HENNGE

台灣資安/網路攻擊大調查

2022

目錄

調查方法

調查方法

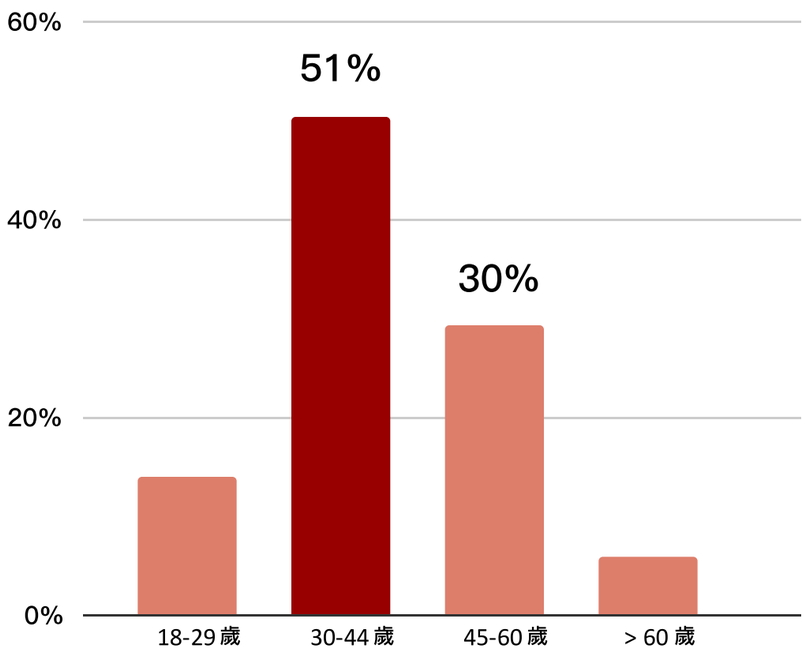
我們使用 SurveyMonkey 的雲端線上問卷，在 2022 年 6 月 3 日調查了 100 位台灣企業 IT 決策者。

透過這份問卷，能夠了解資訊時代下，IT 主管們如何看待網路攻擊、企業有何種防範措施、以及網路攻擊的影響層面為何。

樣本概況

1. 年齡概況

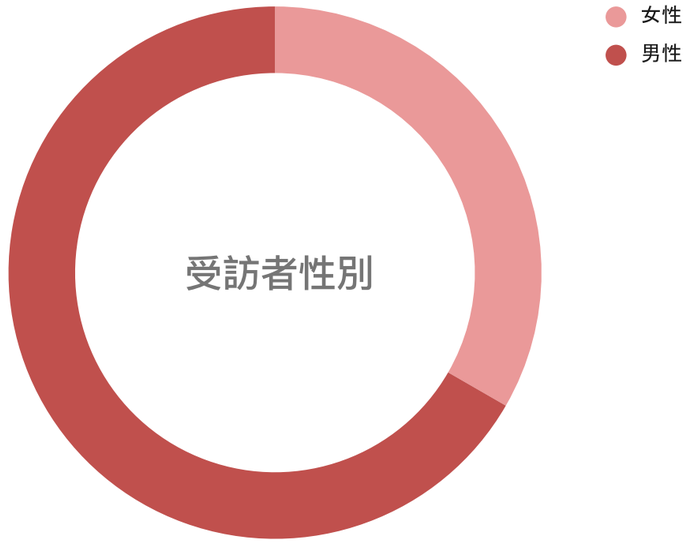
整體樣本以 30–44 歲為大宗，約占 50% 的填答者，其次為 45–60 歲，占比為 30%。



受訪者年齡

2. 性別概況

33% 的填答者為女性，67% 則為男性。女男比約為 3:7。



無處不在的網路攻擊

全球資安/網路攻擊的威脅不容小覷

根據世界經濟論壇（World Economics Forum）於 2022 年 1 月 11 日發布的年度全球風險報告指出。2020 年全球勒索軟體案件數增加 435%，增長趨勢仍在持續。此外，報告也指出，網路攻擊威脅已經連續三年為全球前十大風險之一。

網路攻擊為何而來？如何進行？

網路攻擊是指透過惡意軟體等蓄意手段，試圖非法侵害公司電腦系統與內部資料，並以勒索、威脅等手段從中獲取利益。此外，網路攻擊也可能服務於政治目的或某些難以歸類的私人因素。

當代社會最常見的九種網路攻擊種類，您都知曉嗎？ Icons from flaticon.com

惡意軟體
Malware

網路釣魚
Phishing

中間人攻擊
Man-in-the-middle Attack

阻斷服務攻擊
DDoS Attack

SQL 隱碼攻擊
SQL Injection

零時差攻擊
Zero-day Exploit

密碼攻擊
Brute-force Attack

跨網站指令碼
Cross-site Scripting

社交工程
Social Engineering

近 9 成台灣 IT 決策者認為網路釣魚與惡意軟體是最常見的威脅

惡意軟體與網路釣魚廣為大眾所知

根據調查，約有 90% 的 IT 決策者聽聞/了解何為網路釣魚（Phishing），這類攻擊手法通常透過電子郵件進行，以可信的來源為誘餌引誘受害者上鉤，並從中獲取機敏資訊。

