CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

CISO FORUM

CISO FORUM

# 用數據直視風險：資安衡量的第一原理與實戰轉化

## Metrics: Confronting Cybersecurity with data

TEAM CYBERSECURITY

**李彥民 ANTHONY**

資安長 CISO

# “CYBERSECURITY IS A PEOPLE RISK”

## 要解決資安問題，要先懂人

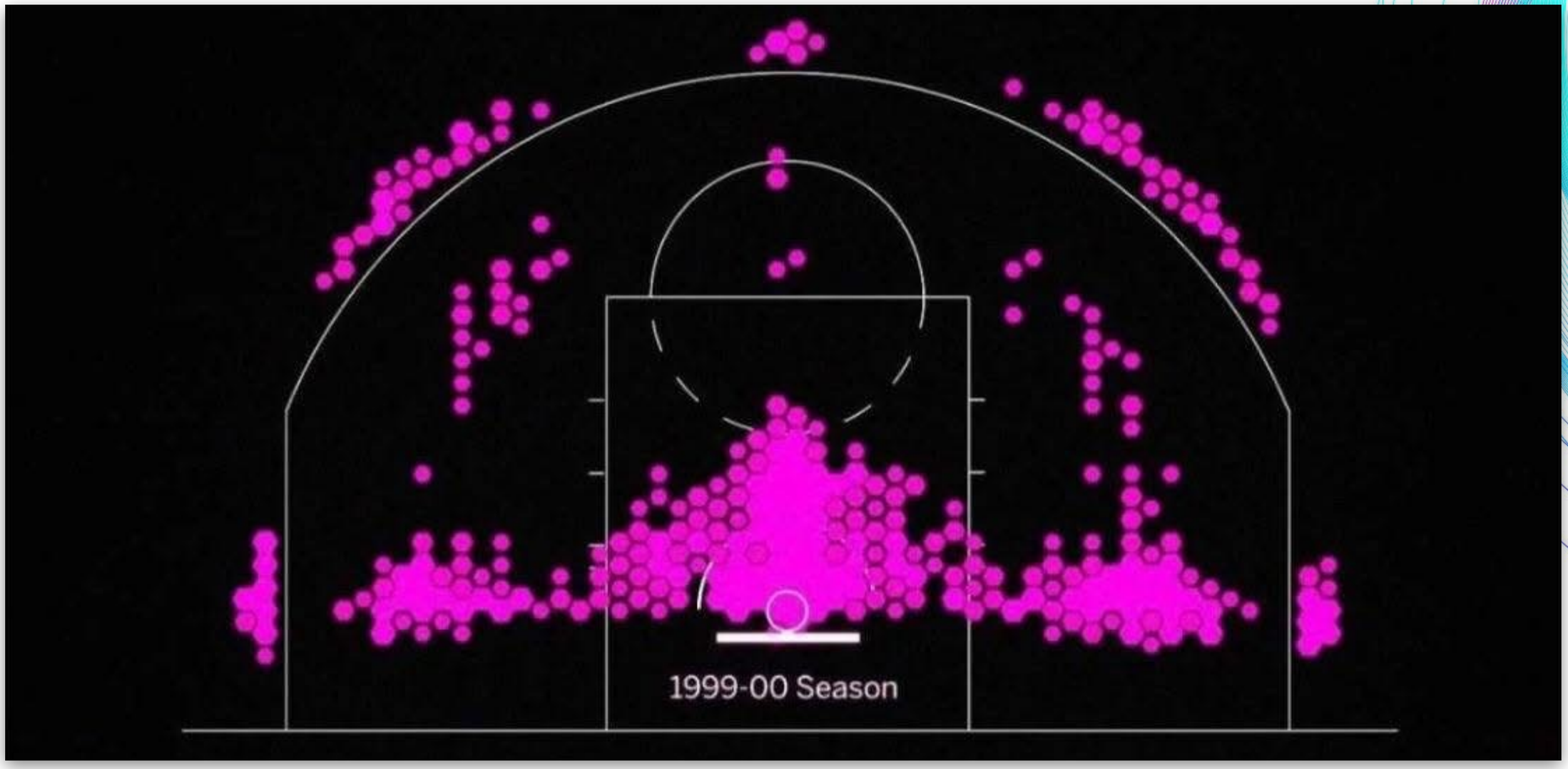
By Anthony Lee

# 目錄 Index

# 1

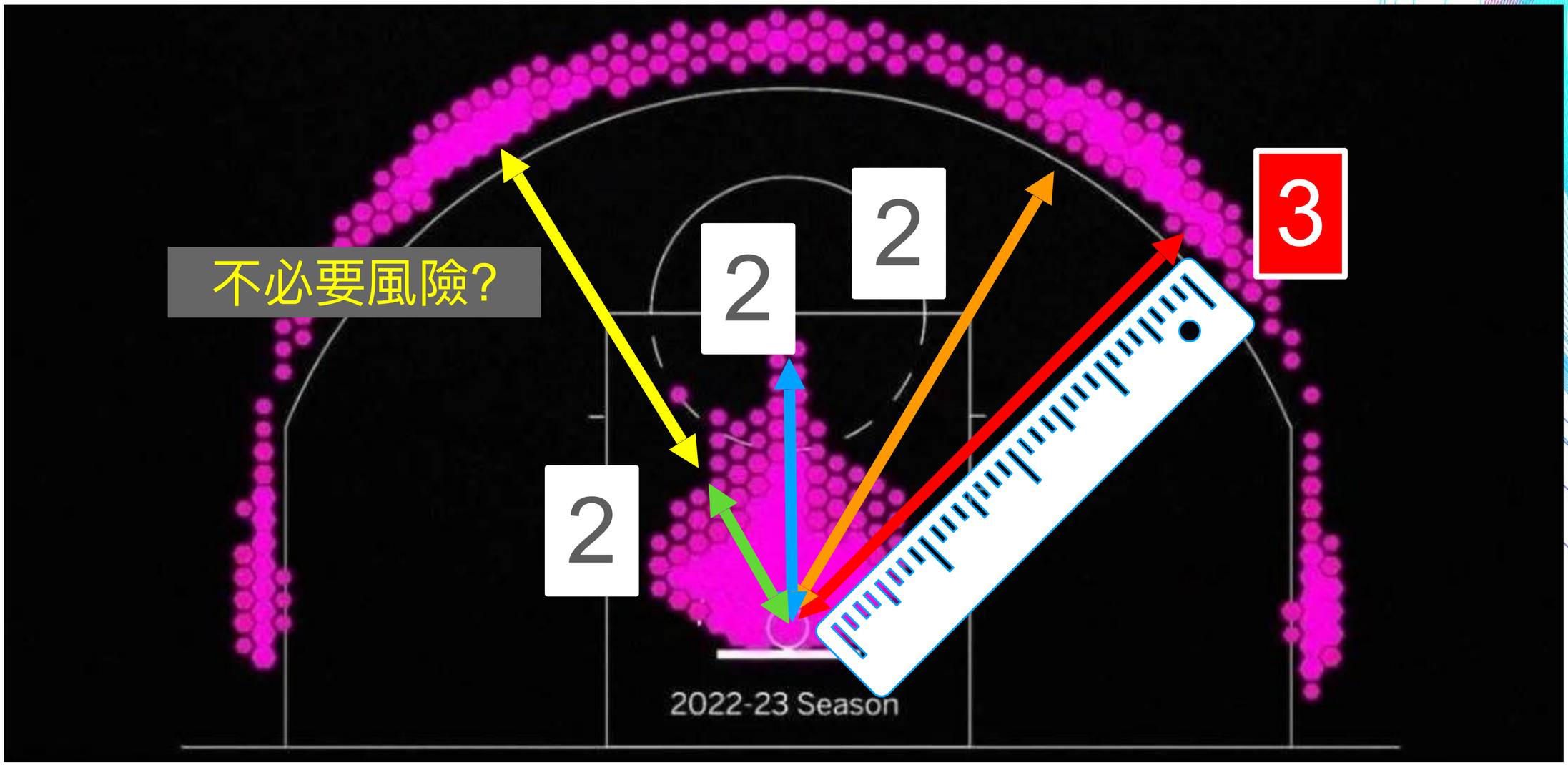
什麼是「Metrics」？(不是 Matrix)
是「衡量」，「量測」，「指標」

