出國報告（出國類別：考察）

2019 以色列金融科技及資安產業考察報告

服務機關：中央銀行
姓名職稱：李瑞杷副處長
派赴國家：以色列
出國期間：**108** 年 **5** 月 **25** 日至 **6** 月 **1** 日
報告日期：**108** 年 **8** 月 **27** 日

摘　要

鑒於以色列歷史背景及天然資源缺乏等情況與台灣有相似之處，且以色列之金融科技(Fintech)及資訊安全相關產業快速進步，已是相關領域之強國，非常值得借鏡及學習，因此銀行公會與駐台北以色列經濟文化辦事處合作，於 108 年 5 月 25 日至 6 月 1 日期間舉辦「2019 以色列金融科技及資安產業考察團」。

本考察活動之規劃，係於5月27日至5月30日4天期間，參訪包括以色列央行(Bank of Israel)等政府部門及非營利機構、創投業者、募資平台、創新中心、實驗室、科技園區及知名資安業者，共14個以色列負責推動或主導金融創新之官方與民間機構、及資安公司，就Fintech及資安這二項重點主題進行交流，並分組聽取多家 Fintech 解決方案廠商簡報，瞭解最新技術發展。

本次考察心得如下：

一、放眼天下，國家雖小志氣高。

二、軍方是以色列科技產業孕育搖籃。

三、信任是情資分享的基礎。

四、銀行監理，鼓勵創新與風險控管並重。

五、解決問題導向之思維，創新才有驅動力。

並提出 3 點建議事項，以供參考：

一、持續關注以色列金融科技及資安技術發展，適時評估導入。

二、網路防禦三要素，不可偏廢。

三、選用軟體工具，可參考業界看法。

目　次

壹、目的

鑒於以色列歷史背景及天然資源缺乏等情況與台灣有相似之處，且以色列之金融科技(Fintech)及資訊安全相關產業快速進步，已是相關領域之強國，非常值得借鏡及學習，因此中華民國銀行公會與駐台北以色列經濟文化辦事處合作，於 108 年 5 月 25 日至 6 月 1 日期間舉辦「2019 以色列金融科技及資安產業考察團」。

本考察團由金融聯合徵信中心郭董事長建中率台灣金融業主管級人員 18 人、及由銀行公會及金融研訓院組成之 7 人工作團隊，赴以色列進行本考察活動(人員名單詳附錄 1)。

本考察活動之規劃，係於 5 月 27 日至 5 月 30 日 4 天期間，參訪以色列負責推動或主導金融創新之官方與民間機構、及資安企業，包括知名資安公司(Check Point、Radware、CyberArk)、以色列出口與國際合作協會(The Israel Export and International Cooperation Institute, IEICI)、Bank Hapoalim 創新中心、花旗創新實驗室(Citi Lab)、JVP 創投公司(Jerusalem Venture Partners)、OurCrowd 大眾募資平台、以色列央行(Bank of Israel)、以色列網路事故準備中心(Israel National Cyber Event Readiness Team：CERT-IL)、網路星火產業園區(CyberSpark)、BaseCamp 新創公司孵化器、Gav-Yam Negev 先進技術園區、Ben Gurion University of the Negev 網路實驗室(Cyber@BGU)等 14 個以色列著名的金融科技創新與資安機構及重要的監管單位，就 Fintech 及資安這二項重點主題進行交流，並分 4 組聽取多家 Fintech 解決方案廠商簡報，瞭解最新技術發展。

透過參訪及拜會活動，與以色列在金融科技、資訊安全、金融監理及風險管理等方面之專家及機構進行深入交流，吸收其發展經驗並瞭解最新技術發展，期以有助於本行未來相關業務之規劃。

貳、以色列簡介

一、以色列概況 (資料來源：銀行公會提供之考察團活動手冊)

首都	以色列於 1950 年宣佈首都為耶路撒冷，惟未獲國際普遍承認，耶城地位具高度爭議性，多數國家(包括我國在內)均將大使館代表處設立於特拉維夫。
面積	21,946 平方公里，南北約長 450 公里， 東西寬由 53 至 135 公里。
地理位置	位於阿拉伯半島西北角，北接黎巴嫩，東北與敘利亞為鄰，東與約旦接壤，南及西南連接西奈半島，西瀕地中海。
人口	879.3 萬人(猶太人 74.7%、阿拉伯人 20.8%、4.5%其他族群)。（2017.12）
種族	猶太人、阿拉伯人、德魯士族等。
宗教	猶太教、伊斯蘭教、基督教等。
語言	希伯來語、阿拉伯語。
幣制	以幣 New Israeli Sheker (ILS，新謝克爾)。 1 以幣(ILS)約合 0.28 USD 或 8.51 元新台幣（2018.03.13）

二、以色列產業概況 (資料來源：JVP 簡報)

1. 超過 6,000 家新創公司。
2. 約有 100 個創投基金。
3. 超過 80 個孵化器(Incubator)或加速器(Accelerator)。
4. 超過 300 個研發團體。
5. 有 9 個優秀大學支援研發及創新。
6. 人均科學家密度全球最高。
7. 在 NASDAQ 首次公開發行(Initial Public Offering, IPO)數量，全球排名第三。

三、FinTech 產業概況 (資料來源：以色列出口與國際合作協會簡報)

1. 超過 500 家 FinTech 公司。
2. 2014～2017 年，FinTech 產業之公司收購及募資達 40 億美元。
3. 80% FinTech 公司位於特拉維夫。
4. 52% FinTech 公司之員工數在 10 人以下。

四、以色列政府對產業之扶植 (資料來源：JVP 簡報)

以色列政府對產業之扶植，向來不遺餘力，相關作法包括在世界各國常見之立法支持、減稅、資助研發費用等措施，還有知名的 Yozma 計畫、首席科學家孵化器計畫等。

1. Yozma 計畫：設立國家型創投 Yozma，由政府出資邀請國際創投參與以色列投資。
2. 首席科學家孵化器計畫(Chief Scientist Incubators Program)：在 1990 年代早期，以色列政府創建了一個技術企業孵化器計畫，於經濟部轄下設立首席科學家辦公室(Office of Chief Scientists)，運用於蘇聯解體後，從蘇聯抵達以色列的大量科學家、工程師和醫生之優勢，啟動孵化器，以促進創業種子萌芽及早期技術開發。主要項目是與科學相關之技術研究及開發。

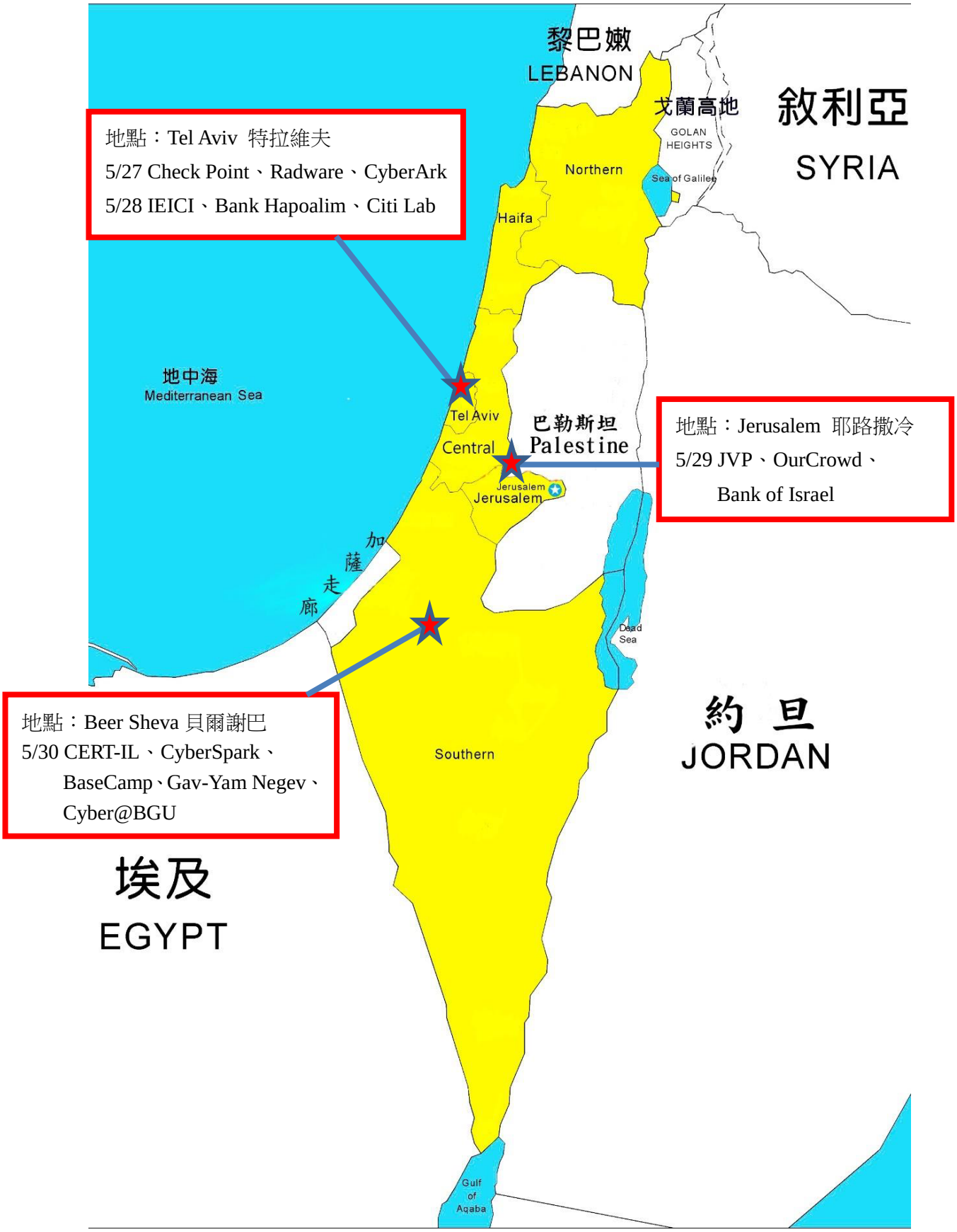
參、考察過程

(壹)行程

本次考察，包含參訪以色列負責推動或主導金融創新之官方與民間機構、及資安公司，行程如下：

活動日期		行程
5 月 25 日(六) ~ 5 月 26 日(日)		搭機前往以色列
5 月 27 日(一)	上午	參訪：Check Point (資安公司) 參訪：Radware (資安公司)
	下午	參訪：CyberArk (資安公司)
	晚上	與以色列 Fintech 與資安領域業者交流
5 月 28 日(二)	上午	參訪 IEICI，並分以下 4 組聽取 Fintech 解決方案業者簡報： (一)Data & Infrastructure 數據和基礎設施 (二)Client-Digital/Offers 數位化客戶服務 (三)RegTech/FinSec 監理科技與金融資安 (四)WealthTech 財富科技
	下午	參訪：Bank Hapoalim 以色列工人銀行創新中心 參訪：Citi Innovation Lab TLV 花旗創新實驗室
5 月 29 日(三)	上午	參訪：JVP 創投公司 參訪：Ourcrowd 大眾募資平台
	下午	參訪：Bank of Israel 以色列央行
5 月 30 日(四)	上午	參訪：CERT-IL 以色列網路事故準備中心 參訪：CyberSpark 網路星火產業園區 參訪：BaseCamp (新創公司孵化器) 參訪：Gav-Yam Negev Advanced Technologies Park (科技產業園區)
	下午	參訪：Ben Gurion University of the Negev 網路實驗室 (Cyber@BGU)
5 月 31 日(五) ~ 6 月 1 日(六)		搭機返回台灣

行程簡圖


地點：Tel Aviv 特拉維夫
5/27 Check Point、Radware、CyberArk
5/28 IEICI、Bank Hapoalim、Citi Lab
地點：Jerusalem 耶路撒冷
5/29 JVP、OurCrowd、
Bank of Israel
地點：Beer Sheva 貝爾謝巴
5/30 CERT-IL、CyberSpark、
BaseCamp、Gav-Yam Negev、
Cyber@BGU
黎巴嫩
LEBANON
戈蘭高地
GOLAN HEIGHTS
敘利亞
SYRIA
Northern
Sea of Galilee
Haifa
地中海
Mediterranean Sea
Tel Aviv
Central
巴勒斯坦
Palestine
Jerusalem
Jerusalem
加薩走廊
Dead Sea
約旦
JORDAN
Southern
埃及
EGYPT
Gulf of Aqaba

