操作技術的網路安全：企業必須具備的 7 大洞見

TENABLE 贊助

Ponemon Institute LLC 進行獨立調查

2019 年 3 月

操作技術的網路安全：企業必須具備的 7 大洞見

執行摘要

操作技術的網路安全：企業必須具備的 7 大洞見，由 Tenable® 贊助，Ponemon Institute 進行研究調查。報告顯示，由於技術無法監控攻擊破綻、安全性人員配置不足以及採用人工處理流程，操作技術 (OT) 產業的企業無法符合保障操作技術 (OT) 及企業物聯網 (IoT) 基礎設施免於停機的明文規定。

本報告係根據我們分析 **衡量與管理企業營運的網路風險**[1] 群體的 701 名受訪者所得之結果，這些受訪者皆屬於 OT 產業的企業員工[2]。OT 產業是指營運仰賴工業控制系統 (ICS) 與其他操作技術的產業。所有受訪者擔任的職務皆與評估和/或管理 IT 和/或 OT 網路安全解決方案方面的投資有關。由於現今的操作系統同時仰賴 OT 與 IT 資產，我們研究的對象是 IT、OT 與 IoT。

以下簡要說明調查研究的結果：

1. **OT 環境下的網路攻擊永無休止地接踵而來。** 絕大多數 OT 產業的企業都曾經歷過多次網路攻擊，造成資料外洩及/或企業營運、工廠與操作設備嚴重中斷與停機。許多企業甚至遭遇由民族國家支持的攻擊。

2. **網路風險的評估主要由企業高層負責。** 負責技術、安全性與風險的高階主管為評估網路風險的主要參與者，評估網路風險也是主要的企業業務風險管理工作。

3. **將近有一半的企業都試圖量化網路事件的風險。** 48% OT 產業的企業 (非 OT 產業的企業則為 38%) 都試圖量化網路事件可能對其業務造成的損失，而他們最有可能採用的量化依據，就是 OT 系統的停機時間。

4. **OT 產業企業預期 2019 年將有嚴重的安全性威脅。** 放眼 2019 年，第三方濫用或洩漏機密資訊與 OT 攻擊造成工廠和/或操作設備停機等疑慮攀升。另一項逐日加深的隱憂，則是由民族國家支持的攻擊行為。

5. **2019 年企業治理的首要之務有別以往。** 2019 年的首要之務是，針對企業所面臨的網路安全威脅，加強與企業高層及董事會的溝通，並確保第三方設有最妥善的安全措施保護敏感/機密資料。

6. **2019 年的安全性首要之務是解決複雜的安全性威脅。** 2019 年的安全性首要之務，就是知己知彼，瞭解攻擊者的算計與謀略。這並不令人意外，因為過去 24 個月以來，眾多 OT 產業的企業都曾遭遇由民族國家支持的攻擊。

7. **這些企業所要克服的難題，就是提高網路安全性。** 只有少數企業對於其攻擊破綻擁有足夠的能見度。在人力不足與重度依賴人工處理流程雙重問題下，要具備所需的能見度將仍是一大挑戰。

1 我們調查了美國、英國、德國、澳洲、墨西哥與日本等地的 2,410 名 IT 與 IT 資安從業人員，調查結果載於先前發表的下列報告中：**衡量與管理企業營運的網路風險**。
2 此研究中的 OT 產業包括能源與公用事業、醫藥產業、工業與製造業和運輸業等產業。

