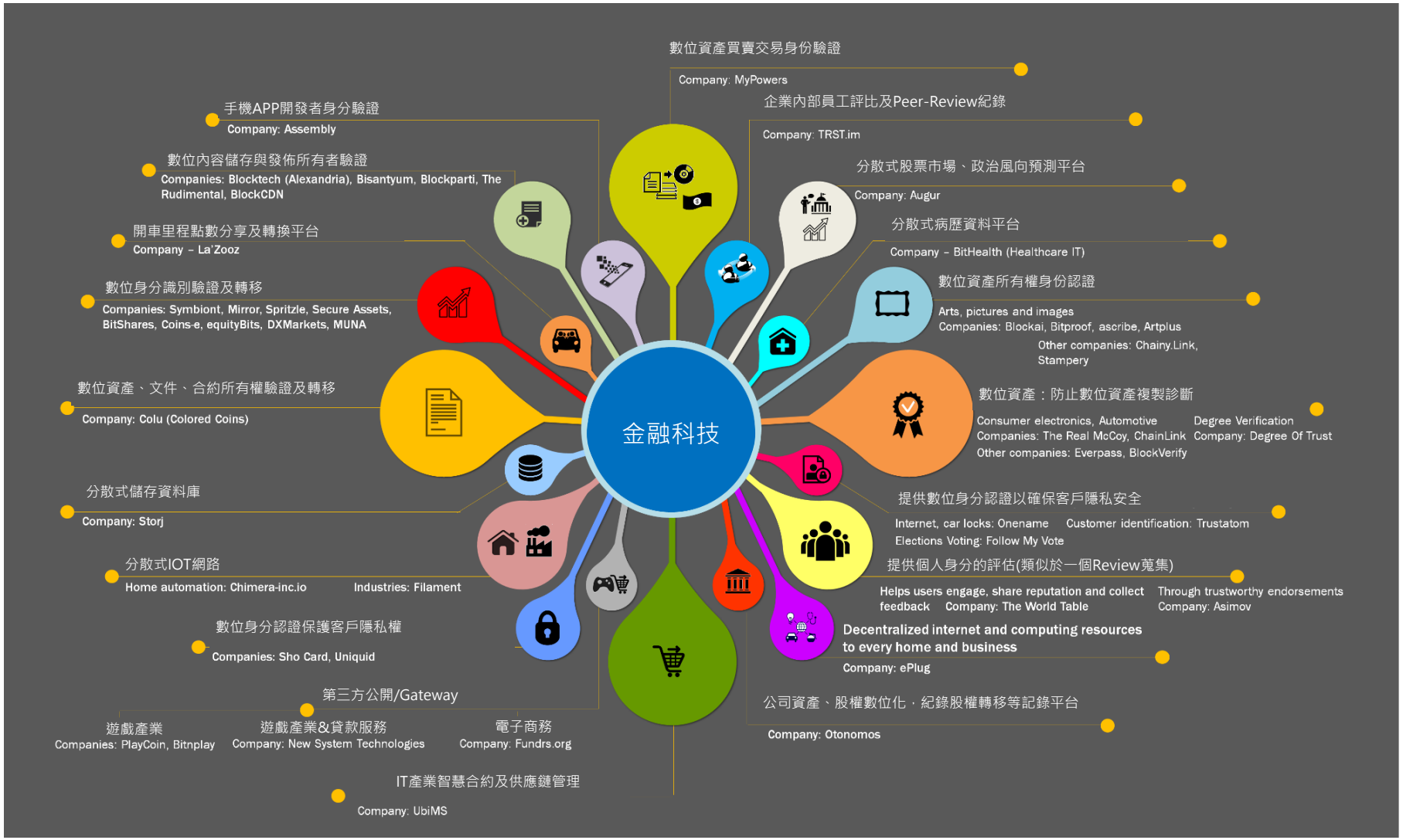
Deloitte.

勤業眾信

產業視野下的 InfoSec

勤業眾信風險管理諮詢股份有限公司　萬幼筠 總經理

充滿無限可能的金融科技生態系



Fintech改變現在金融面貌的重點 – 金融應用 (或說使用者體驗UX)

既有業務

保險業務

- 壽險：死亡生死合險、傷害、健康、年金
- 產險：新險種、天災、運輸、汽車、意外、工程

銀行業務

- 消費金融：授信、募資
- 企業金融：國際金融業務、外匯與匯兌、支付與信用卡、存款、投資理財與信託、債券、憑證與衍商

證券業務

經紀業務、借券業務、融資業務、股務代理

影響重點

- 保險供應鏈重組，普惠保險、社群化、平台化
- 改變資金來源，媒合機制與信用評等平台化
- 無現金、數據驅動、平台化、低交易成本
- 利用科技，改變服務供應方式，提升效率
- 交易基礎架構，數據精細化應用、平台化

新興商業模式

- 線上(社群)保險：friendsurance、metromile、众安保险
- P2P保險：宏利 Manulife、MOVE
- IOT保險
- P2P借貸：SHAcom、鄉民貸
- 群募：flyingV
- 新型支付：歐付寶 allPay、GASH PAY 樂點行動支付、TWQ台灣支付
- 機器人理財與零售演算交易平台：fiserv.、wealthfront
- 新型交易平台：motif、Nasdaq、FRS 基富通、Overstock.com

技術

社群技術、物聯網、雲端運算、身分識別技術、行動技術、機器學習、大數據、區塊鏈

隨著Fintech發展與金融面貌的改變，資安議題不斷擴大影響範圍

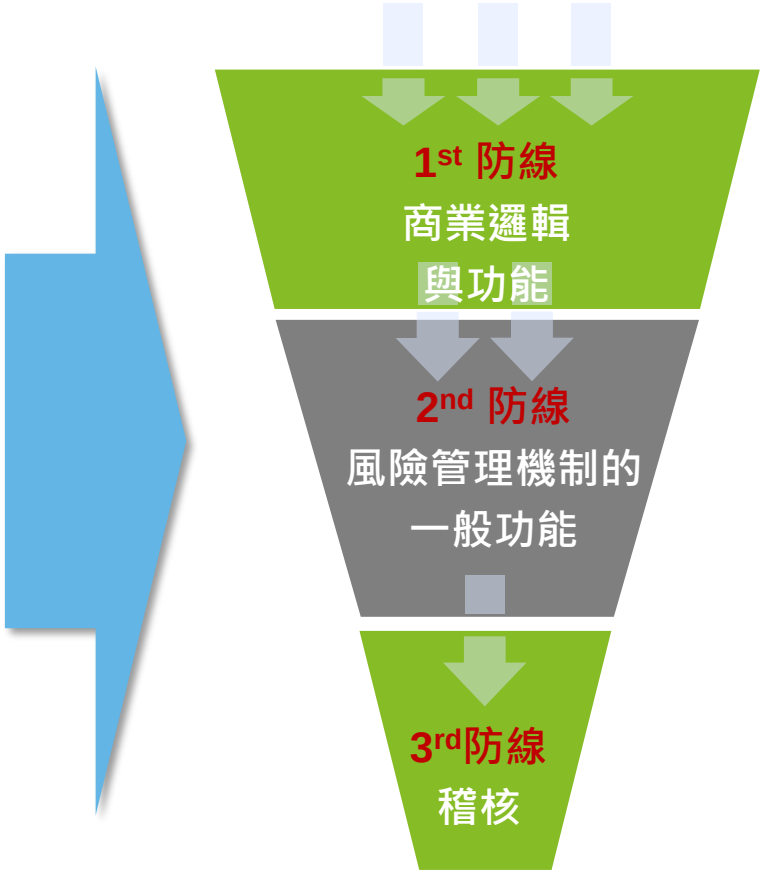
01 金融科技環境下，所謂的傷害概念早已不僅限於金錢

02 攻擊的速度與頻率不斷提升，而應對的時間要求也越來越短

03 所有的事、物都不再能用一種大一統的標準來防護

04 傳統的控制仍然是必要的，卻早已不再夠用

05 法規成了最關鍵的聚焦所在



角色與責任
• 將基於風險之決策整合於企業日常營運與風險管理程序 • 定義風險胃納與風險容忍程度 • 降低風險
• 建立治理與監管機制 • 設定風險基線、管理政策、管理標準 • 導入適用之工具與程序 • 監控並呼叫應存/續之活動 • 提供監管、諮詢、檢核、狀態、企業層級之政策與標準
• 獨立審查相關專案/程序/機制有效性 • 對董事會提供風險管理有效性之確認情況 • 達成相關檢管單位要求之保密義務，同時包括金融與資安，甚至國安層面

Fintech的主要資安議題在於資料(數據)與治理

既有業務

- **保險業務**
  - 壽險：死亡生死合險、傷害、健康、年金、新險種
  - 產險：天災、運輸、汽車、意外、工程
- **銀行業務**
  - 消費金融：授信、募資、國際金融業務、外匯與匯兌、支付與信用卡、存款
  - 企業金融：投資理財與信託、債券、憑證與衍商
- **證券業務**：經紀業務、借券業務、融資業務、股務代理

新興商業模式

線上(社群)保險、P2P保險、IOT保險、P2P借貸、群募、新型支付、機器人理財與零售演算交易平台、新型交易平台

技術

社群技術、物聯網、雲端運算、身分識別技術、行動技術、機器學習、大數據、區塊鏈

Fintech的發展多變且複雜，風險管理與資本計提的適當性仍是監管的重點，並利用技術發展事件分析與回應的機制

1 業務識別

重新辨識Fintech業務內涵，對應或新增既有業務的範疇

2 風險辨識

人員、流程、系統、外部事件

3 分析回應

分析事件根因、衝擊影響與風險回應機制(損失事件)

資安事件持續頻傳，技術挑戰? 管理挑戰? 組織設計/職能不足挑戰?