(貳)參訪機構／廠商清單

序號	機構／廠商名稱	類別
1	The Israel Export & International Cooperation Institute (IEICI) 以色列出口與國際合作協會	政府部門及非營利機構
2	Bank of Israel 以色列央行	
3	CERT-IL 以色列網路事故準備中心	
4	Jerusalem Venture Partners (JVP)	創投業者、募資平台
5	OurCrowd 大眾募資平台	
6	Bank Hapoalim Innovation Center 以色列工人銀行創新中心	創新中心、實驗室、科技園區
7	Citi Innovation Lab TLV 花旗特拉維夫創新實驗室	
8	CyberSpark 網路星火產業園區	
9	BaseCamp (新創公司孵化器)	
10	Gav-Yam Negev Advanced Technologies Park	
11	Ben Gurion University of the Negev 網路實驗室 (Cyber@BGU)	
12	Check Point (資安公司)	資安業者
13	Radware (資安公司)	
14	CyberArk (資安公司)	

(參)參訪紀要

以下就考察團行程，依參訪單位類別，逐一說明參訪重點。

一、政府部門及非營利機構

(一) The Israel Export & International Cooperation Institute (IEICI) 以色列出口與國際合作協會

以色列出口與國際合作協會是一非營利組織，成立於 1958 年。由以色列政府和民間部門提供支持，旨在促進海外企業與以色列公司建立業務關係、組建合資企業、及結成戰略聯盟。IEICI 接待人員 Mr. Otni Oron 針對以色列政府對 FinTech 產業的支持及以色列 FinTech 產業現況進行簡報，重點如下：

1. 以色列政府對 FinTech 產業的支持

(1)重要措施

A. 設立沙盒(sandbox)機制。

B. 設立金融科技監管中心(Regulatory Fintech Hub)。

C. 設立金融資安實驗室(FinSec Lab)。

D. 以色列央行之銀行監理部門(Banking Supervision Department)成立技術與創新組(Technology & Innovation Division)。

(2)產業監理方向

A. 增加產業之競爭力。

B. 服務數位化。

C. 與全球趨勢同步。

2. 以色列 FinTech 產業核心競爭優勢

(1)技能：有大量經驗豐富、受過高等教育之人力資源。

(2)創造力：人民具跳脫框架的思考模式。

(3)具備周邊領域的深層專業知識，如：電腦網路，軟體等。

(4)冒險精神；失敗被真正視為是學習的機會。

(5)技術能力經過軍事任務驗證。

3. FinTech 公司主要分類

序號	分類	重點項目	成功案例
1	支付 (Payments)	個人間 P2P 支付 PoS(Point of Sale) 企業間(B2B)支付 數位錢包(Digital Wallet)	Fundtech Payoneer
2	貸款與融資 (Lending & Financing)	微型借貸(Micro Lending) 個人間借貸平台(P2P Platform) 眾籌(Crowd Funding) 企業間融資(B2B Debt Financing)	Bluevine Fundbox
3	區塊鏈與虛擬貨幣 (Blockchain & Virtual Currency)	P2P 首次虛擬貨幣發行(ICO) Blockchain、分散式帳本(DLT)	Colu Bancor
4	財富管理及資本市場 (Wealth Management & Capital Markets)	機器人理財／演算法交易 (Robo-adviso/Algo-trading) 個人財務管理工具(Personal Financial Management tools, PFM) 投資及交易平台(Investment & Trading Platform)	OurCrowd eToro Check
5	保險科技 (InsurTech)	合規(Compliance) 詐欺預防和認證(Fraud Prevention & Authentication) 節稅(Tax Efficiency)	ThetaRay VAXBox Fraud Sciences
6	監理科技 (RegTech)	P2P 保險(P2P Insurance) 數位保險(Digital Insurance) 資料及風險分析(Data & Risk Analytics)	Lemonade Windward
7	人工智慧及大數據分析 (AI, Big Data & Analytics)	機器學習及大數據(Machine Learning & Big Data)	Forter Earnix Personetics TipRanks

(資料來源：IEICI 簡報)

於 IEICI，分以下 4 組聽取 Fintech 解決方案業者簡報：(1)Data & Infrastructure 數據和基礎設施、(2)Client-Digital/Offers 數位化客戶服務、(3)RegTech/FinSec 監理科技與金融資安、(4)WealthTech 財富科技。

Fintech 解決方案廠商清單如下(廠商簡介請參附錄 2)：

序號	廠商名稱	組別
1	DBH-S	數據和基礎設施
2	OpenLegacy	
3	Centerity	
4	GigaSpaces	
5	Privacy Rating	
6	CallVU	數位化客戶服務
7	Glassbox	
8	PayKey	
9	SecuredTouch	
10	QNomy	
11	Scanovate	監理科技與金融資安
12	AU10TIX	
13	Shield FC	
14	Transmit	
15	Fincom	
16	iAssessments	財富科技
17	I Know First	
18	Capitalise	
19	V-Check	
20	Pagaya	

(二) Bank of Israel 以色列央行

Bank of Israel 是以色列央行，位於耶路撒冷。參訪該行時，由隸屬於該行銀行監理部門(Banking Supervision Department)之技術與創新組(Technology and Innovation Division)主管 Mr. Daniel Hahiashvili 及資安專家 Mr. Elad Kirson 接待，該行總裁 Prof. Amir Yaron 亦出席致辭歡迎，發表簡短談話。

1. 以色列央行總裁 Prof. Amir Yaron 談話重點

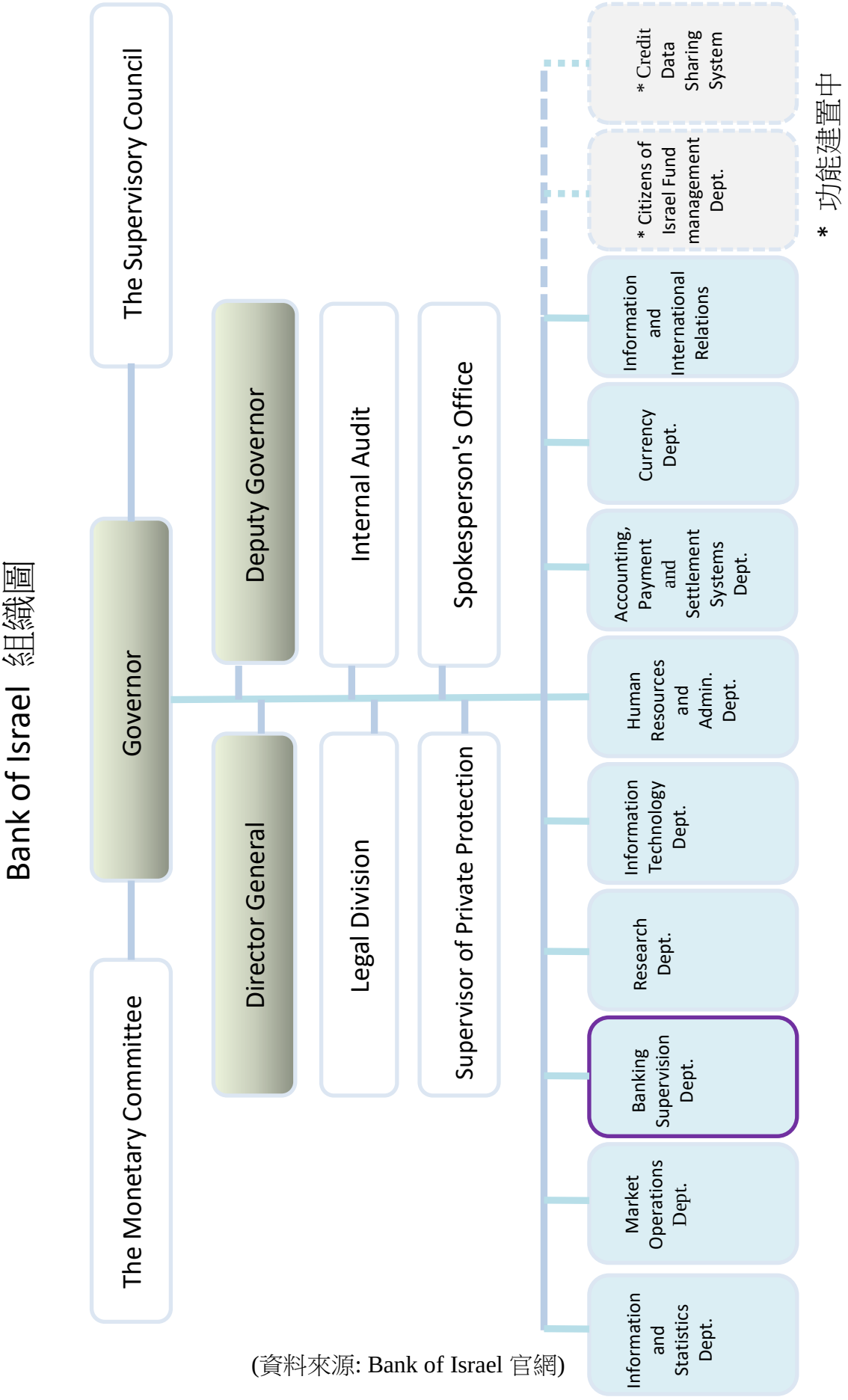
(1)以色列目前經濟受惠於新興科技，狀況不錯，但在三個方面還可再加強：基礎建設、人力資源、及行政效率。

(2)以色列之 CPI 受二個主要因素影響：

A. 實際工資。

B. 全球化因素，如：世界貿易情勢、中美貿易戰、英國脫歐等。

2. Bank of Israel 組織圖



(資料來源: Bank of Israel 官網)

3. Technology & Innovation Division

Mr. Daniel Hahiashvili (Assistant Supervisor of banks, Head of Technology & Innovation Division)針對以色列銀行體系及其掌管之部門 Technology & Innovation Division 進行簡報，重點如下：

(1)以色列銀行體系簡介

A. 主要由 5 個銀行集團構成。

B. 因應金融創新及金融數位化，實體銀行已有減少趨勢，以 2018 年統計，分行數共 1,049 家，最近 5 年內減少 10%；銀行員工約 42,000 人，最近 5 年內減少 10%。

C. 銀行面臨的主要挑戰和風險

(A)挑戰

a.商業模式：須考慮到金融創新、數位化及更大競爭等因素，對銀行業務所造成之影響。

b.在金融服務領域的競爭更加激烈，須具有前瞻性思維。

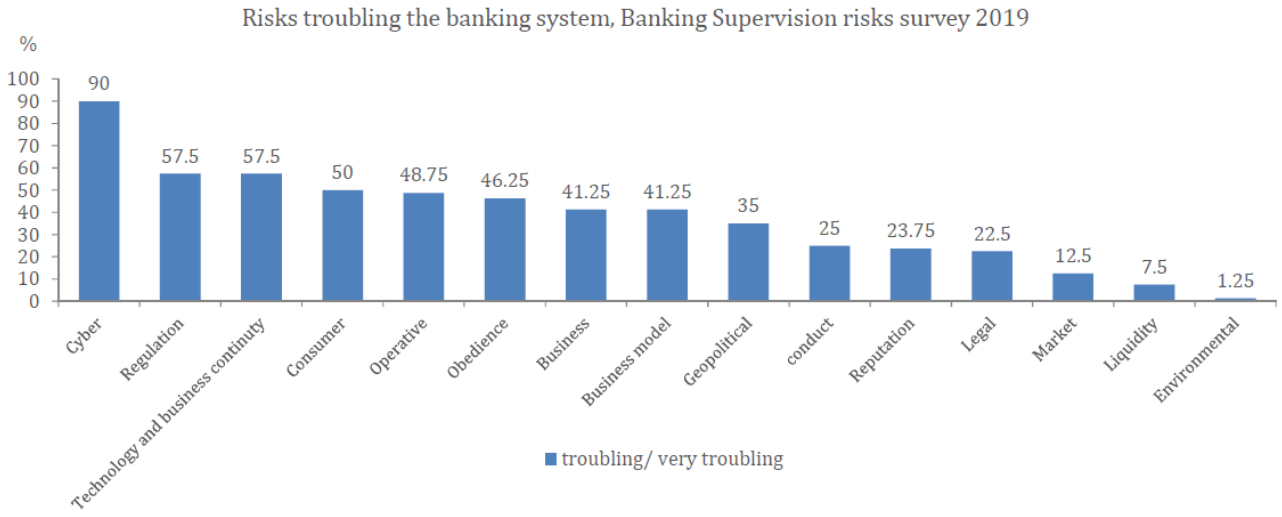
(B)風險

a.網路威脅、資訊科技風險、與資料安全、隱私相關的作業風險等。

b.合規風險，包括跨境風險、業務拓展風險、逃稅風險等。

c.與房地產市場(包括抵押貸款、建築及房地產貸款等)高度相關的風險。

(C)2019 年 Bank of Israel 對銀行面臨的主要挑戰和風險之調查結果如下圖



(資料來源：Bank of Israel 簡報)

