**風險評估**是徒勞的;以讓風險管理決策者的決策和行動負責可能符合組織的利益。
12. 風險管理決策者有義務就所**風險評估報告**是否符合已發佈的要求，或者是否必須修改長期情報要求發出回饋意見。

組織美國國家安全情報企業 US national security intelligence enterprise（USNSIE） 案例研究結果

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Computers & Security 44, 1–15. https://doi.org/10.1016/j.cose.2014.04.005

三點與三險，危險、風險與保險-四種風險最小化策略



三點與三險，危險、風險與保險-資訊安全的保險評估

1.識別和評估資產：明確組織中重要的資訊資產及其價值，包括數據、硬體、軟件和智慧財產權。

2.風險評估：識別可能對這些資產造成威脅的風險，評估這些威脅實現的可能性和潛在的影響程度。

3.分析歷史安全事件：審查過去的安全事件和數據違規情況，瞭解組織的安全弱點和曝險風險。

4.檢視現有的安全措施：評估現有的安全政策和控制措施的效果，包括防火牆、加密技術和身份驗證系統。

5.確定保險需求：根據風險評估和潛在損失，確定需要多少保險覆蓋。考慮包括責任保險、數據恢復和業務中斷保險。

6.選擇合適的保險提供商：比較不同保險提供商提供的條款、覆蓋範圍和保費，選擇最符合組織需求的保險計劃。

7.購買保險並定期審查：購買選定的保險後，需要定期重新評估保險覆蓋範圍，確保它仍然符合組織的安全需求和潛在風險。

三點與三險，危險、風險與保險-零信任與資訊安全風險評估

2.增強風險識別過程：

通過零信任架構中的持續監控和分析，組織可以更早地識別和響應安全威脅，這有助於風險評估過程中更準確地計算威脅的發生可能性和潛在影響。

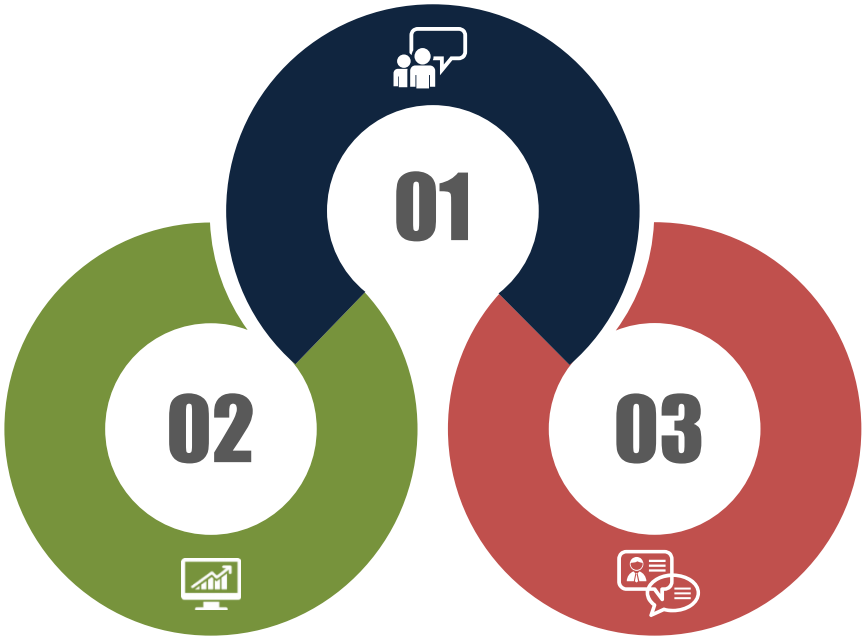
1.精確定義和保護資產：

零信任模型要求組織明確識別並對所有資訊資產進行分類，這可以增強資訊安全風險評估的精確性，使風險評估能夠更具針對性地識別潛在的脆弱點和威脅。

3.微分段實施：

零信任模型推薦的微分段策略有助於限制安全威脅的擴散，這可以降低風險評估中識別的單一點故障的風險，從而減少整體安全風險。

三點與三險，危險、風險與保險-零信任與資訊安全保險



1.證明有效的風險管理：實施**零信任策略**可以向保險公司展示組織對於風險管理的認真態度和有效措施，這**可能有助於降低保險費率**或改善保險條款。。

2.增強保險覆蓋的適用性：隨著零信任減少安全事故的發生，這可能**影響保險覆蓋需求的範圍和深度**，使組織能夠更有**針對性地選擇需要的保險保障。**

3.符合保險要求：許多資訊安全保險提供商要求投保企業必須**有一定的安全措施才能符合投保標準**。零信任模型的實施可以幫助滿足這些標準，尤其是在身份驗證和數據訪問控制方面。

