Global Data Protection Index – Special Edition 2024

重要調查結果 – 2023 年 10 月

VansonBourne

DELL Technologies

重要調查結果重點

1
資料保護風險態勢

2
網路攻擊的威脅與日俱增

3
多雲端的使用

4
保護雲端環境

五大關鍵要點

網路攻擊次數持續上升

網路攻擊造成的後續成本不斷增加

保單不足以因應攻擊造成的後續成本

提高 GenAI 的使用量可能會產生更多高價值資料

網路攻擊造成更高的風險和更深遠的財務影響

我們的訪問對象

2023 年 9 月至 10 月，共有 1,500 位 IT 與 IT 安全決策人士接受訪問

來自各種公有和私人產業的組織

員工人數超過 250 人的組織

4 個地區：

美洲地區 (300)
歐洲、中東及非洲地區 (675)
亞太地區及日本 (375)
中國 (150)

1. 資料保護風險態勢

各組織對於資料保護措施的顧慮逐漸擴大，而且缺乏信心，因而發現自己處於易受攻擊的處境

60%

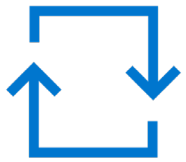
對於組織是否**符合其備份與還原服務等級目標 (SLO)，沒有多大信心**

79%

擔心會在未來十二個月內**遭遇服務中斷事件**

75%

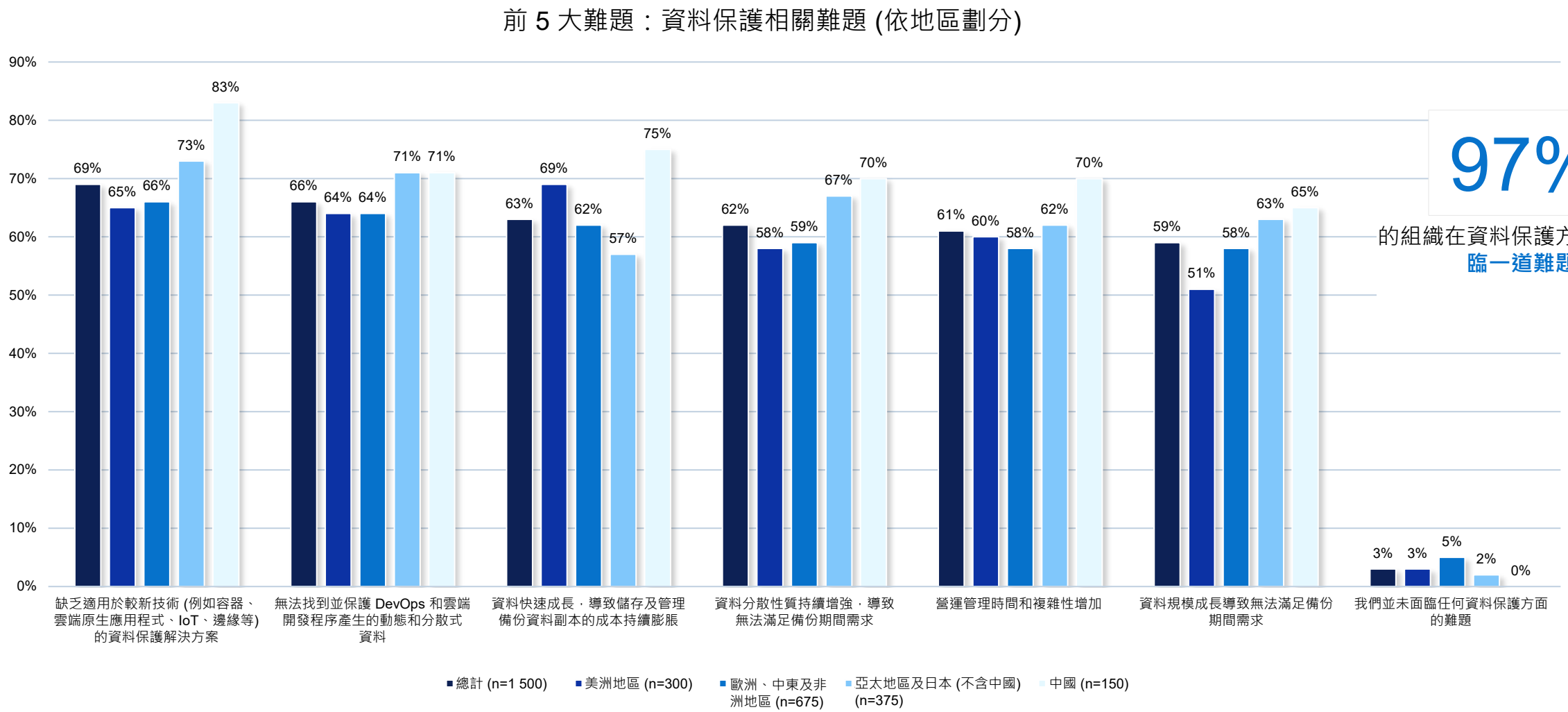
擔心其組織現有的資料保護措施**可能不足以應對惡意軟體和勒索軟體威脅**



65%

對於發生資料遺失事件時，其組織能否完全**還原系統/所有平台的資料，沒有多大信心**

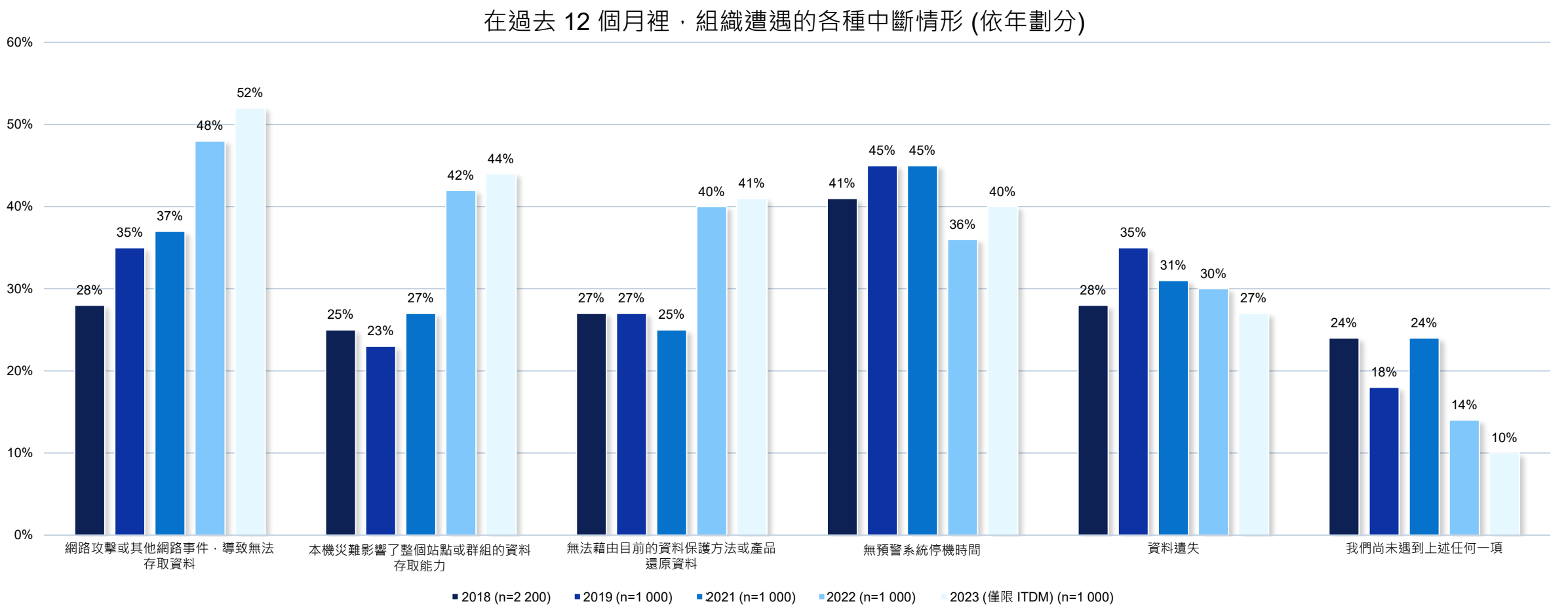
除了對資料保護的顧慮之外，許多組織也面臨各種難題



97%

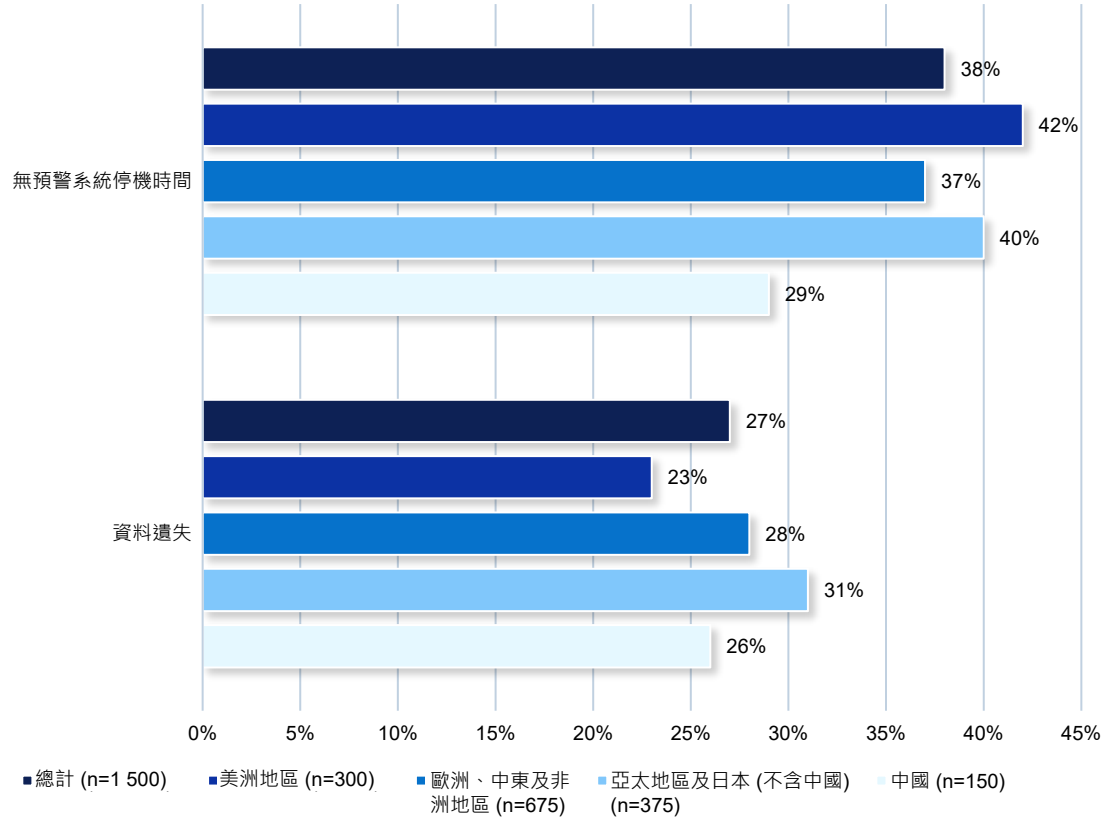
的組織在資料保護方面**至少面臨一道難題**

在過去 12 個月裡，網路攻擊造成前所未有的威脅，致使各組織面臨重大的服務中斷情形



資料遺失不僅會使服務中斷，更會對營收造成影響

在過去 12 個月裡，發生無預警系統停機時間或資料遺失的組織百分比
(依地區劃分)



