「資訊暨產品安全」轉型

“成本中心” 轉化為 "機會中心”

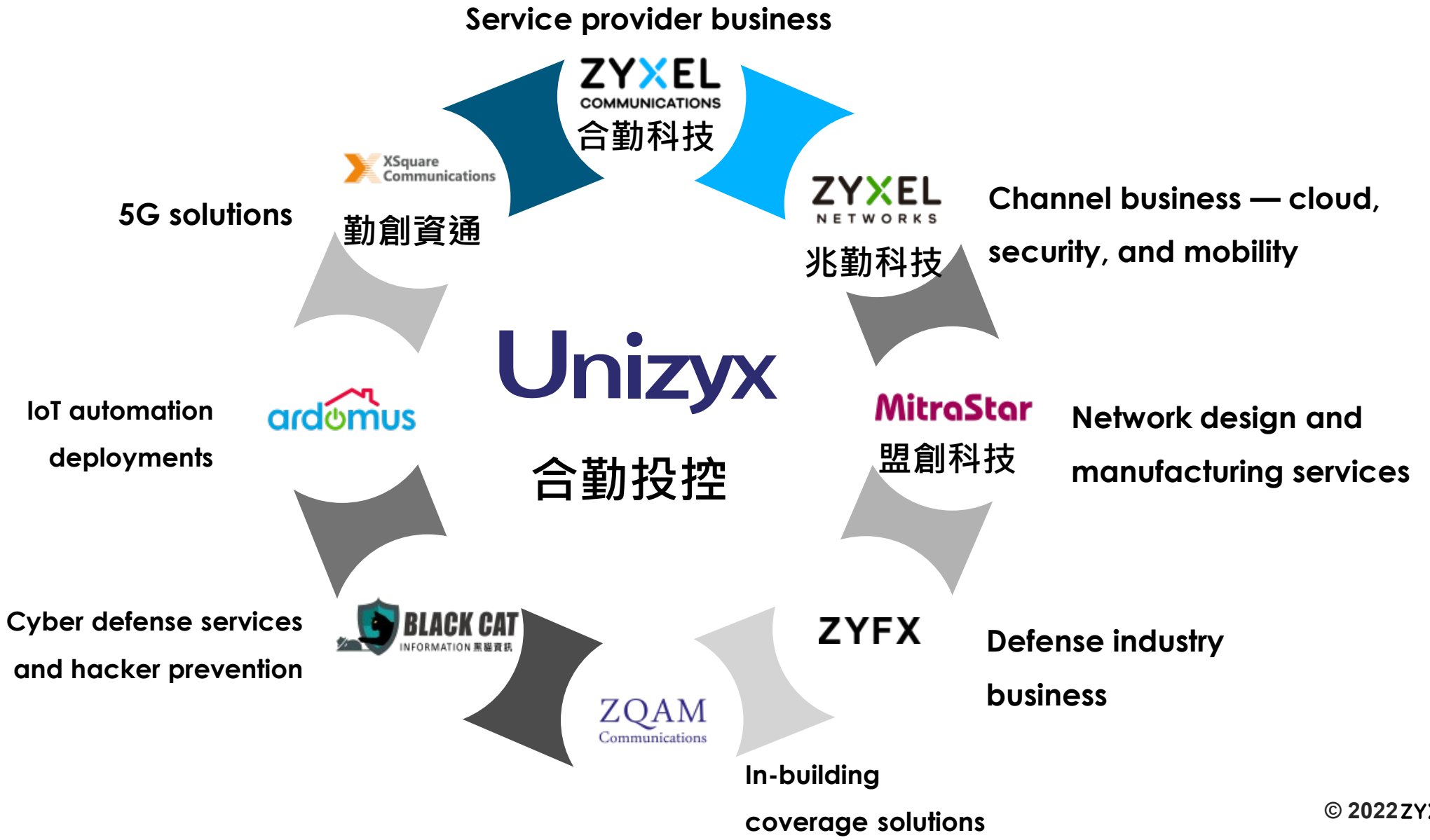
合勤投資控股 Unizyx

游政卿

資安長

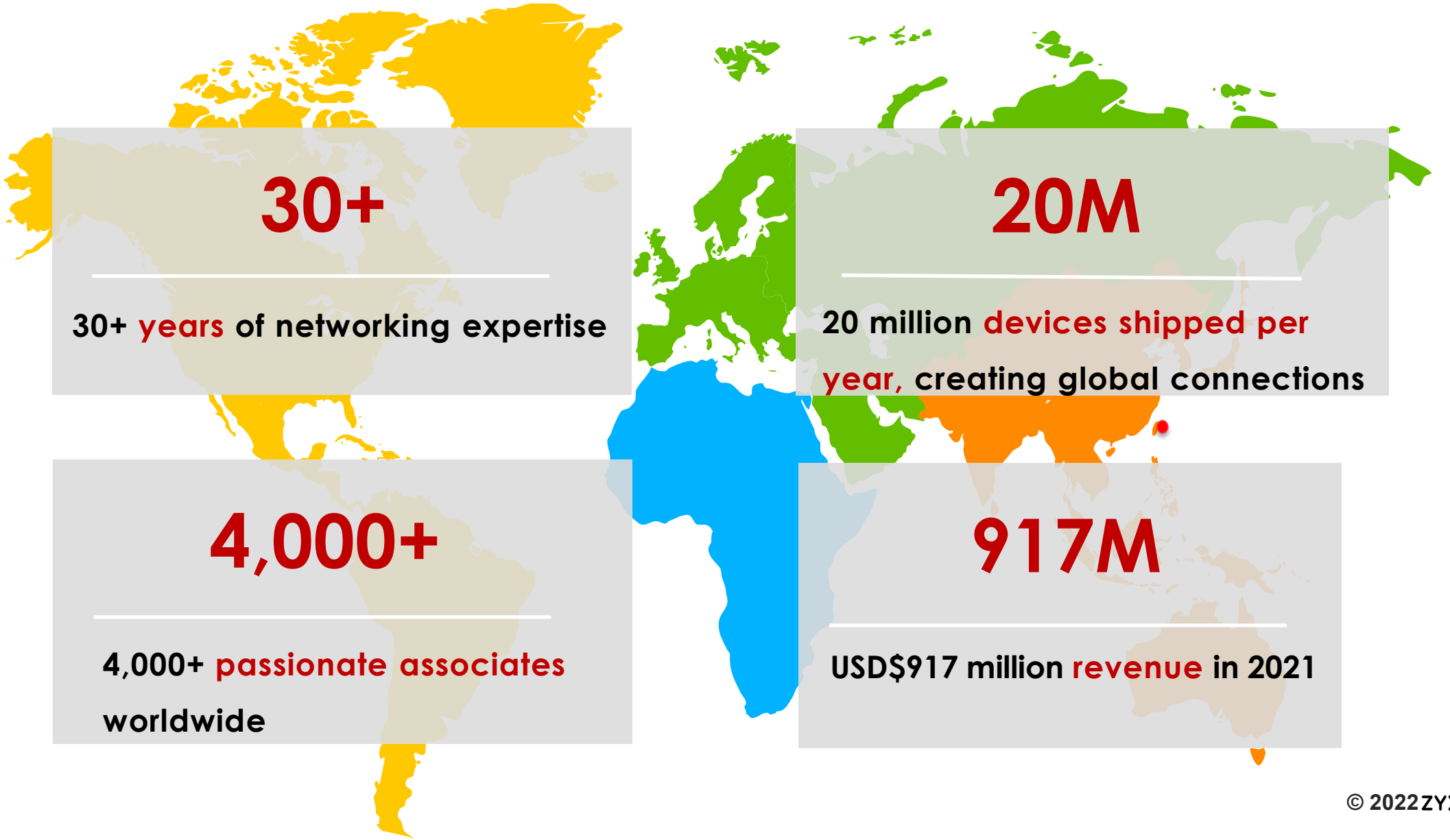
董事長室

合勤集團 (1/3)



ZYXEL
Your Networking Ally

合勤集團 (2/3)



30+

30+ years of networking expertise

