超越定性

FAIR 幫助企業定量化資訊風險

合勤投資控股 Unizyx

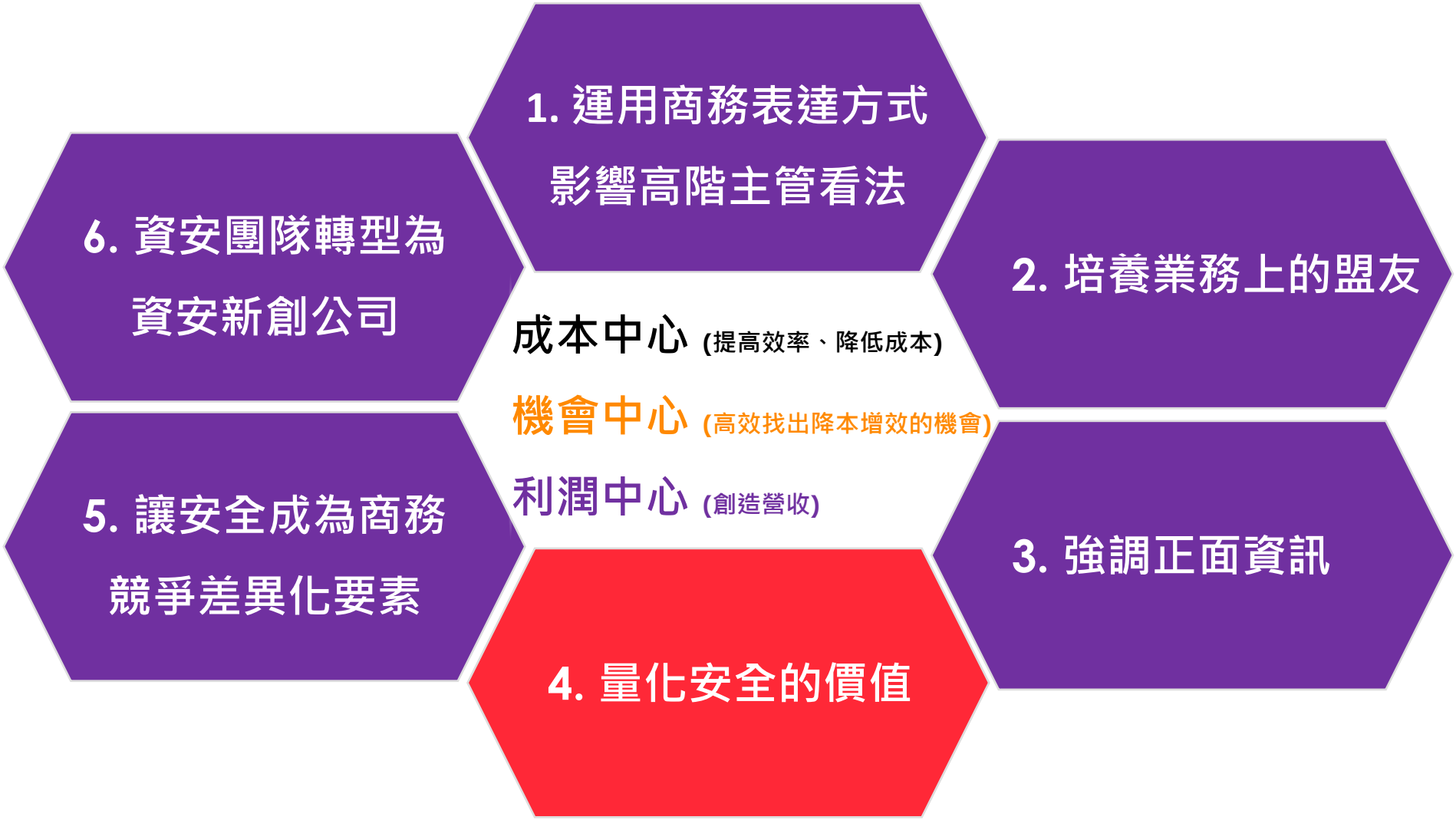
游政卿

資安長

董事長室

ZYXEL
Your Networking Ally

資訊安全投資轉化策略



ZYXEL
Your Networking Ally

資訊安全風險管理

- 定性評估的侷限性
- 量化風險評估的重要性
- FAIR 方法介紹

FAIR 方法應用

- 實際案例分析
- 與其他風險評估方法比較

FAIR 的挑戰與未來

- 定量評估的侷限性
- 資源與工具
- 未來展望

ZYXEL
Your Networking Ally

資訊安全風險的挑戰 (1/2)

- 定性風險評估的局限性
  - 主觀性高
    - 定性評估往往依賴於專家經驗[illegible]直覺，容易[illegible]主觀因素影響，[illegible]果不一致
  - [illegible]
    - 定性評[illegible]

- 量化風險評估的重要性
  - 客觀[illegible]強
    - [illegible]化風險評估通過數學模型和資料分析，[illegible]低評估過程中的主觀成分，提高評估[illegible]明確的數值，便[illegible]分析，有助於制定有效[illegible]和資源分配

決策者的思維

即使你不能告訴我資安事件究竟何時會發生

就告訴我事件發生的機率和估計損失的金額

損失的頻率(次數) * 損失的大小(金額)

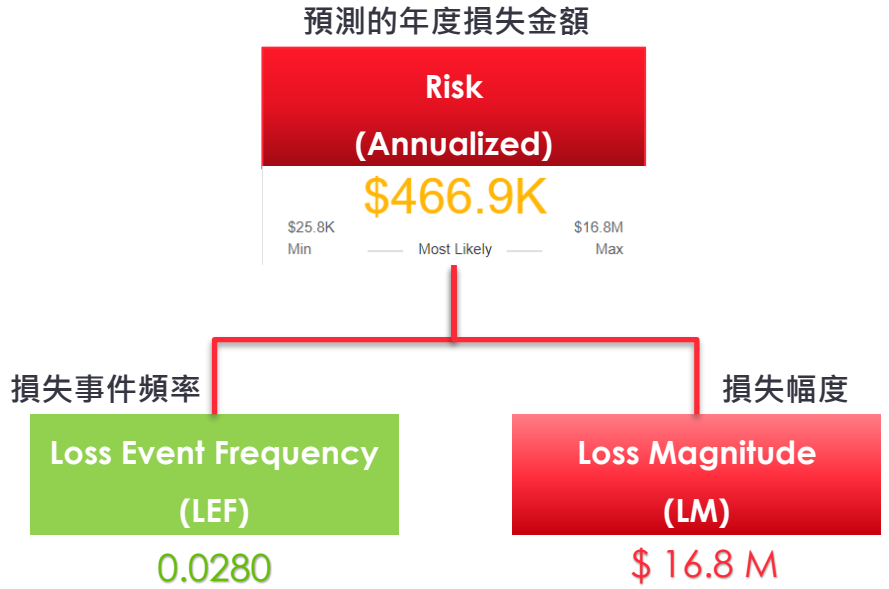
ZYXEL
Your Networking Ally

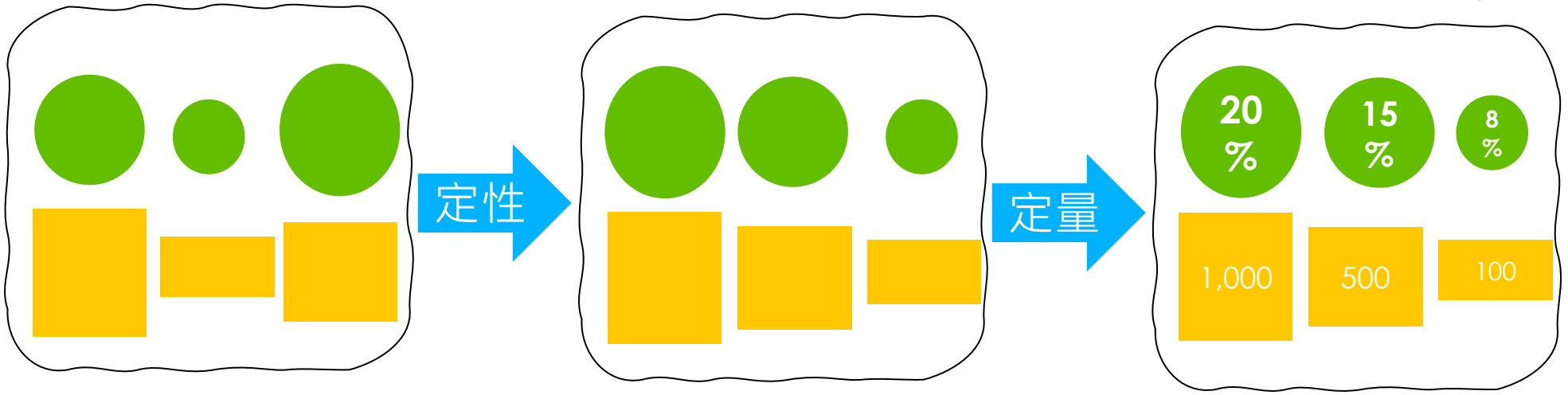
資訊安全風險的挑戰 (2/2)

定性風險評估

衝擊等級	風險等級		
3	3 (高風險)	6 (高風險)	9 (極高風險)
2	2 (中風險)	4 (高分險)	6 (高風險)
1	1 (低風險)	2 (中風險)	3 (高風險)
機率等級	1	2	3

定量風險評估





ZYXEL
Your Networking Ally

風險分析：定性 vs. 定量

特點	定性分析	定量分析
分析方法	通過**專家意見、經驗和判斷**進行風險評估，結果通常以描述性文字和等級表示	通過數學和統計方法對風險進行量化度量，結果通常以數值和機率表示
輸出結果	**風險等級（如高、中、低）和描述性文字**	**風險機率、風險值（如損失金額）**和其他數值度量
精確性	較低，可能受到**主觀判斷**的影響	較高，基於實際資料和模型，但仍可能受到資料品質的影響
資料需求	較低，通常基於專家意見和經驗	較高，需要大量歷史資料、模型和參數
適用場景	適用於**初步風險評估和快速識別優先順序**	適用於**具有充足資料，深入風險評估，以支持決策和資源分配**
複雜性	相對簡單，不需要專業的數學和統計知識	較為複雜，需要專業的數學和統計知識以及相應的工具
易用性	容易上手，適合各類組織和安全團隊	可能需要專業培訓和較高的技能水平
缺點	可能受到偏見和誤差的影響	資料收集和分析過程可能複雜且耗時 **部分風險因素難以量化**，可能需要專業知識和判斷