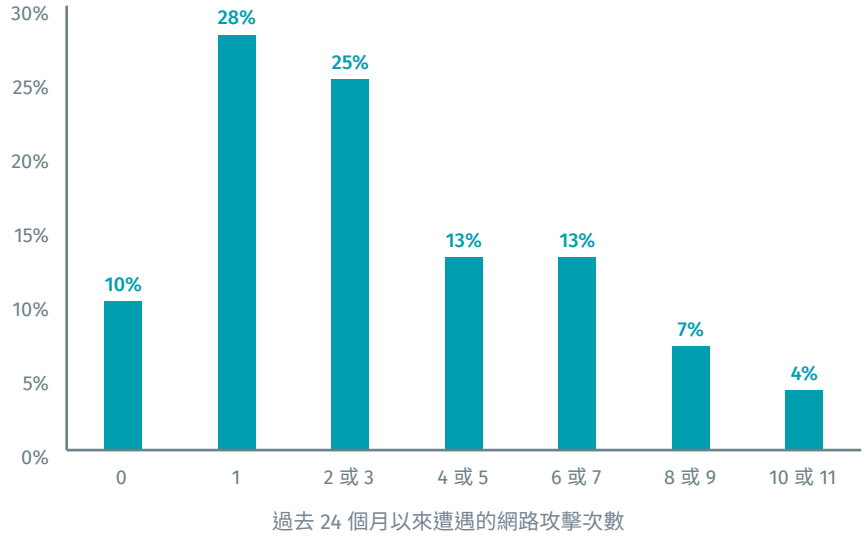
重要洞見

讓我們來仔細探討各項研究結果。

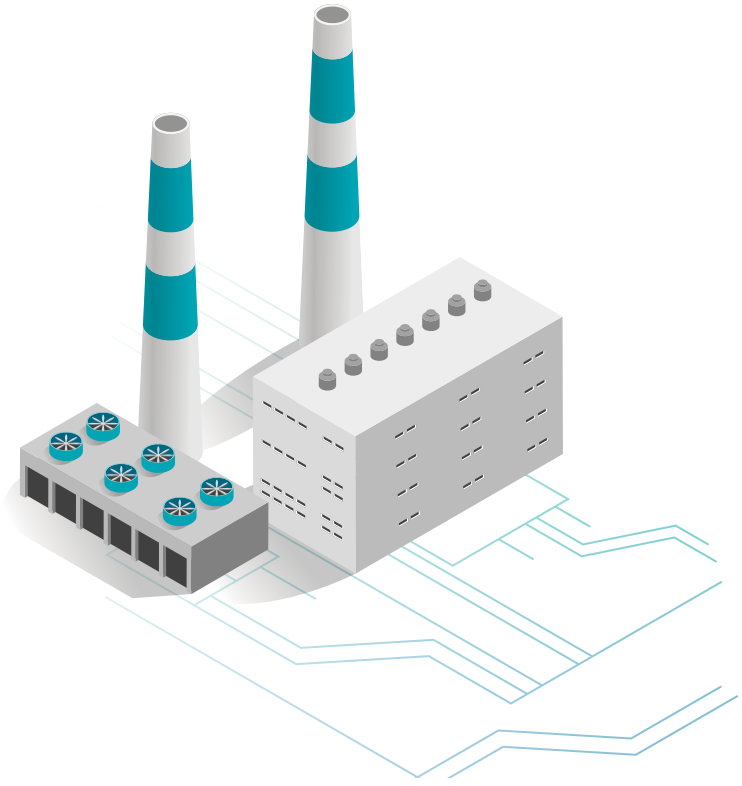
第 1 項結果：網路攻擊永無休止的接踵而來。

如圖 1 所示，本研究中 90% OT 產業的企業在過去兩年中都至少遭遇過一次具破壞性的網路攻擊，甚至有 62% 的企業遭遇到兩次以上。這些攻擊造成資料外洩及/或企業營運、工廠與操作設備嚴重中斷與停機。