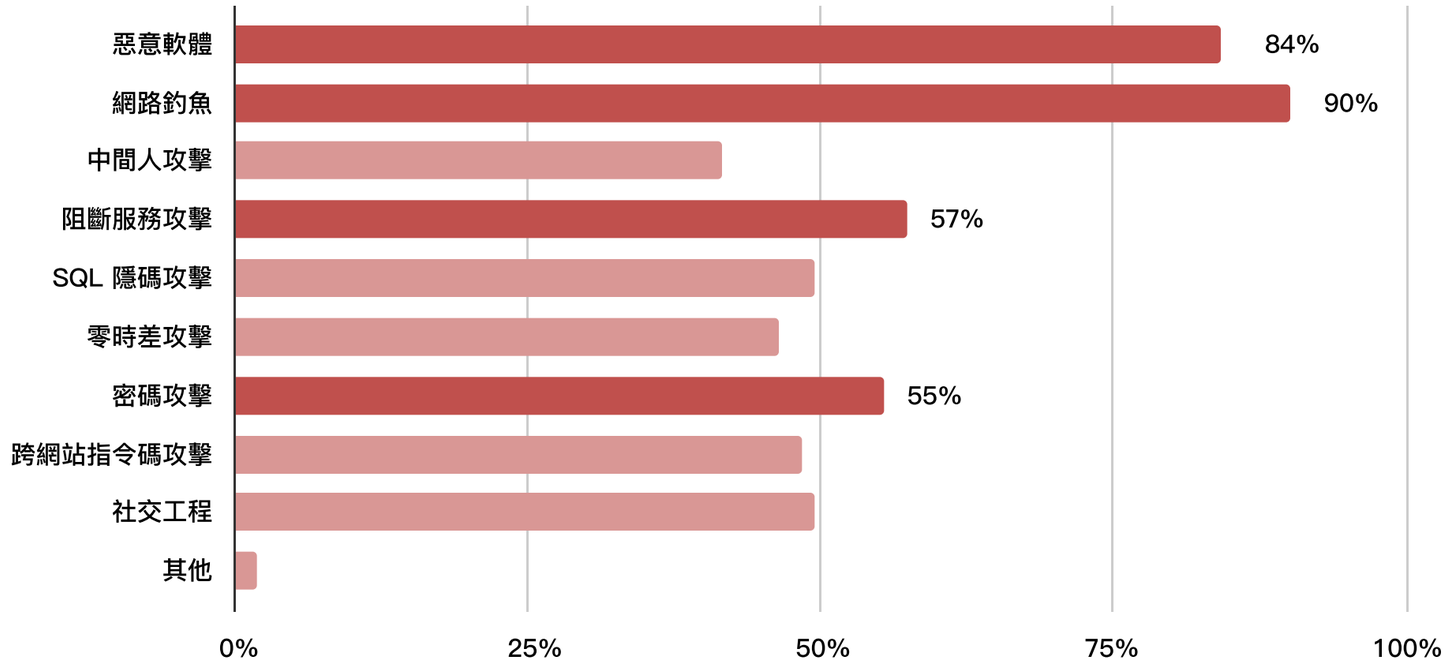
另外，惡意軟體同樣廣為人知，約有 84% 的 IT 決策者聽過此種攻擊威脅。惡意軟體攻擊包含了勒索軟體、病毒、木馬程式等可能入侵資訊系統的威脅。

阻斷服務攻擊與密碼攻擊

57% 的填答者表示曾聽聞阻斷服務攻擊（DDoS Attack），這類攻擊主要透過耗盡目標電腦的網路或系統資源，使服務暫時中斷或停止，導致正常使用者無法存取。

最後，約有 55% 的 IT 決策者認知到密碼攻擊（Brute-force Attack），此種攻擊是透過暴力攻擊的方式逐一測試可能的密碼，直到成功破解密碼為止。