20M

20 million devices shipped per year, creating global connections

4,000+

4,000+ passionate associates worldwide

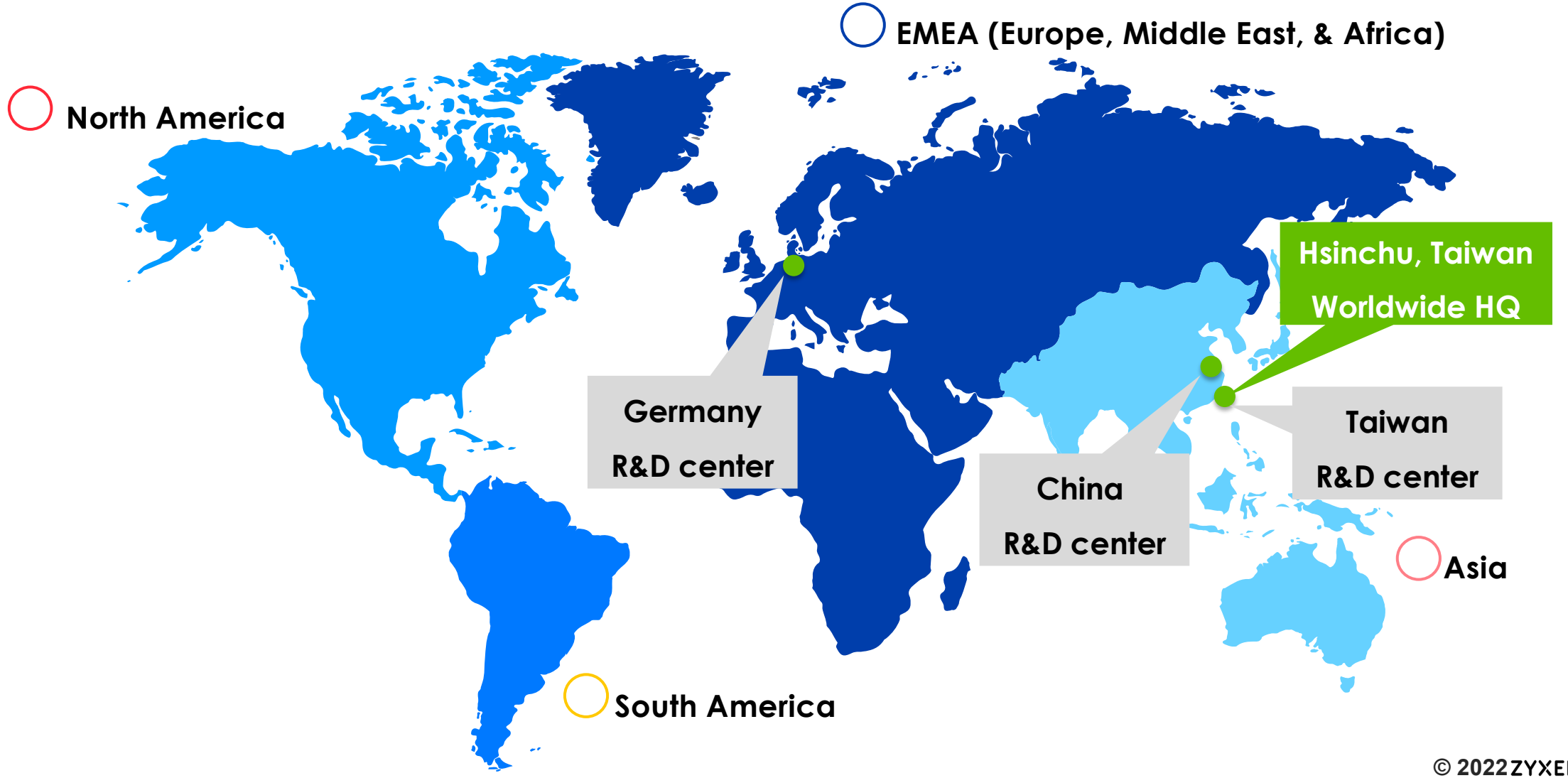
917M

USD$917 million revenue in 2021

ZYXEL
Your Networking Ally

合勤集團 (3/3)