Organizations spent

$ 75.4 billion

On information Security in 2015

According to Gartner

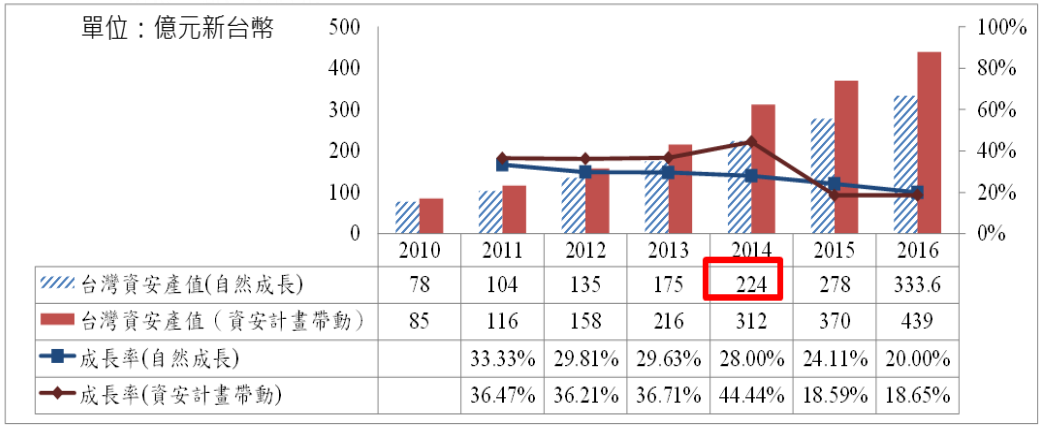
http://technews.tw/2015/09/23/gartner-information-security-cost-in-2015/

Gartner：2015年全球資安支出成長4.7%

國際研究暨顧問機構Gartner發布最新預測指出，2015年全球資訊安全支出將達754億美元，年成長4.7%；支出成長動力主要來自政府專案、更多法律制定及多起重大資料外洩事件。

Gartner指出，數位化企業正逐漸影響人們對資安技術的興趣，尤其是雲端、行動運算以及今日的物聯網。

- 2014年台灣資安產值年增率約44.44% ,台灣資安產值達新台幣312億元



	2010	2011	2012	2013	2014	2015	2016
台灣資安產值(自然成長)	78	104	135	175	224	278	333.6
台灣資安產值（資安計畫帶動）	85	116	158	216	312	370	439
成長率(自然成長)		33.33%	29.81%	29.63%	28.00%	24.11%	20.00%
成長率(資安計畫帶動)		36.47%	36.21%	36.71%	44.44%	18.59%	18.65%

資料來源：MIC，2014年11月

資安挑戰的艱難在於破壞呈現組織化, 從個人漫延到國家與產業

稜鏡計畫簡介（NSA’ S PRISM）

- PRISM的前身是小布希任內在九一一事件後的恐怖分子監聽計劃。在當時這個計劃曾遭到廣泛批評，且其合法性因未經過外國情報監視法庭（Foreign Intelligence Surveillance Court）批准而受到質疑，但之後的PRISM則得到了該法庭的授權令。在歐巴馬任內，國家安全局持續運作PRISM

解密

- 共有四項大型情報偵蒐計畫，除了日前被史諾登揭露的「稜鏡」計畫之外，還有另三項稱為「大道」（Main-way）、「船塢」（Marina）與「核子」（Nucleon）計畫

	Content	Metadata
Telephone	NUCLEON	MAINWAY
Internet	PRISM	MARINA

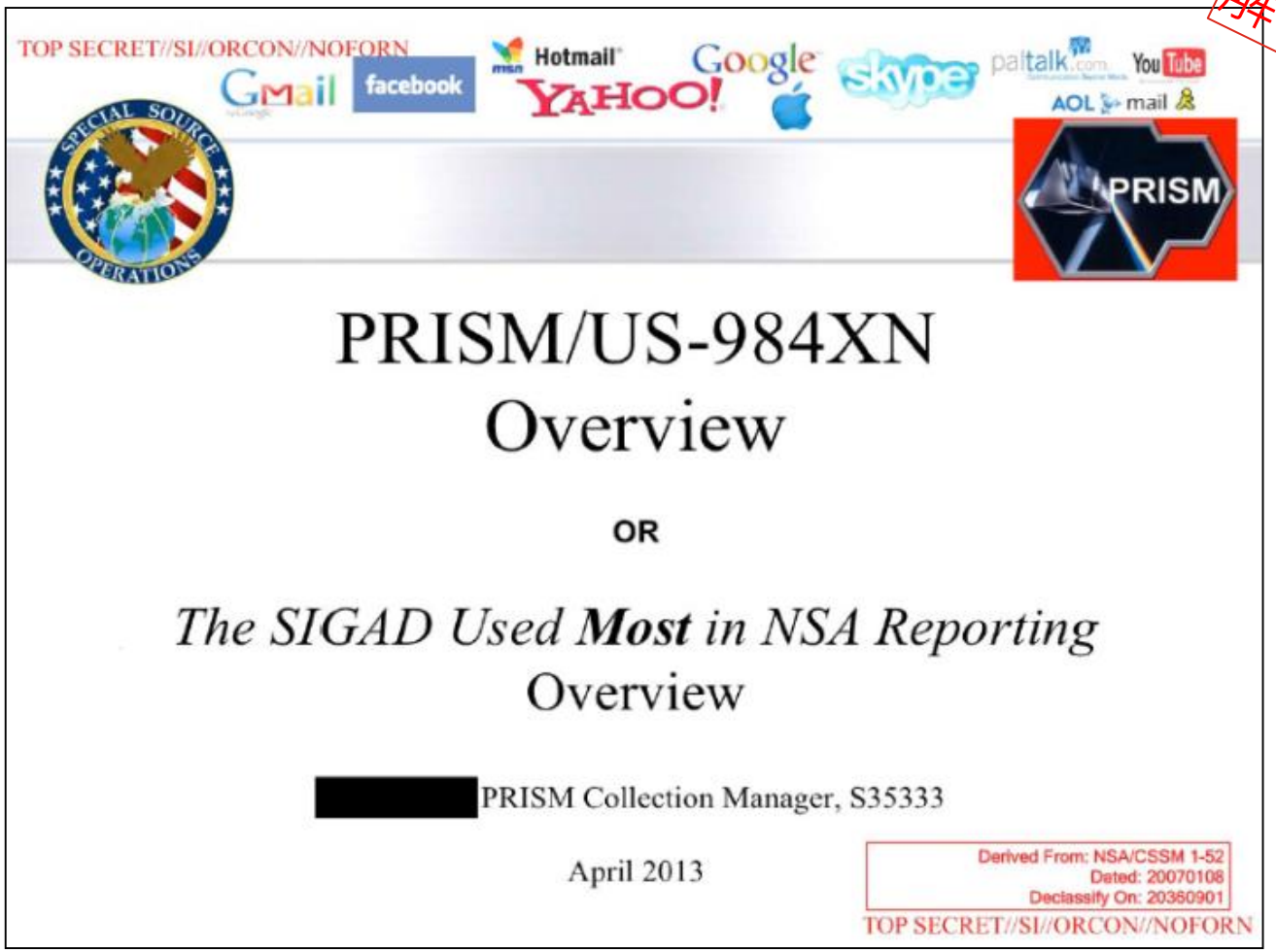
MARINA captures “digital network information” — DNI – including metadata for email, chat, etc. It is the biggest of NSA’s programs.

Plans Since 2007

PRISM | Boundless Informant | X-Keyscore | Dropmire | Fairview | Surveillance Detection Unit | Bullrun | GCHQ | collaboration | MUSCULAR | IMP | Tempora | Mastering the Internet | **Global Telecoms Exploitation** Discontinued Trailblazer Project | ThinThread | President's Surveillance Program (Terrorist Surveillance Program, STELLARWIND)

7

這就是稜鏡計畫



美國國家安全局洩露出的PRISM電子監聽計劃概說的簡報投影片

稜鏡計畫（PRISM）是一項由美國國家安全局自2007年起開始實施的絕密級電子監聽計劃。該計劃的正式名稱為「US-984XN」。

8

這就是稜鏡計畫 (續)

解密

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past. (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page: Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Case Notations

P2ESQC120001234

PRISM Provider	Fixed trigraph, denotes PRISM source collection	Year CASN established for selector	Serial #
P1: Microsoft P2: Yahoo P3: Google P4: Facebook P5: PalTalk P6: YouTube P7: Skype P8: AOL PA: Apple			

Content Type

A: Stored Comms (Search)
B: IM (chat)
C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
D: RTN-IM (real-time notification of a chat login or logout event)
E: E-Mail
F: VoIP
G: Full (WebForum)
H: OSN Messaging (photos, wallposts, activity, etc.)
I: OSN Basic Subscriber Info
J: Videos
. (dot): Indicates multiple types

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//COMINT//REL TO USA, FVEY

Selector Types

Machine IDs
- Cookies
  - Hotmail GUIDs
  - Google prefIDs
  - YahooBcookies
  - mailruMRCU
  - yandexUid
  - twitterHash
  - ramblerRUID
  - facebookMachine
  - doubleclickID
- Serial numbers
- Browser tags
  - Simbar
  - ShopperReports
  - SILLYBUNNY
- Windows Error IDs
- Windows Update IDs