# NBA 最常見的投籃位置: 1999-2000年




By @KirkGoldsberry

# NBA 最常見的投籃位置: 2022～2023年



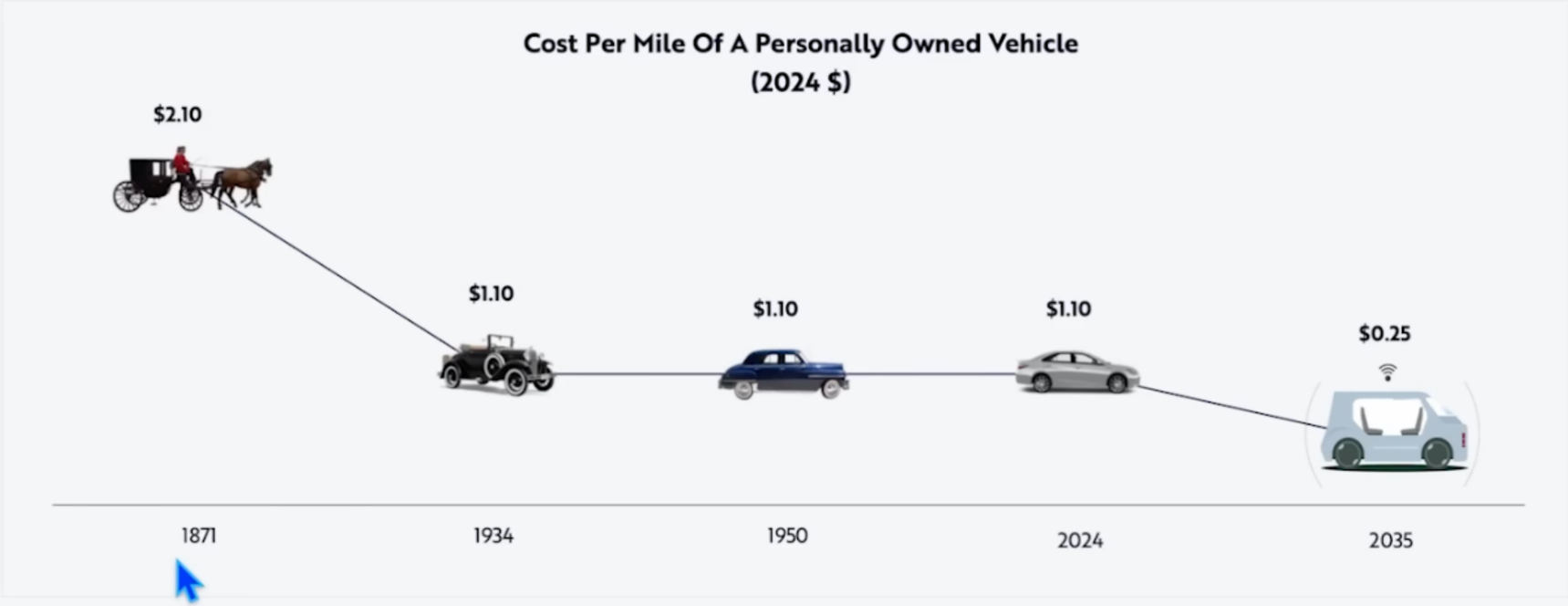

By @KirkGoldsberry

# 自用車每英里行駛成本 1871 ~ 2035年

ARK's Big Ideas 2025: Robotaxis

## Autonomous Ride-Hail Should Increase Access To Convenient Point-To-Point Transportation

Adjusted for inflation, the cost of owning and operating a personal car has not changed since the Model T rolled off the first assembly line more than 100 years ago. ARK estimates that autonomous taxis at scale could cost consumers as little as $0.25 per mile, spurring widespread adoption.




Note: Figures are rounded. Source: ARK Investment Management LLC, 2025. This ARK analysis draws on a range of external data sources, including Ulvog 2012, Model T Ford Forum 2010, American Automobile Association 1950, and American Automobile Association 2024, as of December 31, 2024, which may be provided upon request. For informational purposes only and should not be considered investment advice or a recommendation to buy, sell, or hold any particular security. Past performance is not indicative of future results. Forecasts are inherently limited and cannot be relied upon.

72

By @ARK Investment

# 衡量的第一原理

衡量(Metrics): 將概念轉化為數字，

讓我們能夠隨時間、觀察、推論、比較、改進。

"If you can't measure it, you can't improve it.
如果你無法衡量它，就無法改善它。"

or

“What gets measured, gets done.
有被衡量的事情，才會被完成。”

– (Often attributed to Peter Drucker or Lord Kelvin)

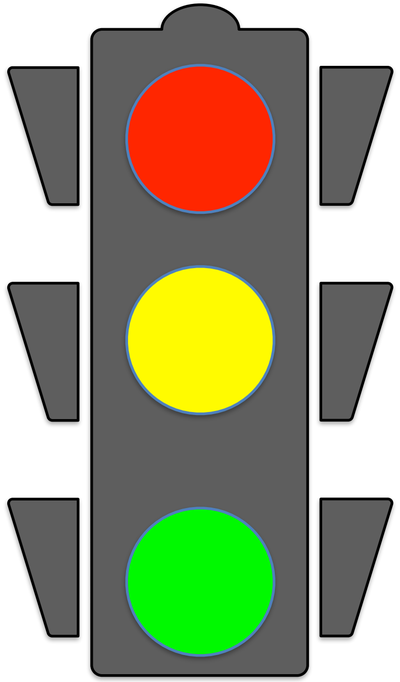
Lord Kelvin

# 為什麼要談「Security Metrics 資安衡量」？
# 不確定性高 Uncertainty

2

# 風險決策中的不確定性邏輯 The Logic of Uncertainty

在資訊不完整、模糊或具機率性的情況下進行推理與決策的方式。



高，1，紅

中，2，黃

低，3，綠

風險矩陣（Risk **Matrix** or Heatmap）

| Likelihood \ Impact | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 4 | 6 | 8 | 10 |
| 3 | 3 | 6 | 9 | 12 | 15 |
| 4 | 4 | 8 | 12 | 16 | 20 |
| 5 | 5 | 10 | 15 | 20 | 25 |