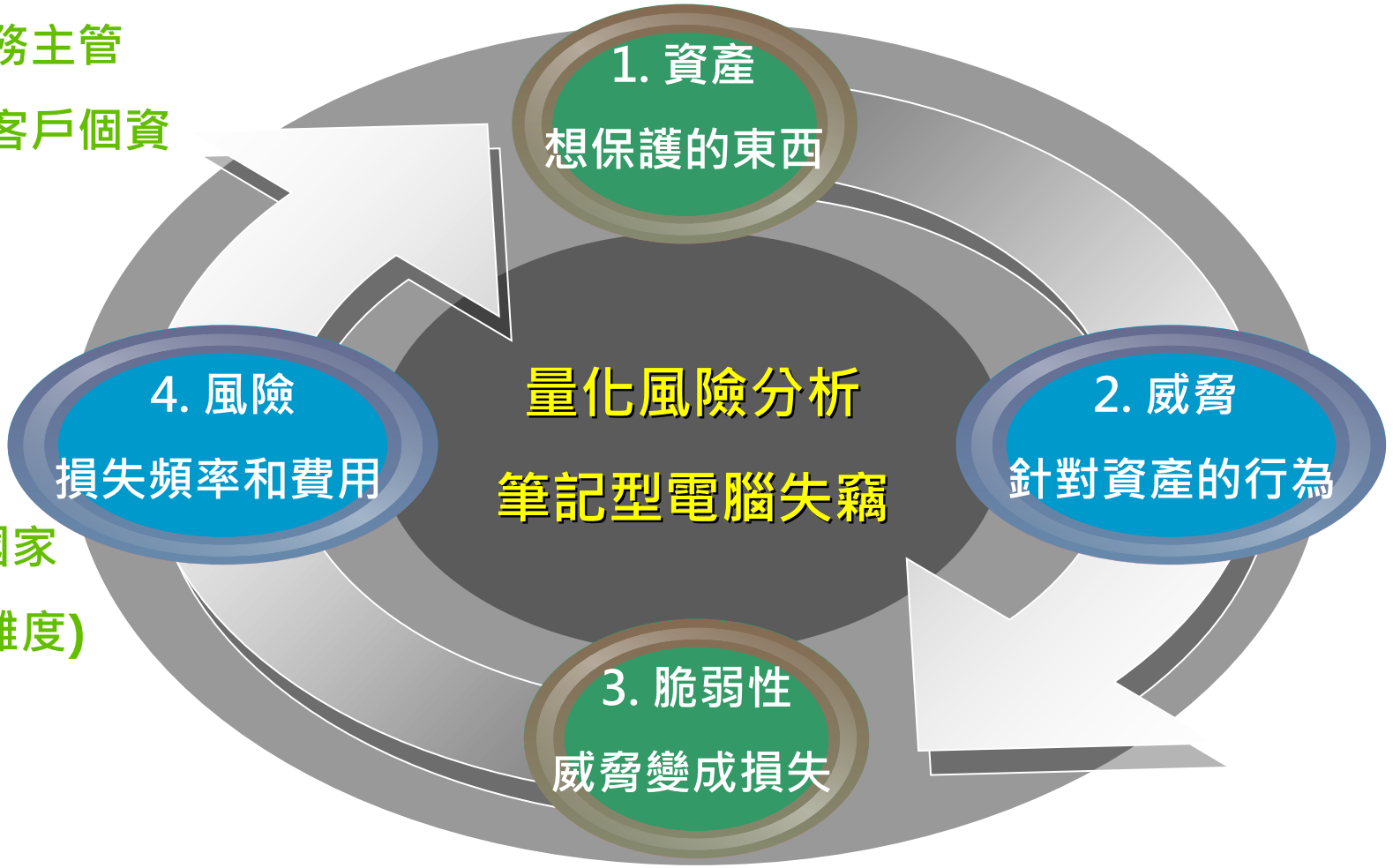
ZYXEL
Your Networking Ally

什麼是 FAIR？ (1/2)

- FAIR (Factor Analysis of Information Risk) – 資訊風險因素分析
  - 定義：FAIR 是一種資訊安全風險評估方法，通過因素分析來量化資訊安全風險
  - 發展：由 Jack Jones 於 2005 年提出，現已成為國際間廣泛使用的量化風險評估標準
- FAIR 的目的與特點
  - 目的：為企業提供一種客觀、可靠的風險評估方法，以支持風險管理決策
  - 特點
    - 定量分析：使用數學模型和資料來量化風險，降低主觀因素的影響，提高評估的客觀性和準確性
    - 易於理解：將風險分解為多個因素，有助於更深入地瞭解風險的成因和影響
    - 跨部門溝通：提供一種通用語言，有助於企業內部各部門之間的風險討論和共識達成

什麼是 FAIR？ (2/2)

- 資產
  - 設備：法務長、技術長、業務主管
  - 資料：攻防證據、智財權、客戶個資
- 威脅
  - 一般偷竊
  - 蓄意竊取
- 脆弱性
  - 駭客猖獗區域/積極執法的國家
  - 攻擊者付出的成本 (價值、難度)
  - 資料外洩防護 (資料加密)
- 風險
  - 筆電資產暨資訊價值



ZYXEL
Your Networking Ally

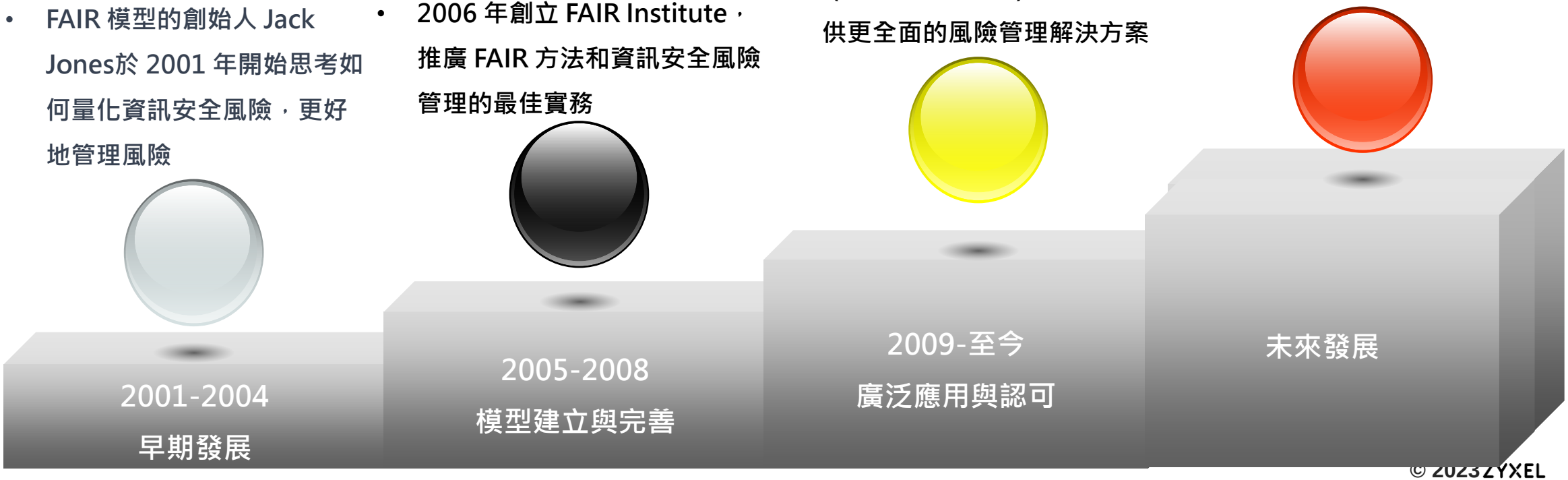
FAIR 發展歷程

- FAIR 模型的創始人 Jack Jones於 2001 年開始思考如何量化資訊安全風險，更好地管理風險

- 2005 年，Jack Jones 在一篇名為 “An Introduction to Factor Analysis of Information Risk (FAIR)” 的文章首次正式提出 FAIR 模型
- 2006 年創立 FAIR Institute，推廣 FAIR 方法和資訊安全風險管理的最佳實務

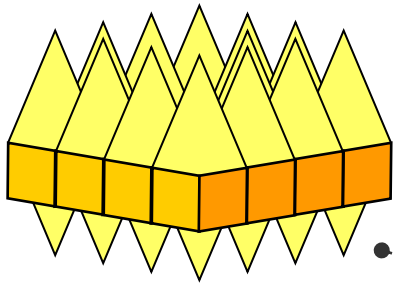
- 2015年， Jack Jones 和 Jack Freund發表 ” Measuring and Managing Information Risk, A FAIR Approach” 的文章
- FAIR 方法與其他風險管理框架（如 NIST 和 ISO）實現整合，提供更全面的風險管理解決方案

- 隨著資訊安全風險日益嚴重，FAIR 方法將繼續在風險管理領域發揮重要作用



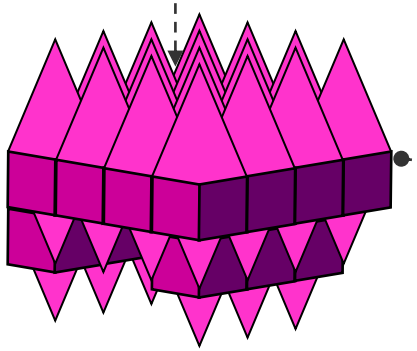
ZYXEL
Your Networking Ally

FAIR 方法



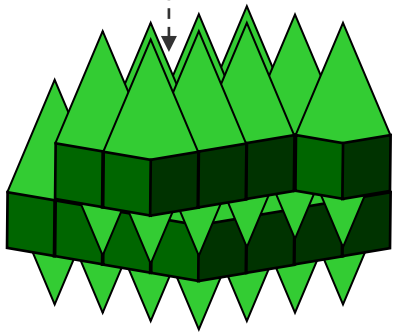
資訊風險因素分析 (Factor Analysis of Information Risk)