Attached Devices
- IMEIs for Phones
  - Apple IMEIs
  - Nokia IMEIs
- UDIDs
  - Apple UDIDs
- Bluetooth?
  - Device Name
  - Device Address

Cipher Keys
- Cipher Keys uniquely identified to a user
  - ejKeyID

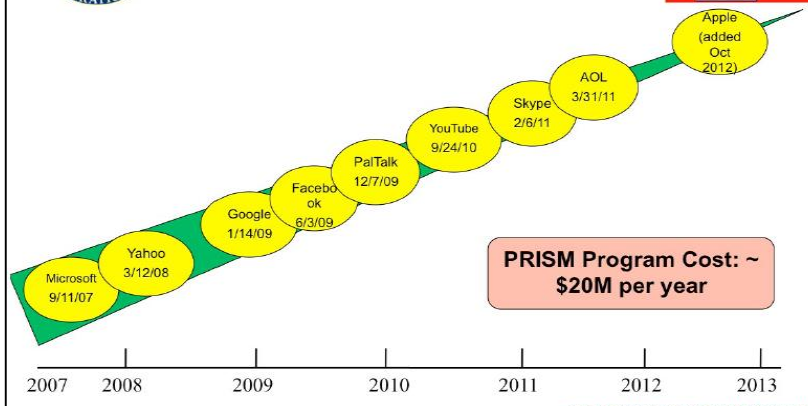
User Leads
- User selectors from Cookies, Registry, and Profile Folders
  - msnpassport
  - google
  - yahoo
  - Youtube
  - Skype
  - Paltalk
  - Fetion
  - QQ
  - hotmailCID
- STARPROC-identified active users

Network
- Wireless MACs
- VSAT MACs and IPs
- Remote Administration IPs
  - Putty
  - WinSCP

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

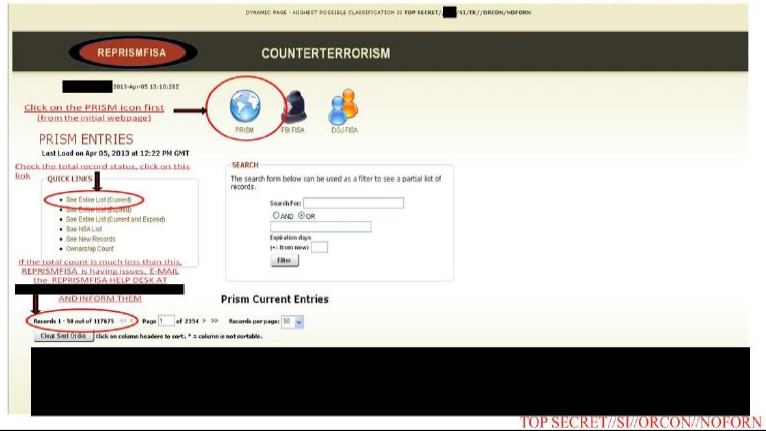


PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) REPRISMFISA TIPS [redacted]



TOP SECRET//SI//ORCON//NOFORN

虛實整合，Fintech安全議題恐將延伸為金融犯罪問題

策略

- 六大面向之策略分析
- 金融犯罪風險之司法剖繪
- 加速發展的規劃藍圖

人員管理

- 中小企業與專家證人
- 工作內容、執掌與權責設計
- 高階管理階層與合規性之對應
- 員工舞弊

治理與外部報告

從以下管道幫助保戶報告或減輕罰款、起訴：

- 執法機構
- 監管機構
- 有牌照之機構
- 政府機構

運作與流程

- 工作流程與權責
- 控制與權限
- 業務流程再造
- 程序與政策之落實

法令遵循

- 符合法規
- 擬定內容包含義務的政策
- 定期獨立審查
- 資訊系統管理

數據質量與分析

- 數據與蒐集目的之吻合度
- 跨越六大面向之數據應用
- 數據掃描
- 建構數據儀表板或數據監控系統

2016年來全球各地金融相關行業仍然持續不斷遭遇挑戰

2016

孟加拉中央銀行遭駭客盜領**8,100**萬美金

香港匯豐、中銀8證券戶口遭入侵，未经授权的股票交易涉款686萬

越南先鋒銀行險遭駭客轉走 120 萬歐元

DAO遭駭客領走逾**360**萬個以太幣，總價約**7200**萬美元

某銀行**ATM**被駭，歹徒盜領鉅額新台幣

OBU亂象多，金管會重罰**7**銀行

1月 2月 3月 4月 5月 6月 7月 8月 9月

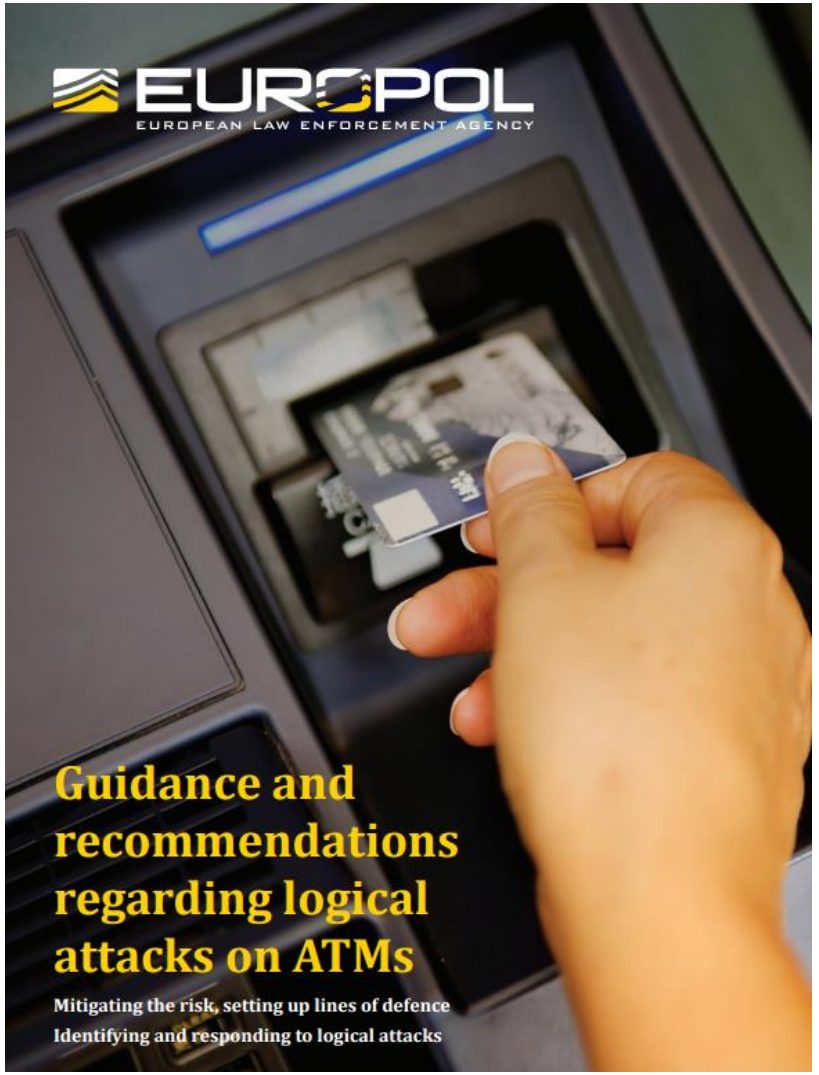
英國匯豐銀行因遭到DDoS攻擊，導致網路銀行停止服務近整個營業日

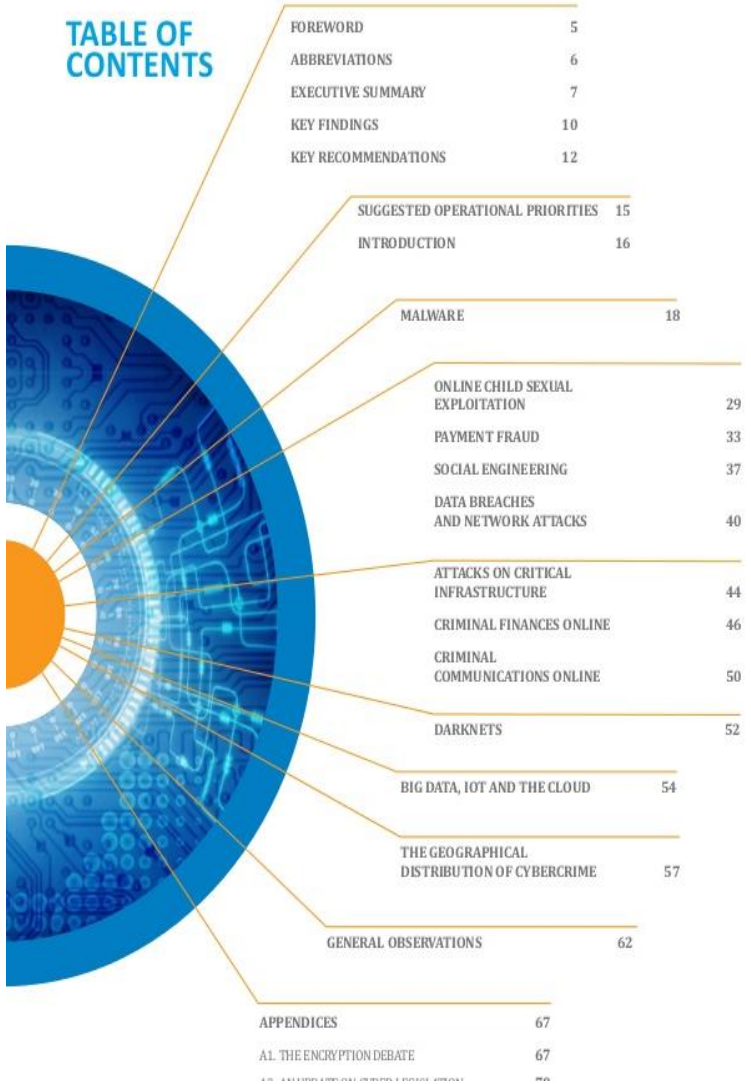
日本**Seven**銀行、**Enet**銀行、郵局等提款機遭盜領**18.6**億日圓