D. 銀行與金融科技業間之關係

(A)向金融科技業購買服務，如：內部資料處理、合規服務(如洗錢防制 Anti-Money Laundering, AML) 等運營服務。

(B)透過加速器或創新實驗室推廣自身之金融科技，如：啟動特定技術的銀行產品和金融服務(如：機器人理財)等。

(C)與金融科技業是協作與合作之夥伴關係，如：引進金融科技公司和聚合金融科技公司之應用作業開發人員、區塊鏈技術等。

(D)直接投資金融科技業，如：網路貸款、線上支付等。

(2)技術與創新組 Technology & Innovation Division 簡介

A. 於 2017 年成立，隸屬於該行銀行監理部門(Banking Supervision Department)。

B. 願景

(A)努力促進金融環境，使以色列銀行體系能夠強壯、可靠及數位化，並能保持活躍、高效率、競爭力、且支持新商業模式之態度。

(B)使銀行體系中之所有客戶都可受益於先進、安全、可取得且有競爭力之服務，以實現最佳財務管理。

C. 對技術與創新管理採取之方法：以能夠促進以色列銀行體系進行變革及創新之態度，對金融領域(含銀行和非銀行)之技術變革作出回應，對變革過程中之風險管理都能規範、監督和執行，期以有助於銀行之商業模式更具穩定性、效率及競爭力。

D. 重點戰略

(A)鼓勵開放之銀行生態系。

(B)促進銀行全面數位化。

(C)開發先進的支付基礎設施。

(D)促進可支持銀行新型態業務之技術基礎設施的建立。

(E)建立技術與創新領域之監理執法基礎設施。

(F)促進銀行體系對網路風險的準備。

(G)鼓勵銀行提供先進可靠的技術基礎設施。

(H)與以色列及國外之其他監管機構建立合作關係。

(I)與相關產業、銀行及金融科技業建立溝通管道。

(J)厚植與銀行監管相關之創新與技術專業知識，並取得最新資訊。

E. 組織：由 3 個單位組成，包括監理與執法(含實地檢查及場外監控)、金融創新、及網路監督。

F. 主要挑戰

金融體系正在發生變化，作為監理機構，需要為創新及技術應用創造一個支持性的監管環境，同時管理其中的新風險。包括：

(A)帶領監理合作夥伴支持數位銀行業務。

(B)注意網路風險。

(C)促進個人資料保護(包括資料安全及資料隱私)。

(D)維持銀行核心系統有效運作。

(E)強化委外管理及雲端服務。

(3)Bank of Israel 近期銀行監理之主要作為

A. 將電子銀行監理更新為：

(A)允許成立全數位銀行。

(B)為促進數位銀行業務消除障礙(如：允許銀行數位保證、臉部識別技術等)。

B. 促使銀行能夠採用先進的支付方式：包括支付應用作業、電子支票、促進 EMV(註)、消除信用卡市場的進入障礙、考慮建立集中化之快速支付及清算系統等。

[註：EMV 是國際金融業界對於智慧型支付卡與可使用晶片卡的 POS 終端機及自動櫃員機(ATM)等所制定的標準，EMV 三個字母分別代表最初制定 EMV 標準之 3 家公司：Europay、MasterCard 與 Visa。]

C. 正在制定一個開放銀行應用程式介面(Open Banking Application Programming Interface, Open Banking API)標準，該標準可實施於以色列銀行體系之下列應用：

(A)成本比較。

(B)帳戶聚合(account aggregation)。

(C)財務諮詢。

(D)支付。

D. 與財政部合作建立聯合運算中心。

E. 促使從銀行到銀行之轉帳更容易。

F. 鼓勵並核准銀行與金融科技公司或其他解決方案之間的合作，並不時與金融

科技業者進行對話，以引導新產品有序的問世。

G. 技術與創新之監理執法基礎設施

(A)實地檢查核心系統、網路風險管理、IT 領域之公司治理等。

(B)為銀行制定技術風險評估(場外監控)。

(C)促進銀行體系對網路風險之準備。

(D)適時更新法規。

(E)衡量、分析客戶使用銀行之直接途徑(含數位部分)情形。

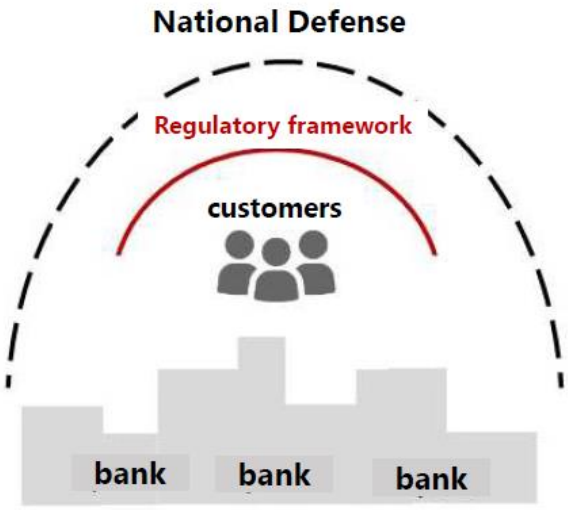
(4)管理網路風險需要多方共同努力，包括要有：

A. 銀行層級之防禦。

B. 管理風險之監管框架(Regulatory Framework)。

C. 國安單位對重大網路事件處理之參與。

D. 客戶之安全意識。



(資料來源：Bank of Israel 簡報)

4. Cyber Defense Unit

Mr. Elad Kirson(任職於 Cyber Defense Unit, Banking Supervision Department)針對網路風險及網路防禦概念、及其任職單位 Cyber Defense Unit 進行簡報，重點如下：

(1)網路風險及網路防禦概念

A. 網路風險(Cyber Risk)和資訊安全風險(Information Security Risk)之區別

網路風險之規模更大，對手更強、更複雜，攻擊特性也更繁複(如進階持續性滲透攻擊(Advanced Persistent Threat, APT)，影響更巨大。

B. 網路安全(Cyber Security)與網路防禦(Cyber Defense)之本質不同，網路安全只重技術，網路防禦則更全面，技術、人員及程序 3 個構面均須關注。

C. 網路風險包括：

(A)直接風險

a.資料洩漏及被竊。

b.金錢被盜，如孟加拉央行事件。

c.服務中斷，如：阻斷服務攻擊(Denial of Service, DoS)。

d.資料被破壞，若是嚴重，必要時須停止服務。

(B)間接風險：由直接風險衍生，包括：

a.聲譽風險：發生安全事件，聲譽必然受損。

b.經營策略風險，如：資料破壞之攻擊，將會影響客戶信心，進而影響銀行數位化創新之推展。

c.穩定風險：客戶若因銀行安全事件關掉帳戶、把錢撤走，將會影響銀行之流動性。

D. 網路防禦管理重點

(A)對於有資金支持之複雜攻擊，不是每次都能夠成功防範的。

(B)資安威脅不只是資安專家的事，整個組織都有關聯。如：考量是否要停止服務，就不是資安單位可以單獨決定的。

(C)多層次防禦(防禦縱深要夠)。

(D)必須兼顧技術、人員及程序。

(E)要做到具積極主動性(proactive)、可預測性(predictive)、且能打破常規思考、具創意性(creative)之防禦。如：從金融科技等新創公司取得服務，或將機器學習、人工智慧等技術運用於防禦。

(F)定期檢驗控制措施之有效性。

(2)Cyber Defense Unit 簡介

A. 於 2012 年成立，目標是強化銀行業對抗資安威脅的韌性。Technology & Innovation Division 成立後，改隸屬其轄下。

B. 主要工作

(A)制定法規

制定下列銀行業務行為規範(Proper Conduct of Banking Business Directives，PCBBD)：

a.網路防禦管理 Cyber Defense Management－PCBBD#361 (2015 年 3 月制定)。

b.雲端運算 Cloud Computing－PCBBD#362 (2017 年 2 月制定)；銀行核心業務(core banking service)以外之其他業務，都可以提供雲端服務。

c.供應鏈網路風險管理 Supply Chain Cyber Risk Management－PCBBD#363 (2018 年 5 月制定)。

d.向央行之銀行監理部門報告網路安全事件 Reporting to the Bank Supervision Department on Cyber Incident (2015 年 7 月制定)。

(B)資訊分享

a.銀行業資安論壇

2012 年成立，6-8 週聚會 1 次，參加成員包括銀行之網路防禦長(Chief Cyber Defense Officer，CCDO) 與營運風險代表 (Operational Risk Representative, OpRisk、以色列央行代表、及以色列網路管理局(National Cyber Directorate)代表。

b.與國安單位及其他政府組織合作

(a) 2017 年 1 月，隸屬於以色列網路事故準備中心 National Cyber Event Readiness Team (CERT-IL)之 Financial Continuity Cyber Center 開始運作，銀行可自願性的加入。

(b)繼續維持自 2016 年開始之以色列網路管理局、央行銀行監理部門、財政部及一些銀行間之資訊分享工作，包括：

。由上而下：由以色列網路管理局提供各機構各國情資及研究服務。

。由下而上：銀行發生資安事件時，主動通報。

(C)銀行監理

a.定期會議，每 6 個月 1 次，銀行的 CCDO 及 OpRisk 必須出席。

b.對銀行發出 Requirement letter，如：要求進行壓力測試、或發生孟加拉央行事件時，要求銀行評估其 SWIFT 系統風險等。

c.金檢被網路攻擊的機構。

d.資安查核，由 Cyber Defense Unit 和央行其他單位一起辦理。

(D)銀行業資安演習

每年 1 次，共 2 天，使用國際組織 FS-ISAC (金融服務業之信息共享和分析中心 Information Sharing and Analysis Center - Financial Services)之支付系統網路攻擊(Cyber Attack on Payment System)演練個案。第 1 天銀行自行演練，第 2 天和央行一起演練，央行也許會增加其他演練情境。

C. 適當之監理法規

(A)採原則基礎(Principle based)而非規則基礎(Rule based)

a.由受監理之銀行根據其風險狀況，調整控管措施。

b.規範銀行要做什麼(What)，而非如何做(How)。

c. Rule based 易讓被監理機構暴露在風險之下。

d.法規必須經常更新，若採 Rule based，其更新要耗極大資源。

(B)採用國際標準。

(C)和本國及國際之其他法規要能相容、不衝突。

(D)定期檢視，必要時要修正。

D. 如何面對資安威脅

(A)加強跨國、跨機構之互助合作。

(B)機構間互相學習、分享資訊、相互支援。

(三) Israel National Cyber Event Readiness Team (CERT-IL) 以色列網路管理局網路事故準備中心

CERT-IL 設置於 Beer Sheva 之 Gav-Yam Negev 園區，本考察團由該中心之 Incident Response Manager Mr. Omer Cohen 接待，並針對該組織進行簡報，重點如下：

1. CERT-IL 於 2014 年成立，隸屬於以色列總理辦公室轄下之以色列網路管理局，為一強化網路安全防護之官方機構。
2. 主要任務：當以色列官方機構或民間單位發生網路安全事件時，提供相關之諮詢及事件應變處理。
3. 於 2015 年加入 Forum of Incident Response and Security Teams (FIRST)組織，與全球 CERT 組織進行交流合作。