FAIR Institute 開發，網路安全和運營風險的價值風險（VaR）框架



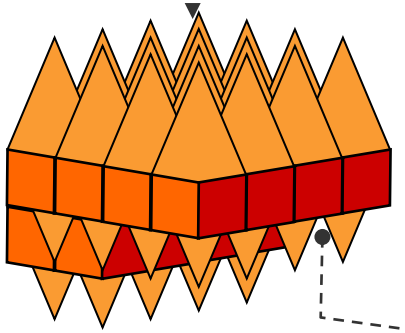
以金額 $ 量化

網路和運營風險



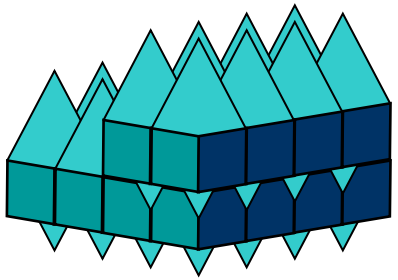
採用 損失事件頻率（LEF）

損失幅度（LM）來計算風險



標準模型，用於理解、

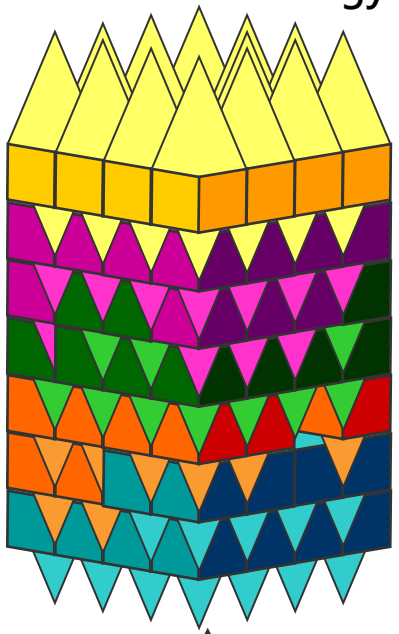
分析和量化資訊風險



根據風險，實現更佳

的決策制定和資源分配

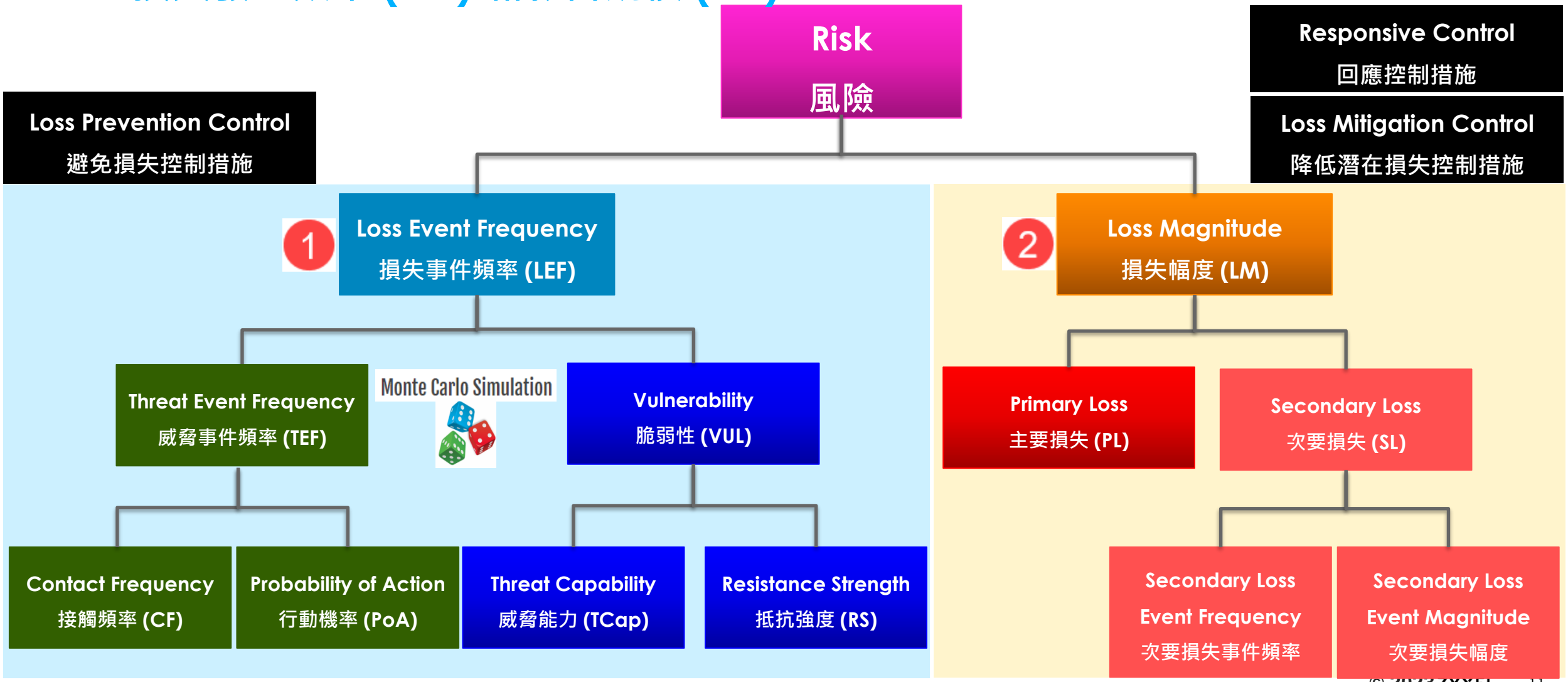
FAIR Methodology



ZYXEL
Your Networking Ally

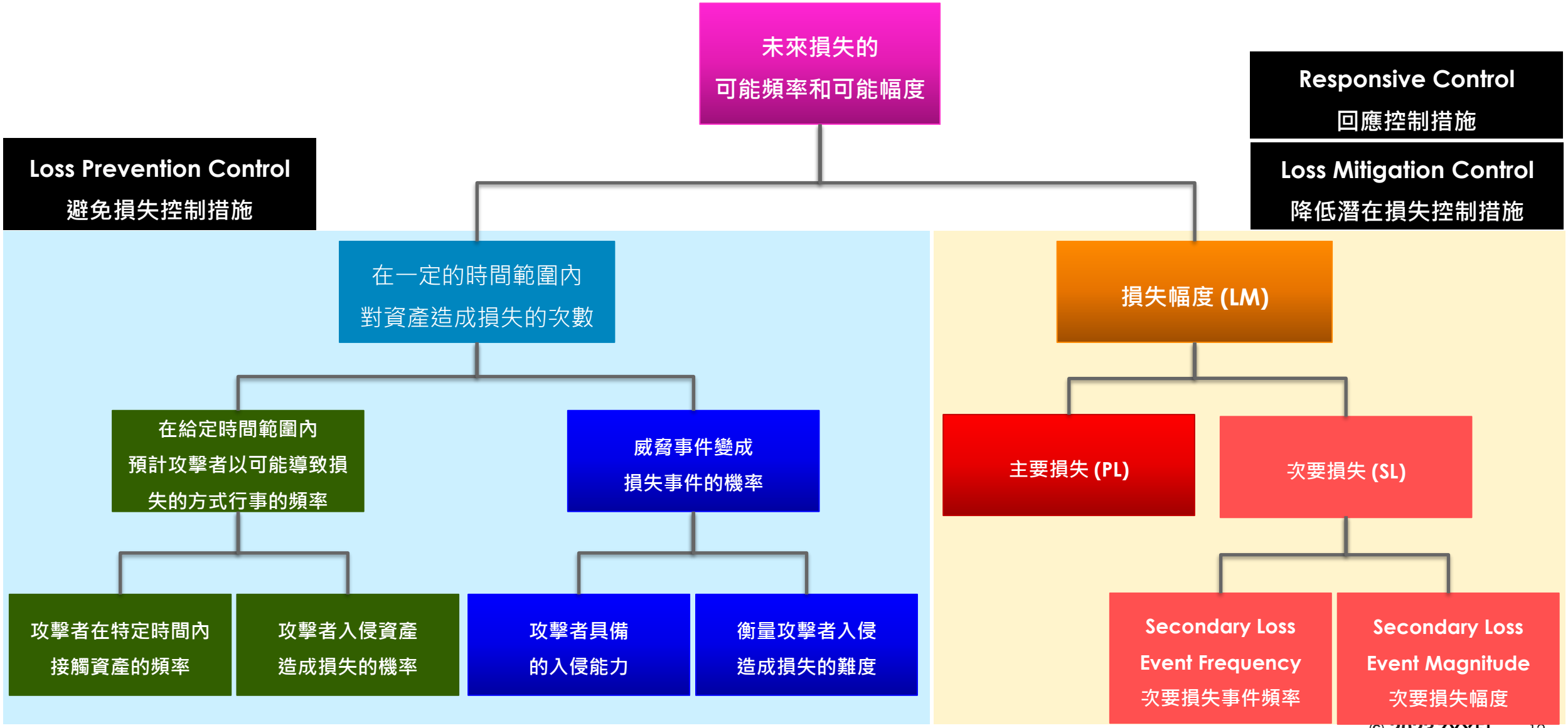
FAIR 模型 (1/4)

- 損失發生頻率 (LEF) 和影響規模 (LM)



ZYXEL
Your Networking Ally

FAIR 模型 (2/4)



ZYXEL
Your Networking Ally

FAIR 模型 (3/4)

5 **Loss Event Frequency**
損失事件頻率 (LEF)

3 **Threat Event Frequency**
威脅事件頻率 (TEF)

1 **Contact Frequency**
接觸頻率 (CF)