- 產品銷售遍佈 150 個國家或地區

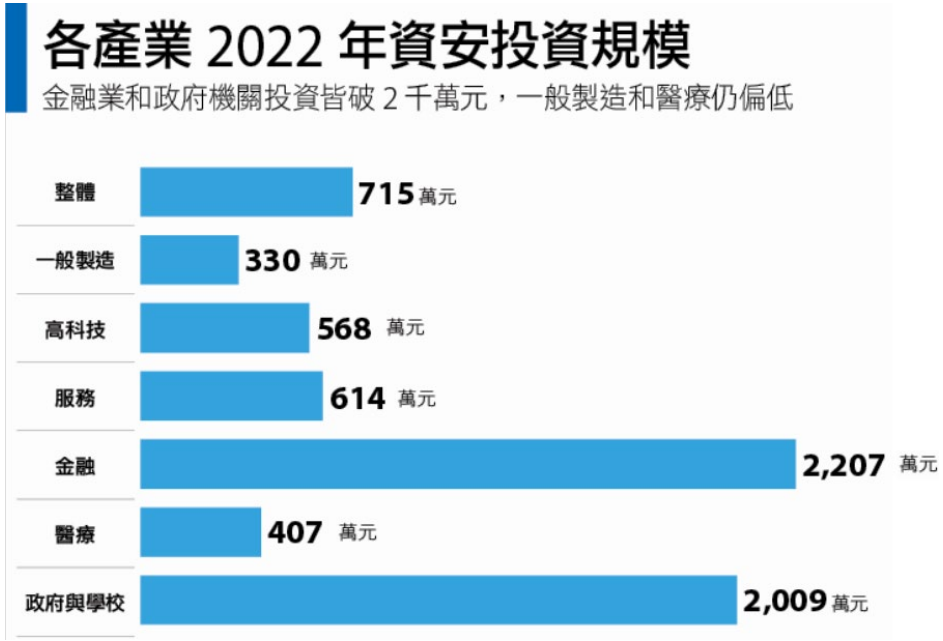


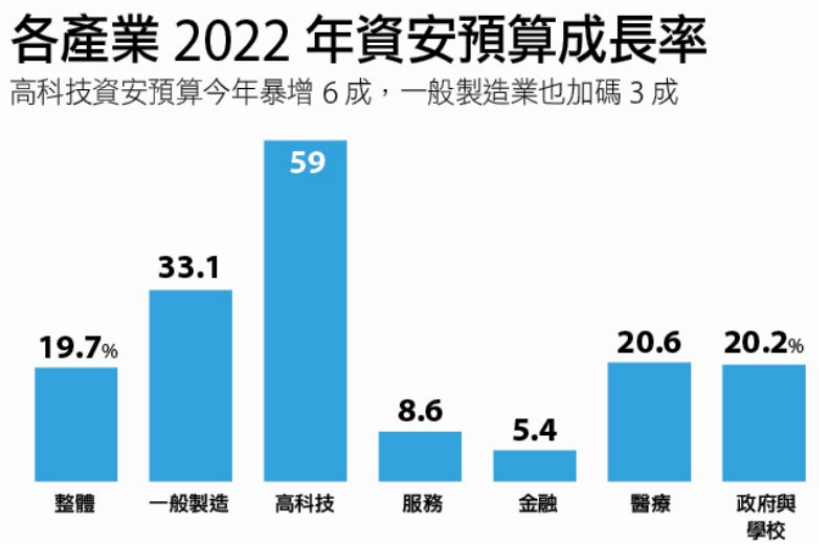
ZYXEL
Your Networking Ally

將「資訊暨產品安全」
由“成本中心” 轉化為 “機會中心”

資訊安全的投資

- 企業進行數位化轉型，帶來的問題就是資料頻繁、廣泛、跨組織地流動，其中資料安全的很多風險其實是感受不到的
- 安全是解決風險的，但是在風險變成事實之前的損失很難評估，大多數公司會把安全看作一種成本