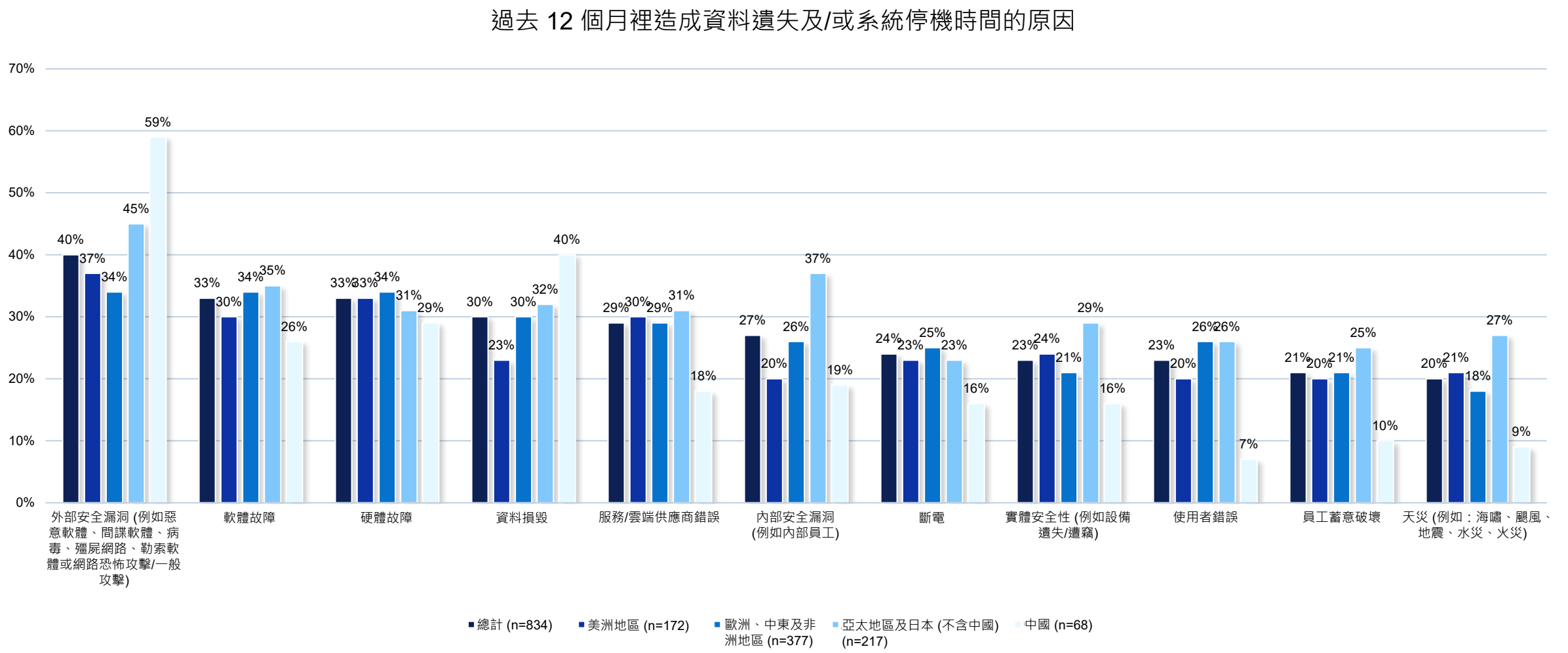
在過去 12 個月裡：

26 小時 **的無預警系統停機時間** (經驗平均值)

