行政院及所屬各機關出國報告

（出國類別：出席國際會議）

參加資安事件應變小組論壇第 22 屆年會

(22nd Annual FIRST Conference)

報告

服務機關：法務部

姓名職稱：林裕泰科長

派赴國家：美國

出國期間：99 年 6 月 13 日至 6 月 18 日

報告日期：99 年 9 月 10 日

摘　　要

「資安事件應變小組論壇 (Forum of Incident Response and Security Teams, FIRST)」第 22 屆年會於 2010 年 6 月 13 日至 6 月 18 日於美國邁阿密舉行，計全球有超過 50 個國家共計 400 餘位人士與會，分享資訊安全方面最新發展趨勢，包含資安威脅型態演變、資安事件因應處理、以及相關技術、工具等，本次會議主題為「跨越消逝的疆界一威脅與事件回應 (Past the Faded Perimeter – Threat & Incident Response)」，強調在網際網路與雲端技術的快速發展下，資安事件之特質已非如傳統犯罪型態侷限於特定國家或區域，相對的資安事件處理在此趨勢下亦將是超越國境之全球性問題，更需要國際間的相互合作。

本次資安事件應變小組論壇第 22 屆年會，以「事件回應」、「管理」與「技術」等 3 個主軸邀請演講者作技術交流與經驗分享，兼具管理層面與技術層面，除有助於掌握國際間資安發展趨勢並增進與國際間資安防護之經驗交流，藉由與會人員的經驗分享並可作為持續強化資訊安全防護及面對資安事件之回應機制之參考借鏡。

目錄

壹、 目的

由於網際網路的迅速發展，各國都對網際網路的發展以及其可能衍生的相關問題投注了相當大的注意力，為了使得其國內的網路安全性更加的鞏固，各網路先進的國家紛紛成立了其國內 CERT(Computer Emergency Response Team)的組織，例如德國的 DFN-CERT、韓國的 CERT-kr、澳洲的 AUSCERT 等。成立 CERT 的目的是希望能夠更加順利的處理危害網路安全的相關事件，以適當的方式來提高網路社群對電腦安全相關議題的注意，並且對於現有的電腦系統進行研究，以提高電腦系統的安全性，進而預防未來可能的電腦安全事件的發生。

CERT 是各個國家、組織或企業自行組成的組織，可以說是一個區域性的組織，但因網際網路的透通性，資安問題已不是單一國家或區域性的問題，而是全球的共同問題，為了協調各個 CERT 的行動，並加強各 CERT 組織的合作，於是成立了一個國際性組織 FIRST（Forum of Incident Response and Security Team），期望達到下列目標：

- 能夠有效的預防可能的入侵事件發生。
- 發生入侵事件時，能及時的察覺，並統合資源，有效的遏止入侵事件擴大並加以控制。
- 入侵事件發生後，能儘快的復入侵行為所造成的損害，並對潛在威脅以及危機事件的處理，提供一個告警及因應處理的機制。
- 提供 FIRST 會員資安相關議題研究之運作平台，讓資訊、技術、經驗及工具等的分享更加容易。

也就是說， FIRST 希望幫助其成員一起分享所擁有的資訊並且處理其共同的問題，甚至訂定未來的策略及計畫，FIRST 年會是該組織所建立之技術交流與經驗分享平台，討論議題兼具管理層面與技術層面，除有助於掌握國際間資安發展趨勢並增進與國際間資安防護之經驗交流，藉由與會人員的經驗分享並可作為持續強化資訊安全防護及面對資安事件之回應機制之參考借鏡。

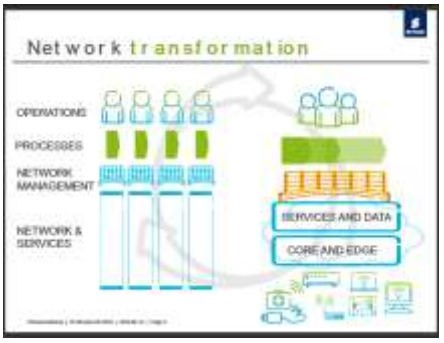
貳、 會議摘要

本次年會於 6 月 13 日至 18 日間在美國邁阿密舉行，於 6 月 13 日下午開始辦理報到程序，當日晚間即舉辦「破冰聚會」(Ice Breaker Reception)，讓各與會成員能在第一時間的交流，自 14 日正式開始為期 5 天的正式會議，會議主題為「跨越消逝的疆界一威脅與事件回應 (Past the Faded Perimeter – Threat & Incident Response)」，強調在網際網路與雲端技術的快速發展下，資安事件之特質已非如傳統犯罪型態侷限於特定國家或區域，相對的資安事件處理在此趨勢下亦將是超越國境之全球性問題，更需要國際間的相互合作。