資料來源：2022 iThome CIO大調查，2022年8月

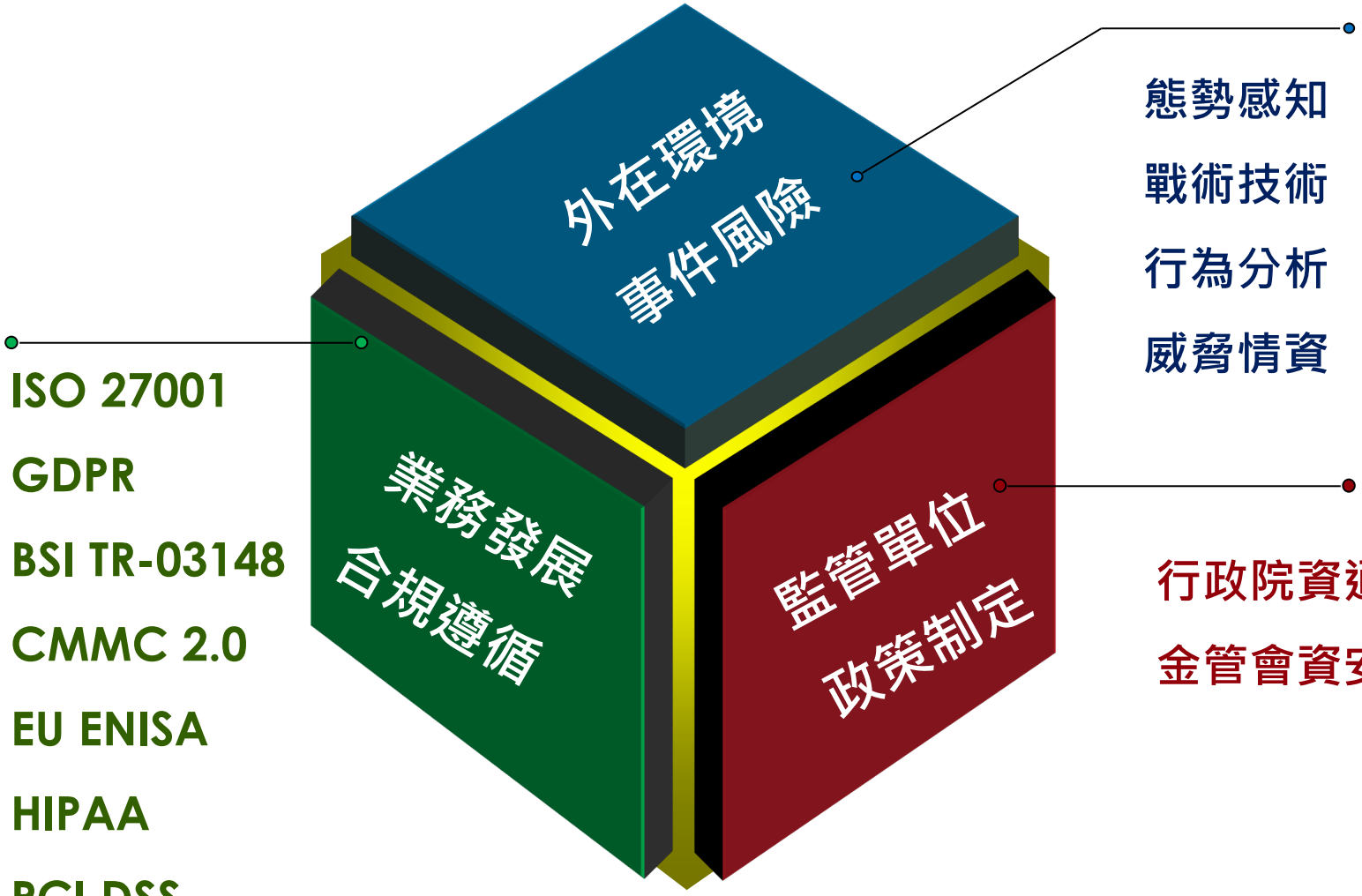
經營階層對資安投資的想法

ZYXEL
Your Networking Ally

將資訊安全投資轉化的策略

1. 運用商務表達方式影響高階主管看法 (1/4)

- 確認董事會及經營階層的期待



1. 運用商務表達方式影響高階主管看法 (2/4)

- 表達方式 (過去式) : 掌握當前資安風險態勢，為確保企業安全所做的一切

網際空間資產風險

分析日期 : 2022/3/31

zyxel.com 合勤科技 | B 82 / 76 Score Industry

網域安全風險

分析日期 : 2022/3/1

成熟等級: 3

Level 1	Level 2	Level 3	Level 4	Level 5
0 項相關	0 項相關	13 項相關	4 項相關	0 項相關

Level 1
重大弱點或是管理與設定缺漏，導致網域內電腦有立即性的危

Level 2
管理與設定缺漏，使所有網域內電腦資產可能遭受滲透攻擊

Level 3
網域具基本安全度，已無網域伺服器預設配置上的弱點

Level 4
展現高度安全的網域管理配置

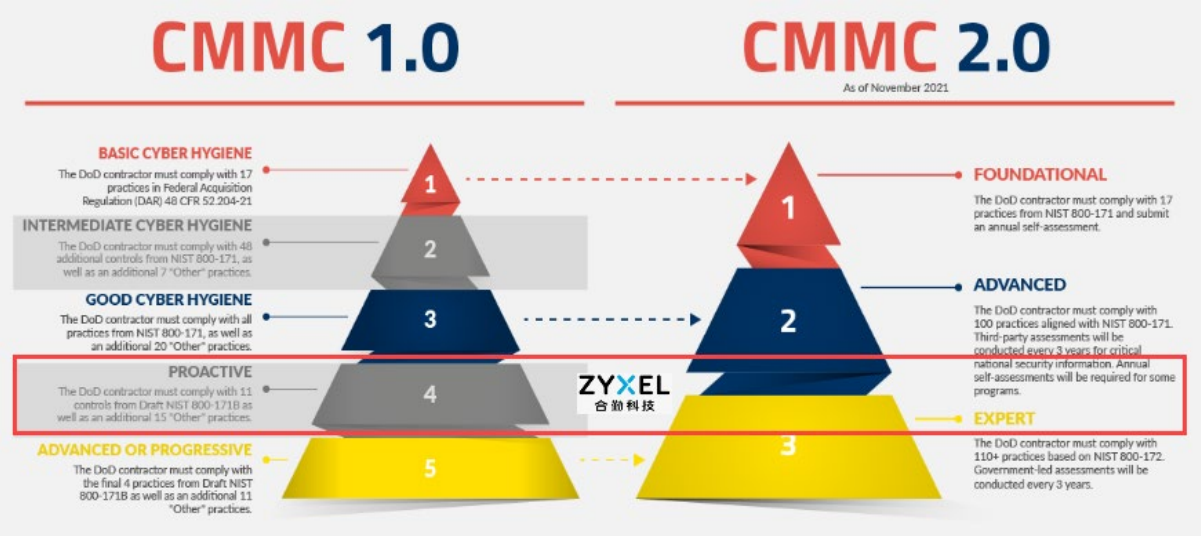
內網安全風險

期間 : 2022/3/1 ~ 2022/3/31

3,844 (PC-3,366、SVR-478)

133

高風險事件	中風險事件
2	5



ZYXEL
Your Networking Ally

1. 運用商務表達方式影響高階主管看法 (3/4)