Q1　請問您聽過哪些網路攻擊類型？（多選）



過半數的台灣企業認為「惡意軟體」構成企業最大威脅

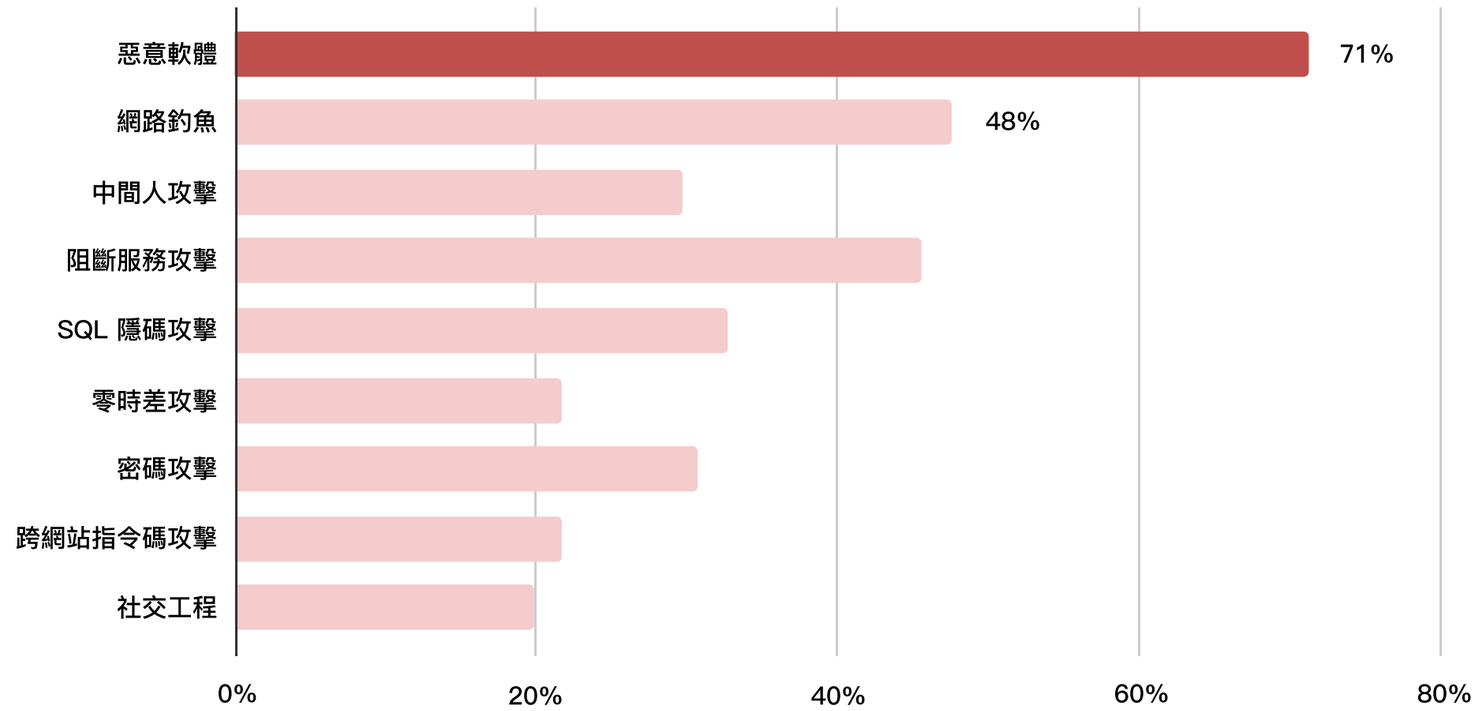
71% 的企業最擔憂惡意軟體的威脅

有 71% 的 IT 決策者表示惡意軟體為企業眼下最擔憂的網路攻擊類型。根據微軟去年釋出的 Microsoft Defender Antivirus 遙測數據顯示，疫情爆發後，亞太地區受到勒索病毒攻擊的頻率增加了 2.4 倍。而其中，台灣遭到攻擊的機率更是相比亞洲其他國家高出整整 2 倍。

惡名昭彰的 Emotet

提到惡意軟體，近期最受人矚目的即是 Emotet。Emotet 自去年 11 月出現後，近期攻擊頻率加劇，全球約有 5% 的企業身受其害，眾多國際企業被要求天價贖金。Emotet 的慣用伎倆是將惡意軟體附件在電子郵件中寄出，這些釣魚信件看似是來自商業夥伴，實則具有巨大危險。

Q2 請問貴公司最擔憂的網路攻擊類型為何？（多選）



網路/資安攻擊正在發生轉變

鎖定攻擊最脆弱的部分

近年來，諸如 Emotet 惡意軟體與 Lapsus$ 組織等威脅甚囂塵上，有些企業甚至因這些攻擊而停工。

那麼這些攻擊手法究竟有什麼樣的不同呢？事實上，這些攻擊和過去相比最大的不同，在於他們攻擊了商業結構中最脆弱的部分。知名企業是經由合作公司的感染而深受 Emotet 攻擊之苦；跨國公司則是因為針對外包人員的社交工程才受到 Lapsus$ 的惡意攻擊。

前往 HENNGE Taiwan 部落格了解網路攻擊究竟發生了哪些變化？ >

請確保所有商業夥伴都有足夠的安全措施

許多企業試圖增強自己的安全措施以確保公司自身在任何情況下都能安全無虞。但如今商業環境有賴多間企業共同合作才能順利運作，因此光是強化企業自身的資安是不夠的，最安全的做法應該是確保所有相關企業皆有足夠的安全措施。

台灣 IT 決策者認為未來的網路攻擊事件可能增加

IT 決策者大多同意未來的網路攻擊事件將會增加

根據調查結果，100 位 IT 決策者填答「網路攻擊在未來五年內是否會增加」題目之平均分數為 76 分，代表不論是大環境、政治、經濟等因素，使得未來的網路攻擊趨勢不減反增。

Q3 請問您認為網路攻擊（Cyber Attack）在未來五年內是否會有增加趨勢？

居家遠距辦公成為網路攻擊的隱憂

近年來，居家遠距辦公（Work From Home）被越來越多企業採納，但居家辦公的資安疑慮與遠距技術的支援需求增加另不少 IT 決策者擔憂，居家遠距辦公可能成為企業資安的隱憂。