本次會議的組成，除每日上午安排的關鍵報告(Keynotes)外，是以「事件回應」、「管理」與「技術」等 3 個主軸邀請演講者作技術交流與經驗分享，並分為 3 個場地同時進行，與會人員可視需要擇場次參加，謹就相關會議簡報摘述如下：

一、 趨勢-跨越消逝的疆界

Ericsson 公司講者 Anu Puhakainen 破題指出[1]，隨者網際網路的快速發展，藉由網際網路可連結的龐大運算資源，因而有了雲端運算概念的興起，龐大的運算資源可作為一個共用平台，提供許多的應用服務提供者共同運用，在共用平台上發展各自的服務，這對資訊安全的思維帶來一些改變：



– 駭客的攻擊行為從原來的網路層及系統層向上提升到資料層與服務層。

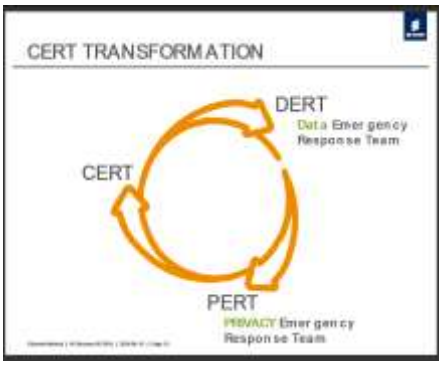
[1] Anu Puhakainen and Michael Skogberg, Ericsson, Fl, “Network Transformation Impact on CERT Teams,” FIRST 2010.

– 藉由網際網路串連的共用平台，提供了更寬廣的攻擊路徑，原有系統間或地理上的疆界將不復存在。

– 信賴與隱私權議題將因共用平台的特性愈益受到重視。

前述改變也將影響 CERT 組織的任務型態與運作模式，除從原來針對電腦危機之緊急應變處理，轉而要兼顧資料危機(Data Emergency)與隱私權危機(Privacy Emergency)之緊急應變處置外，更要做下列準備與提升：

1.國際合作與全時服務：因應資安事件可因網際網路蔓延與跨越地理疆界之特性，各國 CERT 組織間須建立更緊密且零時差的合作關係，且因應不同層級的危機事件（如資料與隱私權），應該要有更專精的應變小組組織（DERT、PERT）。



2.弱點管理與事件回應服務：雲端運算概念興起，但資安事件處理並不會是所有參與者的核心技能，於共用平台上的風險評估、脆弱點管理與資安事件的處理回應機制將會是關鍵服務要項，並有較嚴謹的服務水平要求。

3.新技能發展：因應新型態的威脅與資安事件模次，需要發展新的事件追蹤、數位鑑識等技術與工具；另因應國際合作所需的溝通協調能力亦是不可或缺。

Terremark 公司講者 Robert Rounsavall 特別提及雲端運算對資安事件之回應與鑑識處理帶來新的挑戰[2]，而這挑戰主要來自雲端運所集結龐大運算資源所造成的範圍不確定性。如在雲端運算的某個應用系統發生資安事件時，事件調查者面對的將會是在雲端叢集中的龐大記憶體與磁碟

[2] Robert Rounsavall, Terremark, US, “Challenges for Digital Forensics and Incident Response on Virtualization and Cloud Computing Platforms,” FIRST 2010.

資料，如何從中界定調查範圍就是一個嚴峻的挑戰，此外，由網際網路串起的雲端運算資源，更可能讓資安事件跨過法律管轄權的疆界，使得資安事件鑑識工作猶如「雲海撈針」般充滿不確定性與挑戰。

儘管有重重新的挑戰，但雲端運算對事件處理也不全然是負面的，同樣帶來一些新的契機：

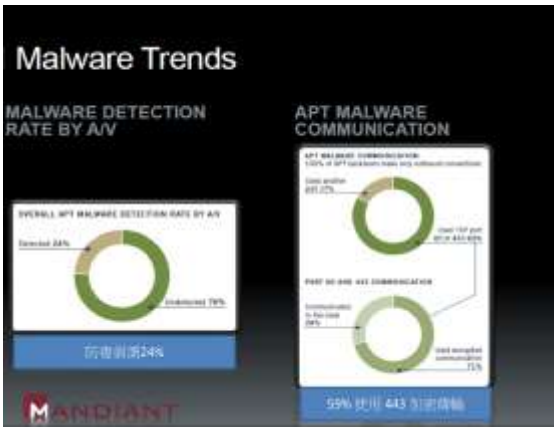
1.因為運算資源的集中管理與共用，因應事件處理的基礎設施與團隊會因受到更多的重視而更加完備。