- 表達方式 (未來式)：用商業術語來表達即將到來的事情，表明安全是創新中心

	邊界安全	終端安全	身份安全	應用安全	資料安全	安全管理	安全服務
價值描述	防止邊界入侵	防止電腦病毒	身份存取管理	防止網頁攻擊	防止資料外洩	安全態勢分析	完善安全體系
核心技術	網路流量分析 網路層協議解析	檔案解析 終端管控 系統漏洞檢測	加密 身分認證 權限管理 AD/LDAP協議	流量清洗 反向代理 網頁漏洞檢測 網頁防禦技術	沙箱作業 文件加解密 資料存取隔離	資訊挖掘 關聯分析 威脅可視化 設備行為分析 使用者行為分析 防護自動化回應	安全框架與體系 資安人員育成 安全回應編排 自動排除網路威脅
解決方案	雲端安全 SASE 郵件防護 防火牆/實體隔離 上網行為管理 入侵偵測防禦 IDPS 虛擬私有網路 VPN 網際資產風險管理	終端設備控管 滲透測試 防毒軟體 資產管理 系統弱點管理 終端檢測與回應 EDR	零信任 生物識別 4A 管理平台 密碼 OTP 特權帳號管理 堡壘機(跳板機) AD 網域安全管理	網頁防竄改 源碼安全檢測 網頁弱點管理 網頁應用防火牆	資料外洩防護 DLP 文件加密 資料庫安全	工控安全 容器安全 威脅情報 蜜罐誘捕 SIEM / SOC 多層式偵測回應 XDR	資安保險 資訊安全顧問服務 資訊安全培訓 資安設備暨 應用服務整合 託管威脅偵測回應 MDR

ZYXEL
Your Networking Ally

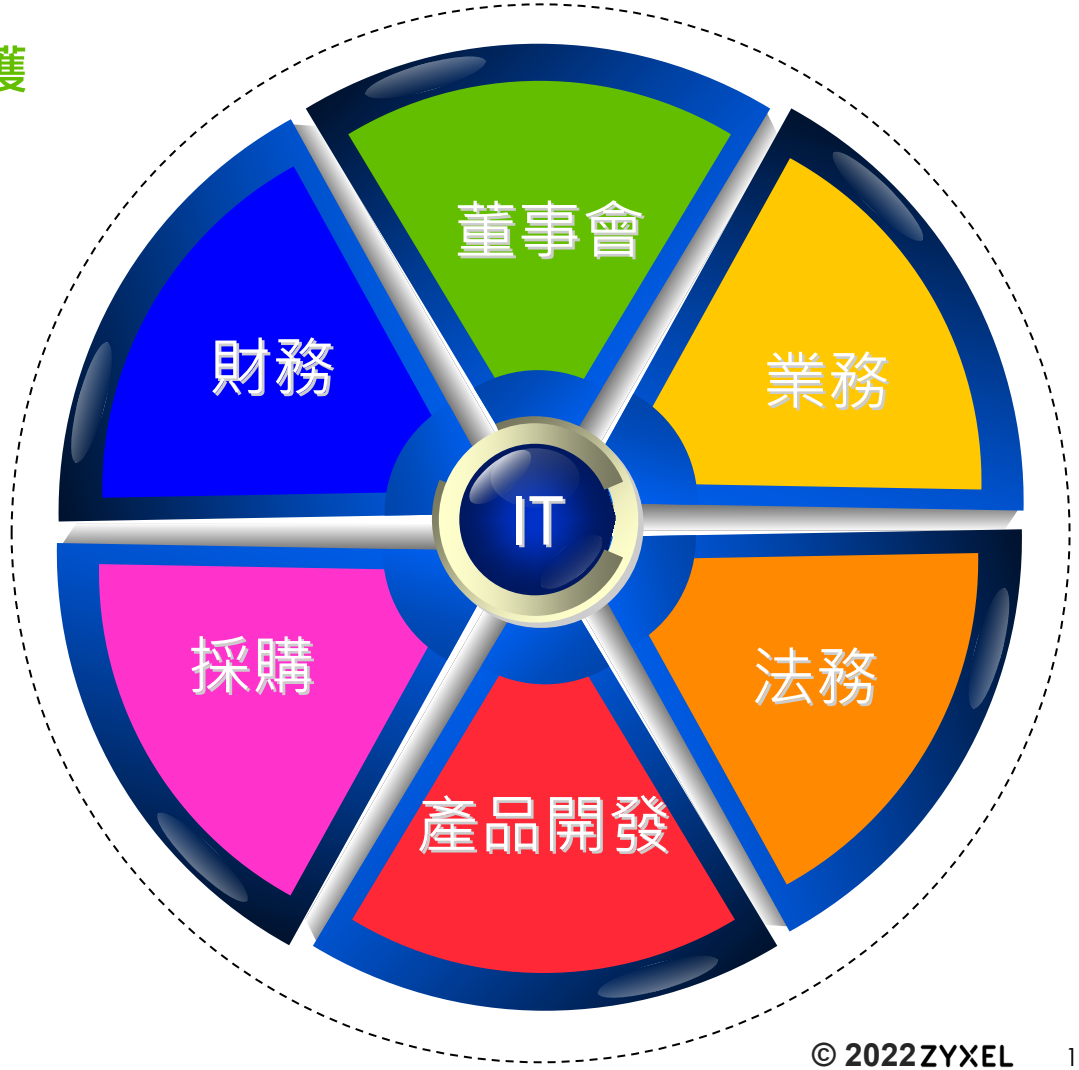
1. 運用商務表達方式影響高階主管看法 (4/4)

- 表達方式 (未來式)：用商業術語來表達即將到來的事情，表明安全是創新中心

合規遵循	ISO 27001、GDPR、BSI TR-03148 CMMC 2.0、EU ENISA				
	識別	保護	偵測	回應	復原
設備	組態管理 弱點管理	防電腦病毒 主機入侵防護	端點鑑識 端點偵測與回應		
應用程式	源碼分析 軟體資產	網頁防火牆 網頁自我防護			
網路	網路封包分析 網路弱點管理	網路防火牆 安全存取服務邊界	網路偵測與回應 抵禦分散式阻斷服務攻擊		
資料	資料稽核 資料分類	加密 權限管理 資料外洩防護	暗網追蹤 威脅情報	數位版權管理	異地備援
使用者	釣魚郵件模擬	社交工程演練 安全意識教育	內部威脅 使用者行為分析		

2. 培養業務上的盟友 (1/4)