三點與三險，危險、風險與保險-資訊安全的保險評估

網路中斷的成本包括侵犯客戶隱私、業務中斷、物理基礎設施損壞、回應成本、訴訟和市場價值損失。

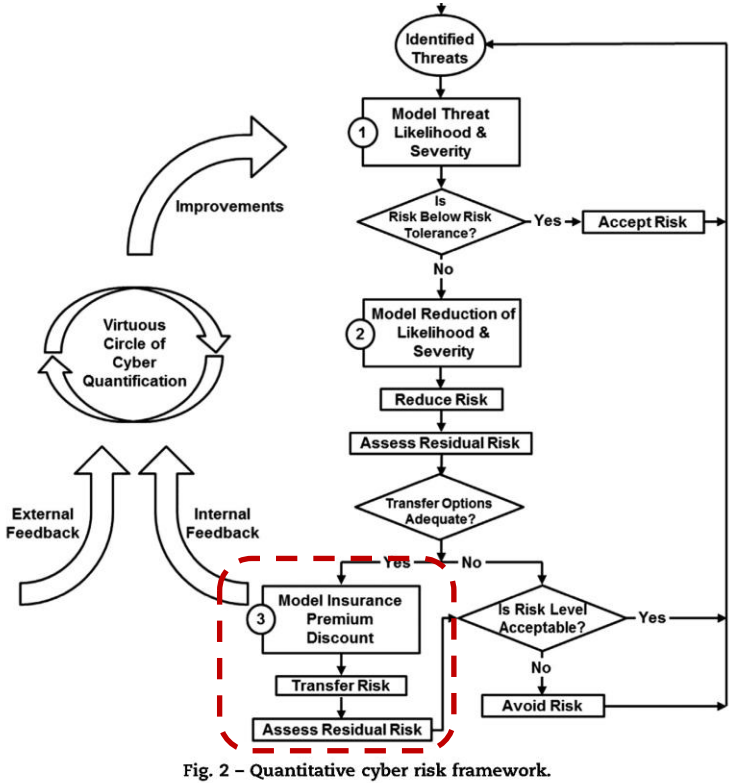


Fig. 2 – Quantitative cyber risk framework.

Young, D., Lopez, J., Rice, M., Ramsey, B., McTasney, R., 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies International Journal of Critical Infrastructure Protection 14, 43–57. https://doi.org/10.1016/j.ijcip.2016.04.001

三點與三險，危險、風險與保險-資訊安全的保險評估

計算所含的可能變數:

- 財務損失
- 被攻擊的機率
- 被攻破的機率
- 不再投資資安的預期損失
- 資安投資金額
- 有資安投資的條件下，被攻破的機率
- 有資安投資的條件下，被攻破的財務損失

Table 2 – Gordon–Loeb model variables and expressions.

Label	Description
λ	Monetary loss caused by a security breach
t	Probability of an attempted breach
v	Probability of an attempted breach being successful (also referred to as vulnerability)
λtv	Expected loss conditioned on no new additional security investment
z	Monetary investment in security
z^*	Optimal monetary investment in security
$S(z, v)$	Security breach probability function expressing the probability that security will be breached given a monetary investment in security z
$S(z, v)\lambda t$	Expected loss conditioned on the additional security investment z (also referred to as residual risk)
α	Measure of effectiveness of security controls

Young, D., Lopez, J., Rice, M., Ramsey, B., McTasney, R., 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies International Journal of Critical Infrastructure Protection 14, 43–57. https://doi.org/10.1016/j.ijcip.2016.04.001

三點與三險，危險、風險與保險-資訊安全的保險評估

- 預估損害程度
- 風險預防投入成本
- 保險費
- 理賠範圍
- 投入總預算

Table 11 – Optimization results for Company C.

Severity (λ)	Controls (z)	Premium (P)	Coverage purchased	Total budget
$30.0M	$500K	$2.19M	$30.0M	$2.69M
$32.0M	$500K	$2.44M	$32.0M	$2.94M
$34.0M	$500K	$2.49M	$34.0M	$2.99M
$36.0M	$500K	$2.50M	$34.1M	$3.00M
$38.0M	$500K	$2.50M	$34.1M	$3.00M
$40.0M	$500K	$2.50M	$34.1M	$3.00M
$42.0M	$500K	$2.50M	$34.1M	$3.00M
$44.0M	$500K	$2.50M	$34.1M	$3.00M
$46.0M	$500K	$2.50M	$34.1M	$3.00M
$48.0M	$500K	$2.50M	$34.1M	$3.00M
$50.0M	$500K	$2.50M	$34.1M	$3.00M

- A:投資金額含保費約是理賠金額的8.8%
- B:投資金額含保費約是損失金額的6~8.9%
- C:保險涵蓋率68~100%.
- B與C 關係性

Young, D., Lopez, J., Rice, M., Ramsey, B., McTasney, R., 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies International Journal of Critical Infrastructure Protection 14, 43–57. https://doi.org/10.1016/j.ijcip.2016.04.001