4. 串連國家及產業之合作，將各機構依領域區分，包含政府、金融、公共安全、能源等，由各領域專家提供網路安全諮詢。對於非特定領域之事件，若有特殊狀況會以 VIP 機制處理，以求時效。
5. 提供資安情資分享與分析服務給其他協同合作機構，以達到資安聯防。
6. 重視提升民眾對網路安全及隱私問題之認識及瞭解，強調對資安事件進行專業評估的必要性，並向民眾發布資安事件處理程序、防禦工具等訊息。
7. CERT-IL 為贏得外界信任，保證向其報告之資安事件資料，絕不會外洩。
8. 建置資訊分享平台 Cyber Net：此一平台有類似 Facebook 之機制，可方便的分享訊息。CERT-IL 鼓勵各界資安人員至該平台分享情資及經驗，並依分享之次數，給予分享者不同等級之評價(如分享較多者，會出現在網頁較顯著的地方)。
9. CERT-IL 正式人員編制不大，有不少退休人員及學生做二線支援。

二、創投業者、募資平台

(一) Jerusalem Venture Partners (JVP)

JVP 曾被研究機構評為全球績效前十大創投基金，有效引導幾個在以色列境外之大型首次公開發行(Initial Public Offering, IPO)，其中包括自 1999 年以來，第一家在美國 NASDAQ 上市之以色列網路安全公司 CyberArk。其接待人員之簡報重點如下：

1. 以色列產業特色

以色列天然資源並不豐富、國內市場又不大，因此採取下列措施，化劣勢為優勢；

(1)策略：建立小型的跨國公司，走向全球。

(2)涵蓋面廣泛的政府激勵措施，包括 Yozma 計畫、首席科學家孵化器計畫、立法支持、減稅、資助研發費用等。

(3)多樣化的生態系統，包括軍方、移民、文化、學術界等。

A. 軍方：以色列的兵役對以色列產業啟動產生巨大影響，軍方的資訊、網路安全、情報等單位，孕育了以色列的創業場域。

B. 移民：90 年代，蘇聯解體，約有 100 萬移民從蘇聯進入以色列，其中有電算科學方面的教授，當時以色列人口僅約六、七百萬人，這些移民為以色列帶來一波創新浪潮。

C. 文化：以色列人民來自世界各地，因此涵蓋各方文化，是許多傳統、宗教、學術等之大熔爐。

D. 學術界：對新創公司(Start-up)的支援不遺餘力，如：Haifa 的 Israel Institute of Technology (被譽為以色列之 MIT)、非常專注於電算科學和健康產業的耶路撒冷 Hebrew University、位於 Beer Sheva 的網路安全領域佼佼者 Ben Gurion University of the Negev。

(4)創業文化：敢質疑傳統智慧、接受具建設性的失敗、非正式管道之商業文化。

A. 以色列人好奇心強，總是希望得到不同的問題答案，”NO”這個答案通常是會被質疑的。

B. “NO”對以色列人來說，只是一個為了找出如何克服障礙的挑戰。

C. 以色列人總是嘗試從不同角度處理問題。如果問以色列人 1 個問題，可能至少可以得到 4 個意見，這是創造力和創新的來源之一。

D. 不怕失敗，失敗被真正視為是學習的機會。

E. 以色列人之人際關係密切，創業家之間、或與世界有名之科技廠商高階人員

間很容易建立非正式管道之商業聯繫，對創業有極大幫助。

2. JVP 簡介

(1)於 1993 年由 Dr. Erel Margalit 在 Yozma 計畫下成立；其使命是在以色列國內創造卓越的創業生態系。

(2)已成立 9 個基金(主要分科技基金、機會成長基金、農業食物科技基金)、共已募集 14 億美元、已投資超過 130 家公司、在 NASDAQ 已有 12 個 IPO；基金之有限合夥人(Limited Partners)，其中有來自美國、歐洲及亞洲之重量級投資者。

(3)政府分擔投資風險：每投資 1 萬元，政府資金也有相對一定比例之投資，且無相關之股權。

(4) JVP 作法

A. 精心策劃基金出路，如：為各類組織所面臨之複雜網路威脅提供解決方案。大多數孵化器都是學術孵化器或企業孵化器，而 JVP 是有設立創業投資(Venture Capital, VC)孵化器之 VC。

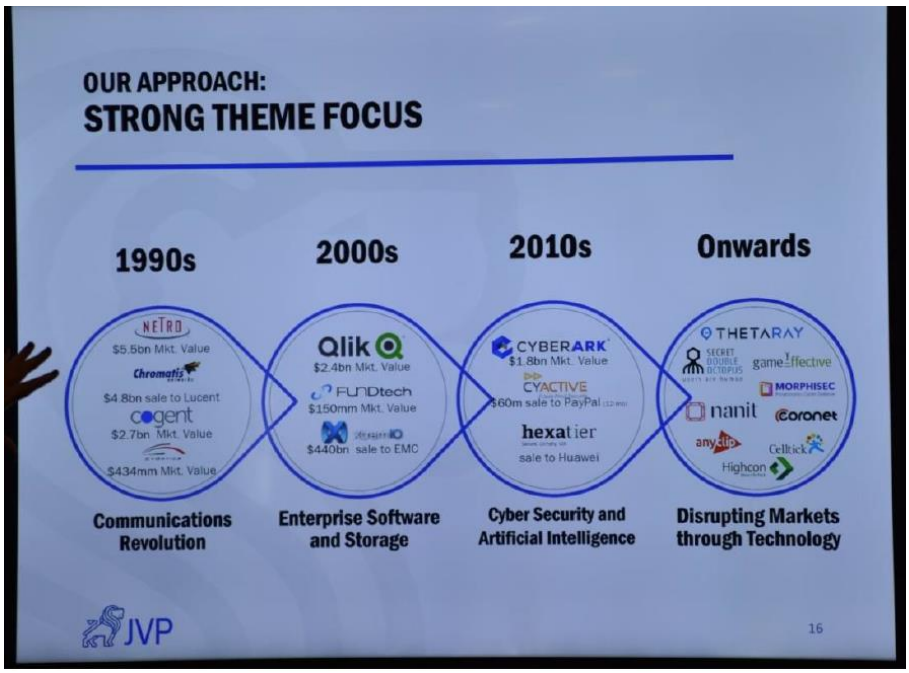
B. 主題驅動之聚焦投資

◦1990 年代－聚焦於通信革命

◦2000 年代－聚焦於企業軟體及資料儲存

◦2010 年代－聚焦於網路安全及人工智慧

◦從現在開始，則是找到技術、顛覆市場；接下來的機會，將在農業、糧食、健康醫療方面。



(資料來源：JVP 簡報)

C. 從初創階段就參與公司創建，且持續參與其後各階段之發展，如：

(A)投資正在申請專利、具顛覆性之大數據分析平台。

(B)可於網路安全、運營保障、反欺詐、風險管理和機會發現等方面運用之技術，及用於監督式學習(supervised learning)、深度學習之演算法。

(C)從學術界採購創新技術以創建公司，並在 JVP Labs 培育。

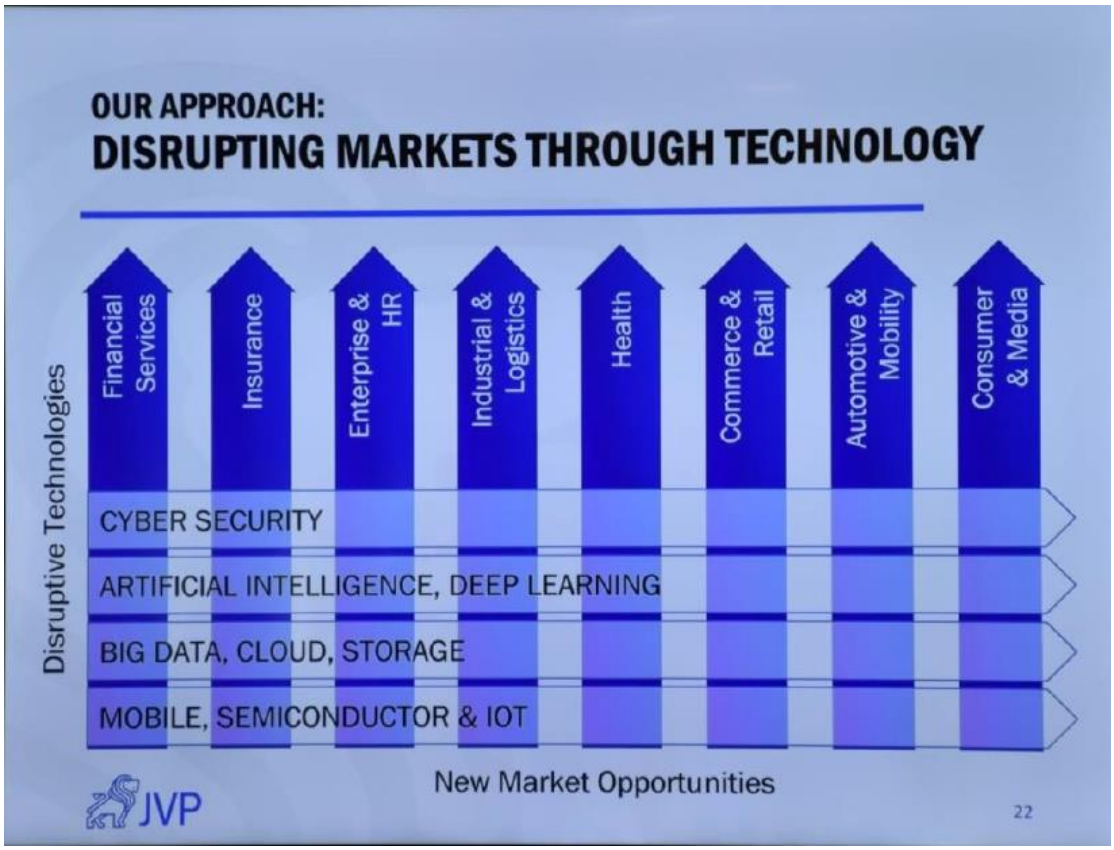
(D)建立管理團隊。

(E)歡迎 GE、Bank Hapoalim 等全球性投資者加入。

(F)針對金融服務及產業市場，訂出產品和市場戰略。

D. 透過技術發展，顛覆市場

在金融服務、保險、企業與人力資源、工業與物流、健康、商業與零售、汽車與機動性、消費者與媒體等領域，透過網路安全、人工智慧、深度學習、大數據、雲端運算、資料儲存、行動化、半導體及物聯網等技術發展，顛覆市場。



(資料來源：JVP 簡報)

(二) OurCrowd

OurCrowd 是一個由跨國公司、企業家、投資者、風險投資家和全球性投資機構組成的股權群募平台，藉由邀集有信譽的投資人以創投基金的方式投資新創事業，為新創企業提供資本募集服務。參訪時由 Mrs. Laly David (Partner, Head of Business Development)接待及簡介 OurCrowd，重點如下：

1. 於 2013 年由現任執行長 Mr. Jonathan Medved 於耶路撒冷創立。
2. 經營模式
   (1)由經驗豐富的投資團隊每年對數千家各產業之各發展階段的新創公司進行研究，嚴格審核可以登上 OurCrowd 平台之籌資者，確保這些公司是有獲利潛力且具前景的。
   (2)審核投資人的身分，確保他們是高淨值投資人，擁有較高風險承擔能力、有經驗而且有資源，足以幫助籌資公司成長。
   (3)以股權眾籌作為營運模式，在股權眾籌中，將公司股票的投資額度匯集在一起，只有經過 OurCrowd 認證的投資者才能投資。
   (4)OurCrowd 本身一定會投資每一個在其平台上架的募資案，藉由和投資人有相同的利害關係，確保投資方和募資方都得利。
3. 經營理念：追求創新、關懷弱勢
   (1)OurCrowd 要求其以色列投資組合公司，在其任何一輪融資結束時，將其部分股權捐贈給慈善機構。
   (2)對利用 FinTech 提供金融服務給無法得到金融機構服務的弱勢族群之新創公司，進行投資。
   (3)2018 年 OurCrowd 宣布，其 Labs / 02 種子階段孵化器將在 10 年內投資 100 個早期創業公司。
   (4)提供諮詢，與世界各地之不同機構合作，幫助這些機構在很早期就能洞察未來 2 到 3 年才會出現的事物，並找出適合這些機構投資之待開發事物。
4. 成果
   (1)自成立以來，籌集了 11 億美元、有 180 家投資組合公司、審核過 10,000 家公司、有 33,000 個經認證之投資者、資金及投資對象來自全球。
   (2)是以色列交易數量最多也是最活躍的創投公司。