圖 1.
OT 產業的企業遭遇多次具破壞性的網路攻擊



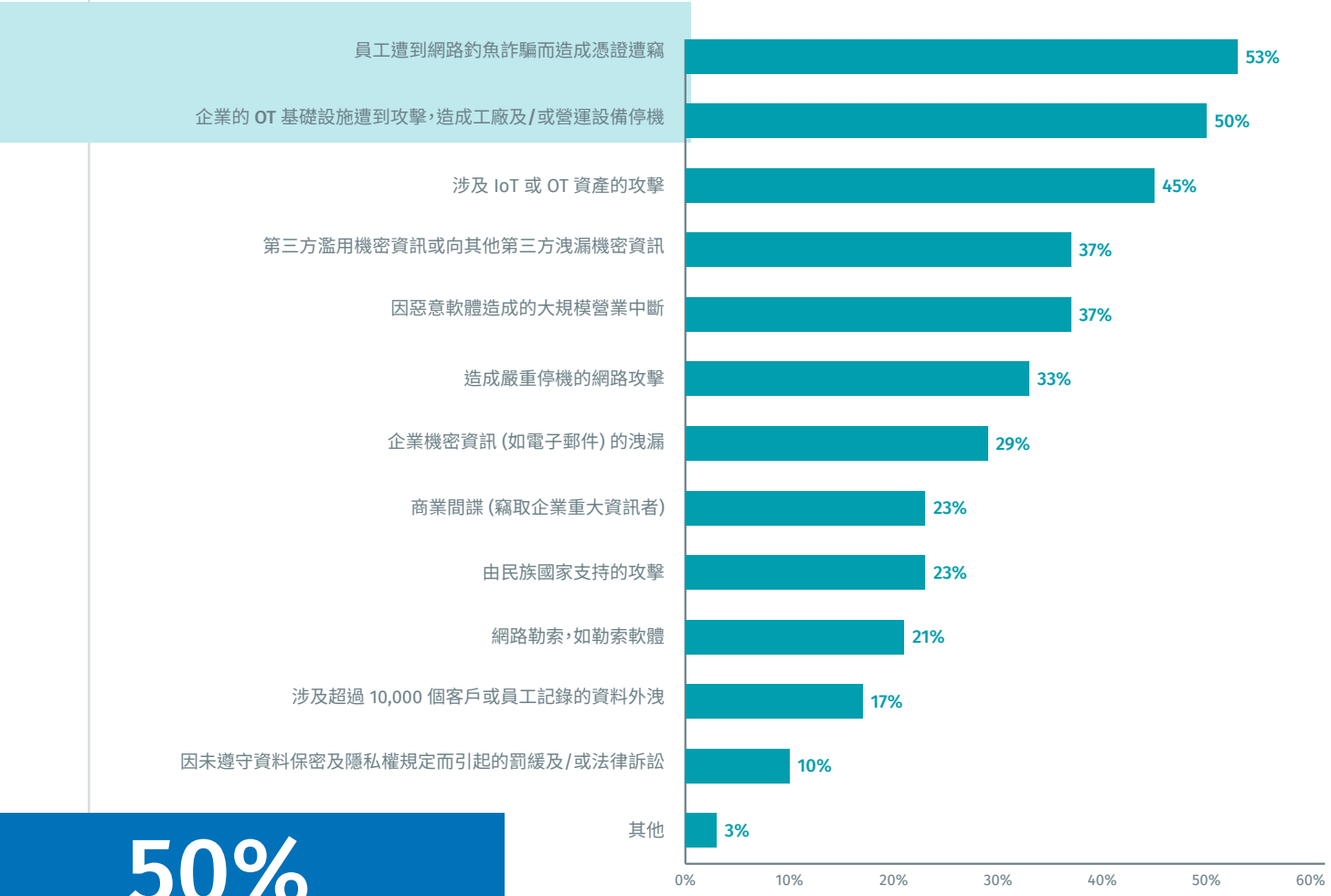
90%
的受訪者在過去兩年間至少經歷過一次破壞性的網路攻擊



幾乎所有的 OT 產業企業都採用 OT 與 IT 融合的系統。因此，OT 產業的隱憂落在 OT 及 IT 系統相關的安全性弱點及攻擊上，包括網路釣魚詐騙。有 53% 的 OT 產業企業曾在過去 24 個月中通報其員工遭到網路釣魚詐騙而造成憑證遭竊的事件 (請見圖 2)。

OT 攻擊者常會利用他們在 IT 環境下取得的憑證潛入及攻擊 OT 基礎設施。有一半的 OT 產業企業表示，他們的 OT 基礎設施曾在過去 24 個月來遭遇至少一次攻擊，造成工廠及/或操作設備的停機。不僅如此，有 23% 的企業曾在過去 24 個月中通報由民族國家支持的攻擊行為。

圖 2. 過去 24 個月中遭遇的網路事件



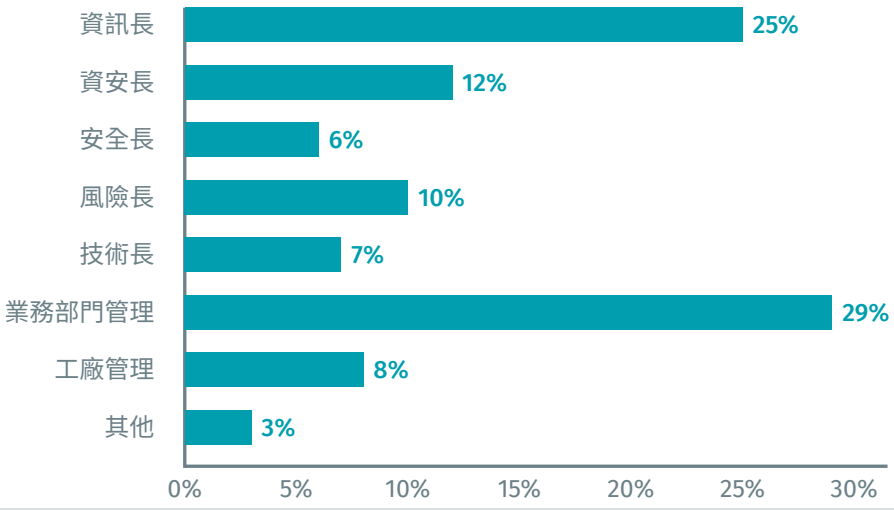
50%

的受訪者曾在過去 24 個月中遭遇至少一次針對 OT 基礎設施展開的攻擊，因而造成停機

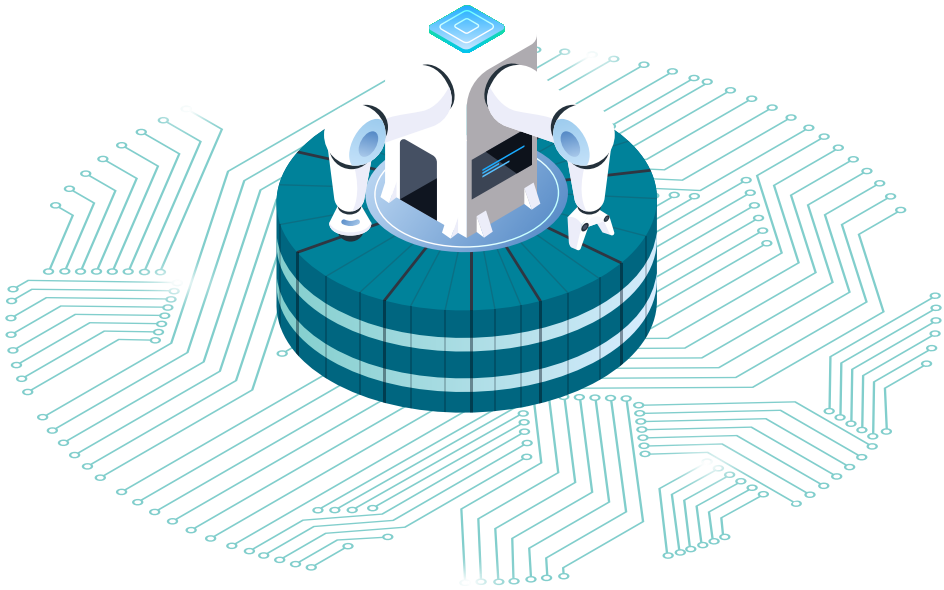
第 2 項結果：網路風險的評估主要由企業高層負責。

結果並不令人意外，超過一半 (60%) 的受訪者表示，企業高層主管為評估網路風險的主要參與者，評估網路風險也是主要的企業業務風險管理工作。主要由部門主管與廠長負責的部分，只佔三分之一 (37%)。