第四部分

資訊安全與數位安全的差異

4

資訊安全

資訊安全專注於保護資訊免受未經授權的訪問、使用、披露、破壞、修改、檢視或擾亂。這包括物理和電子資訊的所有形式。資訊安全的主要目標是**維護資訊的機密性、完整性和可用性，這三個原則也稱為CIA三原則：**

01

機密性：保證資訊只能被授權的人員訪問。

02

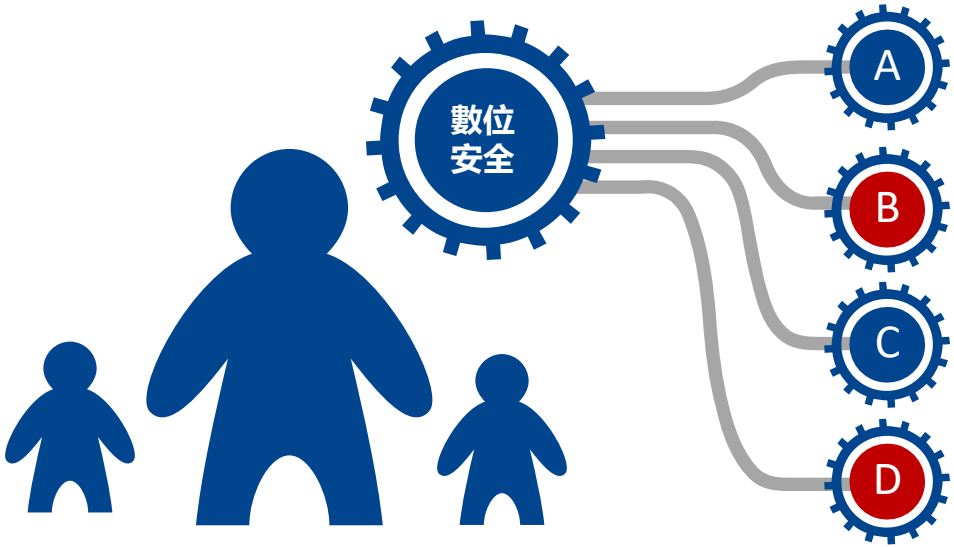
完整性：保證資訊的準確性和完整性，未經授權的人員不能修改。

03

可用性：保證授權使用者能夠在需要時訪問資訊和相關資源。

數位安全

數位安全是一個更廣泛的概念，涵蓋了包括資訊安全在內的所有數字資料和服務的安全。除了傳統的資訊安全措施外，**數位安全還包括保護對網絡基礎設施、數位個人身份資訊和在線隱私的保護**。數位安全的關注點包括：



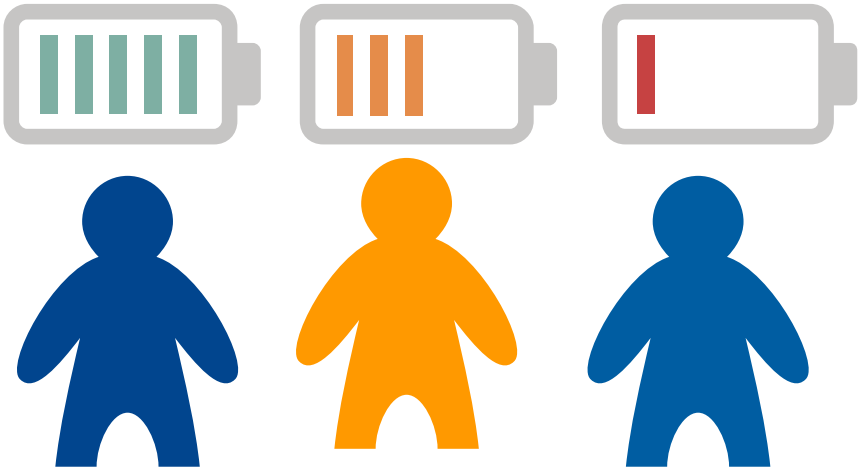
網路安全：保護網絡和數據免受未經授權的訪問和攻擊。

硬體安全：保護電腦和其他數位設備免受實體和邏輯攻擊。

軟體安全：確保軟體應用不含安全性漏洞且能防範惡意軟件和病毒。

操作安全：涉及數據和操作過程中的安全管理，如數據處理和存儲安全。

資訊安全與數位安全的差異



01.**範圍**：資訊安全專注於保護資訊的完整性、機密性和可用性，而**數位安全更廣泛**，包括網絡、設備、軟件和操作的安全。

02 **關注點**：資訊安全主要關注資訊的安全，而數位安全涉及的是**更廣泛的數位場域和互聯網的安全。**

03 **技術和方法**：數位安全包括但不限於資訊安全，使用**更多技術和方法來保護用戶的數位場域。**

價值、差異: 來自認知與決定，是科學或哲學?

THANKS

谢　谢　聆　听

COMPANY：中国某某科技有限公司　　DESIGNER：李小胖　　DATE：2016-3-31