香港**Bitfinex**遭竊，損失近**12**萬比特幣，約**7800**萬美元

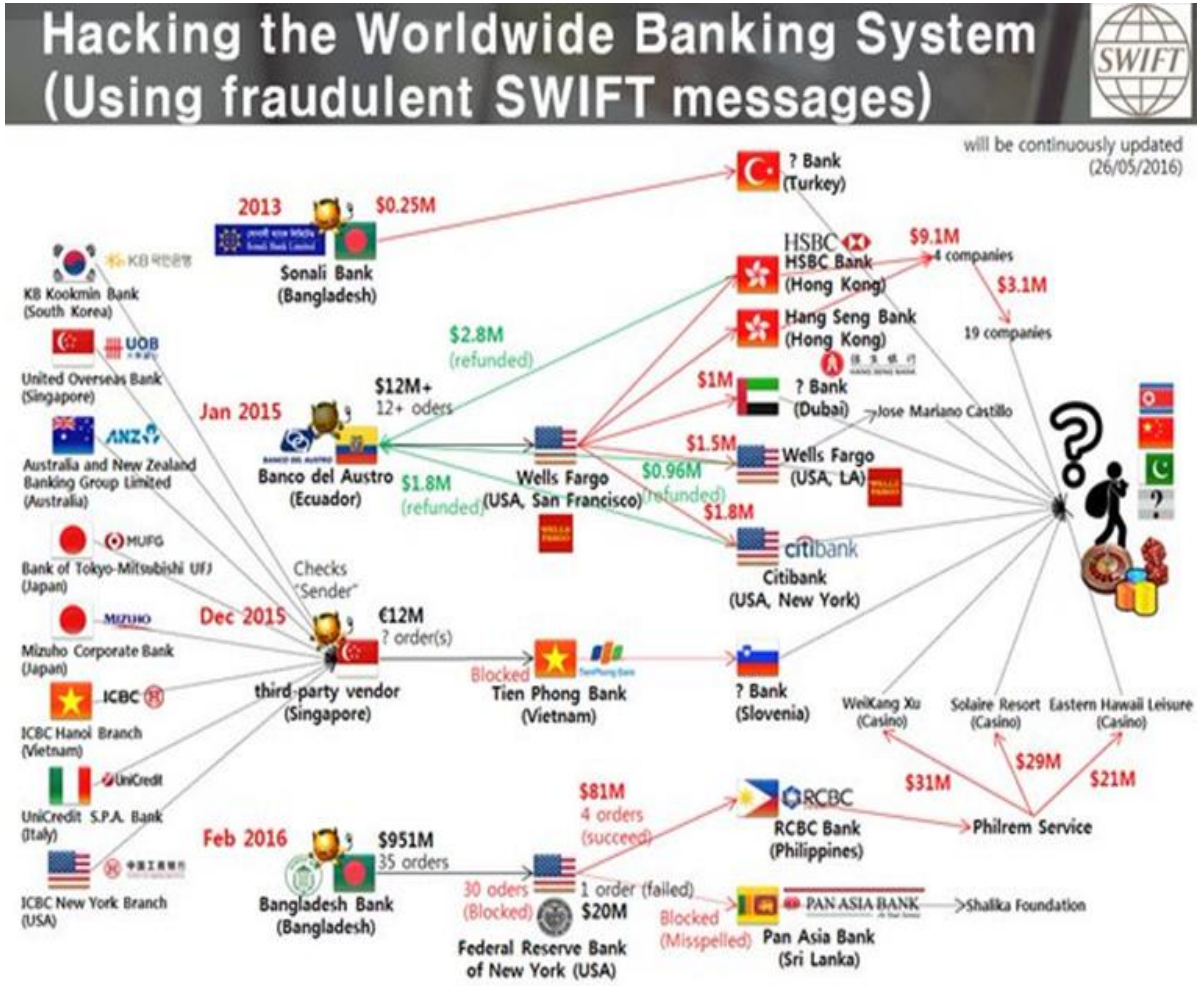
菲律賓**RCBC**因孟加拉央行盜領延伸的洗錢案，被菲律賓央行裁罰十億披索

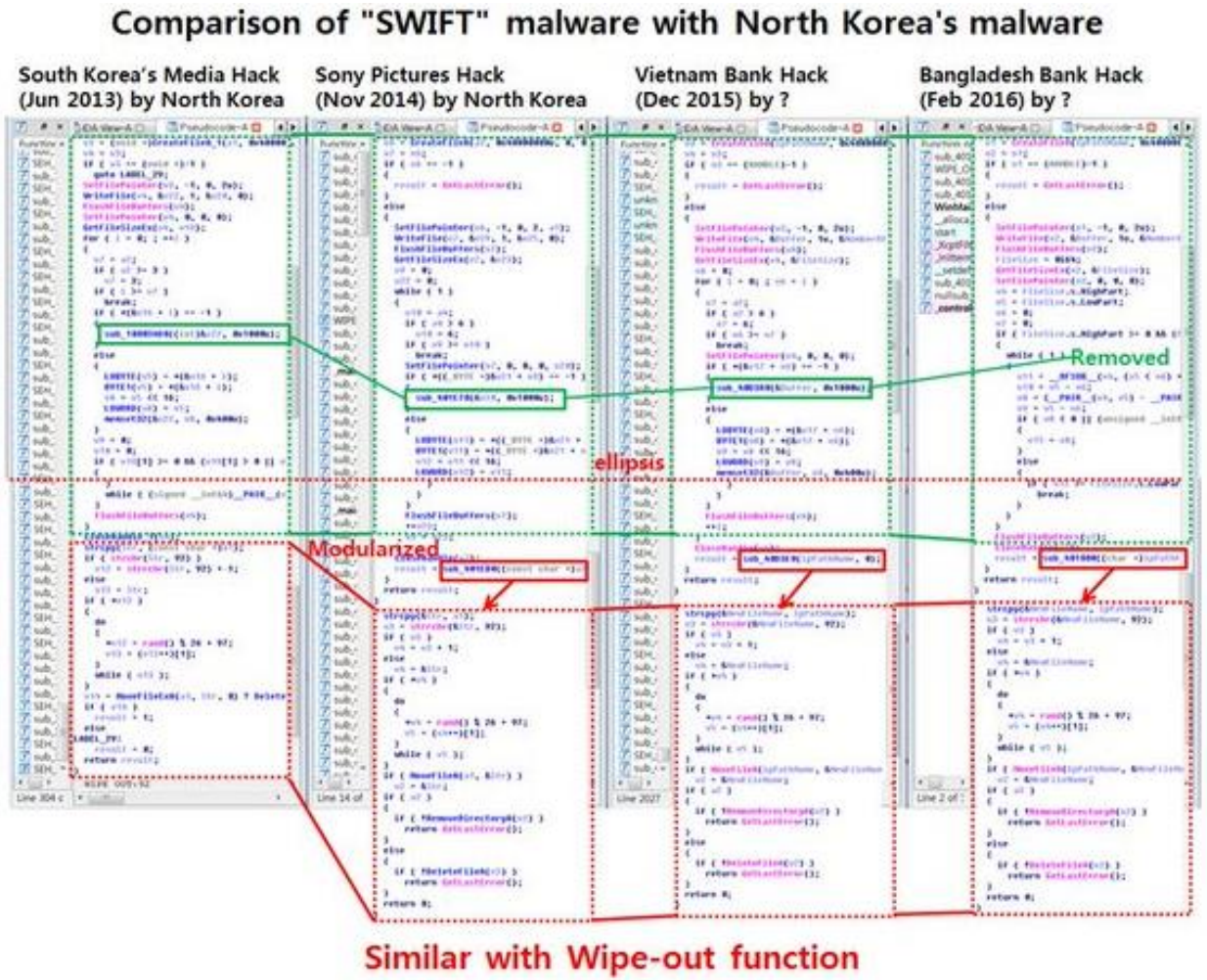
歐盟警察總署Fintech 犯罪系列研究





SWIFT 攻擊分析





Fintech是機會？還是風險？ (即便監理沙盒也不bypass)