安慰劑效應？

# 衡量的目的(第一原理思維)

1.衡量不是為了得到完美答案，而是為了改善決策。

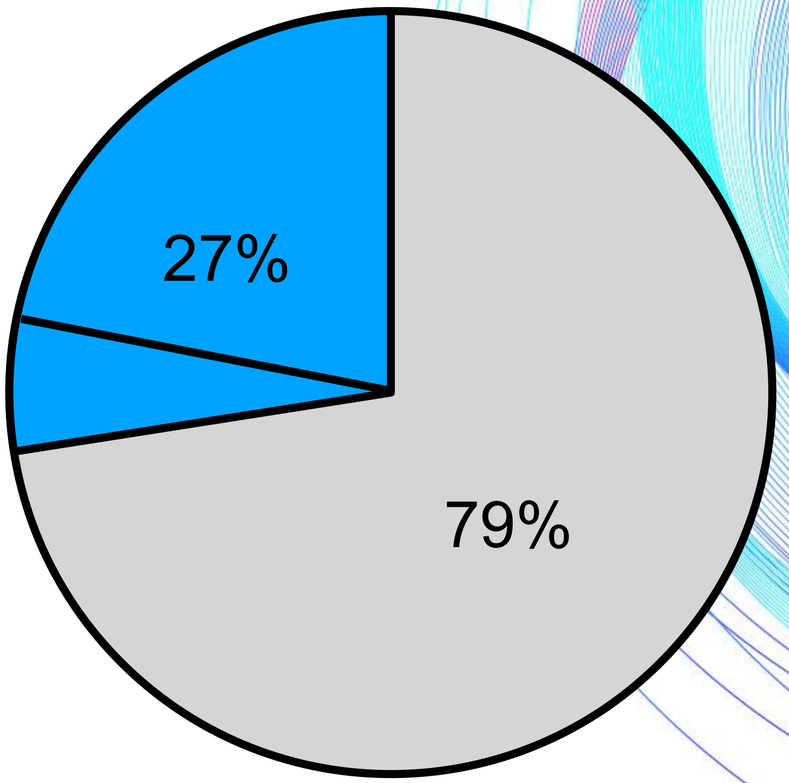
2. 怎麼知道我們變得更好了？

3. 我們應該觀察什麼「現象」來驗證改善？

# 對量化方法的偏見來自哪裡？

研究顯示：

- 約 79% 的資安從業者使用序列尺度；
- 但僅 14% 使用貝氏方法、13% 使用蒙地卡羅模擬；
- 科學證據支持方法仍被大量忽視

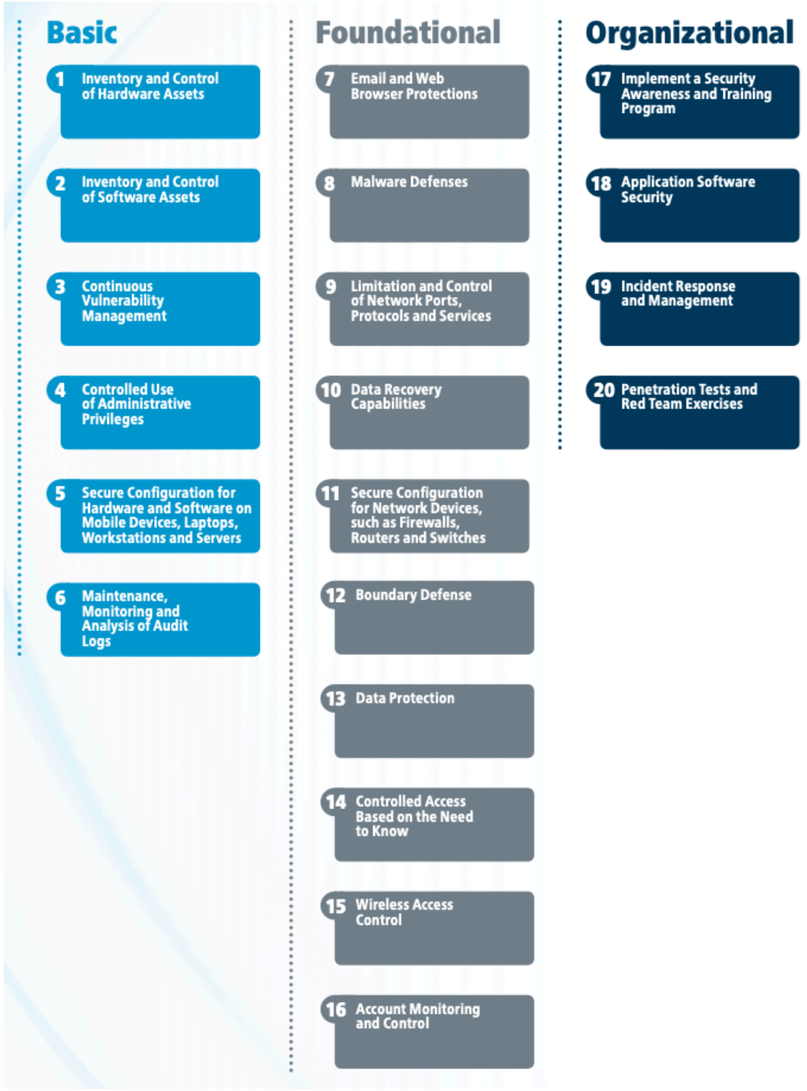


# Security Metrics Framework: Center for Internet Security Controls v.7.1

3

# Center for Internet Security CIS 7.1

**Control Groups**




**Implementation Group**

IG1 – Cyber Hygiene

- Target: **Small to medium-sized** organizations
- Resources: Limited IT and cybersecurity staff and budget
- Primary Goal: Ensure business continuity and basic security (e.g., employee and financial data)
- Sub-controls: Designed to thwart general, non-targeted attacks
- Tech: Often supported by consumer-grade or home-office software/hardware

IG2 – Operational Security

- Target: **Mid-sized organizations** or those with multiple departments
- Resources: Dedicated IT/security staff
- Primary Goal: Manage sensitive customer/company data, maintain public confidence
- Sub-controls: Help manage more complex operations and regulatory requirements
- Tech: Requires enterprise-grade tools and moderate cybersecurity expertise