2.藉由更即時的快照備份機制，使得更接近資安事件發生時間點的資訊得以完整保留。

3.將事件時間點之快照完整保留後，系統可持續運作而不影響資安事件狀態資訊之保全，可將對營運之衝擊減至最小。

二、 威脅-演化與創新

(一) 惡意程式手法推陳出新



防毒軟體是資安防禦不可或缺的一環，惟依據 Mandiant 公司講者 Marshall Heilmann 分享指出[3]，因為駭客手法的精進，惡意程式不斷的推陳出新，一般防毒軟體對新型態惡意程式的偵測率將僅剩 24%，而新型態惡意程式與中繼站間將 100%會使用由內到外的連線手法，讓防火牆、入侵偵測防禦系統等傳統資安設備無用武之地，且其中 83%會利用最常使用的 80 與 443 通訊埠，這裡面使用 443 加秘傳輸埠的又會佔 71%，這使得在資安防護與惡意行為的識別

[3] Marshall Heilmann, Mandiant, US, “Got Spies in Your Wires,” FIRST 2010.

上更加困難。

此外，新型態惡意程式會突破傳統在電腦中植入動態連結服務程式(ServiceDLL)的手法，使得對惡意程式的識別與偵測會更加困難，已經被發現的案例舉例如下：

1.惡意程式透過微軟 MSN client 與發動攻擊者交談(chat)，攻擊者可將指令加密隱藏在 MSN 資料流中，指揮受控管之電腦執行特定指令或進行檔案上傳、下載等。

2.將資料切成許多小的片段，利用 DNS query 隱藏在 UDP/53 通訊埠的網路資料流中，可以支援遠端遙控指令。

3.包裝及安裝為 Microsoft Word 之功能加強模組(Addin)，每當使用者啟用 Microsoft Word 時也同時啟動惡意程式，在將對中繼站之惡意連線與資料傳輸隱藏在 HTTP 資料流中。

除了惡意程式手法的推陳出新外，新型態惡意程式還增加了猶如神風特攻隊的自我毀滅機制，當後門程式發覺無法與中繼站建立連線，這意味著也許惡意連線行為已被發覺，後門程式即會啟動自我毀滅機制，除了執行反安裝程式自系統中移除外，也同時會將系統中所有可追蹤後門程式活動之紀錄同時清除；另也有惡意程式僅設定存在記憶體中，一旦關機後所有活動軌跡亦將屍骨無存，增加資安事件後續鑑識與災損控制之困難度。

(二) 新版惡意程式剖析-BlackEnergy v2

BlackEnergy v1 是目前流傳最廣，廣泛被運用於建立僵屍網路(BotNet)及發動 DDoS 攻擊的惡意程式，同一個作者在 2008 年推出第 2 版，雖至今尚未被廣泛流傳與運用，但對未來的影響已不可輕忽，經過對此第 2 版程式的剖析與解讀，Secureworks 公司講者 Joe Stewart 分享如下[4]：

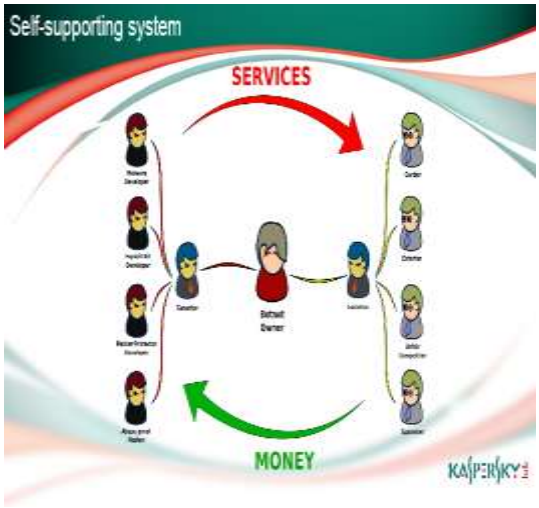
[4] Joe Stewart, Secureworks, US, "BlackEnergy 2 Revealed," FIRST 2010.

1.第 2 版程式主要功能包含下載及執行遠端檔案、使用 cmd.exe 執行本機指令，自動下載及安裝更新程式、設定與中繼站連線頻率，此外，還包含前面提過新型惡意程式會有的自我移除毀滅功能。

2.除了前述主要功能外，第 2 版程式還提供 API 供駭客以 Plugin 方式自行發展客製化功能，而原版程式已有內建 3 種 Plugin 模組可供駭客發動 DDoS 攻擊，寄送垃圾郵件(SPAM)，以及竊取網路銀行相關資訊等。

除上述被發現的主要功能外，被認為最具影響力的，是第 2 版程式中提供了一個開放且易擴充的架構，這意味著，有志之士均可運用此平台進行各種的精進改良及發展客製化功能，猶如一個開放與創新平台，預期可帶動駭客產業更快速的發展。

(三) 僵屍網路市場經濟成型



Kapersky 公司講者 Vitaly Kamluk 指出[5]，電腦被植入惡意程式後往往成為可被駭客控制的僵屍網路，過去僵屍僅為駭客自行運用，但隨著時間的演化，現在已儼然形成了一個自給自足的經濟體系，對僵屍網路有需求者可以透過仲介商向僵屍網路掌控者買得一定數量的僵屍網路電腦，更有甚者，有另一群的服務提供者可為買家特定目的客製化僵屍網路功能，這種交易模式大大降低了有心人士的進入門檻，且因為網路無國界的特性已經成為了一個跨國界的特殊經濟體系。

[5] Vitaly Kamluk, Kapersky Lab, RU, “The Botnet Ecosyatem,” FIRST 2010.