策略風險

眾多的Fintech發展選項，產業競爭，自行發展、併購/結盟的策略，以及國際趨勢與本地市場的綜觀

法規遵循與治理風險

新商業模式面對主管機關的不確定性，以及對於產業法規遵循之調適

作業暨財務風險

無論是既有流程之效率化，或是商業模式創新，應考量既有控管是否有效降低作業與財務 (如信用)風險

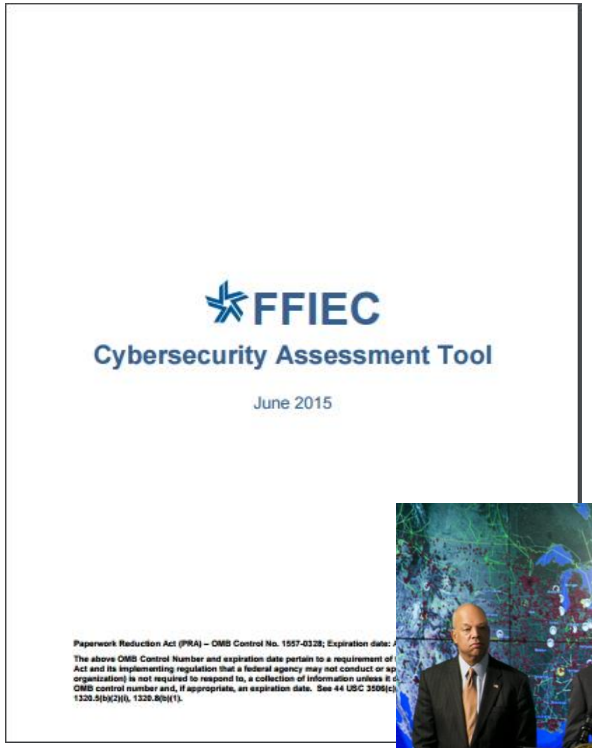
資料治理風險

因應資料驅動、資料管理與分析，以及於數位化過程中，面臨之個資管理與機密資料風險

網路與資訊治理風險

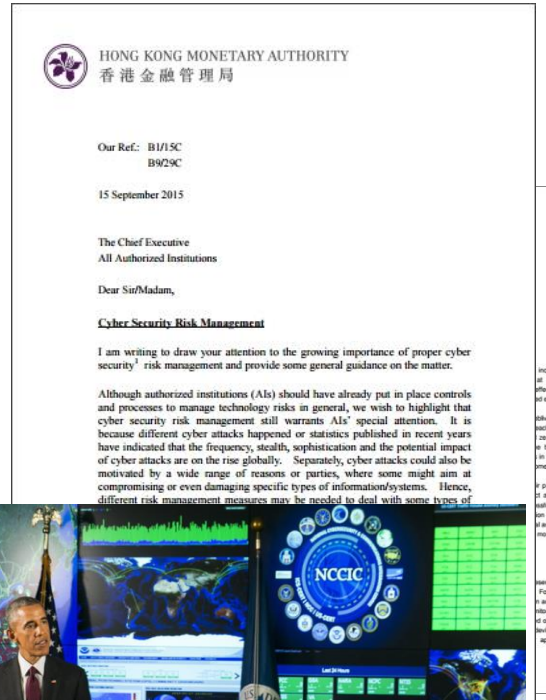
社群、行動、雲端與物聯網特性，讓企業更趨數位化，也面臨更多的網路安全曝險

全球主要金融監理機構紛紛發布金融科技Cyber Security相關要求
(日本與香港均採用)


FFIEC

Cybersecurity Assessment Tool

June 2015


HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

15 September 2015

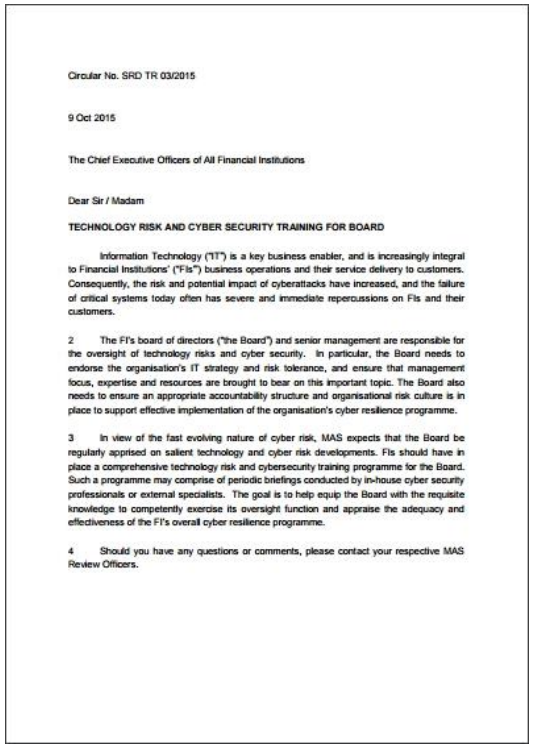
The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Cyber Security Risk Management

I am writing to draw your attention to the growing importance of proper cyber security[1] risk management and provide some general guidance on the matter.

Although authorized institutions (AIs) should have already put in place controls and processes to manage technology risks in general, we wish to highlight that cyber security risk management still warrants AIs' special attention. It is because different cyber attacks happened or statistics published in recent years have indicated that the frequency, stealth, sophistication and the potential impact of cyber attacks are on the rise globally. Separately, cyber attacks could also be motivated by a wide range of reasons or parties, where some might aim at compromising or even damaging specific types of information/systems. Hence, different risk management measures may be needed to deal with some types of


Circular No. SRD TR 03/2015

9 Oct 2015

The Chief Executive Officers of All Financial Institutions

Dear Sir / Madam

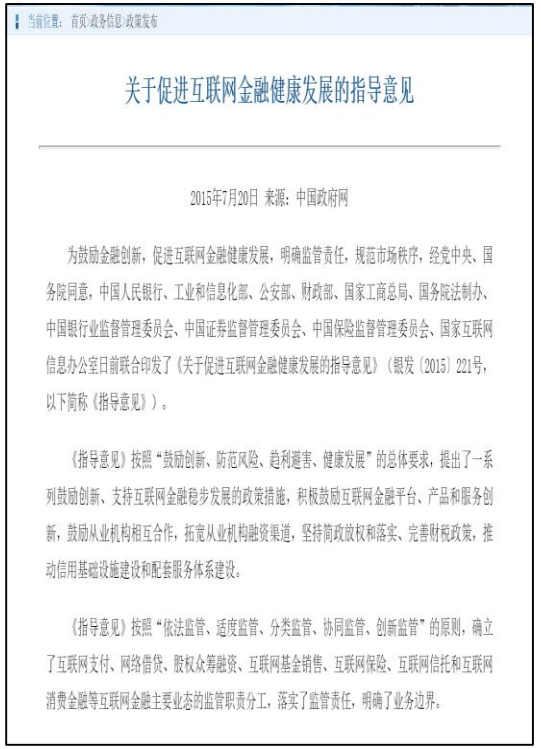
TECHNOLOGY RISK AND CYBER SECURITY TRAINING FOR BOARD

Information Technology ("IT") is a key business enabler, and is increasingly integral to Financial Institutions' ("FIs") business operations and their service delivery to customers. Consequently, the risk and potential impact of cyberattacks have increased, and the failure of critical systems today often has severe and immediate repercussions on FIs and their customers.

2 The FI's board of directors ("the Board") and senior management are responsible for the oversight of technology risks and cyber security. In particular, the Board needs to endorse the organisation's IT strategy and risk tolerance, and ensure that management focus, expertise and resources are brought to bear on this important topic. The Board also needs to ensure an appropriate accountability structure and organisational risk culture is in place to support effective implementation of the organisation's cyber resilience programme.

3 In view of the fast evolving nature of cyber risk, MAS expects that the Board be regularly apprised on salient technology and cyber risk developments. FIs should have in place a comprehensive technology risk and cybersecurity training programme for the Board. Such a programme may comprise of periodic briefings conducted by in-house cyber security professionals or external specialists. The goal is to help equip the Board with the requisite knowledge to competently exercise its oversight function and appraise the adequacy and effectiveness of the FI's overall cyber resilience programme.

4 Should you have any questions or comments, please contact your respective MAS Review Officers.


当前位置：首页>政务信息>政策发布

关于促进互联网金融健康发展的指导意见

2015年7月20日 来源：中国政府网

为鼓励金融创新，促进互联网金融健康发展，明确监管责任，规范市场秩序，经党中央、国务院同意，中国人民银行、工业和信息化部、公安部、财政部、国家工商总局、国务院法制办、中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会、国家互联网信息办公室日前联合印发了《关于促进互联网金融健康发展的指导意见》（银发〔2015〕221号，以下简称《指导意见》）。