IG3 – Advanced/Mature Security

- Target: **Large, regulated, or high-risk organizations**
- Resources: Advanced cybersecurity teams and tools
- Primary Goal: Protect critical infrastructure, maintain availability/confidentiality/integrity
- Sub-controls: Defend against sophisticated, targeted threats including zero-day exploits
- Tech: Requires advanced security knowledge and custom implementations

# Center for Internet Security CIS Control 7.1

CIS Controls™

**CIS Critical Security Controls® (CIS Controls®) Measures and Metrics for Version 7**

| Sub-Control | Title | Description | Sensor | Measure | Sigma Level One | Sigma Level Two | Sigma Level Three | Sigma Level Four | Sigma Level Five | Sigma Level Six |
|---|---|---|---|---|---|---|---|---|---|---|
| 1.1 | Utilize an Active Discovery Tool | Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory. | Active Device Discovery System | What percentage of the organization's networks have not recently been scanned by an active asset discovery tool? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |
| 1.2 | Use a Passive Asset Discovery Tool | Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory. | Passive Device Discovery System | What percentage of the organization's networks are not being monitored by a passive asset discovery tool? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |
| 1.3 | Use DHCP Logging to Update Asset Inventory | Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory. | Log Management System / SIEM | What percentage of the organization's DHCP servers do not have logging enabled? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |
| 1.4 | Maintain Detailed Asset Inventory | Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not. | Asset Inventory System | What percentage of the organization's hardware assets are not presently included in the organization's asset inventory? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |

What percentage of the organization's identified vulnerabilities have not been remediated in a timely manner?

**部署型指標 Deployment Based:**

組織中已識別的漏洞中，有多少百分比未能及時修復？

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 2.6 | Address unapproved software | Ensure that unauthorized software is either removed or the inventory is updated in a timely manner. | Software Application Inventory | What percentage of the organization unauthorized software are either removed or the inventory is updated in a timely manner? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |
| 2.7 | Utilize Application Whitelisting | Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets. | Software Whitelisting System | What percentage of the organization's hardware assets are not utilizing application whitelisting technology to block unauthorized applications from executing on the system? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |
| 2.8 | Implement Application Whitelisting of Libraries | The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process. | Software Whitelisting System | What percentage of the organization's hardware assets are not utilizing application whitelisting technology to block unauthorized applications at the library level from executing on the system? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |
| 2.9 | Implement Application Whitelisting of Scripts | The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system. | Software Whitelisting System | What percentage of the organization's hardware assets are not utilizing application whitelisting technology to block unauthorized scripts from executing on the system? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |
| 2.10 | | | | | | | | | | |
| 3.1 | | | | | | | | | | |
| 3.2 | | | | | | | | | | |
| 3.3 | | | | | | | | | | |
| 3.4 | | | | | | | | | | |
| 3.5 | | | | the software vendor? | | | | | | |
| 3.6 | Compare Back-to-back Vulnerability Scans | Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner. | SCAP Based Vulnerability Management System | What percentage of the organization's identified vulnerabilities have not been remediated in a timely manner? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |
| 3.7 | Utilize a Risk-rating Process | Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities. | SCAP Based Vulnerability Management System | Has the organization utilized a risk-rating process to prioritize the remediation of discovered vulnerabilities? | No | | | Yes | | |
| 4.1 | Maintain Inventory of Administrative Accounts | Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. | Privileged Account Management System | What percentage of the organization's hardware assets have not recently utilized automated tools to inventory all administrative accounts to ensure that only authorized individuals have elevated privileges? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |
| 4.2 | Change Default Passwords | Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts. | Privileged Account Management System | What percentage of the organization's systems utilize default passwords for accounts with elevated capabilities? | 69% or Less | 31% or Less | 6.7% or Less | 0.62% or Less | 0.023% or Less | 0.00034% or Less |

**結果型指標 Outcome Based:**

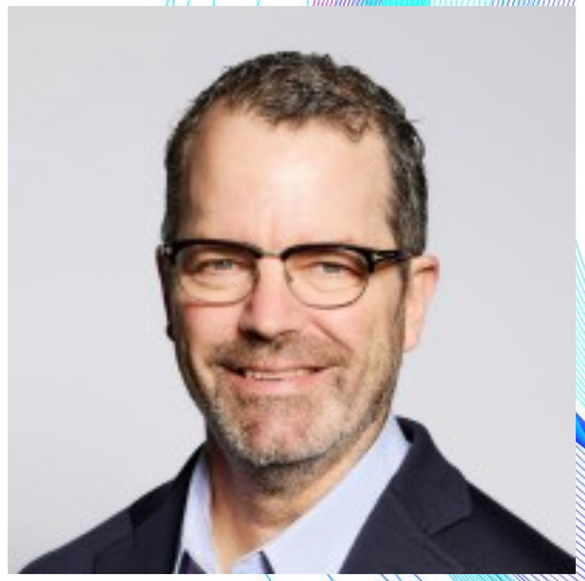
在過去 12 個月內，因未修補漏洞而導致的實際安全事件數量及損失金額?