Damballa 公司講者 Gunter Ollmann 指出[6]，另一種僵屍網路的運用模式是利用熱門的社交網站，於社交網站上號召同志，利用可自網路免費下載的 DDoS 或郵件炸彈工具，發動同志於某一時間點對特定對象發動網路攻擊，這種手法不需要駭客入侵技術，只要透過網路集結足夠的同志，一樣可以如僵屍網路的擁有者般發動大規模攻擊以達特定目的，而目前能提出的解決方案也僅有對社交網站上的言論作深層過濾以能預警及防範，惟在執行上並不容易。

(四) 電腦系統以外的網路-跨越另一道疆界

大多數人將資訊安全議題聚焦於電腦系統，但經常會忽略在網路上其他的設備與元件一樣可能成為資安防禦的漏洞，這些設備與元件包含了交換器、路由器、IDS/IPS、VPN、衛星連線、VOIP、PBX、印表機、影印機、行動電話等，RecurityLabs GmbH 講者 Fabian “Fabs” Yamaguchi 分享其可能帶來的風險[7]彙整如下表，雖然遭受攻擊的機會較少，但仍值得關注。

設備種類	可能風險
交換器	藉由 monitor port 取得所有網路流量封包，或利用動態 VLAN 協定改變網路架構。
路由器	曾被發現可利用系統軟體弱點移除網路流量過濾及存取設定(ACLs)。
IDS/IPS	於實驗室測試過程多未包含設備本身遭受攻擊之情形。
VPN	曾被發現存在系統軟體弱點，致允許遠端未經認證之連線存取行為。
衛星連線	經由 GRE 通道可能成為由外直接介接至內部網路之管道。
VOIP	系統軟體經常被發現存在嚴重弱點，但使用者卻很少更新，且部分產品的更新通常是使用未經認證之明碼通信協定。
PBX	較少被關注及作安全測試，但有些 PBX 是以軟體型式安裝在電腦系統中，但並未進行電腦作業之弱點更新。

6 Gunter Ollmann, Damballa, US, “The Opt-in Social Protesting Botnet,” FIRST 2010.
7 Fabian “Fabs” Yamaguchi, RecurityLabs GmbH, DE, “Your Other Network,” FIRST 2010.

儲存裝置	常發現被用作整個組織之分享磁碟，但卻未設定使用者認證機制而形成漏洞。
印表機	曾被發現有可以從遠端擷取列印資訊之弱點。
影印機	大量使用 Linux 平台，但卻很少作安全測試，也未進行 Linux 系統弱點更新。
傳真機	少被關注，但傳真伺服器會結合網路及 Email 功能，這提供了外來攻擊更多的管道。
行動電話	裝置本身可能安全，但在與 3C 網路整合過程常會暴露弱點。

三、 困境-為何攻擊者總是贏家

FIRST 年會聚集各公、私部門的資安領域專家，然而會場卻鮮見對資安防禦充滿信心的言論，反而有許多參與人士大嘆面臨缺錢、缺人的窘境，相關的經驗分享點出現階段資安工作面臨的困境[8]：

1.網路犯罪與詐騙的經濟規模已超越毒品交易成為全球最主要的犯罪問題。

2.儘管 Facebook、Twitter 等社交網站快速走紅，至今最大的雲端運算叢集仍是由惡意程式 Conflicker 所控制的僵屍網路，其可控制範圍至少包含橫跨 230 個國家的 640 萬部個人電腦，1,800 萬顆 CPU，以及 28TB 頻寬。

3.依據 Cisco 的預估[9]，2010 年至 2013 年，網路上的資安威脅數將會由 200 萬成長到 570 萬，因應資安威脅的解決方案相對會百家爭鳴，但在導入時卻會面臨各家解決方案整合不易的困境。

4.因應外在環境的急遽改變，資安解決方案已難有所謂的最佳典範 (Best Practices)，取而代之的是僅能檢視是否能有預期效益，且在

[8] Martin Pillion, HBGary, US, "Fingerprinting Malware Authors," FIRST 2010.
[9] John N. Stewart, Cisco Systems, US, "Who Moved My Cheese? Why The Security Industry Has Been Turned Upside Down," FIRST 2010.