圖 3.
誰主要負責在企業業務風險管理工作中地位重要的網路風險評估？



60%
的受訪者表示，網路風險的評估主要由企業高層負責

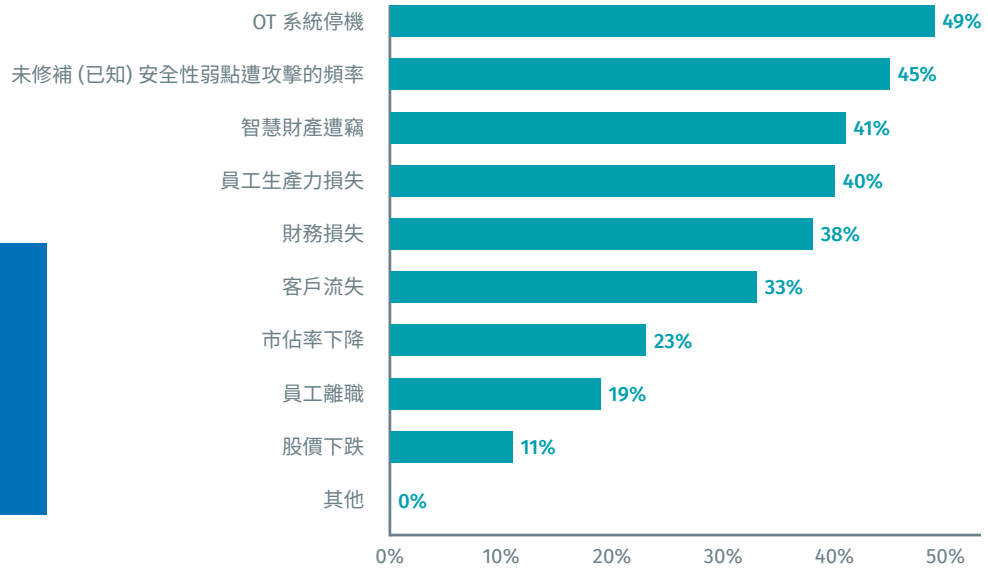


第 3 項結果：將近一半的 OT 產業企業都試圖量化網路事件所造成的損失。

將近一半 (48%) 的 OT 產業受訪者表示，他們的企業試圖將圖 4 所列企業因安全性威脅所遭受的損失予以量化。事實上，將因 OT 系統停機而造成之損失予以量化，可說是量化整體網路風險最主要的因子 (請參見圖 4)。

OT 停機時間可能造成數以百萬美元計的營收損失、生產力降低等。例如，台積電曾通報造成其多個廠房癱瘓的 WannaCry 病毒感染，此事件使其季營收減少 3%[3]，估計損失高達 1 億 5 千多萬美元。