# Security Metrics Framework:
# BOOM 框架介紹 (Baseline Objectives and Optimization Measurements)

4

# BOOM by Richard Seiersen (Qualys CISO)

## Baseline Objectives and Optimization Measurements

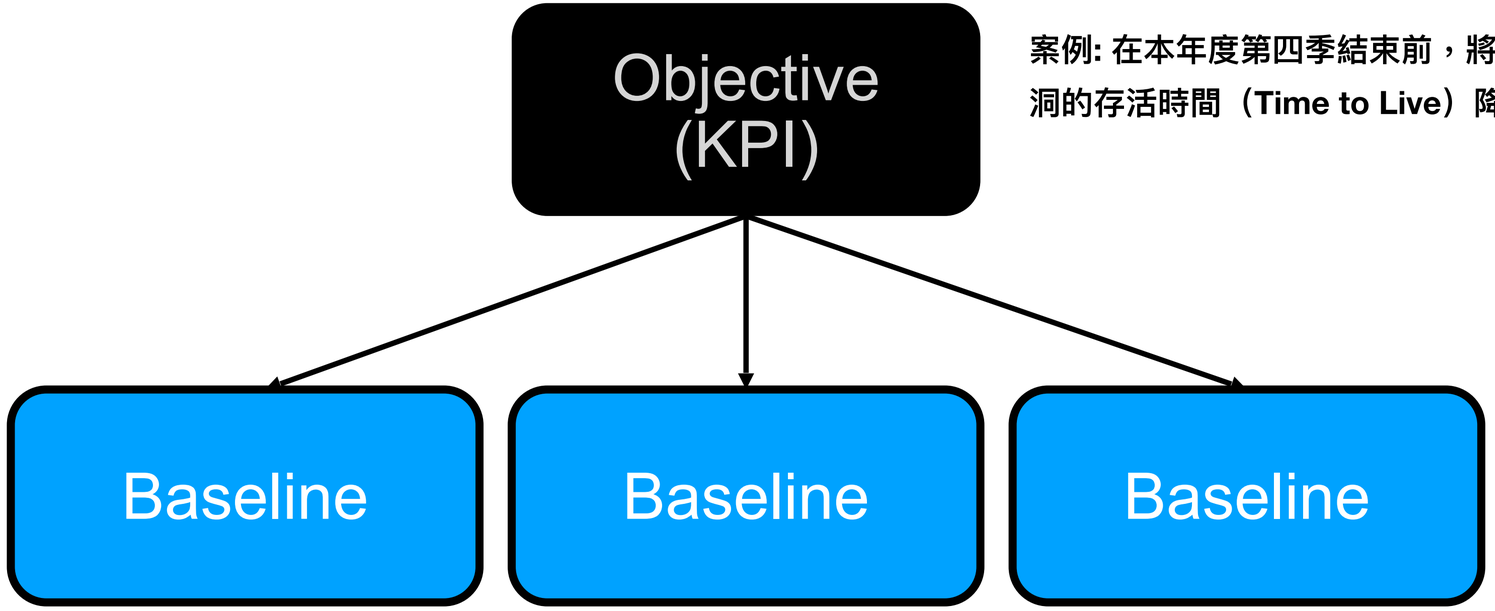


貝式推論（Bayesian reasoning）：處理不確定性

生存分析（Survival analysis）：衡量風險的存續時間

工程指標（如 burndown、wait-time）

資安營運實務（SOC、漏洞處理、威脅回應）

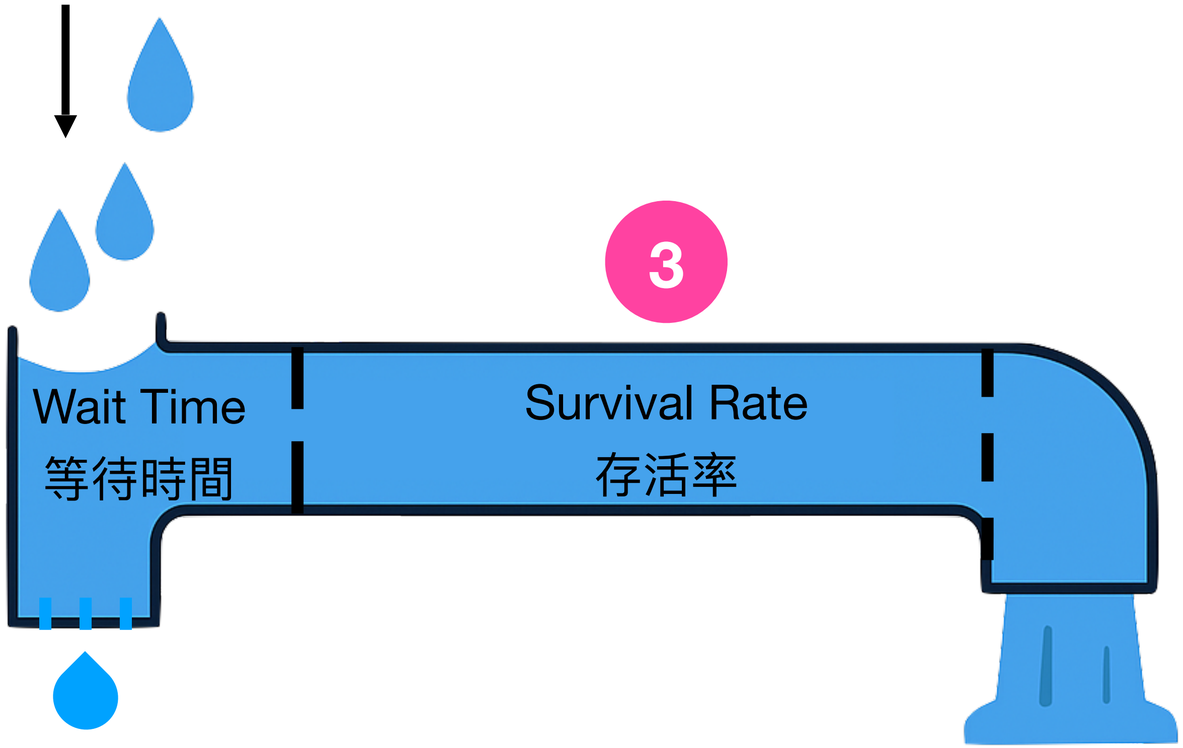



**案例: 在本年度第四季結束前，將可被利用漏洞的存活時間（Time to Live）降低 80%。**

Ref: The Metrics Manifesto

# Five Baseline Measurements: Risk Lifecycle

1 Arrival Rate
產生的速度




Burndown Rate
消減率

5 Escape Rate
破口產生的速度
Risk

Ref: The Metrics Manifesto

# Risk Lifecycle 漏洞管理案例

| BOOM 指標 | 漏洞管理案例 | 數據指標 | 資料性質 | 指標的意義 | 可能的問題 | 應對措施 |
|---|---|---|---|---|---|---|
| Arrival Rate<br>漏洞到達率 | 每週 +50 個新漏洞 | 50 個 / 週 | 頻率型（件數/時間） | 風險進入的速度 | 攻擊面過大<br>工具持續發現新弱點 | ✅ 加強開發安全<br>✅ 降低攻擊面（如關閉不用的端口）<br>✅ 進行威脅建模 |
| Wait-Time<br>等待時間 | 高風險漏洞平均等 12 天才開始修補 | 12 天（平均） | 時間型（天數） | 開始處理前的延遲 | 缺乏自動分派<br>優先順序混亂 | ✅ 自動化漏洞分類與分派<br>✅ 引入漏洞風險排序工具（如 CVSS + 業務重要性）<br>✅ 建立 SLA |
| Survival Rate<br>存活率 | 漏洞平均存在 30 天以上 | 30 天（平均） | 累積時間、比例、壓力 | 風險在系統中「活著」多久或是 有多少機率會存活？ | 修補能量不足<br>流程拖延 | ✅ 提高修補頻率<br>✅ 設定風險存活門檻（如：P1漏洞存活不得超過7天）<br>✅ 定期追蹤未修補列表 |
| Burndown Rate<br>銷減率 | 每週僅修 5~10 個漏洞 | 6 個 / 週 | 頻率型（件數/時間） | 被解決的風險數量 | 人手不足<br>優先順序誤用在低風險漏洞 | ✅ 專注處理高風險漏洞<br>✅ 補丁整合測試與部署流程優化<br>✅ DevSecOps 自動化修補流程 |
| Escape Rate<br>逃逸率 | 有 5 個漏洞被利用造成事件 | 5 / (50–20) = 約 16.7% | 機率型 | 未處理前就造成事件的風險 | 存活太久 +<br>偵測盲區 | ✅ 針對外部可利用漏洞優先處理<br>✅ 偵測與威脅情報整合<br>✅ 實施漏洞利用風險評估（Exploitability） |