Avoidance Control
避險控制措施

Protect

4 **Vulnerability**
脆弱性 (VUL)
TCap > RS

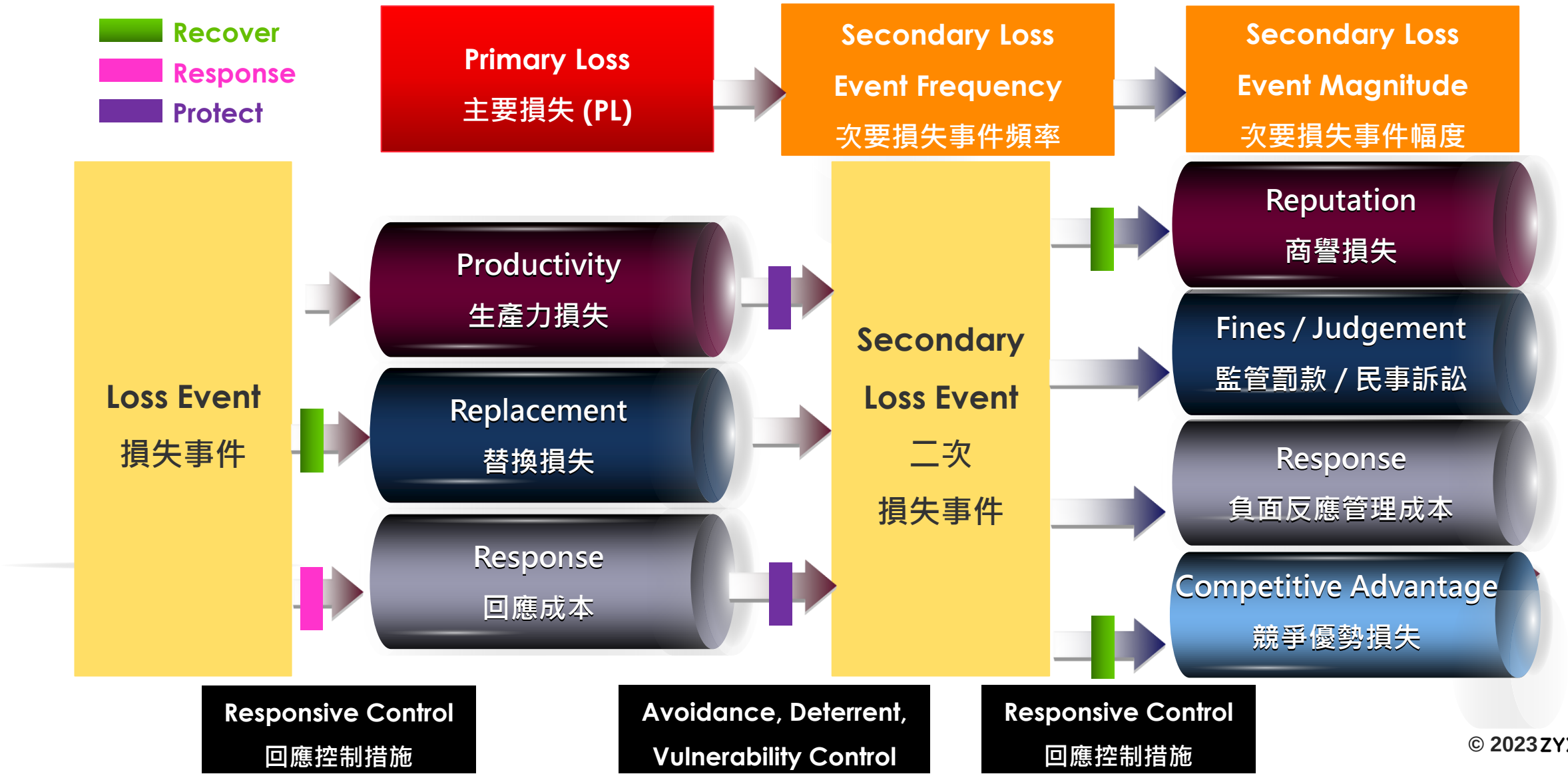
Vulnerability Control
弱點控制措施

2 **Probability of Action**
行動機率 (PoA)

Deterrent Control
阻嚇控制措施

ZYXEL
Your Networking Ally

FAIR 模型 (4/4)



ZYXEL
Your Networking Ally

控制措施 – 面對風險的人員、政策、流程和技術

ZYXEL
Your Networking Ally

FAIR 模型 – 酒後駕駛風險分析

Risk(風險)

經由 FAIR 方法分析酒後駕車風險，政策制定者和交通安全專家瞭解影響酒後駕車風險的各個因素，並制定相應的策略來降低此風險

1. 降低行動概率（PoA）和威脅事件頻率（TEF）
   - ① 透過執法方式對駕駛員進行嚴格的酒精檢測，提高酒後駕車的罰款和法律責任
   - ② 參加聚會飲酒時，提前預定代駕或叫車服務
2. 提高抵抗力（RS）和降低脆弱性（VUL）
   - ① 加強交通安全教育和宣傳

駕駛 使用 的接 高的接觸頻率	人、其他車輛） 繁忙的道路會更	使用者時採取危險行為（如超速、駕駛失控）的機率	造成傷害的能力，可能取決於他們的酒精含量、駕駛技能等因素	員造成傷害的能力，可能包括遵守交通規則、保持警覺等

ZYXEL
Your Networking Ally

資訊安全風險管理

- 定性評估的侷限性
- 量化風險評估的重要性
- FAIR 方法介紹

FAIR 方法應用

- 實際案例分析
- 與其他風險評估方法比較

FAIR 的挑戰與未來

- 定量評估的侷限性
- 資源與工具
- 未來展望

ZYXEL
Your Networking Ally

FAIR 實際案例分析

- 案例介紹
  - 背景說明：跨國營運的寬頻連網設備商的零售通路業務
  - 情境說明：量化客戶個人識別資訊(PII) 和信用卡持卡人(PCI) 的資訊洩漏風險
- 實際應用 FAIR 方法的步驟
  - 資料收集：收集有關資訊安全事件的歷史資料、專家意見、行業報告等資料
  - 風險評估：根據 FAIR 方法分析風險因素，包括損失事件頻率（EF）和損失幅度（LM），進行量化評估
  - 結果應用：將評估結果用於制定風險[illegible]平

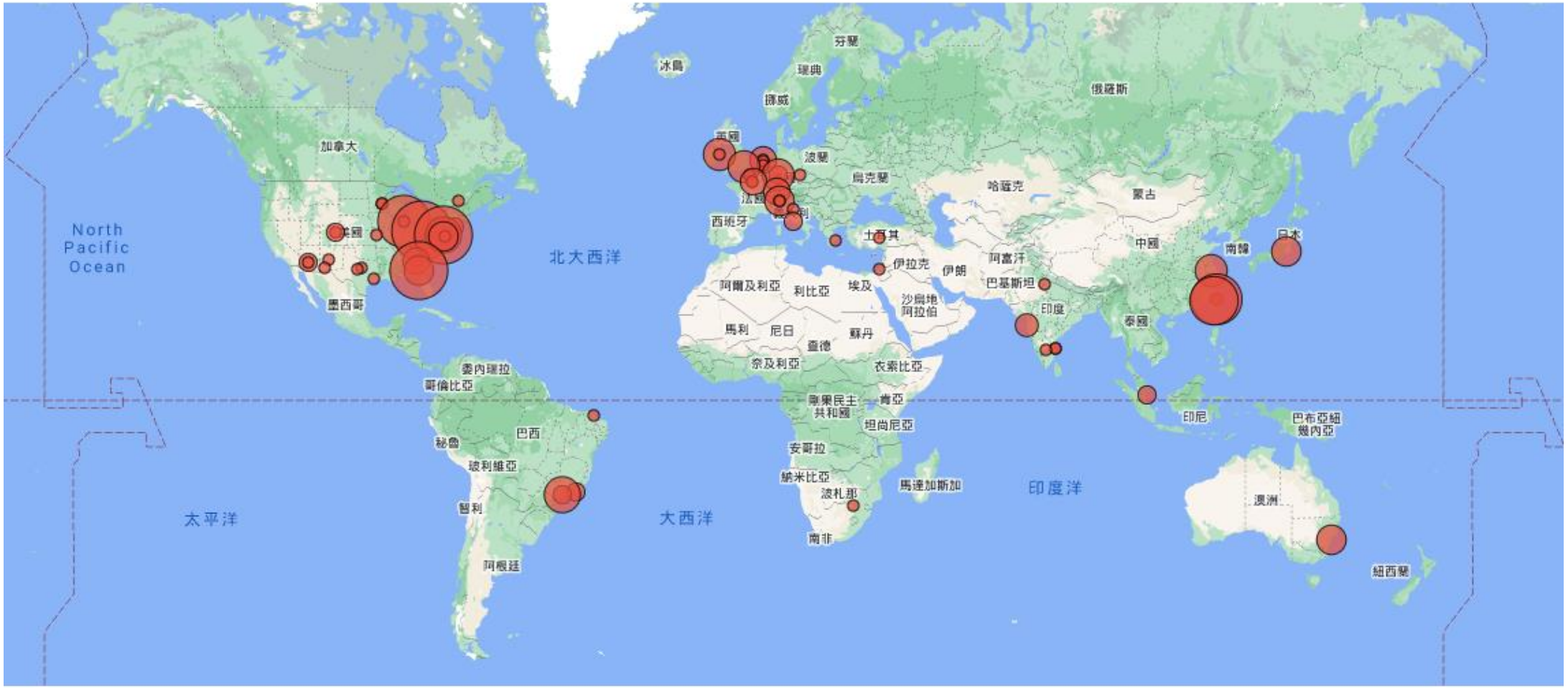
採用網路風險管理平台
輔以 FAIR 方法
分析風險因素、量化網路風險

ZYXEL
Your Networking Ally

企業實際案例分享

Cyber, Computer, Information and Network Security (NAICS: 519190)