三、創新中心、實驗室、科技園區

(一) Bank Hapoalim Innovation Center 以色列工人銀行創新中心

以色列工人銀行創新中心位於特拉維夫，一進門就是三個大字「Knowing、Free Thinking、Optimist」，標榜知識、不受拘束的自由思考、及樂觀。創新中心採開放式辦公空間提供新創業者使用，氣氛活潑，並有數個小空間以便於討論。各新創業者專精項目並不相同，藉由共享空間，創造互相激盪及合作機會。

該中心接待人員談話重點如下：

1. Bank Hapoalim 致力於金融科技發展，成立創新部門(Innovation Division)，負責推動銀行內部服務與產品的創新。
2. 成立子公司 Hapoalim Tech，主要也是扮演資本投資及創投資金管理的角色，藉由搜尋有潛力的金融科技公司，並與其進行合作或是導入創新解決方案，提供更佳之新型金融服務。

Bank Hapoalim 之 Cyber Risk Management Unit 資安專家 Dr. Amir Schreiber 也分享其對資安的看法，重點如下：

1.網路防禦與網路攻擊之作法、趨勢都是隨著 IT 技術演變(如：Big Data、Cloud)而日益升級，二者之重點都是圍繞著 4W1H：攻擊者及受害者是誰(who)、何時攻擊(when)、目標是什麼(what)、哪裡被攻擊(where)、如何攻擊(how)。

2.風險管控措施依風險偏好(Risk Appetite)而定，相關部門之著重點都必須納入，目標是讓未知的網路風險都可以被管理(Making the cyber unknowns to something we can manage it)：

(1)管理者：著重全局。

(2)業務部門：著重業務控制及業務流程。

(3)IT 及資安部門：著重網路及技術控制。

3.風險管理心得

(1)要有創造性思考，思考要跳脫框架。

(2)專注於具有高潛在風險之流程。

(3)不論是商業或技術，群體的智慧是優於個人的。

(4)要容忍、甚至採納不同意見；不具共識的想法仍可被討論。

(5)即使是花費不多的控制措施，只要放對地方也會有效果。

(6)從別人的錯誤和過去的事件中，吸取教訓。

(7)無論已採取多少控制措施，資安意識是不可或缺的一環。

(二) Citi Innovation Lab TLV 花旗特拉維夫創新實驗室

參訪花旗特拉維夫創新實驗室時，由 Mr. Tsafrir Atar (Head of Citi Accelerator)接待，其簡報重點如下：

1.以色列是一個新創公司興盛的國家，主要集中在特拉維夫，每 298 個居民中就有 1 位是新創業者。

2.花旗集團在以色列之創新作為(Citi Innovation)

(1)解決花旗集團自身面臨的行動化挑戰(Citi Mobile Challenge)。

(2)花旗創投(Citi Venture)：在以色列投資 Access FinTech、Contguard、Illusive、Bluevine 等新創公司。

(3)花旗創新實驗室(Citi Innovation Lab)。

(4)花旗加速器(Citi Accelerator)，成果如下：

A. 共 7 個計畫類別：商業與支付(Commerce & Payment)、監理科技與保險(RegTech & Insurance)、資料分析與機器學習(Data Analytics & Machine Learning)、行銷與客戶體驗(Marketing & Customer experience)、資安(Security)、金融服務與技術(Financial Service & Technology)、交易、融資與投資(Trading, Financing & Investing)。

B. 已募集 7.5 億美元。

C. 已造就了 80 家新創公司，其中 5 個公司(Seergate、 Sling、 Paybox*、Mycheck、Credigence) 被收購。

(三) CyberSpark 網路星火產業園區

CyberSpark 簡介如下：

1. CyberSpark 設在位於沙漠中之 Beer-Sheva 的 Gav-Yam Negev 園區，是結合了政府、軍方、學界及企業的力量，由以色列總理辦公室轄下之網路管理局、Beer-Sheva 市政府、Ben Gurion University of the Negev、及數家網路安全產業之頂尖企業所投資之非營利組織。
2. CyberSpark 旨在成為與所有利益相關者聯合開展網路產業活動的中心協調機構，是以色列網路創新競技場。
3. CyberSpark 以最大限度的發揮 Beer-Sheva 作為全球網路中心之潛力，鼓勵聯合學術界的合作夥伴關係，支持吸引其他公司(無論是國際公司還是以色列公司)之各項計畫，以在該地立建立投資項目或自己的研發基地。
4. CyberSpark 提供多個內部平台，幫助企業利用以色列的各種產業促進網絡和高科技，包括：

   (1)研究中心：與 Ben Gurion University of the Negev (BGU)之學者合作。

   (2)研發中心：在政府的支持下，透過在租稅優惠、研發費用資助等激勵方式，企業得以和 BGU 進行共同研究。

   (3)培訓中心：由產業主導及政府對中小企業提供之電腦網路培訓服務。

   (4)創新中心：可以接觸到以色列的先進技術。

   (5)孵化器(Incubator)：由以色列創新局(Israel Innovation Authority)支持。

   (6)情資中心：中小企業可以得到來自 CERT-IL 和產業提供之相關最迫切的網路威脅情資。
5. 以色列政府已經決定在 2020 年前將以色列國防軍(Israel Defense Forces, IDF)中的 8200 部隊以及其他情報和技術機構全部搬遷到此，將有助於將 CyberSpark 建置成全球頂尖資安中心。

(四) BaseCamp

BaseCamp 成立於 2016 年，是以色列相當具有特色的新創公司孵化器，參訪時由其創辦人 Mr. Uzy Zwebner 親自接待。參訪簡報重點如下：

1. 自我定位：是一群可以將觀念、政府支持、設計、社群、學術界、高科技公司等要素妥善整合管理之企業家。

2. 經營基礎：公私協力(Public-Private Partnerships)，包含下列三要素：

(1)與所服務的私人企業間之夥伴關係。

(2)學術界作為催化劑。

(3)政府的支持。

3. 觀念：包含大學之英才中心(Centers of Excellence)、當地公司、區域的優勢、可用的人才、定位等都要納入規劃。

4. 概念設計：包括地理位置、標示規劃、綠地、商業街、國際標準、休閒中心(如健身房)等都要納入考量。

5. 政府支持：包括各項獎勵措施、承租客戶、園區定位、新創公司、公共關係、基礎設施、參觀訪問等方面之支持。

6. 創建充滿活力的科技生活及人盡其才之社群，作法包括：

(1)支持當地技術社群。

(2)創造具獨特性之活動。

(3)透過社交媒體保持聯繫。

(4)提供社群服務。

7. Beer-Sheva 雖在沙漠中，但已具備吸引公司來投資、個人來定居之下列環境，成為以色列南方之都：

(1)在以色列國防軍(Israel Defense Forces，IDF) IT 園區，有 5,000 名技術專家。

(2)SOROKA 醫療中心。

(3)在 BGU 有 20,000 名學生，是很好的人才庫。

(4)有可與以色列其他大城方便往來的火車站。

(5)在 GAV-YAM Negev Advanced Technologies Park，有 3,000 名工程師在 70 家公司工作。

8. BaseCamp 在世界各地之據點：以色列 Beer-Sheva 及 Kfar Kassem、德國 Magdeburg、哈薩克 Astana、南京、及高雄。

9. 機會與挑戰

雖然學術研究，有可創造具突破性技術的新創公司之潛力，但大多數學術研究人員缺乏時間、商業知識或人脈來創建公司，因此如何運用研發文化發展突破性技術，並利用關係網絡達到科技創業，是 BaseCamp 之機會與挑戰。

(五) Gav-Yam Negev Advanced Technologies Park

Gav-Yam Negev Advanced Technologies Park 位於 Beer-Sheva，是以色列先進的研發中心，包括高科技園區和辦公室，佔地面積超過 200,000 平方公尺。參訪簡報重點如下：

1. 園區成功的原因－合作夥伴之願景及對園區之貢獻

(1)BGU

A. 充分利用 BGU 英才中心的潛力。

B. 研究成果向產業開放並專注於應用之方法。

(2)Beer-Sheva 市

A. 願景：成為有成長潛力、有成功動機、有前景之城市。

B. 每年畢業的工程師人數眾多。

(3)全球性的科技產業龍頭(如：IBM、Oracle)在此設立研發中心。

(4)Gav-Yam 房地產公司(Property＆Building Corp 的子公司，屬 IDB 集團)

A. 願景：帶頭創造世界一流的工作環境、成為世界頂級公司的所在地。

B. 在創建先進的科學及高科技園區方面，擁有豐富經驗。

(5)以色列政府

A. 成立 IDF 技術園區。

B. 對科技公司提供如租稅優惠、資助研發費用等之激勵。

C. 建設國家網路資安中心。

D. 對基礎設施投入巨額投資。

(6)KUD International

A. 是全球知名的開發商。

B. 專精公私協力(Public-Private Partnerships，PPP)項目。

2. 園區發展之整體方法

(1)優先租給有招聘員工需求的公司。

(2)提供高級的辦公空間、及休閒設施(包括健身房、娛樂室等）。

(3)提供日托中心、醫療診所等社區服務。

(4)將承租辦公空間的公司，介紹給 BGU 英才中心及可技術轉讓之公司。

(5)協助辦理政府激勵措施。

3. 園區發展之長期目標

(1)未來 10 年內，園區內有 10,000 人在此工作。

(2)開發 15 個高標準的高科技商辦建築。

4. 園區成立 5 年之成就

(1)進駐公司超過 70 家，雇用 2,500 員工，其中約 86%為當地居民。

(2)目前已有之建設，包括 IDF 技術園區、SOROKA 醫療中心、BGU、火車站、住宅區；另已完成 3 棟商業大樓建築，另有 2 棟正在建築中，還有 1 棟還在規劃階段。

(六)Ben Gurion University of the Negev 網路實驗室(Cyber@BGU)

Ben Gurion University of the Negev 網路實驗室設置於 Beer Sheva 的 Gav-Yam Negev 園區，其接待人員針對 BGU 及 Cyber@BGU 進行簡報，重點如下：

1. Ben Gurion University of the Negev (BGU)簡介

A. BGU 創立於 1969 年，坐落於 Beer Sheba。

B. BGU 願景：成為網路安全領域之全球最佳大學。

C. BGU 是以色列成長最快的大學，20 年前有 5,000 個學生、目前 20,000 個學生，預計 10 年內學生數加倍。

D. BGU 在世界創校 50 年之內的大學中排名前 50 名，專利數僅次於 Princeton 大學及 Yale 大學。專利主要是在通訊、電腦、資安、人工智慧等領域。

2. Ben Gurion University of the Negev 網路實驗室(Cyber@BGU)簡介

A. Cyber@BGU 有 3 個主要研究中心：

(A) 電信(Telecommunication)研究中心：是和 Deutsche Telecom 合作的學術研究中心，主要從事電信業網路安全之研究。

〔註：Deutsche Telecom 全球有 3 個創新中心，其他 2 個，一個在德國柏林總部、另一個在美國矽谷(與 Stanford 大學合作)。〕

(B)網路安全研究中心：是和以色列總理辦公室下設的國家網路安全局(National Cyber Security Authority)合作的學術研究中心；官方也是這中心的主要的贊助者。

(C)電腦犯罪學(computational criminology)研究中心：是和 The Israel Police 合作的學術研究中心，從事以大數據分析技術解決犯罪問題之研究。