圖 4.
用於量化風險的因子



1/2
的受訪者表示，OT 系統的停機時間是用於量化風險最主要的因子

3 **TSMS 電腦病毒感染事件詳情**

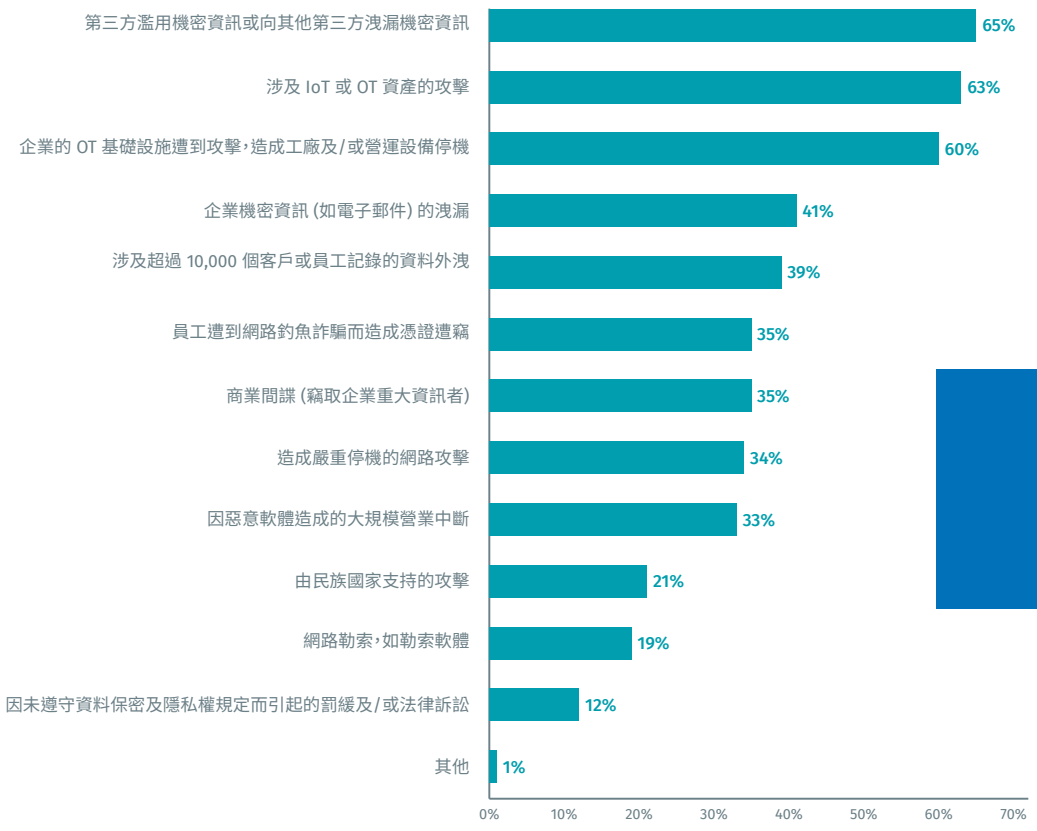
第 4 項結果：OT 產業企業預期 2019 年將有嚴重的安全性威脅。

- **第三方濫用或洩漏機密資訊：**雖然只有 37% 的 OT 產業受訪者表示，過去 24 個月內曾有第三方濫用或向其他第三方洩漏機密資訊 (請見圖 2)，但卻有 65% 的受訪者將安全性威脅列為他們 2019 年的前五大隱憂之一 (請見圖 5)，預期安全性威脅將成為今年的最大隱憂。這一點並不令人意外，因為 OT 產業的許多企業都委託第三方代為管理與維護他們的 OT 基礎設施。

- **造成停機的 OT 攻擊，其威脅程度越來越高：**雖然只有 50% 的企業，其 OT 基礎設施曾在過去 24 個月內遭遇造成工廠及/或操作設備停機的安全性威脅 (請見圖 2)，但卻有 60% 的企業將這些威脅列為 2019 年最大隱憂 (請見圖 5)。

- **由國家支持的攻擊，其威脅性仍舊存在：**超過五分之一 (21%) 的 OT 產業企業將由民族國家支持的攻擊列為他們的最大隱憂之一 (請見圖 5)。OT 產業的企業特別擔心由民族國家支持的攻擊，因為此類攻擊的發動者通常都是資金充裕、技術高超的網路罪犯，他們的目標通常都是重大基礎設施。[4]