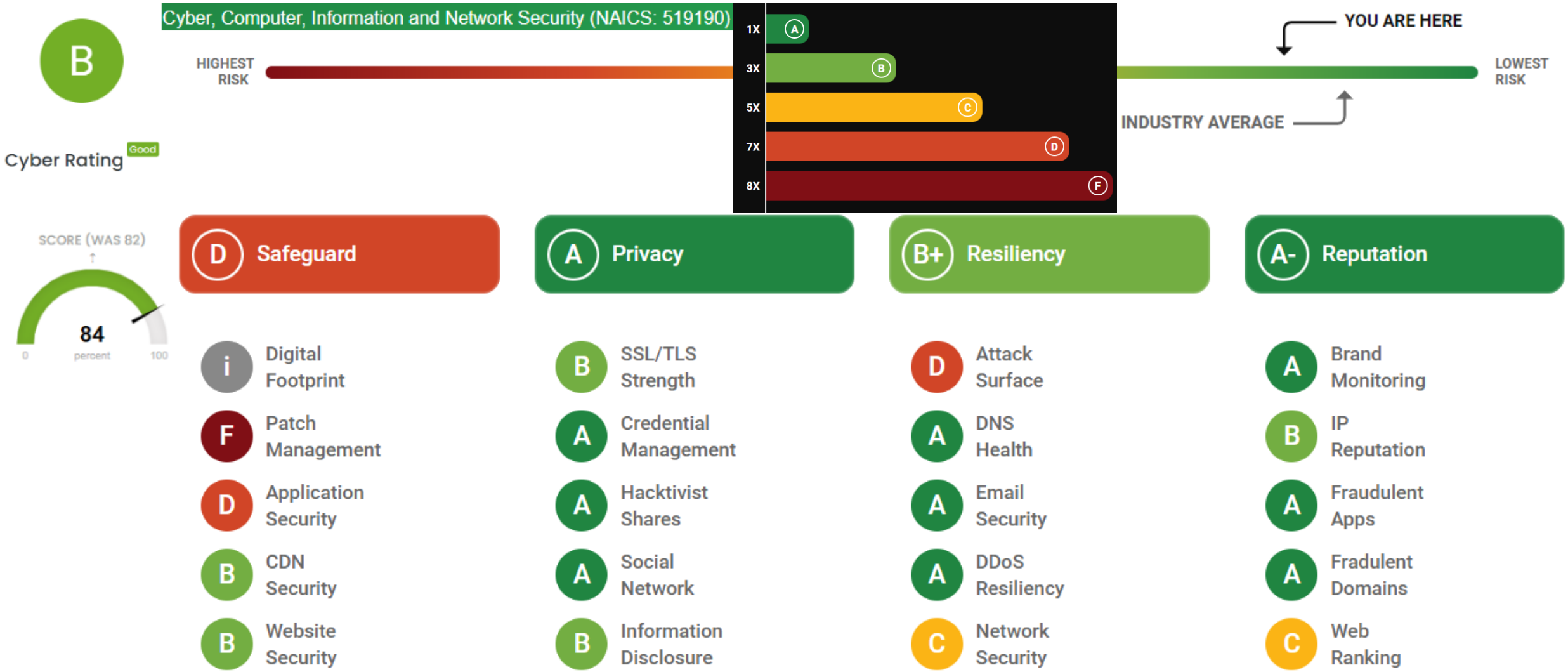
Domains 3 | IP 13248 | Subdomains 1714 | Services 625 | Dns Records 27 | Social Media 4 | Asn 135



NAICS（North American Industry Classification System）由美國、加拿大和墨西哥的產業分類系統，跨國貿易和經濟統計時使用

ZYXEL
Your Networking Ally

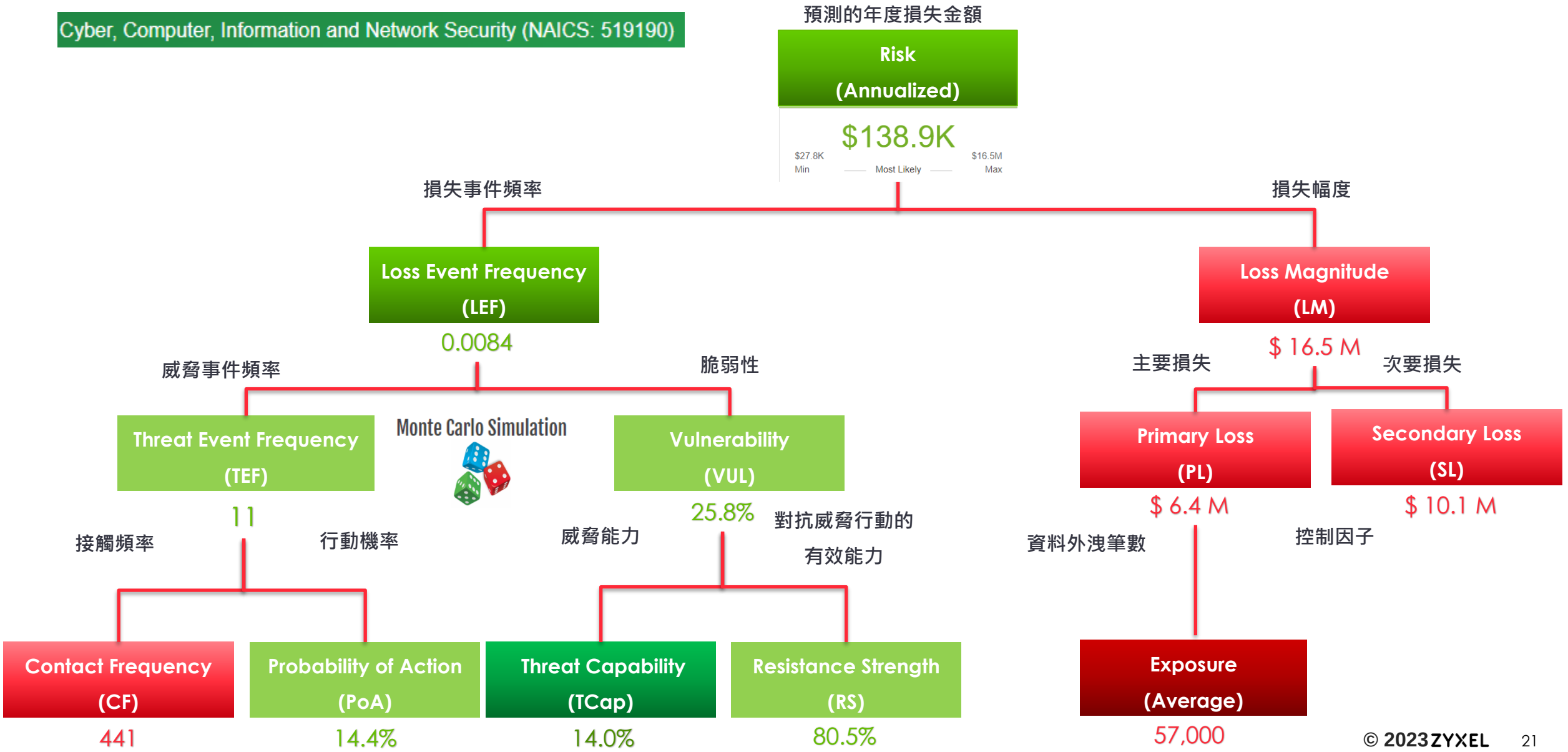
企業實際案例分享 – 定性風險分析



ZYXEL
Your Networking Ally

企業實際案例分享 – 定量風險分析

Cyber, Computer, Information and Network Security (NAICS: 519190)



ZYXEL
Your Networking Ally

RISK – 損失事件頻率 (LEF)

Loss Event Frequency

損失事件頻率 (LEF) = 0.0084

- 表示在一定時間內，資產因威脅事件導致損失的次數
- 損失事件頻率 (LEF) =

  TEF x VUL x Lookup(Company:industry_loss_event_frequency)

參考來源：

Jones, J. and Freund, J. (2015) Measuring and Managing Information Risk, A FAIR Approach. Oxford, UK: Elsevier Inc.

Verizon Data Breach Report 2019 https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

ZYXEL
Your Networking Ally

RISK – LEF – 威脅事件頻率 (TEF)

Threat Event Frequency
威脅事件頻率 (TEF) = 11

Monte Carlo Simulation

- 在一定時間內，資產遭受威脅事件（如攻擊）的次數
- 威脅事件頻率 (TEF) =

  [Contact Frequency (CF) *

  Probability of Action (PoA) *

  Lookup[Company : Industry Threat Event Frequency]]

Valuation	Description
Very High	> 100 times per year
High	Between 10 and 100 times a year
Moderate	Between 1 and 10 times a year
Low	Between 0.1 and 1 times a year
Very Low	< 0.1 times per year Less than once per year

ZYXEL
Your Networking Ally

RISK – LEF – TEF – 接觸頻率 (CF)、行動機率 (PoA)

Contact Frequency
接觸頻率 (CF) = 441

Avoidance Control
避險控制措施

- 表示攻擊者與資產（目標）接觸的頻率
- 接觸頻率 (CF) =

$\sum_{1}$ Digital Footprint (DF)" with FAIL items

[Required Privilege (RP) *

Access Vector (AV) *

Likelihood of Discovery (DI) *

Prevalence (P)]

Probability of Action
行動機率 (PoA) = 14.4%

Deterrent Control
阻嚇控制措施

- 攻擊者在接觸資產後，採取破壞行動（例如攻擊）的機率
- 行動機率 (PoA) =

$\sum_{1}$ Digital Footprint (DF)" with FAIL items

["Level of Interaction (IN) *

Likelihood of Exploit (EX) *

External Control Effectiveness (EC) *

Finding Confidence (FC)]

ZYXEL
Your Networking Ally

RISK – LEF – TEF – 接觸頻率 (CF)

Module	Asset	Detail	Severity
SSL/TLS Strength	acsIteue.zy • 124.	SSL Certificate Invalid, Incorrect, Expired or Self-Signed Warning SSL-001	High CWSS: 6.4

SSL Certificate Invalid, Incorrect, Expired or Self-Signed

Category	SSL/TLS Strength
Control ID	SSL-001
Control Name	SSL Certificate Invalid, Incorrect, Expired or Self-Signed

Mitre Classification

CWE-295 CWE-290 CAPEC-459
ATT&CK T1040 ATT&CK T1056 ATT&CK T1057
ATT&CK T1539 ATT&CK T1600 DEF3ND D3-NTA

CWSS Score

Contact Frequency

High (6.4)

Base Finding

Technical Impact (TI)	Critical (C)(1)
Acquired Privilege (AP)	Regular User (RU)(0.7)
Acquired Privilege Layer (AL)	Default (D)(0.9)
Internal Control Effectiveness (IC)	Not Applicable (NA)(1)
Finding Confidence (FC)	Proven True (T)(1)

Attack Surface

Required Privilege (RP)	None (N)(1)
Required Privilege Layer (RL)	Not Applicable (NA)(1)
Access Vector (AV)	Intranet (R)(0.8)
Authentication Strength (AS)	Not Applicable (NA)(1)
Level of Interaction (IN)	Automated (A)(1)
Deployment Scope (SC)	All (A)(1)

Environmental

Business Impact (BI)	Medium (M)(0.6)
Likelihood of Discovery (DI)	High (H)(1)
Likelihood of Exploit (EX)	Medium (M)(0.6)
External Control Effectiveness (EC)	Not Applicable (NA)(1)
Prevalence (P)	Widespread (W)(1)

ZYXEL
Your Networking Ally

RISK – LEF – TEF – 接觸頻率 (CF)