B. Cyber@BGU 和企業之關係：與許多企業合作(包括 Audi, Fujitsu....)，幫忙企業自己不能或不願以企業自己知道的方式解決之問題。

C. Cyber@BGU 工作團隊目前約有 150 人，包括大學生、研究生、博士、博士後研究、還有高中生。

D. 高中生在 Cyber@BGU 之表現

(A)年輕人希望在服役時可以加入網路安全單位，認為這是一條可以在退伍後快速創業、甚至致富的捷徑，因此在入伍前會選讀相關課程。

(B)BGU 有政府計畫補助，因此在一些高中挑選有天份的學生，從第 9 年級至第 12 年級的 4 年期間，每週 8 小時學習網路安全課程。

(C)這些中學生在假日、還有高中畢業後入伍前之至少 6 個月的時間，到大學研究中心參與研究工作。

(D)17 歲高中生之表現案例

a.完成用勒索軟體攻擊智慧冰箱之概念驗證(Proof of Concept)。

b.完成從被駭的智慧手錶盜取資料之概念驗證。

E. Cyber@BGU 最近的研究成果

(A)Game of drones(偵測無人機操作者是善意或惡意)。

(B)3D 列印風險。

(C)如何駭入完全隔離之電腦。

(D)幾乎每個月都在知名媒體(如 Wall Street Journal、Washington Post、TechCrunch、Bloomberg 等)發表研究成果。

F. 目前主要研究方向

(A)人工智慧(Artificial Intelligence, AI)與網路安全之結合。

(B)駭客如何使用 AI

網路攻擊之動機有 80% 是財務考量，對攻擊者而言，AI 可以讓部分的攻擊工作自動化、可以讓攻擊成本降低、可以不需要透過許多駭客就能擴大攻擊規模。

(C)AI 訓練

AI 對人類是否帶來福祉，仍舊眾說紛紜，Elon Musk 曾說：「有了 AI，我們正在召喚惡魔(With artificial intelligence, we are summoning the demon)」。AI 要能發揮作用，需要大量訓練資料。訓練資料之良窳，就決定 AI 之成敗。

AI 訓練面臨的問題：

a.AI 之訓練資料清理(data sanitization)：訓練資料涵蓋是否全面、是否包含外部資料、是否被惡意導向會產生特定結果之資料。

b.AI model 建立者常較注重效能，較不考慮其他因數，如：

◦AI model 是否容易被駭。

◦偏見(bias)，會導致訓練結果偏差，如：皮膚黑的人似乎較容易被自駕車撞到。

◦資料隱私(privacy)造成資料取得不易。

G. Cyber@BGU 運作模式

Cyber@BGU 接受外界創意概念實驗之委託，透過其研究進行概念驗證，確認該創意概念之可行性後，再由原委託人進行商轉；創意概念若為 BGU 內部自行發想，經實驗可行，他們會賣給企業或自行創設公司進行商轉。

四、資安業者

(一) Check Point

Check Point 是全球知名的資訊安全設備供應及服務商，強調事先的防範重於事中的偵測或事後的鑑識及補救。其次世代防火牆技術為業界第一之領導先驅。Check Point 之參訪簡報重點如下：

1. 公司簡介

(1) 於 1993 年由其現任執行長 Mr. Gil Shwed 創立，1996 年在 NASDAQ 上市。

(2) 公司總部在特拉維夫，在約 90 個國家有辦公室，約有 6,200 家合作夥伴及地區代表，約有 100,000 個客戶。

(3) 員工人數約 5,000 人，超過一半的員工在特拉維夫總部工作。

2. 資安防護觀念分享

(1) 網路攻擊(Cyber Attack)極具成本效益，如：

A. 前幾年有國家網軍駭入核電廠中止其運作，還可以隱藏攻擊來源，這是實體武器做不到的。

B. 美國 CIA 及 NSA 是發展找出零時差弱點的網路工具(cyber tools)及網路武器(cyber weapon)的領導者，幾年前 NSA 的 cyber tools 被 Shadow Broker group 偷走，此一網路武器被某一國家支撐之網路組織使用，造成在 2 天之內有 260,000 台個人電腦(含桌機及筆電)被攻擊。

(2) 資安威脅之演進

。第 1 代的威脅：電腦病毒(Virus)。1980 年代末期，第一隻電腦病毒以磁碟片傳播，防毒軟體因而開始發展。

。第 2 代的威脅：網路(Networks)。隨著 Internet 發展，電腦病毒隨著網路傳播，在沒有網站(website)的時代，必須公布 internal IP 給大眾才能在 Internet 溝通，因此防火牆因應而生。

。第 3 代的威脅：應用作業(Application)。駭客開始針對網站應用作業(Application)使用的協定(protocol)弱點攻擊，入侵預防系統(Intrusion Prevention System，IPS)及入侵偵測系統(Intrusion Detection System，IDS)等防禦工具也開始問世。

。第 4 代的威脅：負載(Payload)。電子郵件附加或由網站下載的惡意檔案及惡意程式開始橫行，因此發展沙箱(sandbox)檢測技術與之對抗。

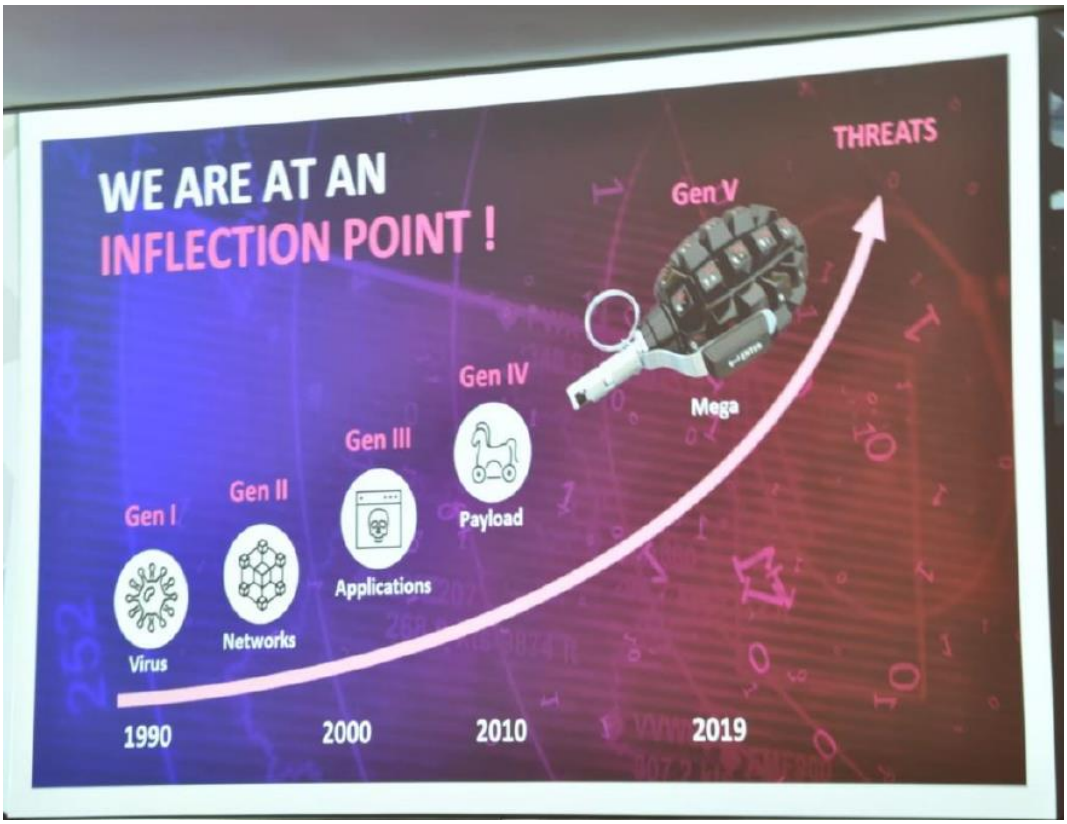
。第 5 代的威脅：超級型的威脅(Mega)，如：如勒索軟體。主要特色有四：

A. 大規模攻擊(橫跨國家及不同產業)。

B. 由國家支持。

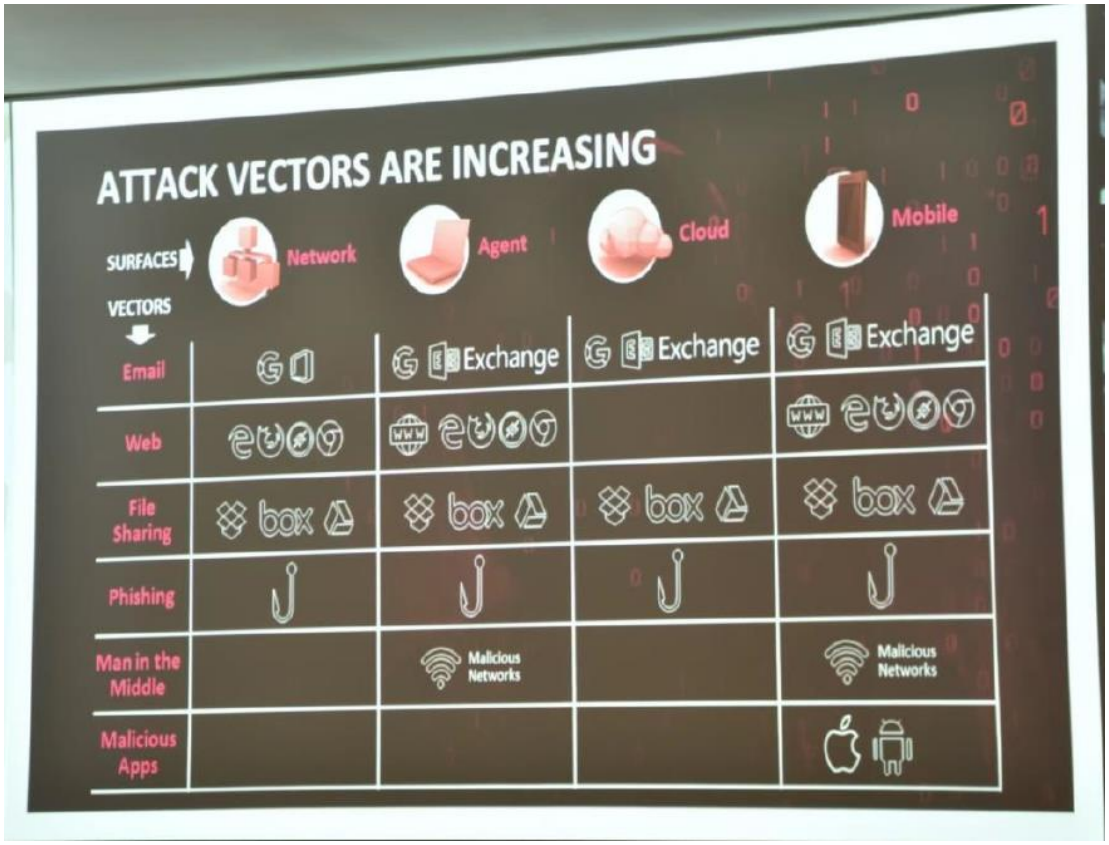
C. 屬毀滅性的攻擊。

D. 多重的攻擊面向(multi-surface)，包含網路、端點、雲端及行動裝置等。



資安威脅之演進 (資料來源：Check Point 簡報)

(3) 攻擊面向(attack surface)正在擴大，攻擊途徑(attack vector)也在增加。攻擊手法包括惡意郵件、惡意網站、惡意檔案分享、網路釣魚(phishing)、中間人攻擊(man in the middle attack)、惡意程式等。



攻擊面向及攻擊途徑 (資料來源：Check Point)

(4) 電子郵件是最普遍的攻擊途徑；行動電話因使用者 7*24 的使用，是最容易的攻擊點。

(5) 網路捕鯨(whaling attack)是針對企業高階主管的網路釣魚攻擊。

(6) 雙因子認證不見得安全。例如目前應用很普遍的以手機寄送驗證碼之應用作業，若其應用系統和用戶手機都被攻擊成功，雙因子認證就無法達到預期之防護效果。

(7) 許多網路攻擊事件及受害程度並不為大眾周知，主因是受害人基於名譽或怕有副作用等因素，不願公諸於世。

(二) Radware

Radware 是全球領先的虛擬數據中心、雲端應用交付與網路安全解決方案供應商，主要著名產品及服務為分散式阻斷服務攻擊(Distributed Denial-of-Service Attack, DDoS)偵測及防護。參訪時由其執行長 Mr. Roy Zisapel 親自接待，參訪簡報重點如下：