此題填答者的平均分為 73 分，表示 IT 決策者同意「居家遠距辦公」可能對公司的資安造成威脅。

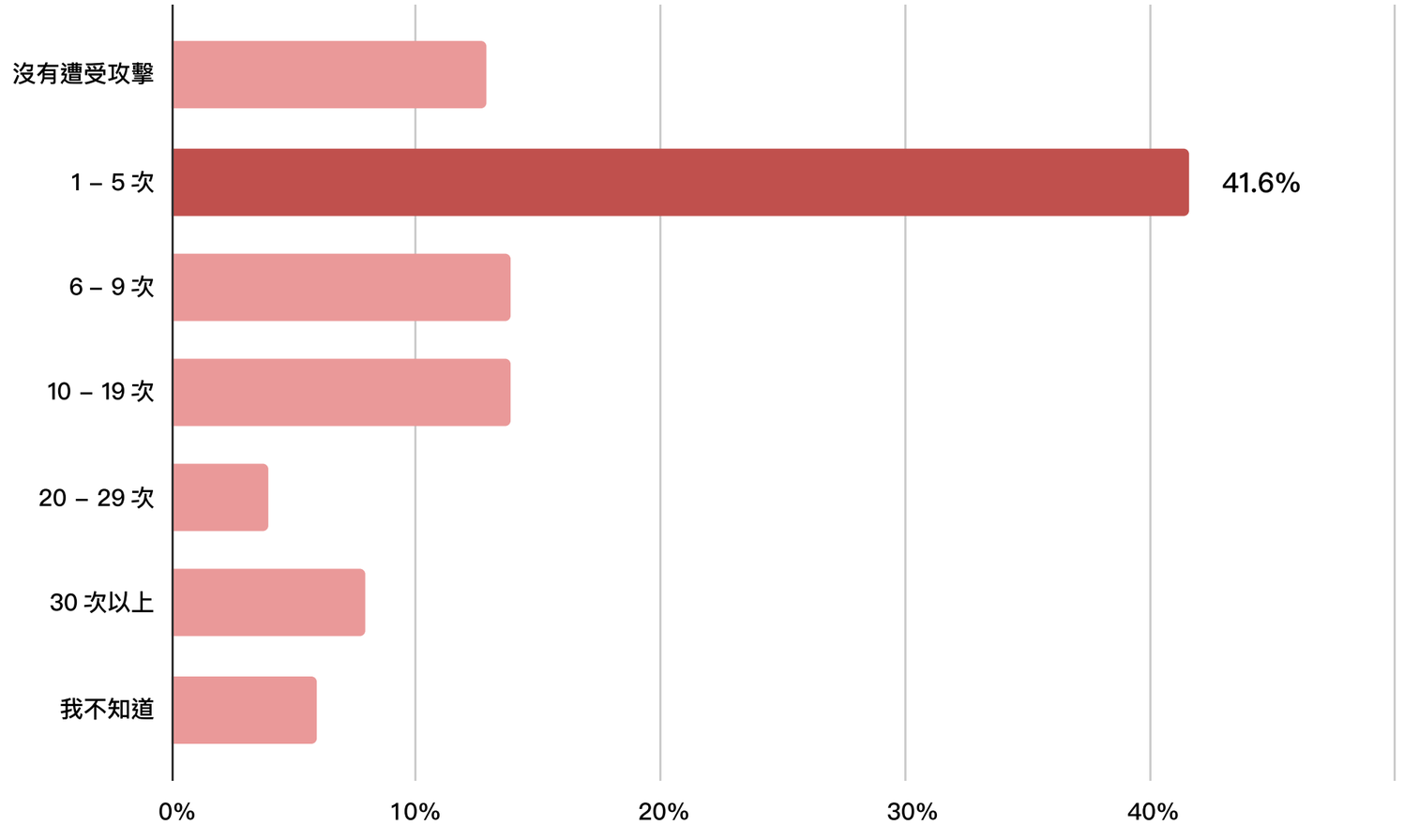
Q4 請問您認為居家遠距辦公（Work From Home）是否會加劇網路攻擊的可能？

約 80% 的台灣企業在過去一年裡遭遇網路攻擊

網路攻擊的頻率超乎想像

從調查結果得出，台灣企業遭逢網路攻擊的頻率遠比想像的高。整體而言，高達 8 成的企業表示過去一年曾遭遇網路攻擊威脅。這其中約有 42% 的企業受到的攻擊次數介於 1 – 5 次之間，有大約 8% 企業表示遭受攻擊的次數超過 30 次。