CWSS_Group	Name	Summary
Attack Surface	Require[illegible]ilege (RP) 攻擊者需要的[illegible]	評估攻擊者在觸及和利用軟[illegible]點之前所需具備的特權類型 • [illegible] (N)：攻擊者[illegible]特殊權限即可觸及和利用弱點 • [illegible]攻擊[illegible]用弱點 [illegible]級權限才能觸及和利用弱點
Attack Surface	Access Vec[illegible] 攻擊者的訪問途徑[illegible]	[illegible]弱點的代碼或功能 [illegible]有本地訪問權限，才能利用該弱點 [illegible]同的本地網路，以利用該弱點 [illegible]以透過網際網路、內網、私網利用該弱點
Environmental	Likelihood of Discovery 攻擊者發現漏洞的可能性	攻擊[illegible]定時間內[illegible]和利用軟體中的[illegible]全漏洞的機率
Environmental	Prevalence (P) 漏洞在產品或系統中的普遍程度	表示[illegible]類軟體弱點在軟體中出現的頻率，也就是這類弱點在整個軟體生態系統的普及程度， 這可以幫助組織預測攻擊者可能針對哪些常見弱點展開攻擊

接觸類型

1. **隨機接觸**
2. **定期接觸**
3. **刻意接觸**

ZYXEL
Your Networking Ally

RISK – LEF – TEF – 行動機率 (PoA)

Module	Asset	Detail	Severity
SSL/TLS Strength	acsiteue.zy • 124.	SSL Certificate Invalid, Incorrect, Expired or Self-Signed Warning SSL-001	High CWSS: 6.4

SSL Certificate Invalid, Incorrect, Expired or Self-Signed

Category	SSL/TLS Strength
Control ID	SSL-001
Control Name	SSL Certificate Invalid, Incorrect, Expired or Self-Signed

Mitre Classification

CWE-295 | CWE-290 | CAPEC-459
ATT&CK T1040 | ATT&CK T1056 | ATT&CK T1057
ATT&CK T1539 | ATT&CK T1600 | DEF3ND D3-NTA

CWSS Score

Probability of Action

High (6.4)

Base Finding

Technical Impact (TI)	Critical (C)(1)
Acquired Privilege (AP)	Regular User (RU)(0.7)
Acquired Privilege Layer (AL)	Default (D)(0.9)
Internal Control Effectiveness (IC)	Not Applicable (NA)(1)
Finding Confidence (FC)	Proven True (T)(1)

Attack Surface

Required Privilege (RP)	None (N)(1)
Required Privilege Layer (RL)	Not Applicable (NA)(1)
Access Vector (AV)	Intranet (R)(0.8)
Authentication Strength (AS)	Not Applicable (NA)(1)
Level of Interaction (IN)	Automated (A)(1)
Deployment Scope (SC)	All (A)(1)

Environmental

Business Impact (BI)	Medium (M)(0.6)
Likelihood of Discovery (DI)	High (H)(1)
Likelihood of Exploit (EX)	Medium (M)(0.6)
External Control Effectiveness (EC)	Not Applicable (NA)(1)
Prevalence (P)	Widespread (W)(1)

ZYXEL
Your Networking Ally

RISK – LEF – TEF – 行動機率 (PoA)

CWSS_Group	Name	Summary
Base Finding	Finding Confidence (FC) 報告問題的確信度	表示對於該問題是否真的是一個可被利用的安全漏洞的確定程度 • 高檢測信心表示該問題很有可能是一個真正的安全漏洞 • 低檢測信心表示該問題可能不是一個真正的安全漏洞或者無法被輕易利用
Attack Surface	Level of Interaction 攻擊者	例如提供個資或安裝惡意軟體。 採取任何行動的情況下進行攻 電腦
Environmental	Likeli Exploit (EX) 攻擊者成功利用漏洞的可	利用該漏洞進行攻擊的概率 易地利用該漏洞 攻擊者在嘗 該漏洞時面臨較大的困難
Environmental	External Control Effectiveness (EC) 外部控制措施的有效性	量了那些非軟體 身的防護措施，如防火牆、入侵檢測系統等，對減少攻擊者利用該漏洞的成功率的影響程度 • 外部控制有效性高，則意味著在軟體以外的控制措施對防止攻擊非常有效 • 外部控制有效性低，則表示這些控制措施對抵禦攻擊的效果有限

蓄意攻擊的三個驅動因素

1. 資產價值
2. 攻擊成本
3. 承擔後果

ZYXEL
Your Networking Ally

RISK – LEF – 脆弱性 (VUL)

Vulnerability

脆弱性 (VUL) = 25.8%

- 資產在面對特定威脅時的弱點或缺陷
- 脆弱性 (VUL) = (TCap/RS) with Monte Carlo simulations
- Vulnerability Control
  - 施降低脆弱性、提高抵抗力，關注攻擊者的能力，綜合應對不同類型的風險
  - 透過漏洞修補、安全意識培訓、多層次防護體系等方法提高資產的抵抗力，同時應對來自不同能力的攻擊者

ZYXEL
Your Networking Ally

RISK – LEF – VUL – 威脅能力 (TCap)

Threat Capability
威脅能力 (TCap) = 14%

- 攻擊者成功實施[illegible]擊的能力
- 威脅能力越強，攻擊[illegible]
  的脆弱性造成損[illegible]

威脅能力

1. 位置 (外部、系統管理員、員工)
2. 技能 (網路、主機、軟體、設備)
3. 資源 (犯罪團體、國家資助駭客)

- 特定產業團體

Industry	Incidents	Breaches	TCap
飯店業	87	61	70 %
[illegible]	31	11	35 %
[illegible]	382	99	26 %
[illegible]	[illegible]	10	1 %
[illegible]	[illegible]	207	22 %
[illegible]	[illegible]	304	65 %
[illegible]	[illegible]	155	14 %
[illegible]	[illegible]	[illegible]	25 %
[illegible]	[illegible]	15	54 %
[illegible]務	[illegible]	157	23 %
[illegible]	22	14	64 %
[illegible]令	234	139	59 %
貿易	34	16	47 %
運輸	112	36	32 %

ZYXEL
Your Networking Ally

RISK – LEF – VUL – 抵抗強度 (RS)

Module	Asset	Detail	Severity
Application Security	ed[redacted].zyxel.com	**Restriction of excessive authentication attempts or login form without bot detection** Failed APPSEC-023 Form Action: Input Name: email Input Name: password	High CWSS: 6.8

Restriction of excessive authentication attempts or login form without bot detection

Category

Control ID

Control Name: APPSEC Improper restriction of excessive authentication attempts or login form without bot detection

Mitre Classification

CWE-307 | CAPEC-49 | ATT&CK T1190 | DEF3ND D3-NTA

CWSS Score

Resistance Strength

High (6.8)

Base Finding		Attack Surface		Environmental	
Technical Impact (TI)	Medium (M)(0.6)	Required Privilege (RP)	None (N)(1)	Business Impact (BI)	High (H)(0.9)
Acquired Privilege (AP)	Regular User (RU)(0.7)	Required Privilege Layer (RL)	Not Applicable (NA)(1)	Likelihood of Discovery (DI)	High (H)(1)
Acquired Privilege Layer (AL)	Not Applicable (NA)(1)	Access Vector (AV)	Internet (I)(1)	Likelihood of Exploit (EX)	Medium (M)(0.6)
Internal Control Effectiveness (IC)	Not Applicable (NA)(1)	Authentication Strength (AS)	None (N)(1)	External Control Effectiveness (EC)	Not Applicable (NA)(1)
Finding Confidence (FC)	Proven True (T)(1)	Level of Interaction (IN)	Automated (A)(1)	Prevalence (P)	Widespread (W)(1)
		Deployment Scope (SC)	All (A)(1)		

ZYXEL
Your Networking Ally

RISK – LEF – VUL – 抵抗強度 (RS)

CWSS_Group	Name	Summary
Base Finding	Internal Control Effectiveness (IC) 內部控制有效性	內部控制在防止特定軟體弱點方面的有效性
Attack Surface	Required Privilege Layer (PL) 需要的權限層級	應用程序權限層級 弱點時所需克服的難度
Attack Surface	認證強	的強度 需要繞過更強大的認證機制
Attack Surface	Level of In 攻擊	個資或安裝惡意軟體。 幾乎不需要採取任何行動的情況下進行 感染其電腦
Environmental	External Control Effectiveness (EC) 外部控制措施的有效性	量了那些系身的防護措施，如火牆、入侵檢測系統等，對減少攻擊者利用該漏洞的率的影響程度 • 外部控制有效性高，則意味著在軟體以外的控制措施對防止攻擊非常有效 • 外部控制有效性低，則表示這些控制措施對抵禦攻擊的效果有限

攻擊者入侵資產的困難程度

1. **縮短威脅應變反應的時間**
2. **減少駭客就地取材的機會**
   - ① **刪除不必要的程式與服務**

ZYXEL
Your Networking Ally

RISK – LEF – VUL – 抵抗強度 (RS)

Resistance Strength

抵抗強度 (RS) = 80.5%

- 抵抗力越強，資產在受到攻擊時遭受損失的可能性越小
  - 修補漏洞、提升資安意識、建立多層防護體系等方法，提高資產的抗力韌性
  - WiFi 網路安全存取，採用 WPA3 (WiFi Protected Access)加密連線機制、身分認證及封包檢查等安全防護方面更加強韌
- 抵抗強度 (RS) =

  {100 – SUM [Internal Control Effectiveness (IC) * Required Privilege Layer (RL) * Authentication Strength (AS) * Level of Interaction (IN) * External Control Effectiveness (EC)] * CWSS}

ZYXEL
Your Networking Ally

RISK – 損失幅度 (LM)

Loss Magnitude

損失幅度 (LM) = 16.5 M

- 損失幅度，表示損失事件中主要損失和次要損失的總和

Code	Name	Cost Per Record (USD)	Primary Cost	Secondary Cost
DE	Germany	748	78	670
UK	United Kingdom	673	68	605
US	United States	233	81	152
CA	Canada	202	86	116
FR	France	169	75	94
ME	Middle East	163	83	80
IT	Italy	152	77	75
	Other (default)	148	64	120

Code	Name	Cost Per Record (USD)	Primary Cost	Secondary Cost
SA	South Africa	142	71	71
SK	South Korea	138	62	76
JP	Japan	135	74	61
AS	ASEAN	125	57	68
AU	Australia	108	47	61
TR	Turkey	105	48	57
ID	India	68	31	37
BZ	Brazil	67	32	35