- 創造資安被需要的價值，建立深層強韌的商務鏈結
  - 董事會：營運與治理、資訊安全與機密資料保護
  - 業務：客戶開發暨業務推展、供應商資安評鑑
  - 法務：智權管理
  - 產品開發：產品安全管理
  - 採購：供應鏈安全管理、外包產品安全
  - 財務：風險移轉管理
  - 資訊技術：兼具效率暨安全的數位服務



ZYXEL
Your Networking Ally

2. 培養業務上的盟友 (2/4)

- **業務：客戶開發暨業務推展 (合規遵循 CMMC 2.0)**

RA.L2-3.11.2 風險評估 (RA)	相關議題	結果
2 級： 漏洞掃描 定期掃描組織系統和應用程序中的漏洞	高嚴重性漏洞	4
發現影響這些系統和應用程序的新漏洞時進行風險評估	中嚴重性漏洞	X
• NIST SP 800-171 第 2 版 3.11.2	低嚴重性漏洞	X

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED	VULNERABILITY DESCRIPTION
CVE-2021-3711	3.216.xxx.xx	443	Jan 8, 2022 11:53 pm	SM2加密緩衝區溢位漏洞，成功的開採將允許駭客變更應用程式的行為或造成應用程式終止
	3.216.xxx.xx	443	Jan 7, 2022 11:53 pm	
CVE-2021-26691	219.87.xxx.xx	80	Jan 7, 2022 11:53 pm	Apache HTTP Server 组件 mod_session 的漏洞利用可導致記憶體空間損壞，造成服務異常
	60.250.xxx.xx	80	Jan 7, 2022 11:53 pm	

ZYXEL
Your Networking Ally

2. 培養業務上的盟友 (3/4)

- ## 產品開發：產品安全驗證報告

類別	測試工具	測試項目
源碼安全檢測	Checkmarx	源碼靜態安全測試
檢測開啟的服務(port)	Nessus Professional	網路掃描
病毒檢測	ApexOne、OfficeScan、ClamAV	病毒、間諜軟體或蠕蟲掃描
設備防攻擊與防破解	Nessus Professional	設備對應Port使用應用服務弱密碼掃描
	MetaSploit	漏洞測試
	Hydra	暴力破解測試
	Binwalk	韌體檔案entropy，評估是否可被逆向之分析
	Soft Perfect Network Scanner	Samba匿名帳號是否能存取目錄掃描及可用帳號。
	slowhttptest	Web DoS壓力測試工具

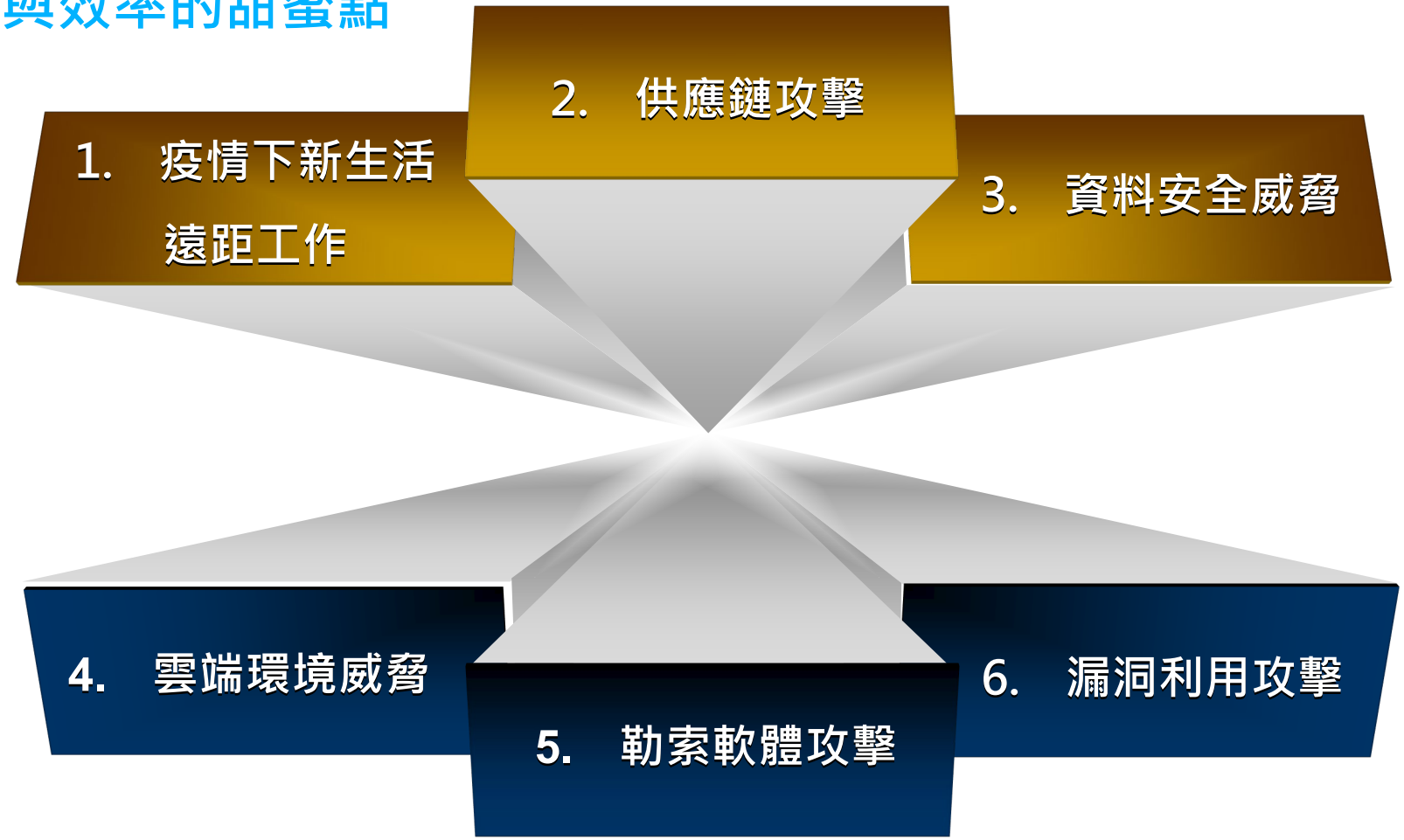
2. 培養業務上的盟友 (4/4)