Q5　貴公司在過去一整年中遭遇網路攻擊的頻率為何？

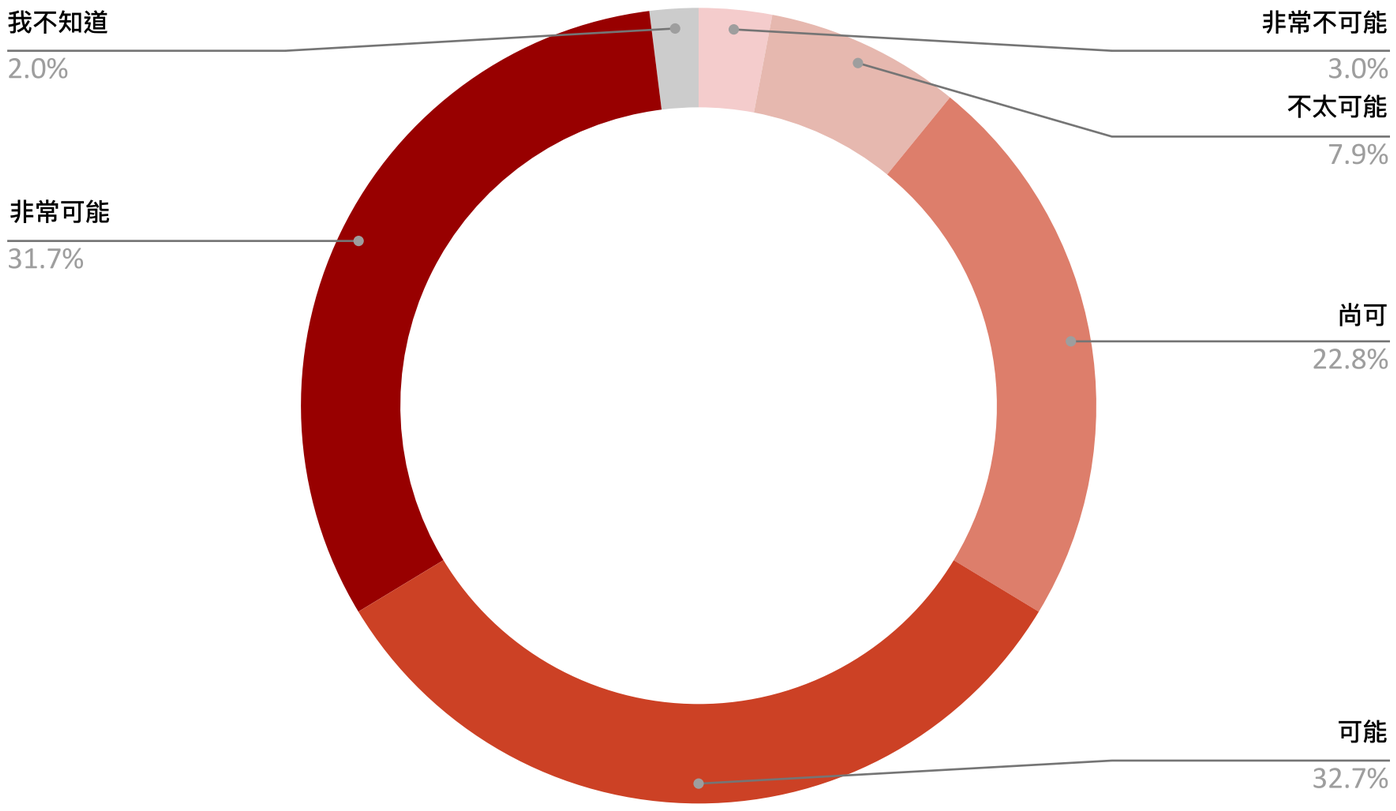


超過 6 成 IT 決策者認為企業未來將會再次受到網路攻擊

企業未來再次遭受網路攻擊的風險甚高

未來或許更令人擔憂。根據我們的調查，高達 64% 的受訪者認為自身企業在未來一年內會再次受到網路攻擊。資安政策的落實、強化因應攻擊的能力是企業面臨的重要課題。

Q6 您認為貴公司在未來一年內遭到針對性網路攻擊的可能性為何？



近 5 成 IT 決策者認為既有的防範系統難以抵禦未來的網路攻擊

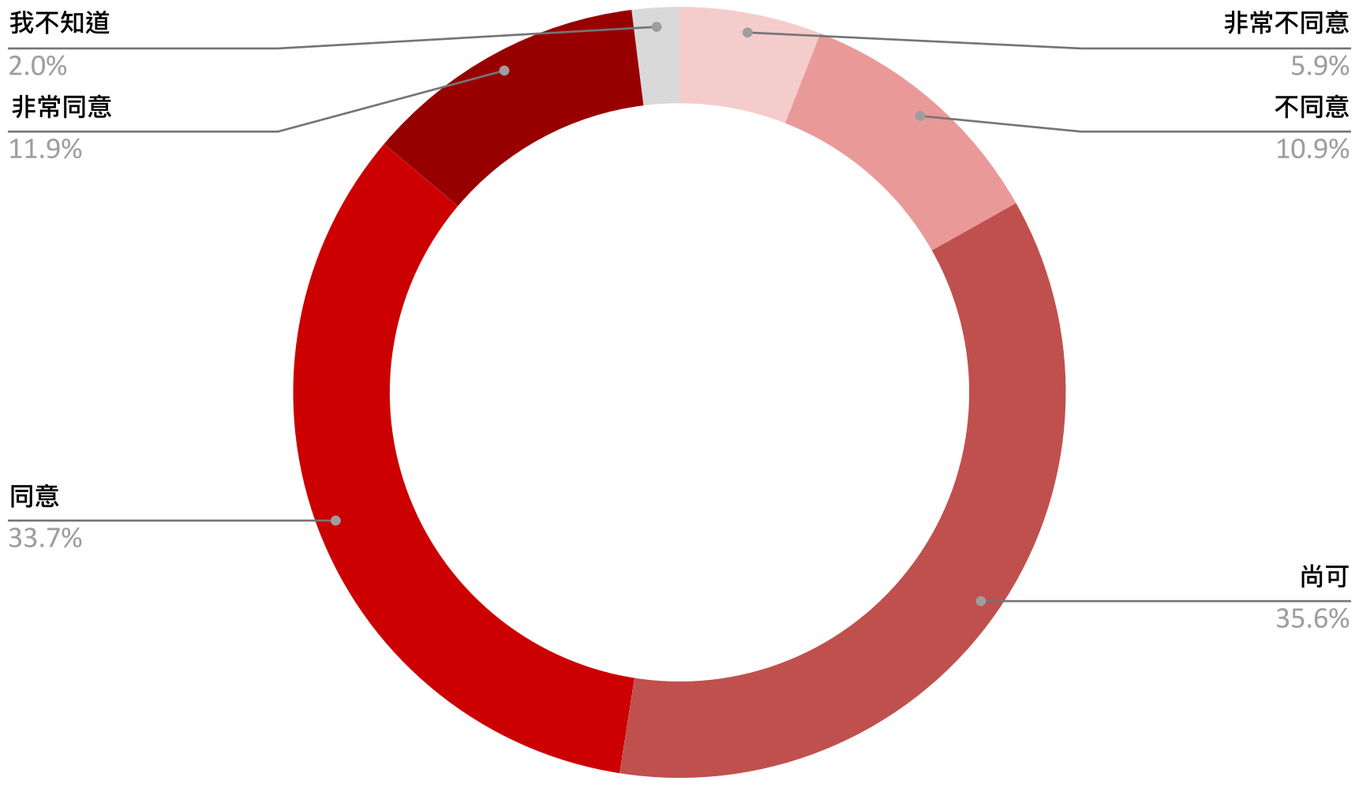
半數填答者擔心既有的防範系統

近年來，網路攻擊手法多變，企業暴露在愈來愈大的風險之中。