參考來源： https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

ZYXEL
Your Networking Ally

RISK – 損失幅度 (LM)

- 損失幅度，表示損失事件中主要損失和次要損失的總和

ZYXEL
Your Networking Ally

RISK – LM – 主要損失 (PL)、次要損失 (SL)

Primary Loss
主要損失 (PL) = 6.4M

Responsive Control
回應控制措施

- 主要利益相關者(企業)的直接損失
  - 罰款
  - 賠償金
- 主要損失 (PL) =

  Primary Loss Per Record * Average Number of Records

Primary Loss	$	6,351,259

Secondary Loss
次要損失 (SL) = 10.1M

Responsive Control
回應控制措施

- 次要利益相關者(客戶、股東、監管機構)對主要損失的負面反應而產生的額外損失
  - 商譽受損
  - 客戶流失
  - 法律費用

Detection and Escalation	$	1,935,379
Notification	$	1,081,355
Post Data Breach Response (Legal)	$	2,543,641
Lost Business	$	4,561,965

RISK – LM – PL – 資料外洩成本 Exposure

資料外洩成本

Exposure (Average)

- 資產在面對威脅時，可能遭受的損失程度
- 根據組織所在行業和國家，利用IBM Security和 Ponemon Institute 的“資料洩漏成本研究”進行計算

DATA OWNER'S COUNTRY	US – United States of America		
DATA OWNER'S INDUSTRY	Cyber, Computer, Information and Network Security (NAICS: 519190)		
	Number of Records	**Unit cost**	
PII/PHI/PCI	57,000	$	398

Reference :

IBM Cost of a Data Breach Report

Verizon Data Breach Investigations Report (DBIR)

Ponemon Institute

ZYXEL
Your Networking Ally

運用定量風險分析決定安全投資策略 (1/5)

決策者的思維

資安投資的必要性

各階段該有的作為

減少的風險相對的價值

ZYXEL
Your Networking Ally

運用定量風險分析決定安全投資策略 (2/5)

STEP I TASKS TO COMPLETE $ 45K decrease

Module	Asset	Detail	Severity
Patch Management	vip	Patch Management Failed CVE-2023-22727 (Product: php/4.4.8) CakePHP is a development framework for PHP web apps. In affected versions the `Cake\Database\Query::limit()` and `Cake\Database\Query::offset()` methods are vulnerable to SQL injection if passed un-sanitized user request data. This issue has been fixed in 4.2.12, 4.3.11, 4.4.10. Users are advised to upgrade. Users unable to upgrade may mitigate this issue by using CakePHP's Pagination library. Manually validating or casting parameters to these methods will also mitigate the issue.	Critical CVSS: 9.8
Patch Management	bbwf	Patch Management Failed CVE-2022-37454 (Product: php/8.1.8) The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge	Critical CVSS: 9.8

STEP I TARGET

Cyber Rating

0 % increase

Probable Financial Impact Rating

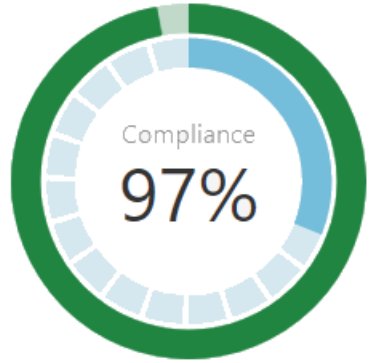
Risk (Annualized)

82.8K	93.1K	11.9M
MINIMUM	MOST LIKELY	MAXIMUM

The forecasted annualized loss based on the given parameters in the FAIR Model.

$45K decrease

Compliance Rating



0 % increase

ZYXEL
Your Networking Ally

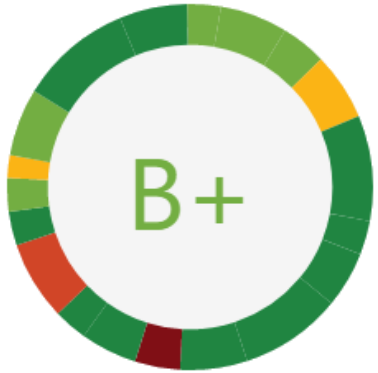
運用定量風險分析決定安全投資策略 (3/5)

STEP 2 TASKS TO COMPLETE $ 123K decrease

Module	Asset	Detail	Severity
Application Security	freed	**Restriction of excessive authentication attempts or login form without bot detection** Failed APPSEC-023 Input Name: username Input Name: pw	High CWSS: 6.8
Application Security	upload	**Restriction of excessive authentication attempts or login form without bot detection** Failed APPSEC-023 Form Action: Form Name: loginForm Input Name: j_username Input Name: j_password Input ID: login	High CWSS: 6.8

STEP 2 TARGET

Cyber Rating



6 % increase

Probable Financial Impact Rating

Risk
(Annualized)

13.6K	15.3K	11.9M
MINIMUM	MOST LIKELY	MAXIMUM

The forecasted annualized loss based on the given parameters in the FAIR Model.

$123K decrease

Compliance Rating

1% increase

ZYXEL
Your Networking Ally

運用定量風險分析決定安全投資策略 (4/5)

STEP 3

TASKS TO COMPLETE **$ 131K decrease**

Module	Asset	Detail	Severity
IP Reputation	[redacted]	IP Reputation Failed REP-001	Medium CWSS: 4.4
IP Reputation	[redacted]	IP Reputation Failed REP-001	Medium CWSS: 4.4
IP Reputation	[redacted]	IP Reputation Failed REP-001	Medium CWSS: 4.4

STEP 3 TARGET

Cyber Rating

9 % increase

Probable Financial Impact Rating

Risk
(Annualized)

7K	7.9K	11.9M
MINIMUM	MOST LIKELY	MAXIMUM

The forecasted annualized loss based on the given parameters in the FAIR Model.

$131K decrease

Compliance Rating

0 % increase

ZYXEL
Your Networking Ally

運用定量風險分析決定安全投資策略 (5/5)

STEP 4

TASKS TO COMPLETE **$ 132K decrease**

Module	Asset	Detail	Severity
Attack Surface	[redacted]	**Attack Surface** Failed SSL/TLS Vulnerabilities • Use of a Broken or Risky Cryptographic Algorithm (SSLv3) SSL-008 CWE-327 CWE-693 • Use of Weak RC4 Stream Cipher SSL-019 CWE-327 • Weak Cipher Suite Support SSL-021 CWE-327 • Lack of Strong Encryption Key Generation SSL-011 CWE-326 Possible Vulnerabilities • CVE-2022-31813 • CVE-2022-37436 • CVE-2023-28625	High CWSS: 6

STEP 4 TARGET

Cyber Rating

11 % increase

Probable Financial Impact Rating

Risk
(Annualized)

6.2K	6.9K	11.9M
MINIMUM	MOST LIKELY	MAXIMUM

The forecasted annualized loss based on the given parameters in the FAIR Model.

$132K decrease

Compliance Rating

0 % increase

ZYXEL
Your Networking Ally

FAIR 與其他量化風險框架

- **FAIR 可以與其他風險管理框架結合使用，達到更全面的風險管理**

風險框架	摘要敘述
ISO 27005	ISO 27005 風險管理標準與 FAIR 方法可以結合使用 對資訊風險進行量化分析，並在整個風險管理過程中提供有用的資訊
NIST 800-37	FAIR 方法可以與 NIST 800-37 框架結合，以提供更詳細的風險量化 NIST 風險管理過程中，FAIR 可以用於評估風險的可能性和影響，從而幫助組織做出更明智的決策
OCTAVE	FAIR 方法可以與 OCTAVE 風險評估方法結合，以便更好地理解組織的運營風險 FAIR 可以幫助組織確定最重要的資產、威脅和脆弱性，從而實現更有效的風險管理
CIS RAM	CIS RAM是基於 FAIR 的風險評估方法，專門為組織提供實用和可操作的風險管理建議 FAIR 方法在此框架中是核心組成部分，用於量化風險並幫助組織確定合適的風險應對措施
ISACA	ISACA 的 CRISC 認證專為資訊系統風險管理專業人士設計的認證，其中涵蓋 FAIR 方法 FAIR 可以與 CRISC 的風險管理知識結合，以實現更有效的資訊風險管理

ZYXEL
Your Networking Ally

資訊安全風險管理

- 定性評估的侷限性
- 量化風險評估的重要性
- FAIR 方法介紹

FAIR 方法應用

- 實際案例分析
- 與其他風險評估方法比較

FAIR 的挑戰與未來

- 定量評估的侷限性
- 資源與工具
- 未來展望

ZYXEL
Your Networking Ally

定量風險評估的侷限性

- FAIR 方法的部分輸入值來自專家判斷，這可能會導致主觀性和偏見
- 在進行風險量化時，可能會出現一定程度的不確定性

- FAIR 方法的風險分析過程相對複雜，需要對多個因素進行詳細的分析
- 對於缺乏風險管理經驗的人來說，學習和理解 FAIR 模型具有一定的挑戰性

- FAIR 方法依賴於足夠的歷史資料和專家知識來進行風險評估
- 在某些情況下，可能缺乏足夠的資料來支持準確的風險評估，影響到分析結果的準確性

- FAIR 方法在高度監管的行業（如金融服務、醫療保健、資通電信、公共能源、國防產業）具有更高的適用性
- 將 FAIR 方法應用於不同行業時，需要進行一定的調整和客製，以確保其有效性

ZYXEL
Your Networking Ally

FAIR 資源與工具 (1/2)

FAIR INSTITUTE

非營利組織，旨在促進FAIR方法的普及和應用
提供包括教育訓練、案例研究、網路研討會等資源

THE Open GROUP

OpenFAIR 是由 The Open Group 開發的標準，為
FAIR提供結構化的框架、流程、方法來分析評估風險

FAIR-U
POWERED BY RISKLENS

基於 FAIR 方法的免費風險分析工具，幫助初學者熟悉
FAIR 框架和概念

RiskLens

基於FAIR的風險管理軟體，幫助企業量化和管理資訊
安全風險

ZYXEL
Your Networking Ally

FAIR 資源與工具 (2/2)

FAIR
POWERED BY RISKLENS

Phishing Database Breach

Created April 26, 2023

ANNUAL LOSS EXPOSURE
The forecasted annualized loss from this scenario.
$0 Min — $2.4M Avg — $6.9M Max

LOSS EVENT FREQUENCY
Loss Event Frequency is being derived from estimates of Threat Event Frequency and Vulnerability.