1. 公司簡介

(1) 於 1997 年由其現任執行長 Mr. Roy Zisapel 創立，於 1999 年在 NASDAQ 上市。

(2) 公司總部設在特拉維夫，在全球 40 多個國家設有辦事處和分公司。

(3) 員工人數約 1,100 人。

2. 執行長創業及營運理念分享

Radware 執行長 Mr. Roy Zisapel 分享 Radware 成長故事及營運理念，重點如下:

(1) 以色列男子高中畢業，一律先至軍中服役，至少 3 年。並依面試及其他測試，確認各項能力後，再分派適合之工作。

(2) Mr. Roy Zisapel 在以色列資通訊部隊服務超過 5 年，累積相關技術及人脈，退伍後經 2 次壯遊後，與在軍中認識之袍澤一起創業。

(3) 創業一開始，以具負載平衡之路由器開始，並以 Cisco 為對手，其想法是所有的客戶會經由 Cisco 得知有更好的產品在 Radware，因為 Cisco 比 Radware 晚約一年才開始進入負載平衡的市場。

(4) 隨著應用作業之重要性日增，Radware 開始應用交付(Application Delivery)領域，在最近 20 年內之市場佔有率都在前 3 名、技術及解決方案則是數一數二。

(5) 2001 年應 eBay 要求，開始進入資安領域。並在機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)資安三大支柱裡特別著重可用性，因此在 DDoS 防禦領域領先業界，世界排名前 20 的多家銀行即使用該公司服務。

(6) 網路攻防已是很大的問題，首先各國政府加入競賽，將資安能量視為國防的一環，其次資安犯罪所得金額十分誘人，如孟加拉央行被盜近 1 億美元，再者激進份子也以網路攻擊以遂行其組織目的，如匿名者(Anonymous)。

(7) 如同保衛國家一樣，資通安全防禦是全面性的，必須能確保於攻擊中仍然可以提供服務，不管敵人使用何種武器，都必須能抵擋所有的侵犯才行。

(8) 必須隨時傾聽客戶的反應，客戶遇到的一些問題，常可以成為公司下一波成長的源頭。Radware 建立雲端 DDoS 攻擊流量清洗中心，就是為了解決客戶 2 個痛點：

A. 預算：若要購買足夠的資安防護系統及設備，必需要投入龐大資源。

B. 人才：人才聘僱必須與政府單位、高科技公司競爭，而且內部人員老化不易跟上新技術。

(9) 金融服務業是 Radware 第二大客群，其因有四：技術考量、有高價值的資料、有高可用性的需求、有安全性的需求。

(10)年輕人不理解風險、不會害怕，造就了典型的以色列創業的心態：

A. 自己一定可以創業。

B. 自己一定可以跟全球競爭。

3. 資安防護觀念分享

(1) 以國內客戶為主的機構，若遇到 DDoS 攻擊的減輕機制無法緩解攻勢時，可試用 GeoIP black-holing 的方法，把非本國的訊息封包拋棄；因為 DDoS 是個資源消耗戰，當主要客戶只在本國，封鎖國外訊息，還是能確保於攻擊中仍然可以提供服務。

(2) 選擇資安產品之考量

A. 必須能夠與原有之資安防護工具及作業流程整合。

B. 可自動化以節省維運人力 。

C. 內部人員必須可以有能力自行管理，而非只能依賴廠商。

D. 要有良好的管理介面(最好有決策支援系統)，以利快速處理經常須面對之大量告警及事件。

(3) 資安防護重點

A. 覆蓋範圍：需要多重防線(防禦縱深要足夠)。

B. 自動化：能夠即時偵測及緩解攻擊。

C. 人員：要具有領域內之專業知識、及解決方案之實務經驗。

(三) CyberArk

CyberArk 關注針對性之網路攻擊威脅、以企業核心為目標的攻擊，並提供資安解決方案的公司，其著名的解決方案為特權帳號安全。CyberArk 之參訪簡報重點如下：

1. 公司簡介

(1) 於 1999 年由 Mr. Alon N. Cohen 及其現任執行長 Mr. Udi Mokady 創立，於 2014 年在 NASDAQ 上市。

(2) 公司總部設在特拉維夫，在約 90 個國家有生意往來，約有 300 個合作夥伴，約有 5,000 個客戶。

2. 資安防護觀念分享

(1) 權限管理的三個重點

A. 特權帳號管理要妥善。

B. 應用作業存取權限控管：包括應用作業之功能及可使用之資料庫，均須有權限者才能授權存取及使用。

C. 終端使用者帳號是最脆弱的，通常是駭客攻擊的起點，因此應謹守最小權限原則。

(2) 駭客入侵手法及步驟

A.侵入系統。

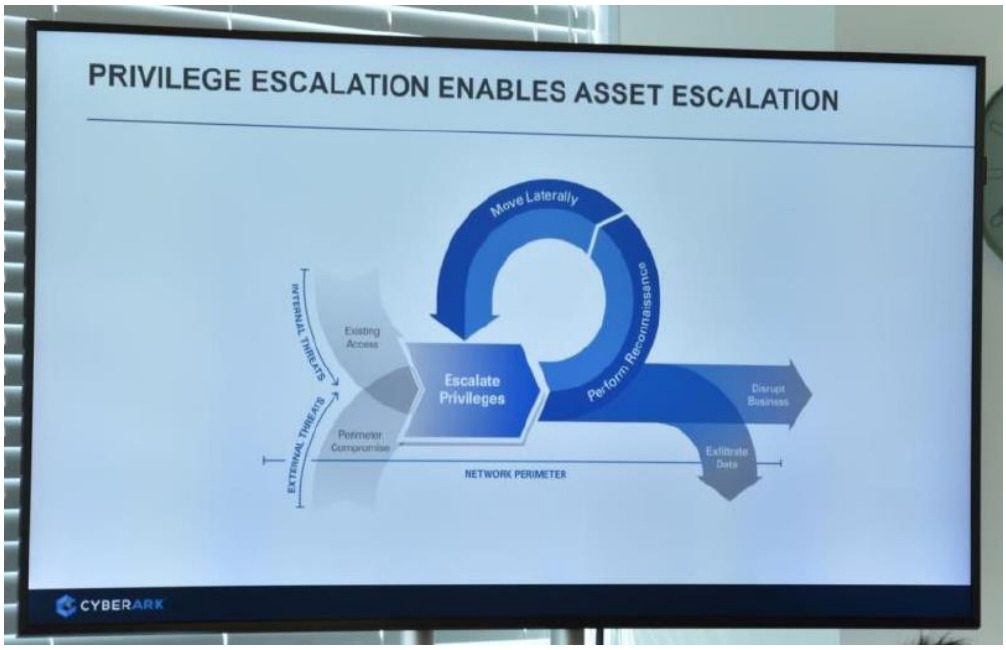
B.重複執行下列步驟，直到攻擊結束：

(A)提升權限(Escalate Privilege)。

(B)偵測要攻擊的目標(Perform reconnaissance)。

(C)水平擴散(Move laterally)。

C.中斷服務或竊取資料，結束攻擊。



駭客入侵手法 (資料來源：CyberArk)

3. 創新實驗室

CyberArk 設有創新實驗室，多位研究團隊成員是以色列 IDF 菁英 8200 部隊退役軍人，平均年齡甚輕，研究主題不限該公司相關產品，研究成果將視公司發展策略，自行商轉或轉賣給其他公司。實驗室辦公室布置，相較於 Bank Hapoalim 創新中心，除有較多隔間，氛圍同樣是非常活潑、自由。

肆、心得及建議事項

(壹)考察心得

一、 放眼天下，國家雖小志氣高

論以色列國土面積、人口，都屬小國，其天然資源也不豐富，今日卻已是科技強國，在科技領域、創業投資等之全球排名，均足以傲人。究其因，與其政府、軍方、學界、企業及人民之願景及努力息息相關。因其國內市場不大，所以產業扶植及創業策略上，就以放眼世界、走向全球，建立國際級企業為目標，自認可以與全球競爭，Radware 就是其中一例。在考察時，數度有以色列業者提到，台灣很好的硬體，加上以色列很好的軟體，成就了以色列科技產業的榮景。反觀國內，常聽到因國內市場太小，所以企業難以壯大之論調；然我國人力素質亦高，實可師法以色列，以創建國際頂尖企業為目標，利用硬體優勢，促進軟體發展，再創經濟成長高峰。

二、 軍方是以色列科技產業孕育搖籃

在本次參訪之不同場合裡，以色列方都有人表示以色列軍方在科技創新領域扮演之角色極為重要。除因軍事需要所促成之科技研發成就外，軍方同時也是科技人才及新創公司很重要的孕育搖籃。如：該國國防軍菁英 8200 部隊，其成員均為分析能力強、具決策力、能團隊合作的年輕人，他們在 18 歲時，就開始在保家衛國之軍事任務中與袍澤協同進行複雜的網路攻防戰，在實戰中練就一身本事、結識創業夥伴、建立事業人脈，因此年紀輕輕就已有經手複雜大案之經驗，退役後不論是創業或進入企業工作，均有成就。此次不少參訪之業者創辦人或重要研發成員，即出自於 8200 部隊。

三、 信任是情資分享的基礎

網路威脅無所不在，曾發生之資安案例，可為其他單位防範之參考，因此情資蒐集是資安防護工作重要的一環。但發生資安事件之機構通常會擔心一旦暴露其事件資料，名譽會受損，甚至受到其主管機關責罰。

CERT-IL 為贏得外界信任，保證向其報告之資安事件資料，絕不會外洩；且為便利訊息分享，因而建立類似臉書機制之資訊分享平台 Cyber Net，鼓勵各界資安人員至該平台分享情資及經驗，並依分享之次數，給予分享者不同等級之評價(如分享較多者，會出現在網頁較顯著的地方)，另外界人員若怕曝光，也可匿名參加該平台。藉由不斷的溝通，逐漸建立大眾對其之信賴與支持。

四、 銀行監理，鼓勵創新與風險控管並重

為管控銀行風險，以色列央行之銀行監理採 Principle-Based，而非 Rule-Based；管理原則為：只規定銀行該做哪些(What)，而不規範銀行該如何去做(How)，給予銀行較大營運空間。為避免扼殺創新，相關法規也隨時因應新興科技進行研議及修訂。

另為因應數位化趨勢，以色列央行在銀行監理部門下成立專責部門，技術與創新組(Technology and Innovation Division)，推動金融數位轉型，鼓勵銀行與金融科技公司間不同型態的合作，導引業者建立金融科技發展準則，進而在鼓勵創新和風險控管之間取得平衡，其彈性與務實，令人佩服。

五、 解決問題導向之思維，創新才有驅動力

此次訪問以色列，除了驚豔於其 FinTech 及資安之發展成果外，以色列人在創新領域之毅力及突破，也有深刻印象，同時也體認到，創新不僅在於個人，更重要的是整個國家都要有創新之共識，形塑成為共同之社會文化，才能讓全體國民，具備創新之 DNA，並且致力於創新。

以色列因為生存環境極其艱困，故能激發出人民透過科技、創新來解決難題、改善現況之生存意志。“Innovate or die.”絕不是口號，因有來自於團體力量之集結，整個社會價值觀、政府政策，乃至於人民之努力，才能在 FinTech 及相關產業展現豐碩的成果。其解決問題導向之思維，使其對於創新有強勁的驅動力，如 Ben Gurion University of the Negev、CyberSpark、BaseCamp、Gav-Yam Negev 等機構設在位於以色列中部沙漠地帶之 Beer Sheva，使其成為以色列科技之都，其設立原意在解決以色列南北失衡、大學生就業及新企業在特拉維夫等大城設立不易等問題。