建置過程中須隨時檢視是否因外在環境變化而有與預期效益的落差。

進一步剖析現時的資安防護困境，歸結出下列 3 個原因[10]：

1.工具的複雜化：惡意程式的研發比重超越資安工具的研發，且在不斷創新的機制運作下，資安工具變得愈來愈難偵測到新型態的惡意程式。更具體而言，資安工具的發展其實是追隨著惡意程式的創新前進，追隨者的角色很難改變。

2.攻擊者的複雜化：實務上，一個好的攻擊只需要一個好的攻擊者，而一個防禦團隊如果不是個個精良就無法作好成功防禦，相對經常處於劣勢，另駭客甚至有比資安專家更專業的知識，且因為靠網路犯罪與詐欺可以有豐厚的收入，可以支援相關資源的不斷投入與創新；在人力部分，更可以集結相當多遊手好閒的人投入，優勢相對不站在資安工作者這一邊。

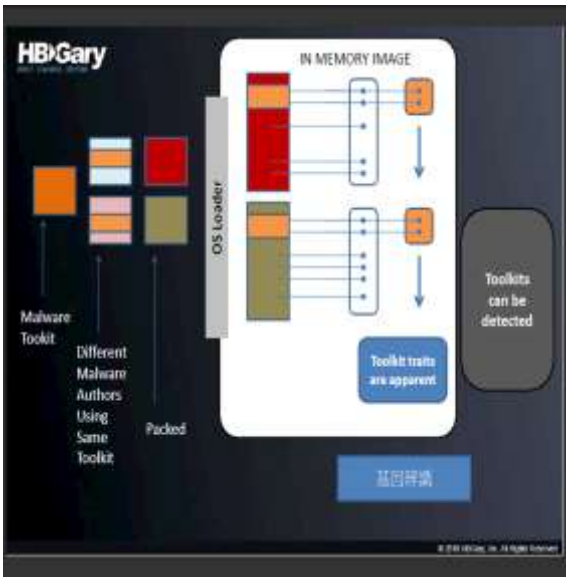
3.資安事件回應的複雜化：一旦發生資安事件時，相關的調查與鑑識太耗成本與時間，且現況普遍缺乏經過良好訓練的資安事件處理團隊。另在投資報酬率的計算上，對資安的投資永遠無法評量，一般企業大部份的資源仍會投注在可實質獲利的商業利益上，這也使得資安事件回應團隊永遠無法取得有利的地位。

四、 發想-改善與突破

集結各方資安專家的年會當然不能僅有洩氣的言論，會議中也有針對資安防護的創新想法與交流,演講者就在規劃中或進行中的創新想法、計畫等提出報告，雖然離產品實作仍有一段距離，但可藉此徵求與會的專家評論與建議。

[10] Marshall Heilmann, Mandiant, US, “Got Spies in Your Wires,” FIRST 2010.

(一) 追本溯源-找出幕後黑手



因惡意程式會不斷演化，如僅是擷取已知惡意程式的特徵值作為辨識依據，將因永遠無法趕上惡意程式演化的速度而偵測效率不。HBGary 公司講者 Martin Pillion 分享一種想法是追本溯源[11]，找出發展惡意程式的源頭工具集，從源頭剖析在惡意程式演化過程會帶著走的辨識特徵碼，此舉如同在各種不同演化的惡意程式版本間作共通之基因辨識，使得惡意程式的偵測不需要再一味的追隨其各種演化與變形，藉由找出幕後黑手可將其徒子徒孫一網成擒，大幅增進惡意程式辨識之效率。

(二) 商業智慧的創新運用-阻絕不合理的存取行為

Intel 公司講者 Matt White 分享商業智慧的應用在資安的概念[12]，其主要來自企業對智慧財產權的保護，如依據對企業智慧財產權的風險因子調查結果，有關智慧財產權之資安事件 71%會發生在技術員工身上；發生在離職與現職員工之佔比為 25%、75%；70%發生在員工離職前 3 週；80%當事人擁有相關資訊的存取權；這樣的統計數據已經可以提供企業作為資安防護重點期間與重點對象的觀察指標，甚至做存取權限調整之重要考量參據，相關處理程序如下：

1.辨識高價值與關鍵性資訊資產。

2.辨識高價值與關鍵性資訊資產存取來源：如與人員相關之職務角色、與地理區間相關之存取地點等。

---

[11] Martin Pillion, HBGary, US, "Fingerprinting Malware Authors," FIRST 2010.
[12] Matt White, Intel, US, " Business Intelligence," FIRST 2010.