有大約 45% 的填答者認為其企業目前所具備的防範系統難以抵禦未來發生的網路攻擊，僅有 26% 左右的填答者持有相反立場。

整體而言，IT 決策者多半擔憂自身的資安系統。

Q7 您是否認為貴公司目前既有的防範系統難以抵禦未來的網路攻擊？



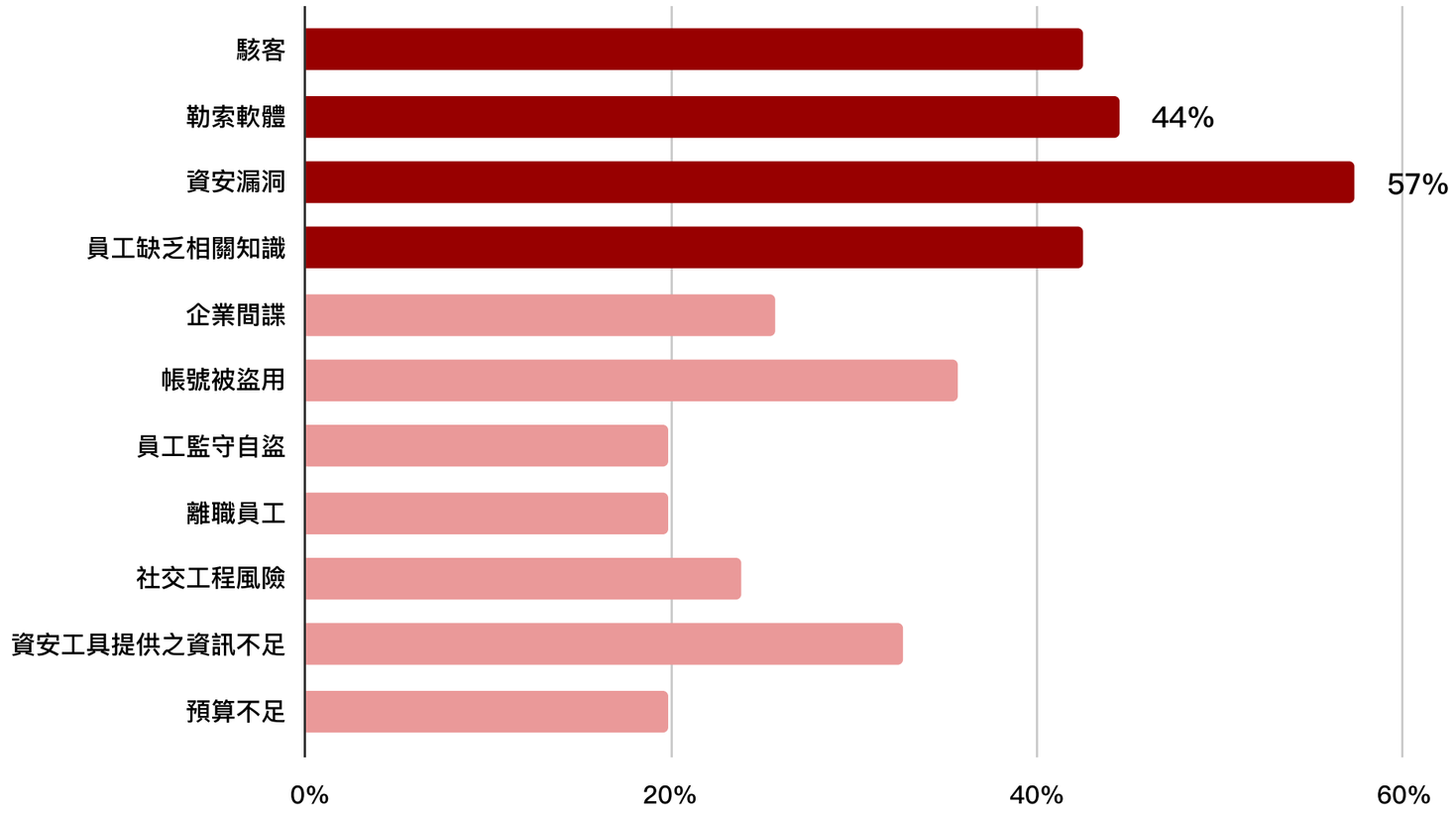
「資安漏洞」是企業防範網路攻擊的主要挑戰

外部與內部資安防範都須重視

約有 57% 的填答者認為「資安漏洞」為企業在防範網路攻擊上的最大挑戰。而諸如勒索軟體（如 Emotet）與網路駭客等威脅同樣構成企業的資安挑戰。

除了上述提及的外部威脅，內部威脅同樣是企業不可忽視的重要因素，不少填答者認為「員工缺乏相關知識」為企業資安上的主要挑戰。此外，如「社交工程」、「離職員工」、「員工監守自盜」等也是許多企業在意的內部威脅。