圖 5. 2019 年最大的隱憂：安全性威脅



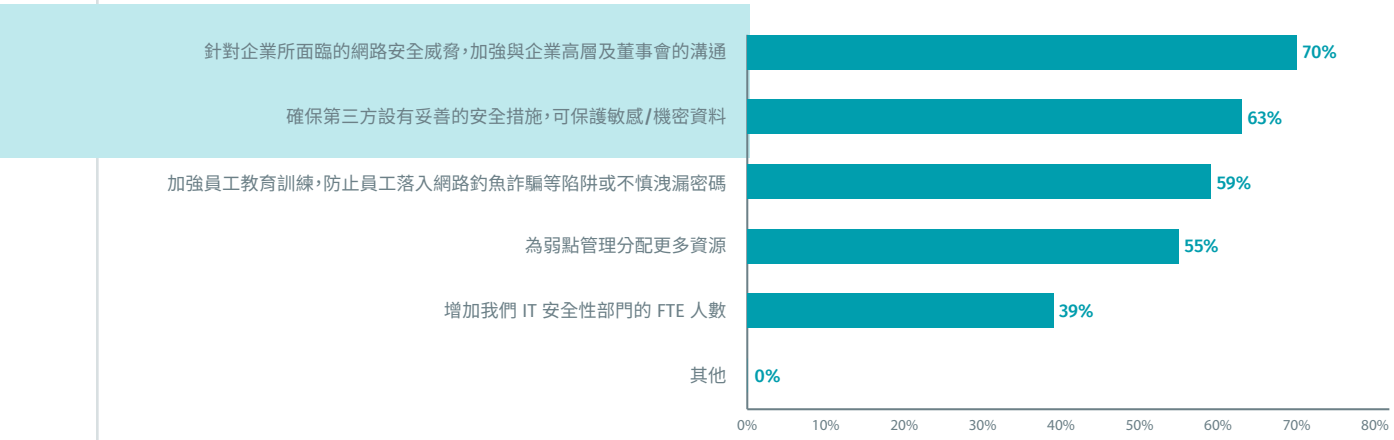
60%
的受訪者擔憂其 OT 基礎設施遭到攻擊

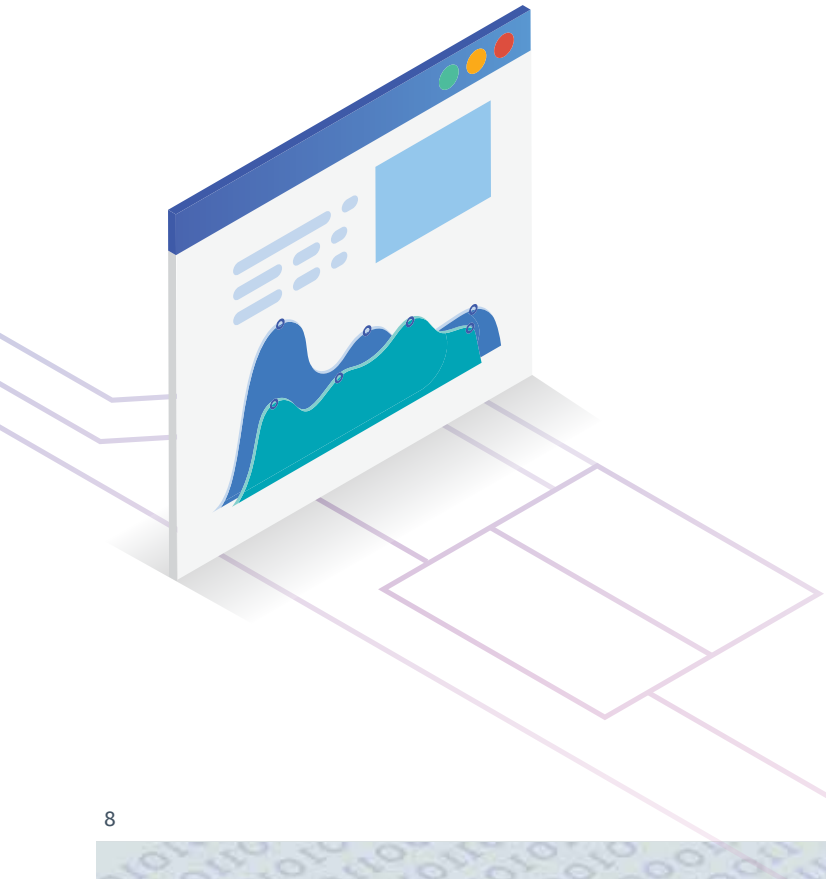
4 請參考**美國國土安全部電腦緊急應變小組技術警示「鎖定能源與其他重大基礎設施產業為攻擊目標的俄羅斯政府網路活動」**

第 5 項結果：2019 年企業治理的首要之務有別以往。

針對企業所面臨的網路安全威脅，加強與企業高層及董事會的溝通，是 2019 年的第一大首要之務 (請見圖 6)。第二大首要之務，是確保第三方設有妥善的安全措施，可保護敏感及機密資料。此目標也直接印證了 2019 年最令人憂心的安全性威脅：第三方濫用機密資訊或向其他第三方洩漏機密資訊 (請參見圖 5)。