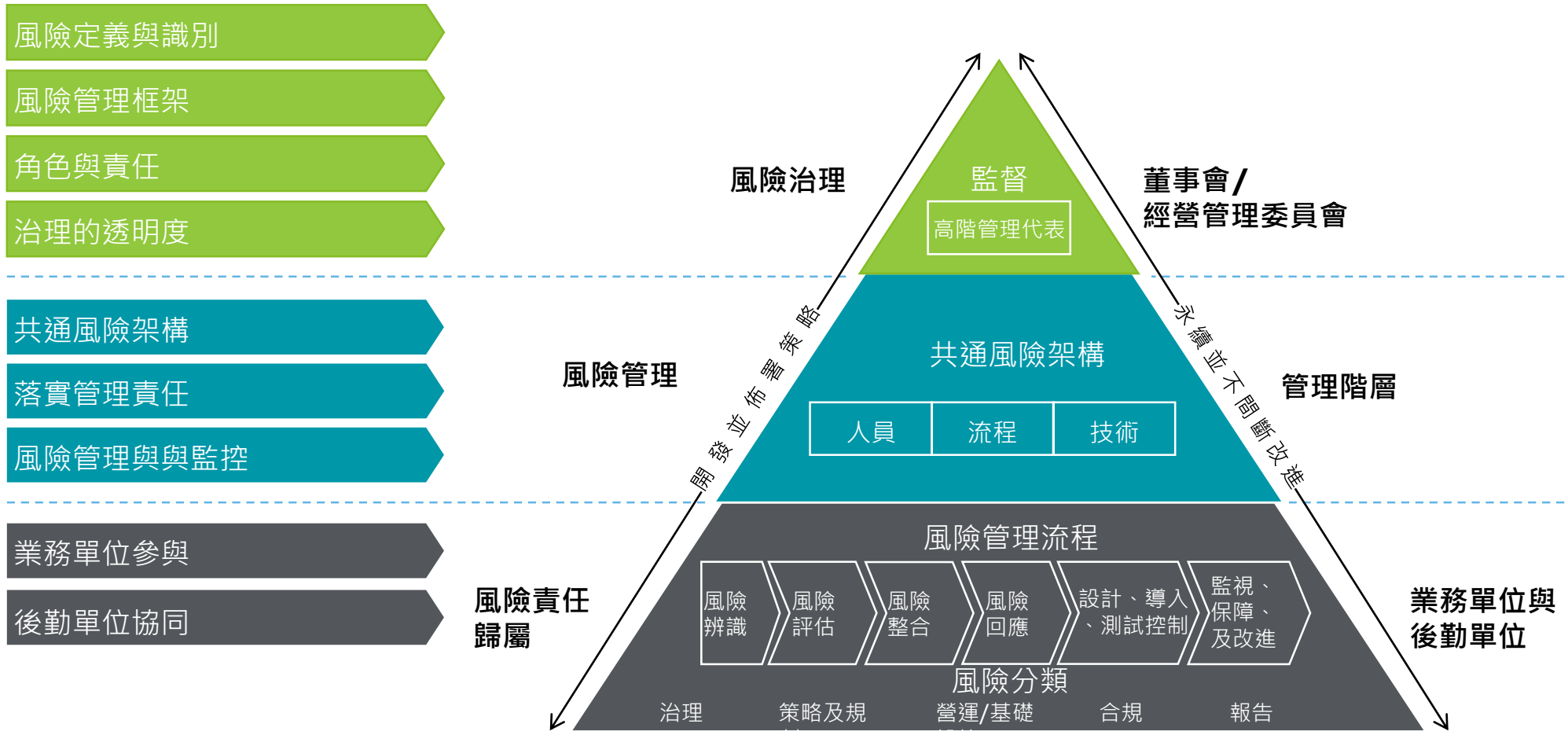
《指导意见》按照“鼓励创新、防范风险、趋利避害、健康发展”的总体要求，提出了一系列鼓励创新、支持互联网金融稳步发展的政策措施，积极鼓励互联网金融平台、产品和服务创新，鼓励从业机构相互合作，拓宽从业机构融资渠道，坚持简政放权和落实、完善财税政策，推动信用基础设施建设和配套服务体系建设。

《指导意见》按照“依法监管、适度监管、分类监管、协同监管、创新监管”的原则，确立了互联网支付、网络借贷、股权众筹融资、互联网基金销售、互联网保险、互联网信托和互联网消费金融等互联网金融主要业态的监管职责分工，落实了监管责任，明确了业务边界。

美國政府除設置網路安全部門、網路威脅情報整合中心、資安長外，2017年資安預算達190 億美元，比2016年高出35%。

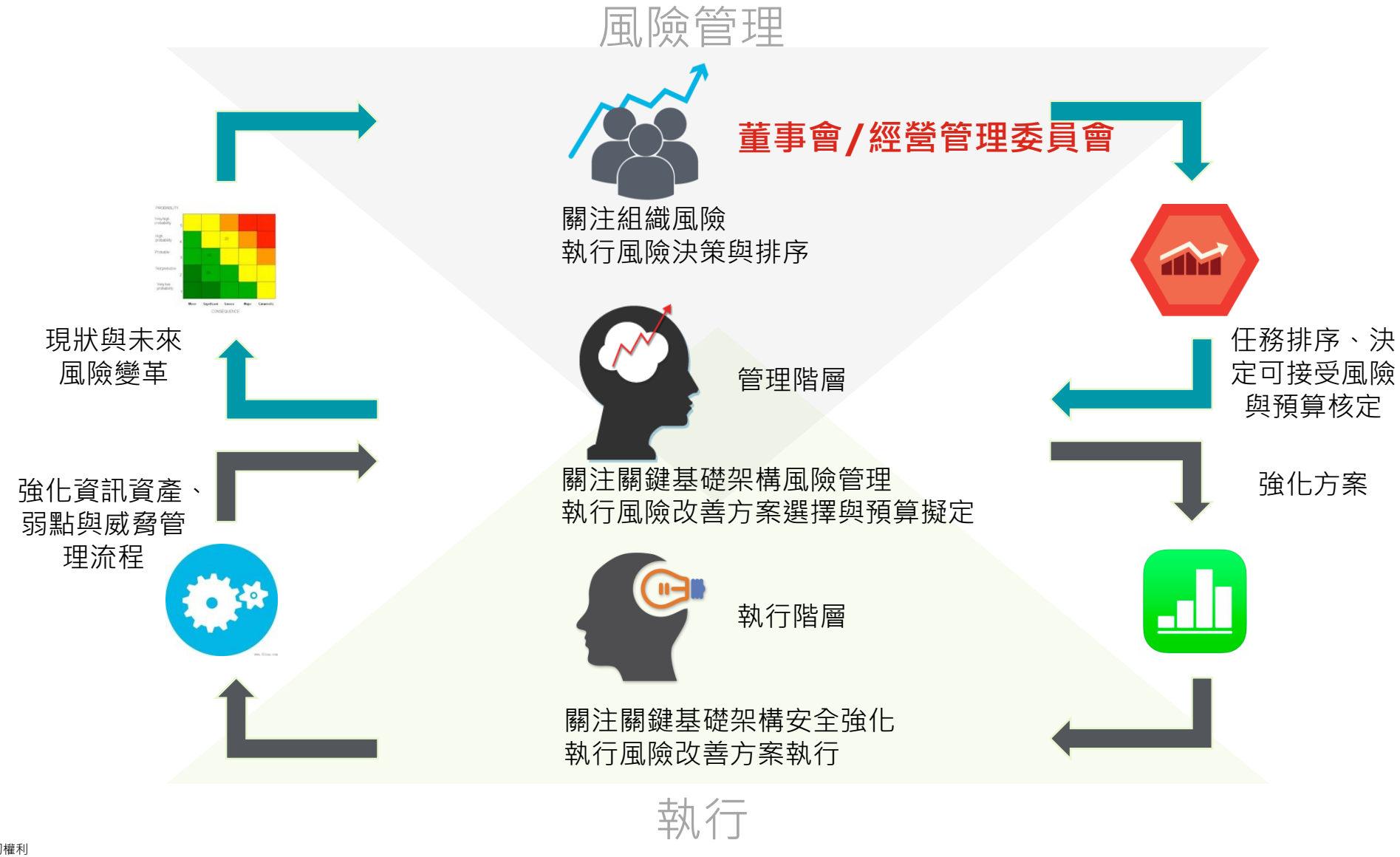
Fintech 安全思維 I - 風險治理

與風險共存的時代，資安管理金融機構治理議題 (董監事層級), 並非IT課題 (FFIEC要求)