3.評估採取的行動：評估風險發生機率、衝擊與風險後，決定所要採取的行動。

舉例而言，某位員工帳號從遠端連線存取公司重要資訊資產，但依據公司差勤資訊顯示，該位員工當日並未到該遠端存取地點進行差旅，這即是一個可疑的連線行為，應該及時加以阻絕。另如對離職前 3 週的員工（較可能發生智財權竊取事件）亦可以於系統紀錄觀察是否相較於平時有異常之存取行為，以即時提供預警與防範。此種應用模式須對企業內部的組織行為有完整的觀察與蒐集，並據以訂定風險因子與採行措施，雖然實作不易，但相較於一般性防禦手法，確為一可以辨識存取行為正當性的較有效方法。

(三) 認識敵人-以人為本辨識脆弱點與風險

Intel 公司另一位講者 Timothy Casey 分享另一個類似的構想[13]，是以人的角色為出發點，分析那些人可能造成資安危害，對象可能包含惡意人士，如恐怖分子、商業間諜、競爭對手、小偷、不滿的員工等；另一種可能是不具惡意的人員，如不小心或未經訓練的員工，進而以風險人物為核心建立人員的威脅屬性，從而建立標準化風險評鑑程序。演講者分享目前已定義以人為核心的威脅屬性包含下列：

1.存取(Access)：對內部網路或設備之存取權限。

2.意圖(Intent)：是否有對組織造成損害之意圖。

3.限制(Limits)：法律或道德上對人員的限制。

4.產出(Outcome)：攻擊的主要目的。

5.目標(Objective)：獲致產出的攻擊標的與方法。

6.資源(Resources)：可用時間、金錢及技術。

---

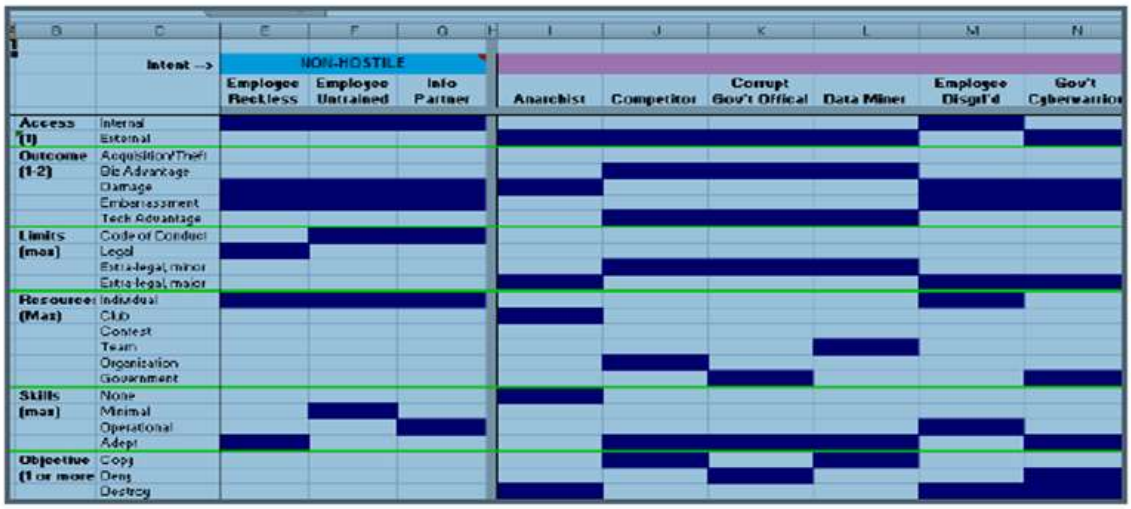
[13] Timothy Casey and Steve Mancini, Intel, US, "Know The Enemy: Cataloguing Agents of Threat for Improved Risk Assessments," FIRST 2010.

7.技巧(Skills)：人員具有的特別訓練與專業。

8.可視性(Visibility)：人員身分與採行異常行動的隱蔽性。

定義風險人物與風險屬性後，即可用以製作標準化人與風險屬性對應表(如下表)，從而建立標準化的風險評鑑程序，除可簡化過去因缺乏標化而導致的每次評鑑結果須進行差異處理之額外負擔外，並進而可依據評鑑結果觀察與設計防護措施，如針對較漫不經心或未經訓練的員工設計防呆輔助防護措施，或針對高風險族群增設檢核點以即時預警等。

Excerpt: Agents-Attributes Map



		Intent →	NON-HOSTILE									
			Employee Reckless	Employee Untrained	Info Partner	Anarchist	Competitor	Corrupt Gov't Offical	Data Miner	Employee Disgr'd	Gov't Cyberwarrior
Access (1)	Internal										
	External										
Outcome (1-2)	Acquisition/Theft										
	Dis Advantage										
	Damage										
	Embarrassment										
	Tech Advantage										
Limits (max)	Code of Conduct										
	Legal										
	Extra-legal, minor										
	Extra-legal, major										
Resources (Max)	Individual										
	Club										
	Contest										
	Team										
	Organization										
	Government										
Skills (max)	None										
	Minimal										
	Operational										
	Adept										
Objective (1 or more)	Copy										
	Deny										
	Destroy										