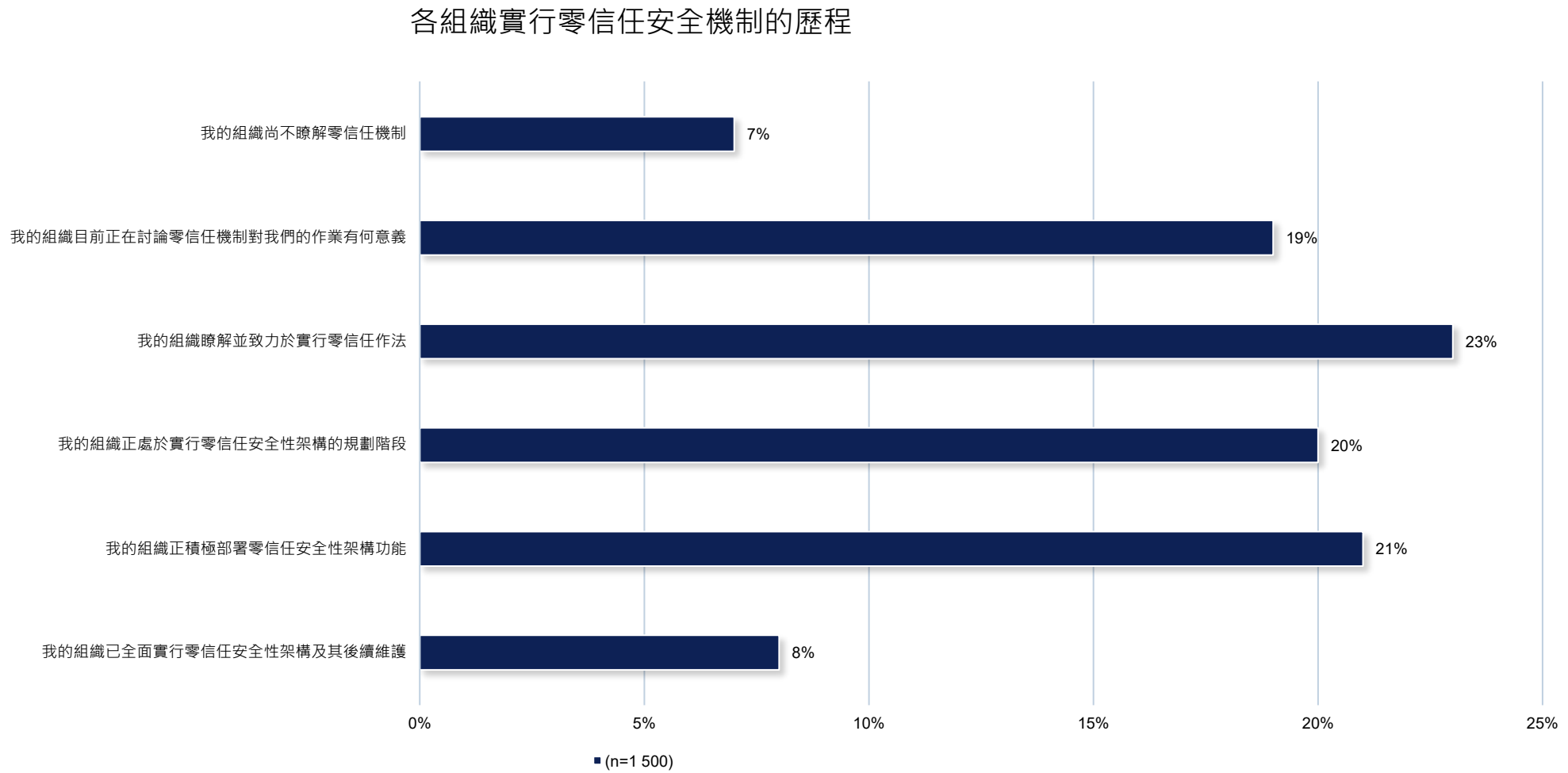
2.45 TB **有價值資料**遺失 (平均值)