# 計算「不確定性」- 漏洞修補案例
# Counting on Uncertainty

5

# Counting on Uncertainty - 貝氏方法

賭徒、科學家和神學家—以及它們如何處理不確定性

賭徒 Antoine Gombaud（又名 Chevalier de Méré）發現自己下注失利，覺得原本的勝率計算有問題。他求助於數學家 Blaise Pascal，Pascal 又拉來了數學家 Pierre de Fermat。他們的通信交流催生了現代機率論的奠基。

貝氏定理的誕生：Thomas Bayes 在晚年對機率產生濃厚興趣，撰寫了一篇關於機率推論的手稿。他於1761年逝世後，好友 Richard Price 將該手稿整理並於1763年以《An Essay towards solving a Problem in the Doctrine of Chances》為題，發表於《皇家學會哲學會刊》。該論文提出了一種從觀察結果推斷原因的機率方法，即後來的貝氏定理。

貝氏方法證明了，有時即使只有一筆觀察，也能逐步改變我們對不確定性的認知。

# Approximate Bayesian Computation Methodology (ABC)

ABC 是一種方法論，用來在難以直接使用貝式公式的情況下，仍然能夠進行合理的機率推論。

因為**資安風險的 Likelihood 似然性未知。**

**先前的知識**
**（Prior 先驗分佈）**

→

**新數據**
**（Likelihood 似然性）**

→

**新的結果**
**（Posterior 後驗分佈）**

$$P(\theta \mid D) = \frac{P(D \mid \theta) \cdot P(\theta)}{P(D)}$$

在觀察到資料 D 之後，參數 θ 為真的機率 等於
在 θ 為真的前提下，觀察到資料 D 的機率（機率模型）
乘以
θ 原本發生的機率（先驗機率）
除以
觀察到資料 D 的總體機率（邊際機率）

| 參數 | 定義說明 | 漏洞修補案例中的具體對應 |
|---|---|---|
| θ | 想要推論的未知參數 | 平均漏洞修補時間（未知） |
| D | 觀察到的資料（evidence） | 你觀察到的 10 筆修補資料：[12,15,30,18,...] |
| P(θ) | 先驗機率（prior） | 你認為修補時間落在 10–60 天之間，mode = 30（PERT 分布） |
| **P(D\|θ)** | **似然性（likelihood）** | 如果平均修補時間是 25 天，那這些觀察數據的機率是多少？ |
| P(D) | 資料的總體機率（標準化常數） | 所有可能修補時間的總體加權機率（用於標準化） |
| P(θ\|D) | 後驗機率（posterior） | 根據觀察資料後你更新的「相信修補時間是多少」的機率分布 |

# Survival Rate - Vulnerability Management Example (1/2)

**Metrics: 高風險漏洞在識別後的 30 天內，有多少比例被成功修補？**

**假設狀況 1 (你有數據):** 你觀察了 20 個高風險漏洞，其修補時間如下（單位：天）：

[8, 12, 15, 20, 25, 28, 33, 35, 36, 40, 42, 43, 44, 47, 50, 55, 60, 70, 75, 80]

Step 1: 製作 Kaplan–Meier 存活曲線（Survival Curve）
每一筆資料代表一個事件（漏洞「死亡」＝被修補）

Y 軸為「尚未修補的比例」，X 軸為時間（天）

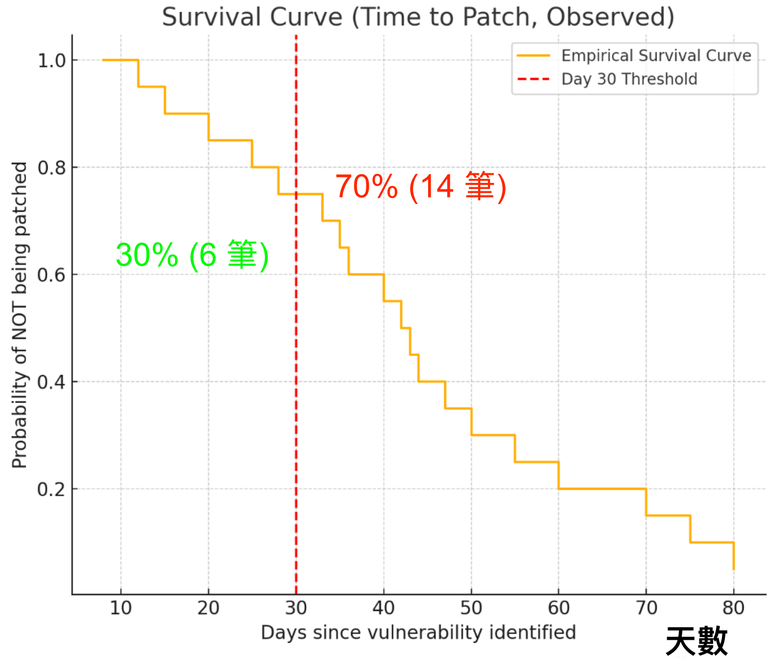
在第 30 天之前被修補的有： [8, 12, 15, 20, 25, 28] → 共 6 筆

所以 30 天內的生存率（未修補）＝14/20 = 70%

➡️ Survival Rate@30days = 70%

你也可以反推： ➡️ Burndown Rate@30days = 30%（已修補）

觀察資料的存活曲線



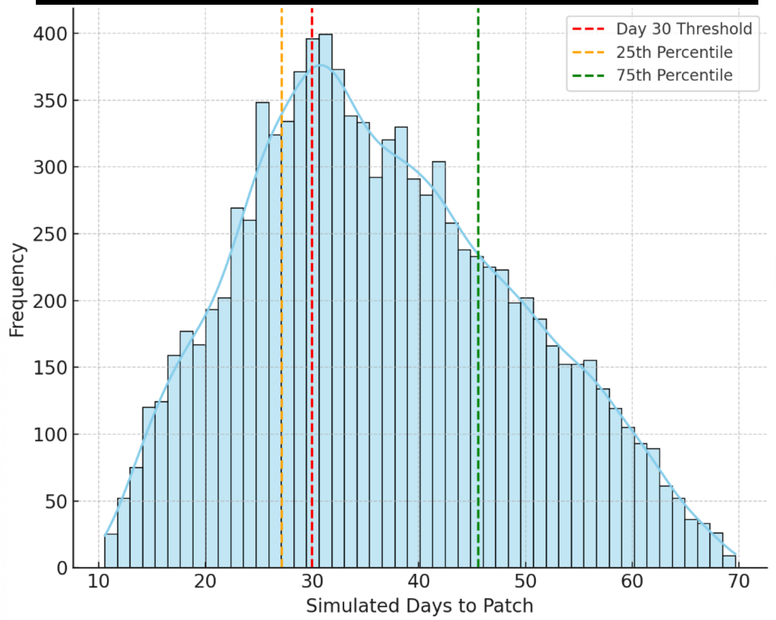
# Survival Rate - Vulnerability Management Example (2/2)