五、 經驗分享-攘外必先安內

(一) 內部資安事件防範-典範案例與因應處理建議

除了防範外來入侵外，如何減少內部資安事件也是一項重要的課題，依據 CSO Magazine 2009 年對美國五百餘家企業所做調查，曾經發生過內部資安事件的企業約略佔了一半，且有三分之二表示內部事件所造成的損害比外來攻擊來的嚴重，美國 CERT/CC 講者 Randall Trzeciak 並進

而整理了16類內部資安事件的典範案例與因應處理建議於會中進行分享[14]，整理如下表供參：

序號	事件案例	因應處理建議
1	電信公司、信用卡公司及銀行的委外機構系統管理員偷走上百萬筆個人資料。	組織的核心資訊的保護基準，必須同時將外來、內部集合作夥伴風險皆列入考量。
2	前承包商遠端連線竊走商業計畫及軟體，並進而宣稱其具有所有權。	必須有明確可執行的政策與控制措施，可有效減少員工或合作夥伴的不法意圖。
3	委外設計師於離職前一天晚上進入工作夥伴辦公室偷走關鍵程式碼，帶到競爭者公司。	應持續加強員工資安認知與警覺性教育，增進對內部異常行為的防範與警覺，減少發生的機會。
4	憤怒的系統管理者誇大邏輯炸彈之衝擊，脅迫工作夥伴使用備份磁帶。	對情緒或行為異常之問題員工應主動監控及處理。
5	資料庫管理者在與主管長期衝突後，清除關鍵性資料 。	建立可溝通的組織環境，掌控工作環境氛圍。
6	電力公司下包廠商打破緊急電源開關之防護玻璃，關閉供電之電腦系統。	應該加強實體防護措施以避免來自內部或外在的威脅。
7	系統管理這因工作效率欠佳被解雇，離職前建立可遠端攻擊之系統帳號。	應建立嚴謹的帳號及密碼管理機制。
8	憤怒的系統管理者在權限被限縮之前，於系統中置入邏輯炸彈維持管理者權限。	應建立適當分權原則與最低權限賦予機制。

[14] Randall Trzeciak, CERT/CC, US, “Understanding the Insider Threat: Lessons Learned from Actual Insider Attacks,“ FIRST 2010.

9	離職程式設計師在離職前半年於系統中加入惡意程式，離職後半年造成系統癱瘓。	考量軟體發展生命週期中可能隱藏的內部威脅。
10	系統管理者於離職前變更管理者密碼，與公司談判交換離職薪酬。	對系統管理者或特殊權限使用者，應有特別的制衡管控措施。
11	程式設計師擅自變更關鍵程式碼從事個人獲益行為。	應建立系統變更管理機制，預防被蓄意植入惡意程式。
12	研究人員於離職前下載大量營業秘密，帶槍投靠競爭對手。	應建立存取紀錄蒐集、監控與稽核機制。
13	離職 CTO 遠端入侵系統，進行將大量訊息轉向 CEO 之報復行為	應建立分層防護機制，防止遠端入侵行為。
14	管理者於離職夜藉由事先開啟遠端登入口，中斷公司生產線。	應即時撤銷離職員工權限。
15	內部人員造成系統毀損並偷走備份磁帶。	建立安全的備份保存與還原程序。
16	因內部資安事件面臨被調查的主管運用社交工程手法，指使部屬在不知情下摧毀犯罪紀錄	建立具即時性的內部資安事件的處理程序，防止二次傷害。

(二) 企業資安組織發展程序-日本經驗

日本 CDI-CIRT 講者 Toshio Nawa 分享在日本推動大型企業成立資安應變組織的經驗[15]，因國情的不同，日本企業內的資安組織並無法如同歐美般獲得管理階層的充分授權，相較之下，資安組織發展程序也就不同，比較如下：

[15] Toshio Nawa, CDI-CIRT, JP, "CSIRT Models in Japanese Large Companies," FIRST 2010.

步驟	日本以外地區資安組織	日本資安組織
1	獲得管理階層支持	取得員工支持
2	擬定發展策略及計畫	擬定說服計畫
3	蒐集相關資訊	蒐集負面信息
4	規劃願景	設計資安組織定位
5	溝通願景與運作計畫	借力於外部資安專家
6	建立資安組織	建立資安組織文件
7	宣告運作計畫	向管理階層提出資安組織規劃
8	評估運作成效	爭取資安組織預算

整體而言，因為國情的不同，在日本企業的資安組織運作顯得較為艱辛，要花費許多精力去取得管理階層及一般員工的支持，然而，成立資安組織後，對資安事件的減少與因應的即時性仍然有相當大的助益，並爭取到 2009 年的 FIRST 年會在日本舉辦，本屆年會亦有三十餘人繼續參與。我國的國情有幾分類似日本，企業對資安的認知與重視程度不一，日本推動大型企業成立資安組織的經驗或可作為參考。