2.61 百萬美元，平均**資料遺失成本**

過去 12 個月裡，外部安全性威脅是造成資料遺失及/或無預警系統停機時間最常見的原因



儘管資料保護面臨各種難題和顧慮，但仍有少數組織已完全實行零信任安全機制

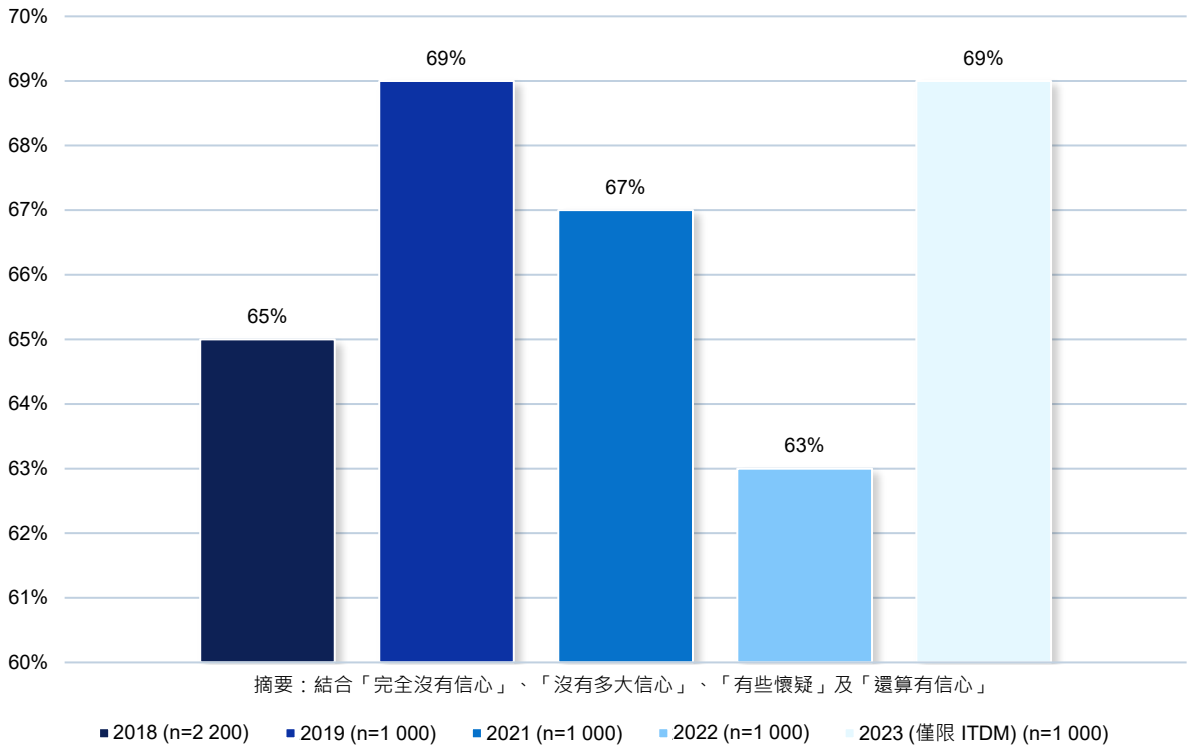


篩選條件：資料 劃分：地區 = 總計

2. 網路攻擊的威脅與日俱增

各組織對於資料保護措施的顧慮逐漸擴大，而且缺乏信心，因而發現自己處於易受攻擊的處境

遭遇破壞性網路攻擊時，「沒有多大信心」能夠可靠地還原所有業務關鍵資料