Q8 貴公司在防範網路攻擊上面臨了以下哪些挑戰？



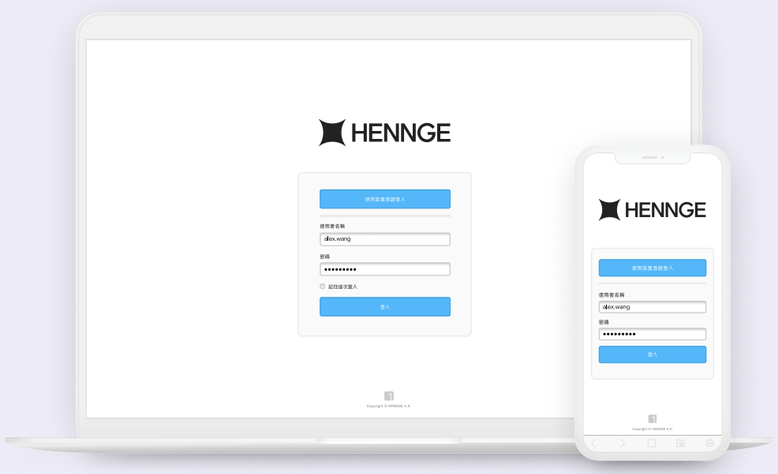
避免攻擊的最佳解方 –「零信任」策略

什麼是「零信任」策略？

零信任的核心概念是「永不信任，一律驗證」，這句話出自俄羅斯諺語，「doveryay, no proveryay」，因為美國雷根總統多次用這句話表達美蘇兩國核武裁減的立場而聲名大噪。這句話凸顯了「驗證」的重要性。

「永不信任，一律驗證」

企業以「永不信任，一律驗證」的立場審視所有可能的威脅。舉例來說，如果有使用者想要透過內網存取內部的資料，通常會推定該使用者是內部人員所以給予權限，但在零信任安全的視角下，即便使用者來自公司內網，他仍然需要經過驗證才能存取內部資訊。



HENNGE One IdP 幫助企業實現零信任的第一步

透過存取控制、裝置控管、多因素驗證、單一登入等功能，HENNGE One IdP 可以幫助企業輕鬆實現零信任的第一步，亦即統一管理所有的帳號密碼，以及對所有登入存取進行身分驗證。