**Metrics: 高風險漏洞在識別後的 30 天內，有多少比例被成功修補？**

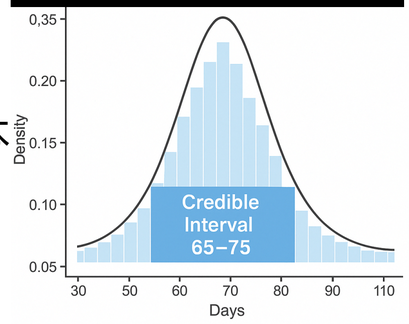
**<u>假設狀況 2 (你沒有數據)</u>**：你只知道最近平均修補時間約落在 20–50 天，但沒有全部修補時間資料。

1. 設定「先驗分布」（Prior）
   你估計漏洞修補時間可能符合一個 PERT 分布，如下：
   PERT(min=10, mode=30, max=70)
   (＊這反映你的專家直覺：(眾數) **大部分應該 30 天左右被修補。)**
2. 模擬 10,000 筆漏洞修補時間（用 Monte Carlo）
   從這個分布中隨機抽樣 10,000 筆資料，建立模擬群體。
3. 設定「接受條件」
   你篩選出模擬結果中 30 天內修補的比例落在 28–32%(±2%)的樣本
   形成 ABC 過濾後的 Posterior 分布。
   (＊你從真實事件知道，30 天內大約 6/20 被修補 ≈ 30%)
4. 從這個「後驗分布圖」中估算：
   可信區間：Survival Rate@30days 落在 65%–75%
   中位數預測值：70%（與實測吻合）

ABC 模擬的漏洞修補時間分布



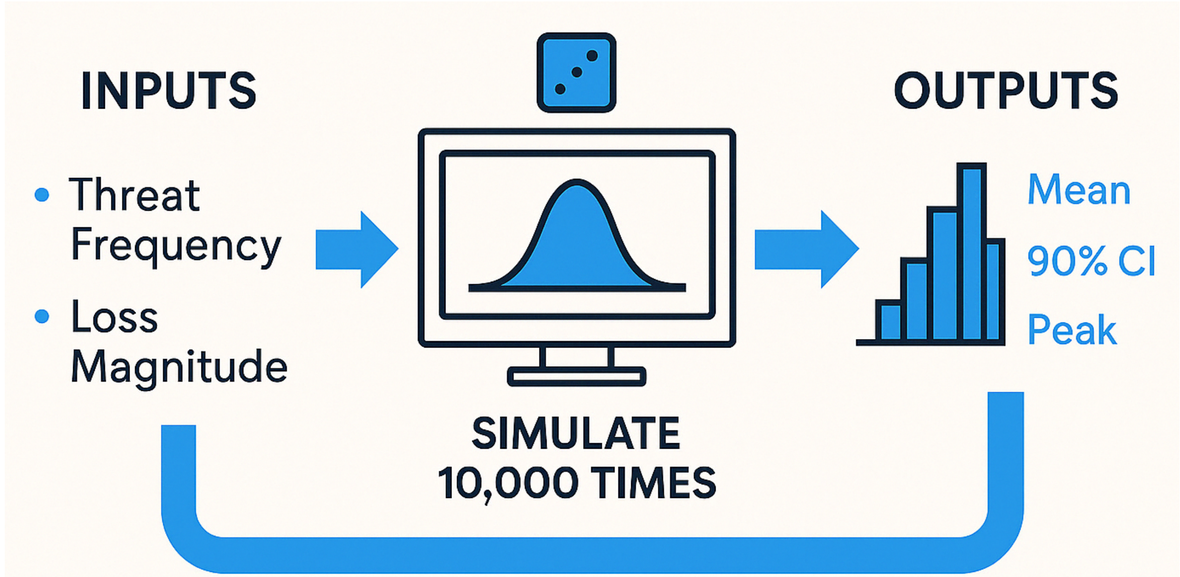

貝氏後驗分布
可信區間 65~75%




- 目前的修補效率偏慢（70% 高風險漏洞仍存活超過 30 天）
- 若你將「30 天內完成修補」作為 KPI，現況遠未達標
- 可結合 **<u>Wait-Time 分析</u>**，進一步找出哪些步驟造成延遲

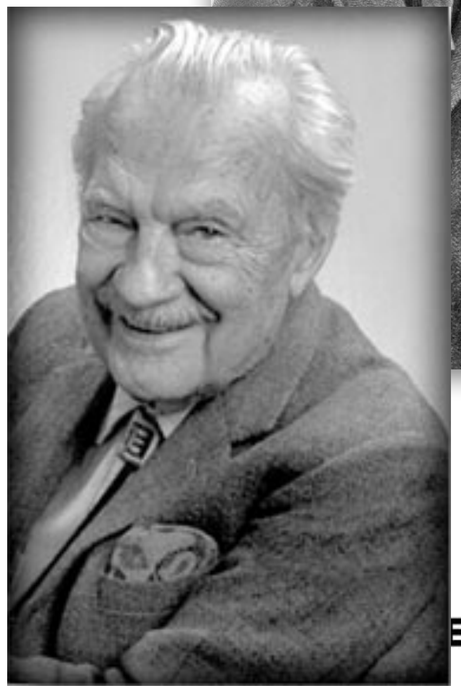
# Counting on Uncertainty - 蒙地卡羅模擬

1946 年，數學家史坦尼斯拉夫·烏拉姆 Stanislaw Ulam 在病後休養時，無聊地玩著接龍紙牌。他忽然想到：「成功完成遊戲的機率是多少？」他沒用公式解，而是親自跑幾百次實驗，記錄結果。這股隨機的魅力引發了他更深的思考。後來在參與核子物理研究時(「曼哈頓計劃」)，他與馮·諾伊曼 John von Neumann將這方法應用在粒子行為的模擬上，命名為「蒙地卡羅法」，取自他叔叔最愛的賭場。從一場紙牌遊戲出發，這套方法成了科學革命，幫助人類掌握不確定性，從核彈、金融到資安，影響深遠。起點，只是一場遊戲。