圖 6. 2019 企業治理的首要之務

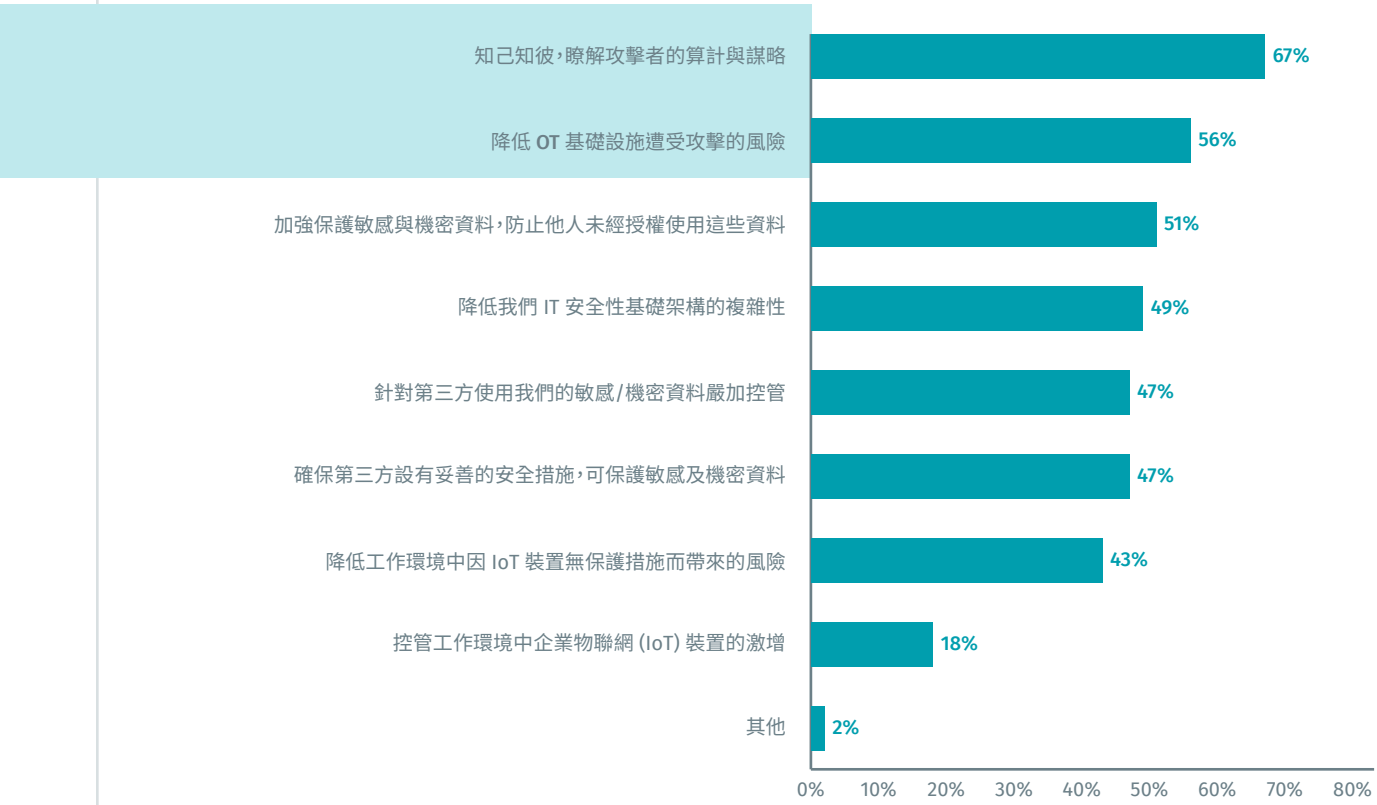




第 6 項結果：2019 年的安全性首要之務是解決複雜的 OT 安全性威脅。

如圖 7 所示，前兩大首要之務「知己知彼，瞭解攻擊者的算計與謀略」與「降低 OT 基礎設施遭到攻擊的風險」也印證了之前所討論的「由民族國家支持的 OT 基礎設施攻擊」(請參見圖 2)。

圖 7. 2019 年安全性首要之務



第 7 項結果：這些企業所要克服的難題，就是提高網路安全性。

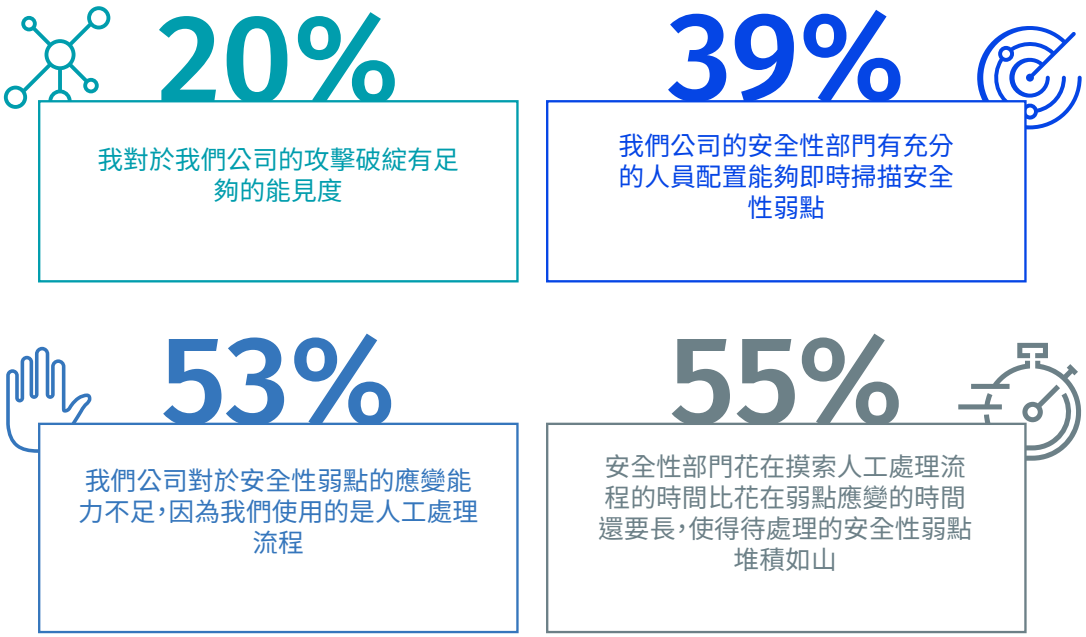
對於攻擊破綻的能見度不足

要求受訪者在五個等級 (從非常同意到非常不同意) 中選擇時，只有 20% 的 OT 產業受訪者同意或非常同意他們對於企業的攻擊破綻擁有足夠的能見度 (請見圖 8)。這個結果令人憂心，因為所有的安全性控管與處理流程都取決於完整資產庫的能見度。硬體與軟體資產庫是否完備，對於所有的安全性架構及合規性要求十分重要，包括了改進重大基礎設施網路安全的 CIS Controls、NIST Framework 以及 NERC CIP。