參、　心得及建議

FIRST 年會提供一個資安訊息分享與交流平台，與會人員多是各國 CERT 組織或公私機構負責資安人員，藉此機會齊聚一堂，不管是發牢騷或分享經驗與新的想法，或都能激發出新的火花，個人以為可以另一種方式來詮釋 FIRST 年會進行的樣態：

– F(Freestyle)：雖然有大會安排的制式議程，但仍營造一個給與會人員相當自在的環境,貼心的提供小團體討論與腦力激盪的小場地，也在每日正式議程結束時，撥出一段時間讓與會人員可以登記上台發言，讓非正式議程的演講者也有上台表達意見的機會。

– I(Innovation)：提供一個創新構想的交流平台，演講者可將在規劃中或進行中的創新想法、計畫提出報告，藉此徵求與會的專家評論與建議，也可號召有志之士共同進行。

– R(Relationship)：於第 1 天即安排「破冰聚會」(Ice Breaker Reception)，讓各與會成員能在第一時間的交流，在會議串場時間也見與會人員三五成群自由交流，有助於建立與會人員相互間之合作關係。

– S(Share)：不管是演講者的報告，與會者的即興發言，亦或會場外的交流，都是與會人員分享的場合。

– T(To-be)：就如同本次年會主題–「跨越消逝的疆界(Past the Faded Perimeter)」，由大會邀請的演講者以關鍵報告勾勒出資訊安全相關議題的發展趨勢,提供與會人員對未來的脈動有較深切的認知，有助於對未來變動準備與因應。

另會議是以「事件回應」、「管理」與「技術」等 3 個主軸邀請演講者作技術交流與經驗分享，雖受限於時間每位講者僅有 30 分鐘至 1 小時的時間進行報告與問答，較偏重於意念的表達而無法太深入，但仍有一些觀點可供本部參考借鏡：

一、加強資安宣導：新型態惡意程式多是利用由內而外的連線模式，令傳統防火牆、入侵偵測防禦系統等資安設備無法攔截，而其入侵的

第一關卡管主要仍是類似電子郵件社交工程手法，於內部人員開啟惡意程式後建立由內而外的連線，因此，持續提升每位同仁的資安意識與警覺心仍是資安防護首要。

二、深化連線及資料存取控管：用商業智慧模型分析、阻絕不合理存取行為之應用，雖僅是會議中發表且仍在研究中之構想，但仍可參採其精神，進一步分析個關鍵資訊系統之使用者連線或資料存取模式，如伺服主機如經分析並無主動對外連線之需求，即可由防火牆予以阻絕，避免遭植入惡意程式後建立由內而外之連線致重要資料外洩；另亦可對使用者連線存取行為作較深切的了解，對不合常規之連線存取建立告警機制以能較即時的因應。

三、增進事件紀錄保全：為應前述使用者行為的分析，異常行為告警，必須先建立完整的存取紀錄蒐集機制，特別是在個人資料保護法修正之後，保管責任加重，如能建置個資資料庫使用記錄保存及分析系統，以彙集存取紀錄，除作為定期稽核之依據，精進個資使用管理及稽查程序與內涵外，更可藉此不間斷掌握個資蒐集、處理、利用流程之每個環節，進一步分析鑑別常規與異常存取行為，建立較即時之告警機制，歸檔記錄另可提供資安事件鑑識研判、證據保全。

四、建置內部防護體系:發生內部資安事件的機會據調查佔有相當比例，且其危害往往更甚於外來入侵，本部因資源有限，資安防護資源多數投注在對外部駭客的防範，內部網路所屬機關並無資安防禦，如能爭取到較多的資源佈建內網所屬機關間之防護設施，可使本部資安防護體系更為完備。

五、增加人力資源妥適分散權責：內部資安事件相當比例源自無法適當的分散系統管理者權責，本部過去辦理依資訊安全管理系統(ISMS)規定辦理風險評鑑時即存在此問題，惟限於現有人力，每個系統負責人已要兼管多項系統，更遑論進行系統管理人員之妥適分工、分散權責，能改善空間依然有限，如能爭取到更合理的人力配置，對降低內部資安風險將可有相當大的助益。

六、普及資安基本能量：就趨勢而言，資安事件跨越國界成為全球性共同問題已是必然，資安事件應變小組將面對更多的挑戰，也需要更多的能量，為我國政府部門多因人力、資源不足，無法建立資安自有能量，大量仰賴行政院國家資安安全會報下設置之技術服務中心，惟此種運作模式是否真能因應資安愈益嚴峻的挑戰是一需要深層檢視的問題，給予各政府機關必要的資源，以及鼓勵民間企業的重視與投入，讓資安能量能夠較為普遍建立應是未來該思考與規劃的方向。

附件：會議議程與相關報告資料