史坦尼斯拉夫·烏拉姆
Stanislaw Ulam



# 用數據直視風險
# Confront Cybersecurity (Uncertainty) with data

6

# 衡量三合一：BOOM, FAIR and CIS Controls v7.1

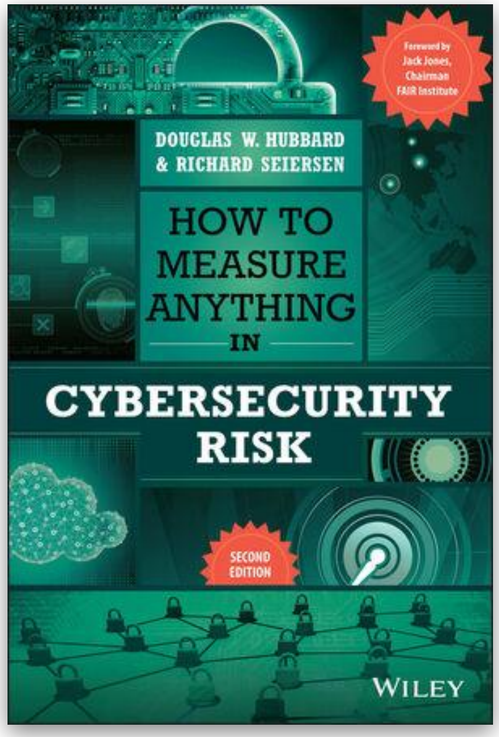
| 項目 | **BOOM (Baseline Objectives and Optimization Measurements)** | **FAIR (Factor Analysis of Information Risk)** | **CIS Controls v7.1** |
|---|---|---|---|
| 本質 | 一個能力衡量框架<br>(Capability Measurement Framework) | 一個風險量化模型<br>(Risk Quantification Model) | 一組實務控管指南<br>(Security Control Framework with KPIs) |
| 用途 | 衡量控制成效、行動效率、資源壓力 | 衡量風險值（如：年預期損失、風險分布） | 管理控管成效、政策合規、測量改善 |
| 焦點 | 過程導向：控管是否有效、行動是否改善 | 結果導向：風險大小與資損估計 | 控制導向：控制是否部署、生效、有紀錄 |
| 使用資料 | 模擬生存分析、流程效能指標 | 頻率、損失、漏洞機率等估算 | 控制活動記錄、執行情境、事件應對時效 |
| 科學方法 - 貝式風險模型 | 推估控制表現與指標分布（如 Burndown 成效、Escape 機率） | 計算風險（年預期損失、概率損失） | 無。強調控制達成率與時間指標（Time-to-Detect, Time-to-Patch） |
| 科學方法 - 蒙地卡羅模擬 | 模擬指標變化趨勢、建立可信區間（例如 Survival Rate 的分布） | 模擬損失範圍、決策 ROI | 無。固定 KPI + 效能衡量，可量化但不預測未來變化 |
| 典型問題 | 我們修補漏洞的速度夠快嗎？瓶頸在哪？哪些問題沒解決就已經爆炸？ | 如果不修補這個漏洞，我的年損失是多少？ | 某控制是否部署？是否符合SLA（如15天內修補）？偵測時間是否超過上限？ |
| BOOM指標定義 | **Baseline** | **Objective (KPI/KRI)** | **Objective (KPI/KRI)** |
| 互補 | • FAIR 可告訴你：「若將 Survival Rate 從 60% 降到 30%，年損失可減 100 萬」<br>• **BOOM 再追蹤**：你是否真的讓 Survival Rate 降下來？ | • TEF（Threat Event Frequency）可以由 Arrival Rate + Survival Rate 推估<br>• Vuln（Vulnerability）可從 Escape Rate 模擬失敗機率<br>• Resistance Stregnth 可從 Burndown, Wait-Time 衡量改善幅度 | CIS 為控制活動提供標準化度量，如：<br>‣ Time to Patch（3.4）<br>‣ Time to Remediate（3.6）<br>‣ Time to Contain/Recover（19.3 / 19.4）<br>→ **是 FAIR & BOOM 資料來源** |

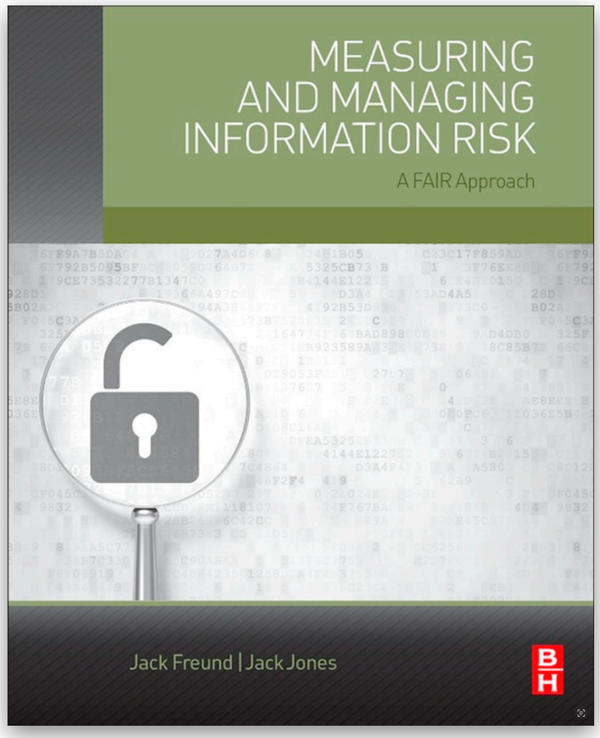
CYBERSEC 2025
臺灣資安大會

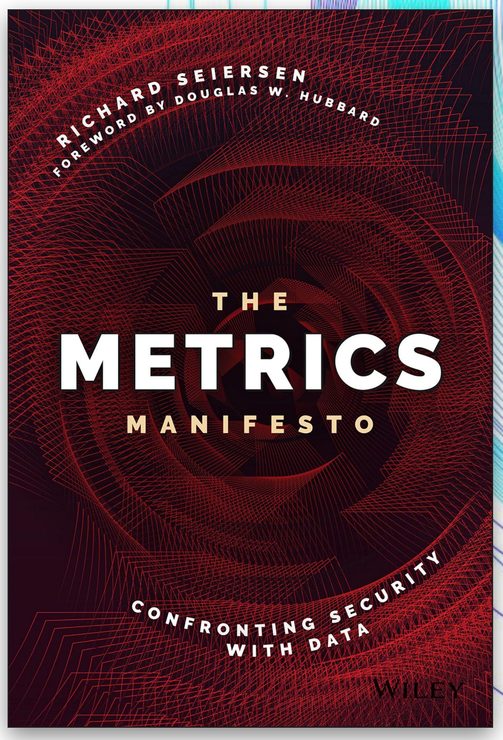
# THANK YOU

# References


Start Secure. Stay Secure.®
CIS Center for Internet Security®
CIS Controls™
V7.1


Foreword by Jack Jones, Chairman FAIR Institute
DOUGLAS W. HUBBARD & RICHARD SEIERSEN
HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK
SECOND EDITION
WILEY


MEASURING AND MANAGING INFORMATION RISK
A FAIR Approach
Jack Freund | Jack Jones
BH


RICHARD SEIERSEN
FOREWORD BY DOUGLAS W. HUBBARD
THE METRICS MANIFESTO
CONFRONTING SECURITY WITH DATA
WILEY