Deloitte.
勤業眾信

2013 TMT Global Security Study

2013 年全球高科技、媒體及電信業資安調查

勤業眾信所屬之德勤全球（Deloitte）高科技、媒體及電信業（簡稱 TMT）服務團隊，近日發表了第六屆的「全球高科技、媒體及電信業資安調查」（2013 TMT Global Security Study），本報告樣本涵蓋全球 38 個國家，120 多位高級資安管理人員，訪問他們對於 2013 年資訊安全需要改進的部分以及如何處理網威脅的看法。

報告中指出，企業將資安策略和規劃當成實務因應的第一要素(去年首重焦點為符合法令規範)；另外企業也開始視資訊安全為企業基礎問題，除聚焦安全性外亦強調增加網路的恢復力。本報告也顯示員工缺乏警覺性和第三方風險，為企業主要安全弱點，並建議管理者著重投資於資訊安全訓練和提高員工警覺性，來減輕新科技所帶來的風險。

德勤全球 TMT 服務團隊表示，企業現在面臨最大的問題已經不是會不會被攻擊，而是何時及如何因應攻擊的發生。有效的資訊安全風險管理應包括一套健全的預防、提早偵測及快速回應機制。換句話說，網路恢復力已經比單一注意網路安全還來的重要。

本報告整理出五大趨勢重點並一一進行剖析：

一、資訊安全投資

在去年，如何符合相關法令規範，是企業首重前三大行動之一，但今年卻連十名內也排不進去，取而代之的是資安策略和規劃，顯示出 TMT 企業現在已意識到資安對於一個企業的成功有多重要，並開始進行投資，因為他們追求的是聰明企業，而非僅僅為了法規要求；但在此同時，卻也有百分之四十九的受訪者認為，缺少預算是改進資安最大的障礙。

德勤觀點：企業開始關注資安議題不再是因為法規需要，而是源於顧客和市場導向的助力。

二、處理外部威脅

許多 TMT 企業可能對於公司內部的資安層級感到過度自信了。今年的調查顯示，88%的受訪者表示他們「非常有自信」或「很有自信」能夠對抗外部的網路威脅，這其中有高過九成二為高科技企業，但是實際上這樣的認知並不實際。目前三大被認為具高度或中度資安威脅的項目為：

1) 第三方的資安漏洞。
2) 阻斷服務攻擊(DOS)。
3)員工的錯誤及疏漏。

德勤觀點：預防措施是重要的一步，但沒有企業可以百分之百防範任何攻擊。企業應增強資安偵測並事先做好預防和規劃，避免安全漏洞變成更大危機。

三、科技與人

新科技是不可避免的，人們必須學著如何去管理它；而科技的進展和使用這些科技的人們，帶來了新的資安風險。受訪者認為人的因素是資安風險最大的來源，也是最難控制的，高過七成受訪者認為其員工缺乏安全意識的程度為中度平均或高；另外根據今年的研究顯示，兩項科技趨勢所造成重大的安全問題為：

1)員工自攜行動裝置(BYOD)潮流。
2)雲端運算潮流中的流氓 IT(Rogue IT)。

德勤觀點：說到資訊安全，不一定會提到因人所帶來的風險，所以這部分也必須成為解決方案中的一項要素。訓練員工和提高其警覺性，可幫助 TMT 企業新科技中有效管理風險。

四、第三方的資安風險

身處於數位供應鏈、委外機制和雲端運算息息相關的世界中，TMT 企業將比昔

日更依賴第三方所提供之服務，也難怪公司會將第三方的風險和弱點，視為他們最大的安全威脅。之前的研究顯示這個問題已經存在一段時間了，但今年更躍升至關注焦點之首，有九成以上雇員超過一萬人的企業認為資安漏洞是他們的「中度」或「高度」威脅，另外有 79%的受訪者認為，提供其服務的第三方具有「中度」或「高度」的資安威脅。

德勤觀點：TMT 企業必須和持續第三方合作，藉以更了解並進一步結合彼此的資安能力，光靠簽訂合約是不夠的。

五、準備採取行動

與去年相比本調查發現，TMT 企業更開始重視資訊安全的面向，並轉而從商業的角度來看待這個議題，而不僅僅是因為法規的需求。企業的下一步是甚麼？商業環境瞬息萬變，傳統的資訊安全方法已經不夠。企業首要的行動應是發展一套策略和規劃，幫助他們了解不斷增加的威脅。不幸的是，許多組織似乎都高估了自己的資安層級，使得他們更容易遭受攻擊。TMT 企業也須主動和政策制定者、監管機構和執法單位進一步合作，因應網路風險問題。

德勤觀點：有效管理資訊安全風險，需要企業同時與在第三方商業夥伴及公共部門合作，加強預防、提早偵測風險並快速做出反應。