- 產品開發：產品安全驗證報告

類別	測試工具	測試項目
WEB服務安全檢測	**Nessus Professional**	搭配登入帳號密碼，檢測設備管理網頁內頁弱點或漏洞： 1. 過舊版本 2. 網頁伺服器管理功能使用預設密碼 3. RCE 、Remote Overflow、Buffer Overflow漏洞 4. SQL Injection、XSS、Request Traversal File Access 5. SSL/TLS加密強度
	OWASP ZAP	OWASP Top 10
	BurpSuite	網頁滲透測試
	Chrome - EditThisCookie	Session/Cookie強度

3. 強調正面信息 (1/2)

- 由恐懼、不確定性和懷疑的負面訊息，轉換為對業務及利益相關者的正面資訊
- 找出安全與效率的甜蜜點



ZYXEL
Your Networking Ally

3. 強調正面信息 (2/2)

- 讓業務、營運更安全，不受地域差異與外在威脅而中斷
- 隨著時間的推移跟蹤業務變化。確保風險和安全服務組合和價值描述的有效性

4. 量化安全提供的價值 (1/3)

- 歐盟網路使用者的隱私權保障規範：2018/5/25 生效
  - 最高的罰金為 2 千萬歐元或全球總營業額 4%

amazon 7.46 億歐元

WhatsApp 2.25 億歐元

Google 0.9 億歐元

facebook 0.6 億歐元

Google YouTube 0.6 億歐元

Google 0.5 億歐元

H&M 0.35 億歐元

TIM 0.278 億歐元

enel 0.265 億歐元

BRITISH AIRWAYS 0.22 億歐元

ZYXEL
Your Networking Ally

4. 量化安全提供的價值 (2/3)

- 2021/3/20：宏碁電腦(2353)-上市電腦週邊
- 2021/4/6：日月光投控(3711)_環旭上市半導體
- 2021/4/22：廣達(2382)-上市電腦週邊
- 2021/5/26：威剛科技(3260)-上櫃半導體
- 2021/6/3：翔名科技(8901)-上
- 2021/8/6：技嘉科技(23
- 2021/10/18：帝寶工業(
- 2021/10/19：宏碁電腦(2353)-上市電腦
- 2021/10/27：中鴻(2014)-上市鋼鐵
- 2021/10/29：日勝生(2547)-上市營建
- 2021/11/1：矽格(6257)-上市半導體
- 2021/11/2：京站(2942)-興櫃
- 2021/11/9：雙美實業(4728)-上櫃生技
- 2021/12/20：東元電機(1504)-上市電機
- 2021/12/20：東捷資訊(6697)-上櫃資訊服務
- 22：台達電(2308)-上市電子零組件
- 環球晶(6488)-上櫃半導體
- 16：健鼎(3044)-上市電子零組件
- 022/7/ 鈺創(5351)-上櫃半導體
- 2022/7/18：永昕(4726)-上櫃生技
- 2022/7/22：台灣虎航(6757)-興櫃

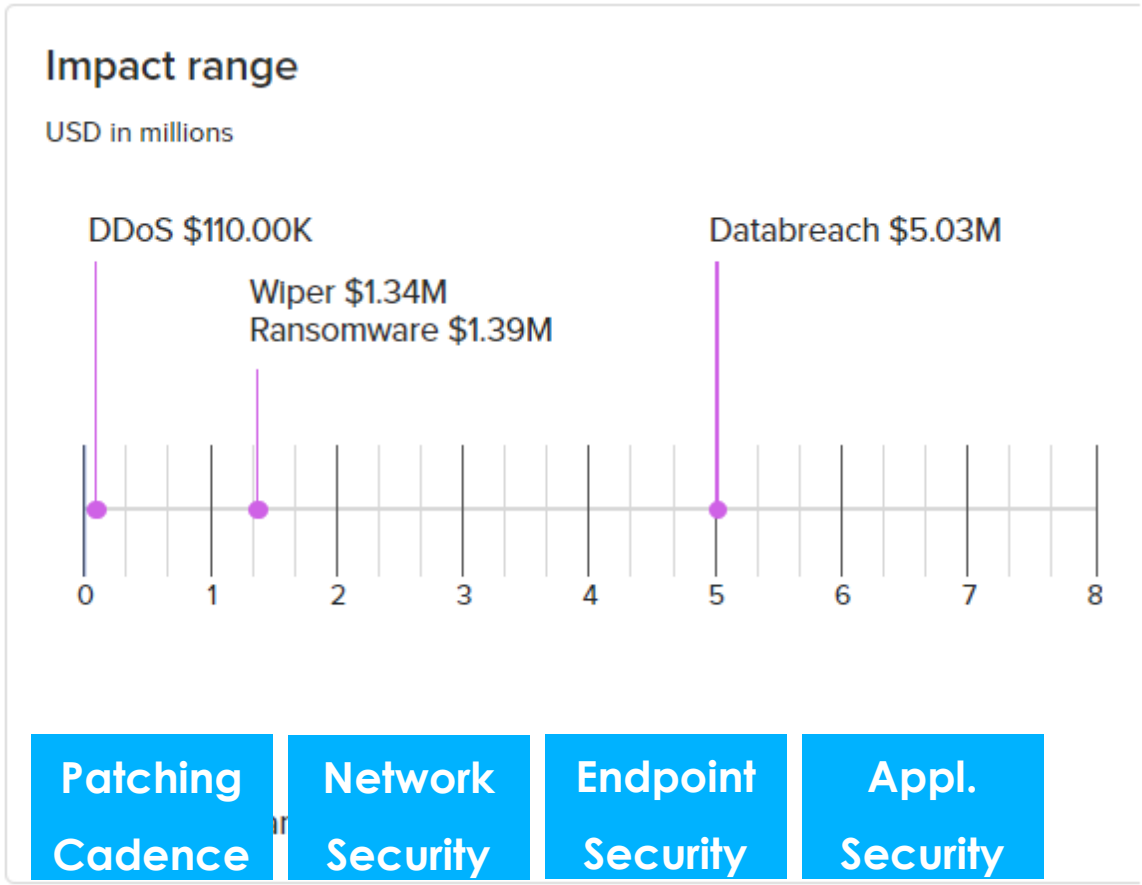
營運中斷損失 (可量化)