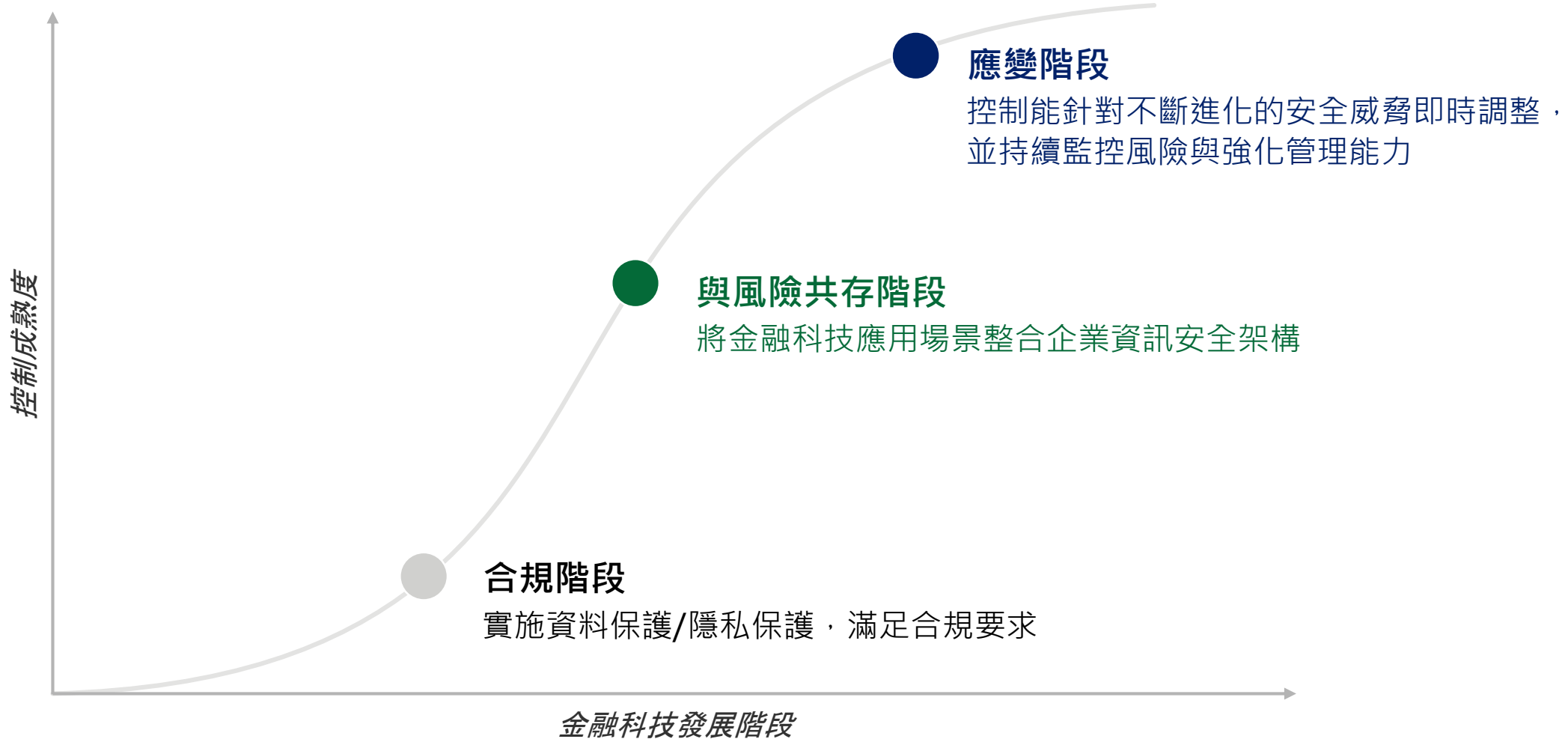
與風險共存的時代，董事會/經營管理委員會將是資安管理的關鍵角色

美國NIST / FFIEC 要求的安全風險治理邏輯

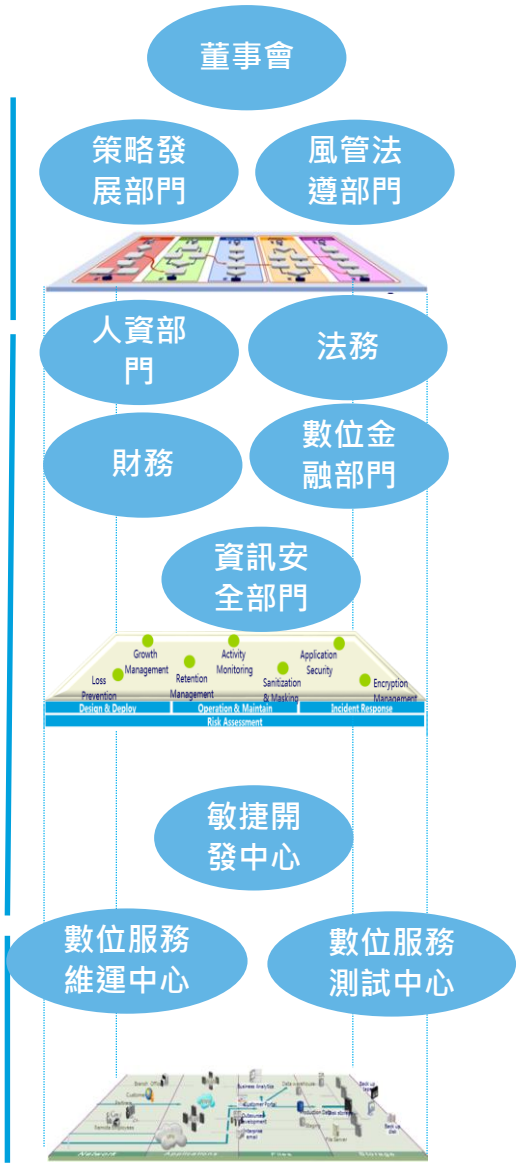


Fintech 安全思維 III – 能夠在資安事件下存活

合規只是起點，企業真正的需求是管理金融科技服務所面臨的資安風險



Fintech 安全思維 IV – 環繞在Cyber Space的安全機制有效性與風管



策略與營運	策略與模式	金融科技策略	新興商業模式與科技應用			
	監管與風險	監管與治理	金融風險管理	產業法規合規遵循		
	營運管理	數位人才資本	虛擬經濟法規	足夠的財務支撐	業務與產品發展	
平台與應用管理	大數據管理	資料蒐集	資料儲存	資料分析/利用	資料傳輸	資料刪除
	存取管理	身份識別	存取控制			
	業務連續與可用性	基礎設施恢復	技術服務恢復	雲端供應商的營運持續管理	供應鏈連續性	
	供應商管理	廠商遴選	監控	廠商鎖定	合約管理	資源供應
基礎設施管理	營運管理	資產管理	專案管理	事件管理	變更管理	維運	實體與環境安全
	監管與風險	弱點管理	網路安全	系統安全	應用安全	加密

金融科技服務風險

資訊安全/資料保護/隱私保護

平台基礎安全

Fintech 安全思維 IV – Cyber Security 風險評估

組織固有風險圖像五大分類				
• 科技應用與存取方式	• 對外服務管道	• 線上/行動金融產品及金融科技服務	• 組織特色	• 外部威脅

五大核心控制領域成熟度				
控制領域1 風險管理&全景	**控制領域2 威脅情資管理**	**控制領域3 安全控制**	**控制領域4 委外及依賴關係管理**	**控制領域5 事件管理及應變**
• 安全治理 • 風險管理 • 資源管理 • 訓練宣導與組織文化	• 威脅情資運用 • 監控與分析 • 威脅情資交換	• 預防性控制 • 偵測性控制 • 矯正性控制	• 委外及依賴關係分析 • 委外及依賴關係管理	• 事件應變計畫及策略 • 事件偵測、回應、風險控制及鑑識 • 事件升級、通報及事件報告

固有風險圖像與控制成熟度關聯示意圖		固有風險圖像 (往右複雜度越高、風險越大)				
		最低	小	一般	顯著	最大
控制成熟度(往上成熟度越高)	創新				■	■
	進階			■	■	■
	中等		■	■	■	
	發展中	■	■	■		
	基礎	■	■			

其他先進國家對於金融科技的監理規範與指引

支付技術

- Payment Card Industry Data Security Standard(PCI DSS) – 自律規範 (self-regulated)
- European Banking Authority Guidelines on the security of internet payments – ENISA

區塊鏈

- UK Government-Distributed Ledger Technology: beyond block chain

大數據

- NIST-Big Data Interoperability Framework Volume 4, Security and Privacy
- EU Data Protection Regulation

物聯網

- Online Trust Alliance- IoT Trust Framework
- ENISA-Securing Europe IoT Devices and Services

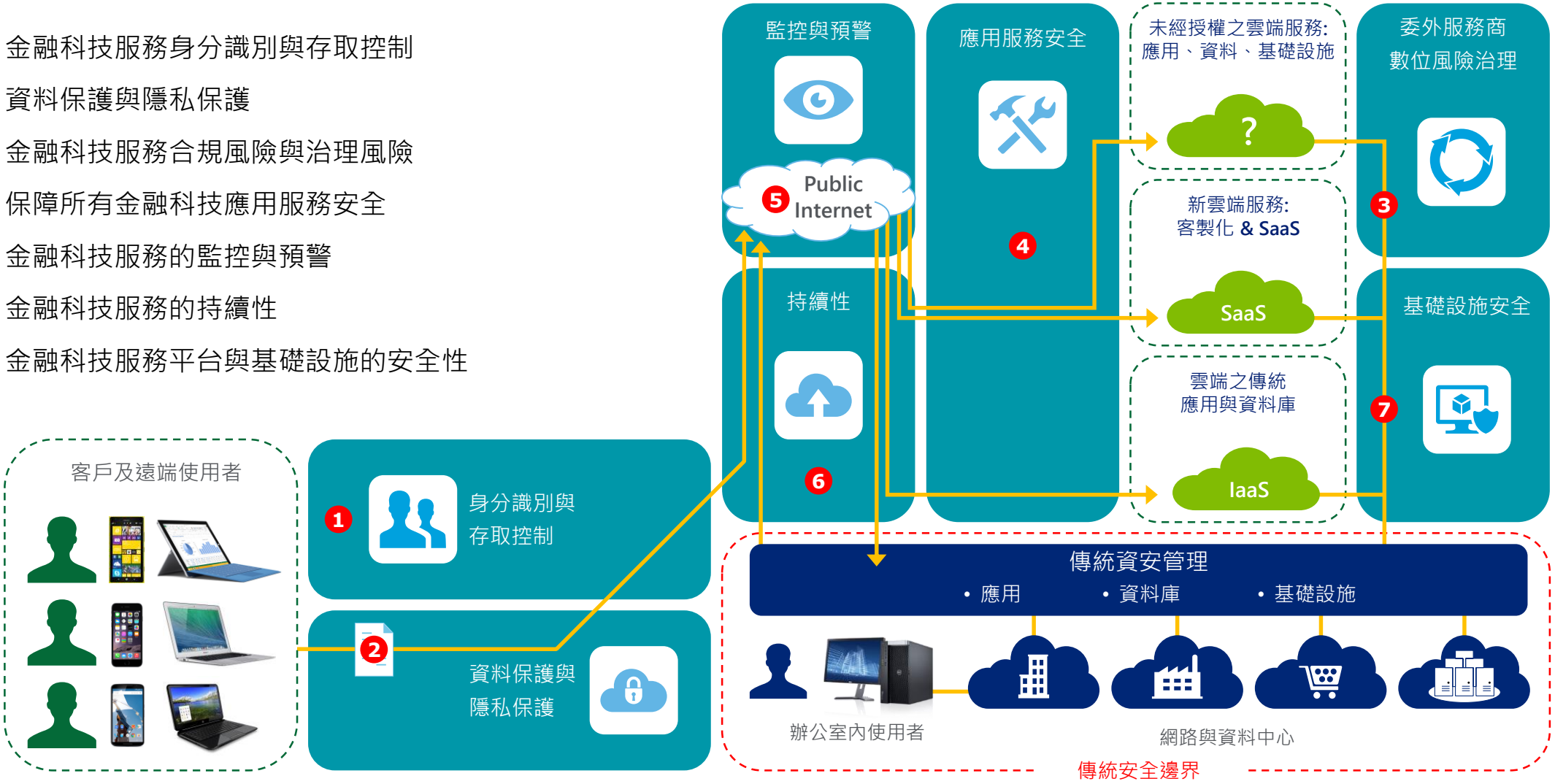
雲端運算

- CSA-Security Guidance for Critical Areas of Focus in Cloud Computing
- ENISA-Cloud Computing: Benefits, Risks and Recommendations for Information Security
- ISO/IEC 27017 -Information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018 -Protection of personally identifiable information (PII) in public clouds acting as PII processors