(貳)建議事項

一、 持續關注以色列金融科技及資安技術發展，適時評估導入

以色列金融科技蓬勃發展，且年輕世代研發人員不受傳統框架的限制，發展出許多別具創意的商品與應用；另以色列多面向的資安防禦技術，也頗可觀。但現行仍有待市場與時間的試煉，以確定其適用性、穩定性、有效性及安全性；可持續關注以色列金融科技及資安技術發展，並與我國及其他國家產品相互比較、評估，適時導入。

二、 網路防禦三要素，不可偏廢

以色列央行資安專家提到網絡防禦三要素：程序(Processes)、人員(People)、技術(Technologies)，不可偏廢。一般人常以為只要有好的技術就可以解決網路安全問題，但網路防禦要做得好，必須訂出妥善的資安政策及作業流程(Processes)，才能遵行、採用適當的技術(Technologies)，才能有效防禦、且要有好的組織管理能力(People)，所有機制及措施才能落實，三者相輔相成，缺一不可。

三、 選用軟體工具，可參考業界看法

依常理論，業界專家對於其業內之產品用途及良窳判斷，有其專業，如：Radware 技術專家對於資安防護工具之採用考量，提出之 3 點建議，即甚具參考價值：

1.新購之工具必須能夠與原有之資安防護工具及作業流程整合。

2.內部人員必須可以有能力自行管理，而非只能依賴廠商。

3.要有好的管理介面，以利快速處理經常須面對之大量告警及事件。

伍、附錄

附錄 1－2019 以色列金融科技及資安產業考察團成員

序號		姓名	機構名稱	職稱
1	團長	郭建中	金融聯合徵信中心	董事長
2	副團長	雷仲達	合作金庫商業銀行	董事長
3	團員	蔡福隆	金融監督管理委員會／資訊服務處	處長
4	團員	廖英傑	金融監督管理委員會／銀行局	副組長
5	團員	李瑞杷	中央銀行／資訊處	副處長
6	團員	黃崇哲	台灣金融研訓院	院長
7	團員	郭春明	合作金庫商業銀行／董事會秘書部	主任秘書
8	團員	蘇清偉	富邦金控股份有限公司	副總經理 資安長
9	團員	王靖欽	富邦金控股份有限公司／資訊處	資深協理
10	團員	王堯德	國泰世華商業銀行／資訊安全部	協理
11	團員	方振維	財金資訊股份有限公司／安控部	協理
12	團員	陳嘉宏	財金資訊股份有限公司／安控部	組長
13	團員	劉美玲	玉山商業銀行 ／用卡暨支付金融事業處	副總經理
14	團員	邱顯堂	臺灣銀行／資通安全處	處長
15	團員	張銘志	臺灣銀行／電子金融部	副經理
16	團員	李嘉銘	玉山商業銀行 ／數位金融事業處資訊發展部	技術協理
17	團員	周芷維	玉山商業銀行／數位金融事業處	代襄理
18	團員	李培蘭	中國輸出入銀行／資訊安全管理中心	專員
19	工作人員	楊 枏	中華民國銀行公會	秘書長
20	工作人員	温國恩	中華民國銀行公會／業務組	組長

21	工作人員	張美華	中華民國銀行公會／業務組	專員
22	工作人員	曹慧蘭	中華民國銀行公會／業務組	助理幹事
23	工作人員	鄭凱名	中華民國銀行公會／業務組	助理幹事
24	工作人員	張凱君	台灣金融研訓院／金融訓練發展中心	副所長
25	工作人員	林秉貞	台灣金融研訓院／海外業務發展中心	專案副理

附錄2－FinTech解決方案廠商簡介 (資料來源:銀行公會提供之考察團活動手冊)

分組一：Data & Infrastructure

DBH-S

DBH-S 藉由關鍵系統產生將其從關鍵系統連續流式傳輸到大數據/數據，從而解開高價值、高核心的內部營運和業務數據。提供的技術對來源不會有任何影響，且可以匯集到廣泛的技術目標。可以幫助啟用分析、行動裝置/網絡 APP，並整合報告和其他重要應用案例。產品 CR8™目前在美國前五大銀行使用，作為從 40 多個高靈敏度系統中提供大量客戶導向數據的基礎。

OpenLegacy

OpenLegacy 專精於自動化 API 創建、優化、測試、部署和管理核心系統，此為整個 API 生命週期。專利方法繞過了複雜的層次，可以直接進入和擴展業務邏輯到 Web、行動裝置或雲端創新，以 Java 客體、RestAPI 或 SOAP 的形式。最重要的是，這個過程不僅快速，簡單和安全，而且不需要特殊的人員技能或對現有系統或架構的更改。

Centerity

Centerity 創建了企業級 IT 監控和性能分析平台，以幫助組織提高性能，降低成本並提高可用性。Centerity 獲獎的軟體提供統一的企業級 IT 監控和性能分析平台，可提高業務服務的性能和可靠性，以確保關鍵系統的可用性。通過在技術堆棧的所有層（包括應用程式、大數據、操作系統、數據庫、存儲、計算、安全、網絡、雲端、Edge 和 IoT / IoT 設備）上提供整合視圖，提供早期性能問題警告以及糾正措施工具。

GigaSpaces

GigaSpaces 為交易處理、事件驅動分析和機器學習提供即時分析平台。協助主要的銀行，如德國商業銀行、美國銀行、瑞銀、法國巴黎銀行、法國興業銀行等，為風險分析、價格預測、欺詐檢測、交易平台、市場數據和其他實際案例，部署關鍵業務應用程序。GigaSpaces 的 InsightEdge 平台是一個開源的內存洞察平台，統一了快速數據分析、人工智慧和交易處理，以實現即時業務洞察和行動。

Privacy Rating

Privacy Rating 是一家監管技術的初創公司，發展為可擴增的企業級平台，用於管理、控制和防止從最終用戶的設備在瀏覽公司網站或使用其應用程序時收集未經授權的私人數據。qprivacy 解決方案適用於所有平台，可以處理所有類型的通信，包括加密或非結構化數據，同時通過設計概念保護隱私，而不影響性能或用戶體驗。

分組二：**Client - Digital/Offers**

CallVU

CallVU 結合豐富的數位互動式媒體和語音，提供極具吸引力的協作式客戶體驗。CallVU 創新客戶服務平台使客戶服務組織能夠在 IVR 呼叫對話期間向智慧手機裝置提供可視內容。CallVU 被 Gartner Research Group 評價為“2016 年在 CRM 客戶服務和支持領域中很酷的供應商”。

Glassbox

Glassbox 利用網路和手機應用程式來增加企業收益，並提高顧客對於企業的滿意度。Glassbox 於 2010 年在以色列開始運營，並得到了美國風險投資公司的支持。原因是因為 Glassbox 擁有一種獨特的技術，可實現無標記分析和會話重播。客戶來自於各個領域的大企業：如最大的銀行、保險公司、電信公司、旅遊公司和電子商務公司。

PayKey

PayKey 通過將智能手機鍵盤轉換為新的服務、信息和通信渠道，從任何應用程式啟用 P2P 傳輸，餘額檢查，銀行通知等，重新定義客戶體驗。PayKey 消除了用戶體驗中的所有摩擦，推動新收入增長，提供全數位客戶服務以及提高客戶參與度和忠誠度。

SecuredTouch

SecuredTouch 的使命是查看用戶在與不同數位頻道交互時生成的看不見的數據。SecuredTouch 的專有機器學習模塊在幕後分析這些獨特的數據，再為客戶和全球合作夥伴帶來關於欺詐和身份的重要見解。

QNomy

Qnomy 開發並實施旨在幫助組織優化其分支機構或商店中的客戶體驗的軟件解決方案。該公司的願景是充分利用每一次客戶訪問藉以提升更多銷售和更高的客戶滿意度。Qnomy 的旗艦產品是 Q-Flow，這是一個集客戶流管理和分支活動管理於一體的軟件包。

Q-Flow 被世界各地的客戶用於各種行業，包括電信、醫療保健、政府、零售、銀行和教育。

分組三：**RegTech/FinSec**

Scanovate

Scanovate 一體化的網絡身份平台，通過自動化和自定義前端和後端流程，使合規性和 KYC 簡單安全。從前端提供整體，無摩擦的客戶端入職解決方案，同時從後端管理所有 KYC 風險和合規性檢查。我們的每個解決方案都非常靈活，可以輕鬆適應或在任何環境中實施。

AU10TIX

AU10TIX 是第二代身分驗證和入門自動化的先驅。 AU10TIX 技術支持全球主要業務，如 Paypal，Goolge，Visa，BBVA 銀行，Payoneer，eToro，Coinbase 等。技術可實現 100％自動取證級身分驗證，多模式生物識別人臉匹配，POA / POR 處理和數據驗證以及 KYC 篩選。第二代技術具有法醫級偽造，變造和附帶風險檢測功能;邊緣質量圖像的轉換率高達+ 300％;多語言文檔支持和快速響應可操作異常報告 所有平均處理速度均為 8 秒或更短。

Shield FC

Shield FC 正在從事金融合規領域中一些最嚴峻的挑戰，例如貿易和電子通信監控、貿易重建、記錄保存、整體調查等。採用新穎的合規方法，建立平台來幫助使用 MiFID II、MAR 要求、AML、記錄保存、GDPR 及甚至電子隱私。

Transmit

Transmit 自 2014 年以來，一直在精心設計和建構一個平台，解決身份空間中最具挑戰性的問題之一。平台提供了跨應用程序管理身份的解決方案，同時保持了安全性和可用性。在日益複雜的環境中，許多企業都在努力快速創新，為客戶提供全通路體驗，使他們能夠領先於新出現的威脅。研發部門位於以色列，是一個網絡安全、應用程序開發和分析人才中心。

Fincom

Fincom 開發了世界領先及時的合規解決方案，基於獨特的語音指紋識別技術，該技術比目前可用的任何 AML 解決方案更快，更準確，更便宜。此外亦開發了一個強大的複雜專有技術平台，可以結合數據庫並匹配他們的條目，使用超過 36 種演算法甚至跨語言和/或具有拼寫錯誤的音譯。同時是世界上第一個自動 AML / KYC 篩選系統，通過利用其專有的先進數學和計算技術來滿足國際貿易，商業和金融交易的監管要求，從而實現全面合規。

分組四：**WealthTech**

iAssessments

iAssessments 旗下產品 Worthy Credit，是一個專有平台，可根據借款人的角色準確評估信譽。Worthy Credit 衡量與消費者債務潛在心理相關的個人能力，並增加傳統信用評分。提供了一個額外的分析層，可以幫助貸方批准更多貸款申請和信貸增加，減少違約和付款拖欠，並更有效為當前帳戶提供服務。

I Know First

I Know First 基於先進的自習演算法提供日常投資預測，該演算法利用人工智慧和機器學習技術來分析/建立模型/預測股票市場。每日都會有超過 3,000 種證券（包括股票，世界指數，ETF，利率等）的預測。該公司的演算法用於發現最佳投資機會，並作為現有投資流程的決策支持系統，以及製定系統化交易策略。

Capitalise

Capitalise 讓您使用自然語言讓您的投資理念變為現實。通過簡單的單詞並將其轉換為可執行和優化的投資，簡化了投資流程。在常見詞彙的簡單性和自動化交易的複雜世界之間架起了橋樑。 Capitalise 基於書面投資方案提供投資組合管理自動化。借助 Capitalise，您可以即時優化您的投資理念，以分析和改善投資。

V-Check

V-Check 是以色列初創公司，在行動支付中，發展出一種創新全球生態系統的解決方案。創造一種新的簡便方法，用革命性的 FinTech 方法取代目前使用的支票、信用卡、銀行轉帳、現金支付。通過 V-Check 用戶的智能手機簡單地控制生態系統，並允許立即和預定（過期支票）付款，指定受益人或第三方受益人。

Pagaya

Pagaya Investments 是一家資產管理公司，為投資於數十億美元在線信貸市場的大型機構提供諮詢服務。利用其機器學習演算法，Pagaya 全程指導機構之投資。Pagaya 透過開發包括先進機器學習技術和大數據分析在內的全套專利技術，為固定收益和替代信貸市場中以替代、數據驅動之投資管理開闢新方法。我們服務於廣泛的機構和高淨值投資者市場，包括銀行、養老金計劃、基金會、私人財富和主權財富基金。