機敏資訊竊取 (無法量化)

資料來源：台灣證券交易所資訊觀測站

4. 量化安全提供的價值 (3/3)

- 資安風險量化工具 FAIR(Factor Analysis of Information Risk) Methodology
  - 業務運營中斷、勒索贖金、法律費用、名譽受損、法規罰金



Estimated financial impact

Data breach	DDoS	Ransomware	Wiper
$5.03M	$110.00K	$1.39M	$1.34M

Probability of compromise

Data breach	DDoS	Ransomware	Wiper
1.00%	48.64%	**77.04%**	**77.04%**

Predicted frequency in years

Data breach	DDoS	Ransomware	Wiper
1 out of 20	**1 out of 20**	1 out of 34	1 out of 34

資料來源：SecurityScorecard & ThreatConnect

5. 讓安全成為商務競爭差異化要素 (1/3)

- 德國政府資安監管單位 BSI (聯邦資訊安全辦公室) 於 2018 年 11 月公佈的 Technical Guideline for Secure Broadband Routers
  - ZYXEL 與 LANCOM、Deutsche Telekcom 符合 BSI 制定的Router 技術指南 (BSI TR-03148) 標準，大幅提高產品的安全級別

Companies support the technical guidelines for broadband routers

date December 14, 2018

Manufacturers and Internet providers want to implement the technical guidelines for secure broadband routers of the Federal Office for Information Security (BSI). In the past few weeks, Lancom , Deutsche Telekom and Zyxel have publicly announced their support for the " Router - TR " published on November 16, 2018 . This means that the security standards formulated by the BSI are implemented in practice and considerably increase the IT security level for users. The BSIalso assumes that the companies will continue to participate in the further development of the document regardless of the outcome of individual discussion points and thus ensure more security in the digital world. The Router - TR is thus a first step towards the implementation of sustainable risk management.

Because technical guidelines of the BSI generally have a recommendatory character, the implementation is router - TR not mandatory for manufacturers and Internet service providers. The basic acceptance of the router - TR therefore plays a central role. This also had to be weighed up again and again during the discussions in the working group that created it. The manufacturers and Internet providers have shown a willingness to compromise on many points in order to be able to encapsulate the entire range of existing solutions in a reliable standard.

The BSI TR -03148 " Router - TR " was discussed controversially after its publication. These had BSI already on November 21 adopted a position . The public debate ties in almost seamlessly with the intensive discussions that had already taken place within the working group.

5. 讓安全成為商務競爭差異化要素 (2/3)

- 德國政府資安監管單位 BSI (聯邦資訊安全辦公室)
  - 2022 年 5 月公佈
  - 兩款 Zyxel 產品已通過 BSI “Secure Broadband Routers” (TR-03148) 認證

Federal Office
for Information Security

Certificate

according to Technical Guidelines of the Federal Office for Information Security

BSI-K-TR-0500-2022

Digitalisierungsbox Premium 2
HW: GX5502-D0-DE02V1F
SW: 16.40.2.09.01

from	Zyxel Deutschland GmbH
Conformity to:	**BSI TR-03148** - Secure Broadband Router, Version 1.1
Valid until:	09 Mai 2027

Federal Office
for Information Security

Certificate

according to Technical Guidelines of the Federal Office for Information Security

BSI-K-TR-0499-2022

Digitalisierungsbox Smart 2
HW: GX3502-D0-DE02V1F
SW: 16.40.2.09.01

from	Zyxel Deutschland GmbH
Conformity to:	**BSI TR-03148** - Secure Broadband Router, Version 1.1
Valid until:	09 May 2027

5. 讓安全成為商務競爭差異化要素 (3/3)

- 安全的傳統任務是確保公司免遭駭客攻擊，現在安全成為擴大業務的推動要素

6. 轉型成為資安新創公司 (1/2)

1. 網際網路資產暨曝險分析
2. 弱點掃描、滲透測試、原碼檢測

KALI LINUX · Nessus vulnerability scanner · OpenVAS · Atomic Red Team · OWASP · Checkmarx

3. Active Directory 安全檢測
4. 防毒、資安、網路設備日誌整合
5. Windows、Linux、MacOS、應用服務日誌整合

Agent based	Agentless
Windows Event Log	SNMP
Linux Audit Log	Syslog
MacOS Audit log	Flow (Net Flow / sFlow)
Endpoint Detection Response	
Software Asset Mgmt.	
Patch Management	
Performance Metrics	

6. 資訊收集器

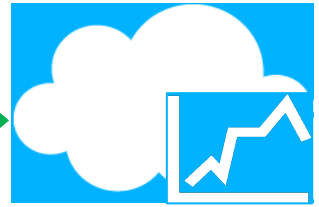
系統弱點、日誌、效能、系統組態、軟體資產

營運管理

7. 資安管理儀表板

攻擊軌跡追蹤

事件報告分析



建議

防護

對策

8. 執行對策並追蹤效果

人員 網路 終端 應用

紀律 設備 服務

6. 轉型成為資安新創公司 (2/2)

SOC – 安全運營中心

專職的安全運營 (SecOps) 團隊持續監控、分析和回應安全事件

XDR – 擴展檢測和回應

- 蒐集並分析多個防護層的威脅偵測事件
  - 電子郵件、端點、伺服器、網路及資安設備
  - 提高 IT 系統維運、網路暨應用的管理效率

SIEM – 安全資訊和事件管理

- SOC的技術骨幹：集中式日誌管理
  - 應用程序、系統、服務器等日誌整合
- 即時關聯分析、溯源調查與研擬對策

ZYXEL
Your Networking Ally

結語

- 將風險和安全服務情況以量化圖表展現，向董事會、經營階層呈現產品暨網路安全的價值，證明資訊安全確實“值錢”

ZYXEL

Your Networking Ally