Fintech 安全思維 V – 資訊安全的運作需要轉型

傳統資安管理需要轉型以符合金融科技特性

1. 金融科技服務身分識別與存取控制
2. 資料保護與隱私保護
3. 金融科技服務合規風險與治理風險
4. 保障所有金融科技應用服務安全
5. 金融科技服務的監控與預警
6. 金融科技服務的持續性
7. 金融科技服務平台與基礎設施的安全性



Fintech 安全思維 VI – 涵蓋業務與IT的緊急應變與攻防演練

STAGE 1 目標及情境規劃及訂定

STAGE 2 協調資源

STAGE 3 規劃及準備

STAGE 4 執行及評估

STEP 1 確認演練目標

STEP 2 設計演練情境

STEP 3 協調人員、資源及行程

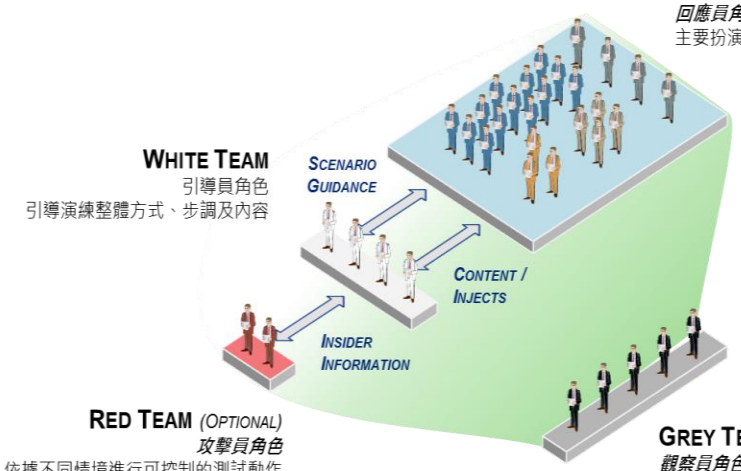
STEP 4 發展演練計畫及檢核表

STEP 5 準備工具及環境

STEP 6 執行攻防演練

STEP 7 計分機制及報告內容

演練角色



BLUE TEAM
回應員角色
主要扮演事件回應及處理角色

WHITE TEAM
引導員角色
引導演練整體方式、步調及內容

RED TEAM *(OPTIONAL)*
攻擊員角色
依據不同情境進行可控制的測試動作

GREY TEAM
觀察員角色
觀察各角色決策判斷及執行方法

演練情境

Use Case #1:
對外網站系統遭受駭客的分散式阻斷式服務攻擊。

Use Case #2:
大量洩露敏感的客戶個資資訊（例如銀行帳戶，個人資料，理賠資訊等）。

Use Case #3:
主要提供營運伺服器主機遭受勒索病毒的威脅。

Use Case #4:
APT攻擊事件，長期潛伏內網，並取得大量使用者的個人資料。

Use Case #5:
竄改已大量佈建至客戶端的相關應用程式原始碼內容

Use Case #6:
網域名稱遭竄改，客戶被導入偽造網站，駭客藉機竊取客戶憑證

Use Case #7:
針對管理層級和董事會成員進行目標式的攻擊，取得相關營業秘密及進行權限升級。

Use Case #8:
內部舞弊事件(員工竊取公司機密資料).

美國金融機構進行網路攻擊演習(量子曙光3)

核心思維：與風險共存 – 並非防範事件不發生, 而在於如何在資安事件後存活

鑑於駭客入侵擾亂金融交易秩序的事件頻傳，超過80家美國金融機構及政府機關2015年9月16日加入美國證券暨金融市場協會(Securities and Industry and Financial Markets Association, SIFMA)名為「量子曙光3」（Quantum Dawn）的網路攻擊演習，模擬如何因應交易所遭駭、客戶資料外洩及系統當機等突發狀況。

「量子曙光」演習係美國證券業暨金融市場協會（SIFMA）自2011年發起，已是第3度舉行，銀行和政府機構共650人參與，主要參與者包括政府部門(如國土安全部、聯邦調查局、財政部、證券交易委員會(SEC)以及大型金融機構(如紐約證券交易所、那斯達克、高盛、美國銀行等) 。

量子曙光3演習主要模擬了5種金融系統遭網攻的情況如下：

- **網域名稱遭竄改，銀行客戶被導入偽造網站，駭客藉機竊取客戶憑證**
- **駭客向銀行勒贖，威脅不付錢就癱瘓網站。**
- **入侵銀行電腦盜取客戶資料。**
- **連不上交易資料處理系統。**
- **清算系統被植入惡意程式，導致交易失靈。**

Fintech 安全思維 VII – 還原真相與訴訟支援的數位鑑識能力

攻防爭點	攻擊對策	防禦對策
數位證據來源	庭呈之數位證據非出自於與案件相關之當事人	1.依該數位證據蒐集者之證述證明出處。 2.依其他證據資料證明該數位證據來源與案件相關之當事人有關。
數位證據蒐集方式	所蒐集之數位證據非公開在網路上之資料	公開蒐集數位證據之方法及步驟。
數位證據作者	庭呈之數位證據非當事人所製作	蒐集其他數位證據及數位證據以外之證據資料個化數位證據之作者。
數位證據格式	庭呈之數位證據格式非原始儲存格式	利用專家證人、鑑定、勘驗證明數位證據格式之變更不會更動數位證據之內容
數位證據儲存版本	提出之數位證據儲存版本非原始儲存版本	利用專家證明版本更新不會變更睥位證據儲存之內容
數位證據儲存環境	提出之數位證據與原始儲存之軟硬體環境不同 數位證據所在之儲存設備被植入惡意程式	提供原始檔案 利用專家證明軟硬體作業環境不會變更數位證據儲存內容
數位證據內容	庭呈之數位證據內容遭增刪修改	1.利用數位證據鑑識技術證明該數位證據之內容未曾遭增刪修改。 2.說明數位證據自蒐集到庭呈至法院之過程。
數位證據建立時間	與案件相關之當事人在數位證據建立時間、存取時間、修改時間有不在場證明	以其他證據資料證明該數位證據係與案件相關當事人所製作。

資料來源：邱獻民，刑事數位證據同一性之攻擊與防禦，民國96年。

Fintech 安全思維 VIII – 借力生態，資安防禦提昇為威脅情資的對抗

將外部資安資料以及內部資訊架構所接受之攻擊或是潛在弱點，統一彙整至資安情資中心。

外部資安資料來源

- Knowledge bases
- Open & subscription based Malware repositories
- Honeynets
- Tracking websites
- Phishing repositories
- Trap email accounts
- Domain databases
- Social media sites
- Paste sites
- Subversive media
- Mainstream news
- TOR sites
- Forums
- IRC channel monitoring
- Security research sites blogs
- Vulnerability databases
- Think tanks
- Blog sites

Web-based
弱點掃描/滲透測試/社交工程工具

內部資訊架構

Agent-based
弱點掃描工具

威脅情資
(Cyber Intelligence)
之生命週期管理

組織

資安情報中心

Cyber Security
管理平台

重大資安事件
呈報及處理

借鏡國外，Fintech生態系需要更多元的ISAC機制

核心為技術專業

技術/產業know-how協作

核心為產業know-how

威脅情資

Dark Web Monitoring	Commercial Threat Intelligence	Open Source Threat Intelligence
Security Research Intelligence	Shared Industry Intelligence	Corporate Brand Intelligence
Human Resource Intelligence	Organization Analytics	National Security

ISAC

Critical Notifications	CINS Crisis Notifications	24x7 Monitoring (dashboard)
Cyber/Physical Alerts from Govt, Partners, other ISACs	Cyber/Physical Alerts from Members	Anonymous Submissions
Portal Access Credentials	Document Repository	Member Contact Directory
Risk Mitigation Toolkit	Threat Viewpoints	Regular Report
Cyber Security Tip Newsletter	Participate in Community Institution Council Teleconferences	Conduct Surveys
Complimentary Webinars	Professional Meetings	Complimentary Regional Workshops
Inclusion in Threat Exercises	Meets Regulatory Compliance Requirement	

Deloitte.

勤業眾信

歡迎指教