LOSS
Enter Loss
Primary and

THREAT EVENT FREQUENCY
Minimum: 0.5
Most Likely: 1.25
Maximum: 2
Confidence: Medium

VULNERABILITY
Vulnerability is being derived from estimates of Threat Capability and Resistive Strength.

PRIMARY LOSS
Minimum: $4,000
Most Likely: $16,000
Maximum: $216,000

CONTACT FREQUENCY
You are estimating at the Threat Event Frequency level; no estimate is needed here.

PROBABILITY OF ACTION
You are estimating at the Threat Event Frequency level; no estimate is needed here.

THREAT CAPABILITY
Minimum: 60%
Most Likely: 85%
Maximum: 99%
Confidence: Medium

RESISTANCE STRENGTH
Minimum: 75%
Most Likely: 85%
Maximum: 95%
Confidence: Medium

Analysis Results

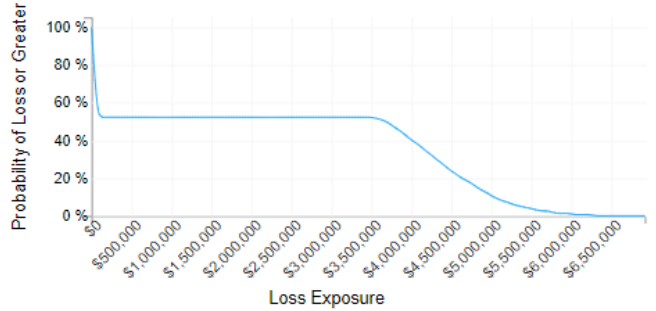
Risk

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario.

$0 Minimum — $2.4M Average — $6.9M Maximum

Loss Exceedance Curve

Linear Scale



Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	0.54	1
Loss Magnitude	$4.0k	$47.2k	$193.3k

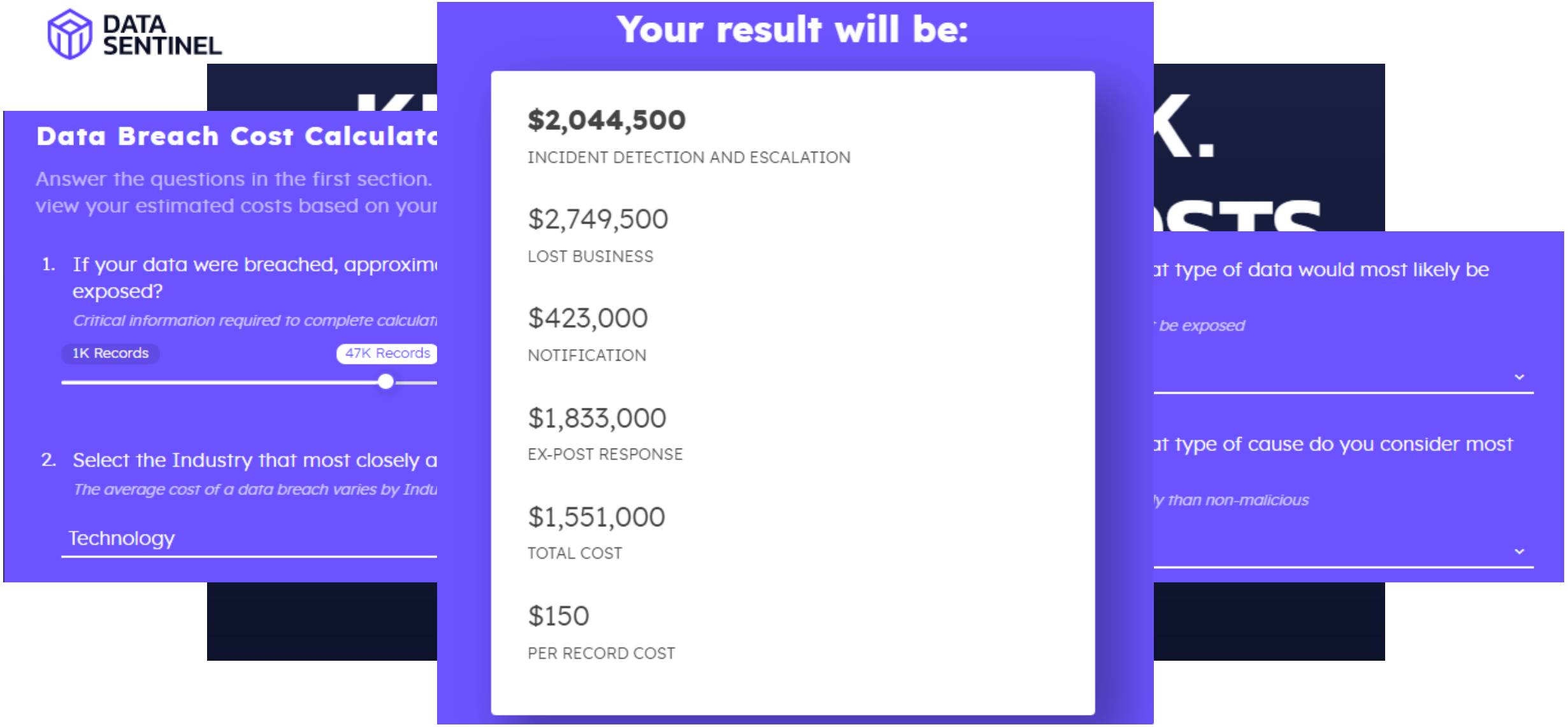
Secondary

	Min	Avg	Max
Loss Events / Year	0	0.52	1
Loss Magnitude	$3.4M	$4.5M	$6.9M

Vulnerability 43.07%

ZYXEL
Your Networking Ally

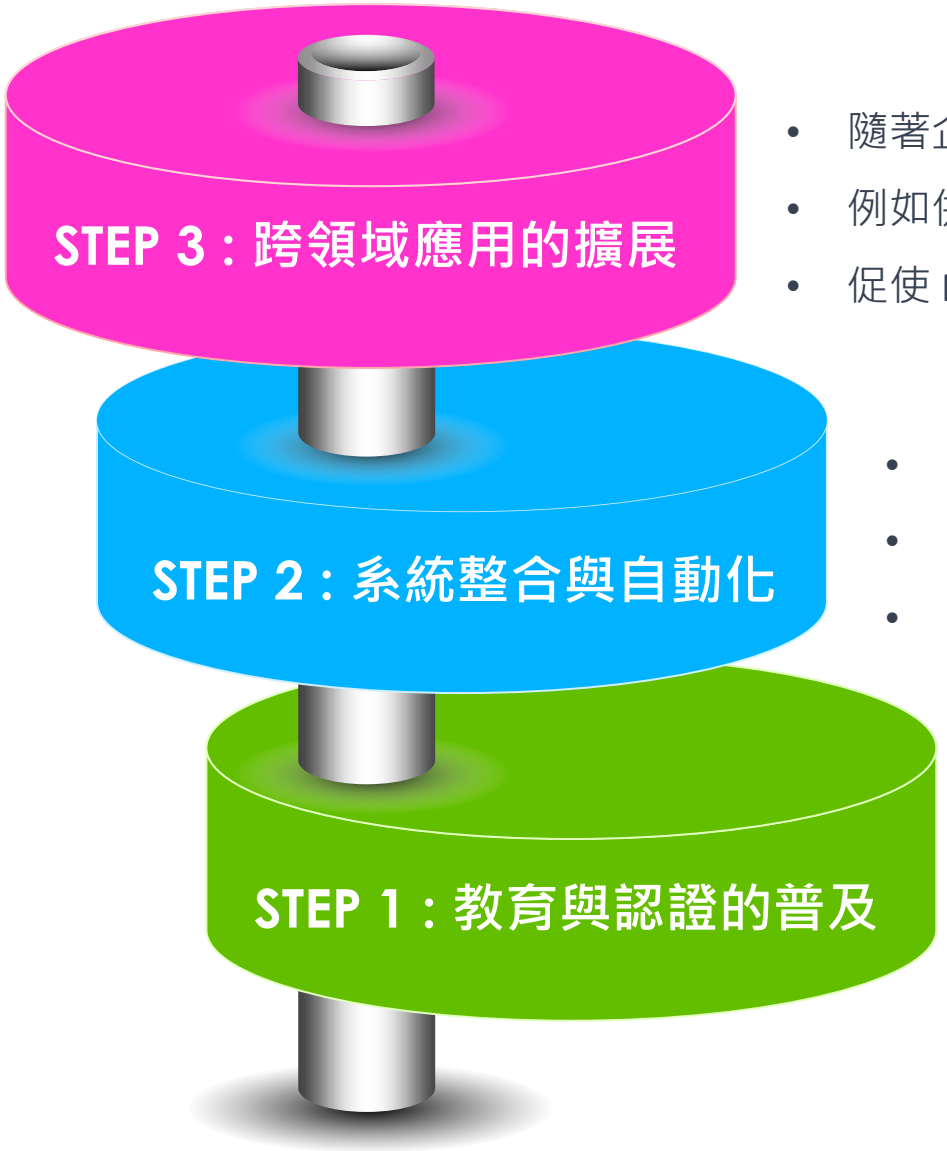
資料外洩成本計算器



參考來源： https://www.data-sentinel.com/data-breach-calculator#calculator

ZYXEL
Your Networking Ally

未來展望



- 隨著企業認識到風險量化的重要性，FAIR 會在更多領域中得到應用
- 例如供應鏈風險管理、物聯網（IoT）安全和隱私風險管理
- 促使 FAIR 方法持續演進與改善，以滿足不同領域的特定需求

- 將出現更多將 FAIR 與其他風險管理工具和平台整合的解決方案
- 實現風險評估和管理流程的自動化，提高分析效率並降低人為錯誤
- 機器學習和人工智慧技術的發展會使風險分析更加精準

- 教育和培訓機構開設 FAIR 課程，滿足市場對 FAIR 專業人員的需求
- 擴展認證計劃，確保專業人員具備知識和技能來應用 FAIR 方法

ZYXEL
Your Networking Ally

結語

ZYXEL

Your Networking Ally