人員配置不足以及採用人工處理流程侷限了弱點管理

網路安全技能不足使仰賴人工處理流程的問題變得更加嚴重。此類的技能不足在弱點管理方面尤其明顯，因為企業所配置的弱點管理人員數量通常都不足以執行人工處理流程。

圖 8. 對於安全性團隊所面臨之難題的看法



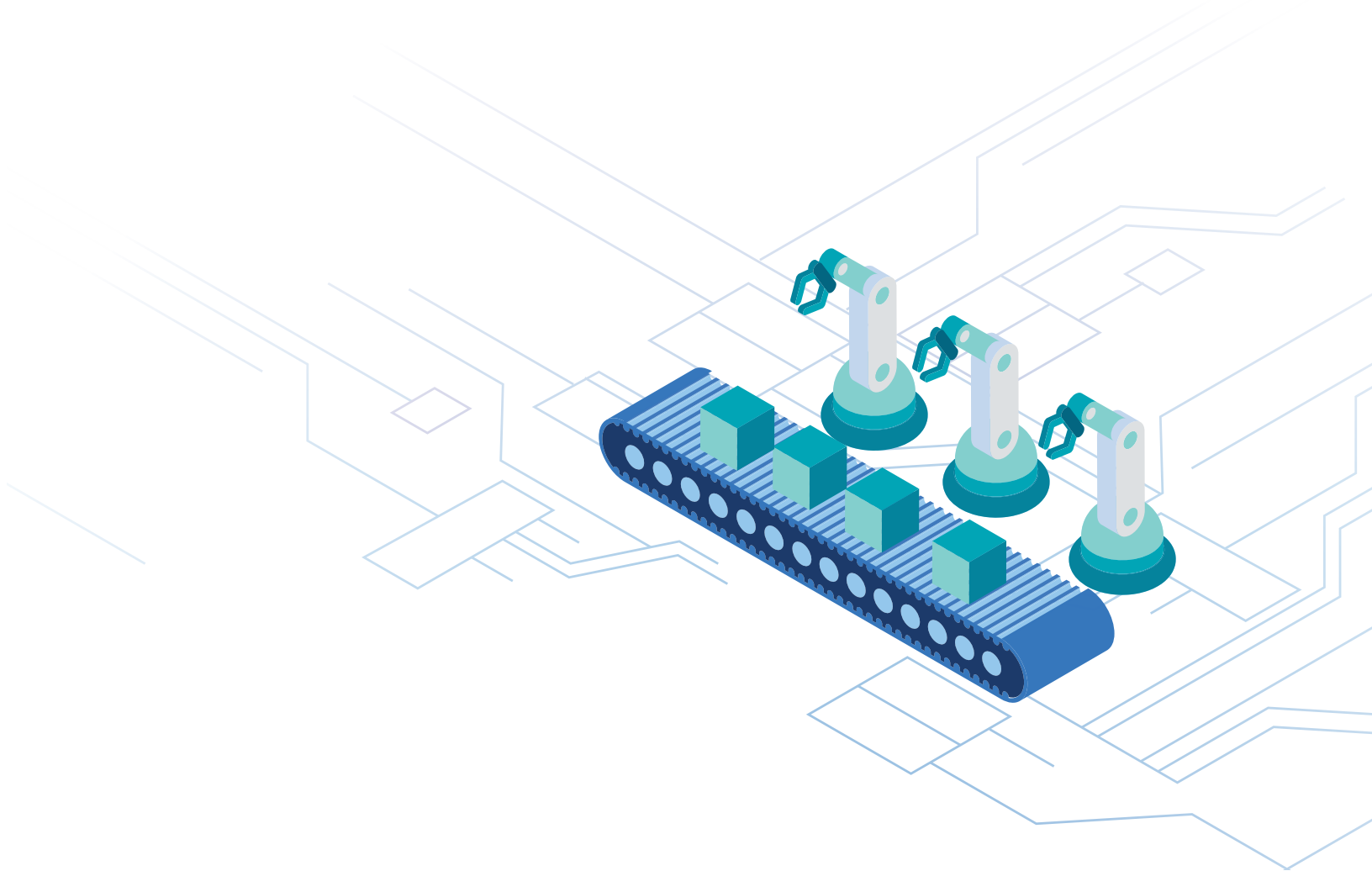
百分比表示非常同意與同意之受訪者加總後的比例

結論

OT 產業的企業正在調整 2019 年安全性首要之務，以解決 2019 年的最大隱憂。調查結果針對改進 2019 年及其後的安全性問題提出建議事項：

- **針對企業所面臨的網路安全威脅，加強與企業高層及董事會的溝通**。這種做法可找出並消弭企業風險偏好與實際曝險之間的差距。
- **提高對攻擊破綻的能見度**。盲點會造成 IT 與 OT 系統脫離控管而無保護措施。企業需有完整的能見度才能評估其風險。
- **擴大使用自動化處理流程**以彌補安全性人員配置的不足。
- **持續留意因 IT 與 OT 系統之間相互依存而對安全性造成的影響**。IT 系統的安全性弱點與其他弱點可能會使與其相互關聯的 OT 系統也曝於風險中，反之亦然。

您是否需要監控 OT 基礎設施方面的協助？請瀏覽部落格貼文「**進一步深入瞭解操作技術環境**」。



如果有任何疑問，請寄信至 **research@ponemon.org** 或撥打 **800.887.3118**。

Ponemon Institute

促進可靠的資訊管理

Ponemon Institute 致力於獨立研究及教育訓練，其宗旨為在企業與政府中促進資訊與隱私權管理措施的可靠性。我們的使命是針對影響人員與企業相關機密資訊之管理與安全性等重大議題，進行高品質的實證研究。

我們對於資料嚴格保密，嚴守隱私權與高度道德標準。我們不會向任何個人索取用於辨識個人身份的資訊 (研究對象為企業時，亦不會索取用於辨識企業的資訊)。不僅如此，我們設有嚴格標準，保證絕不詢問受訪對象其他無關緊要、不相關或不適當的問題。

7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

http://zh-tw.tenable.com