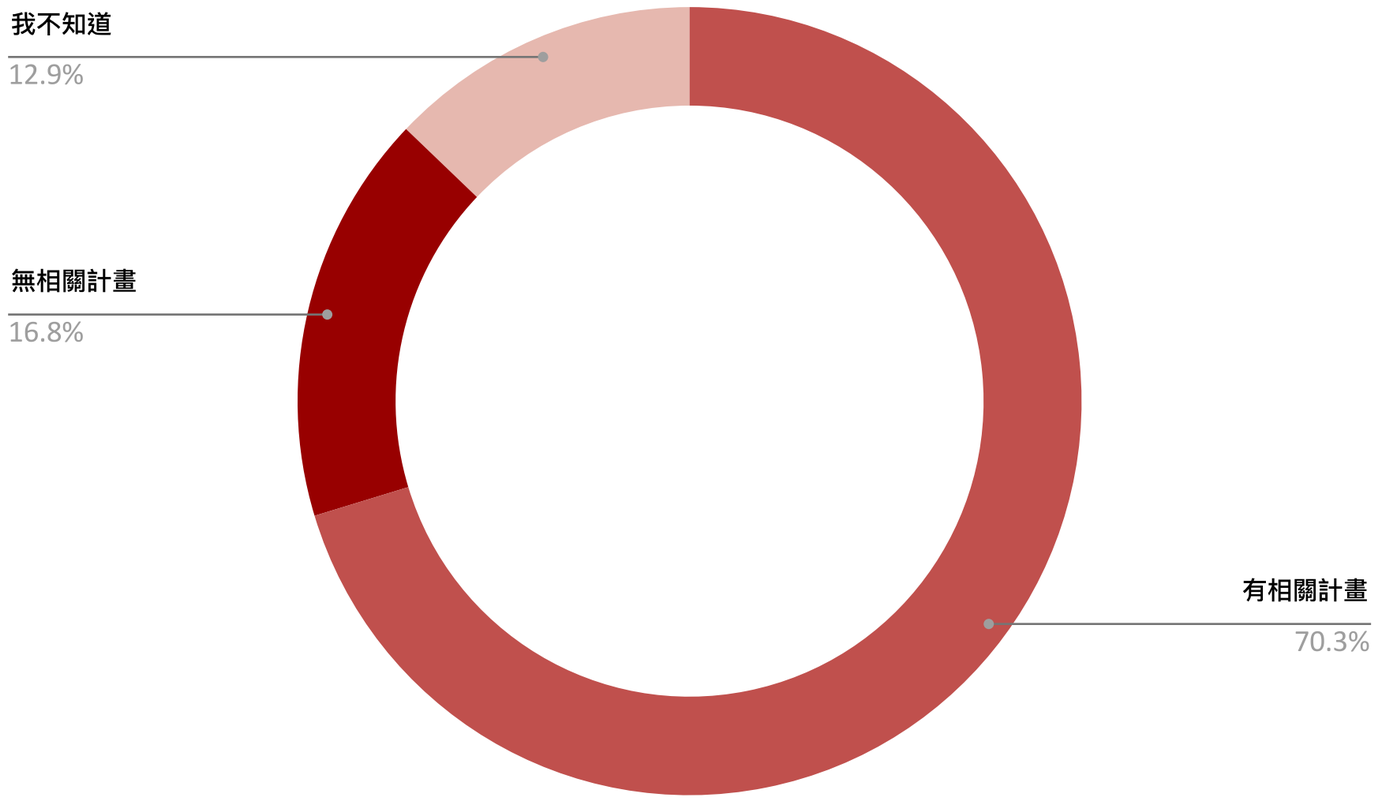
前往 HENNGE 官網進一步了解 >

近 7 成企業在未來一年有內部資訊安全升級計畫

企業多意識到威脅而提前部署

來自外部及內部的資安威脅增加，根據調查，有高達 7 成的受訪者表示企業在未來一年中有內部的資訊安全升級計畫以面臨徒增的資安攻擊趨勢。

Q9 貴公司在未來一年內是否有內部資訊安全提升計畫？



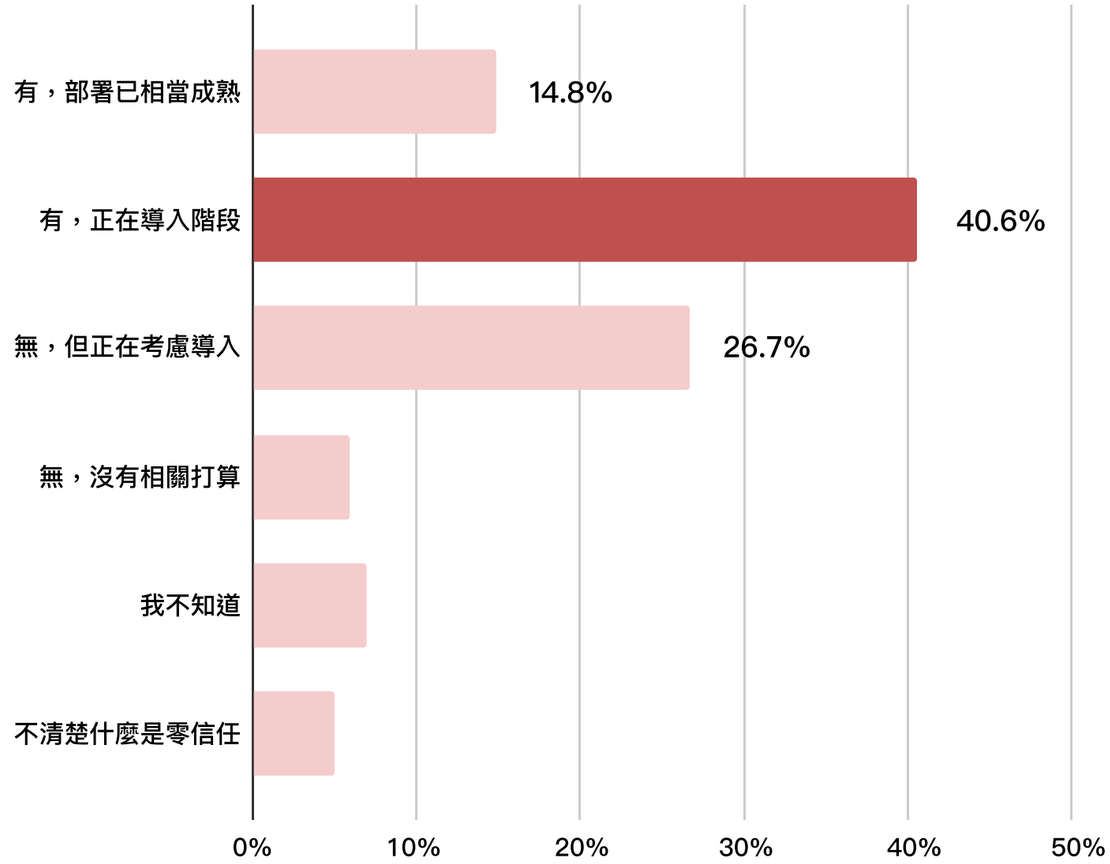
8 成企業對「零信任」策略有所了解或投資

過半數企業已導入或正在導入零信任策略

近年來，一些惡名昭彰的駭客組織經常透過尋找商業系統中的漏洞進行攻擊。而提升企業資安強度的關鍵，便是導入「零信任」策略。

約有 54% 的填答者表示公司內部已經完成或正在導入「零信任」策略，有大約 26% 的填答者也提及公司正在「考慮」導入，可見不少企業充分意識到保障資訊安全的重要。

Q10 貴企業是否就「零信任（Zero Trust）」策略有所投資？



關於 HENNGE

HENNGE 是日本雲端資安業界的領導者，1996 年成立，2019 年於東京證交所上市。秉持著 Liberation of Technology 的理念，我們致力於提供雲端資安 SaaS 服務「HENNGE One」，希望讓企業都能安全安心地運用 Microsoft 365、Google Workspace、Salesforce 等雲端科技，並能靈活地面對未來的變化與挑戰，進而提升生產力。

前往官網進一步了解

https://hennge.com/tw/

台灣惠頂益股份有限公司
HENNGE Taiwan, Inc.

地址：110-502 台北市信義區基隆路二段 51 號 14 樓
電話：02-2736-3223
信箱：tw-sales@hennge.com

HENNGE