81%

同意，隨著越來越多員工在家工作，**網路威脅造成組織資料遺失的風險也隨之增加**

74%

擔心其備份資料可能會被**勒索軟體攻擊感染或損毀**

讓風險再增加的因素是，對於勒索軟體攻擊造成的後果，有被誤導的過度自信情形

72%

同意，其工作和組織內的員工**不會受到勒索軟體攻擊的影響**

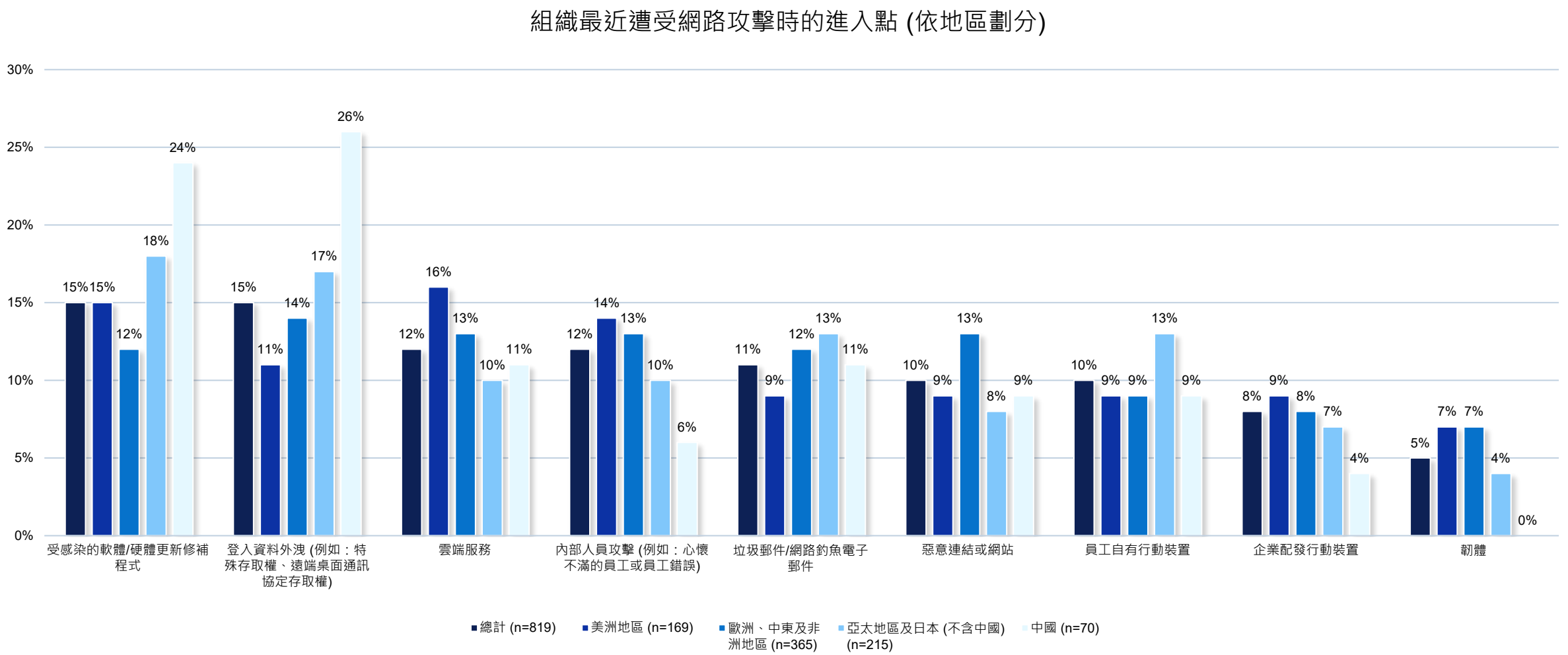
74%

同意，當組織遭受勒索軟體攻擊時，**若組織支付贖金**，**他們能拿回所有資料**以恢復業務

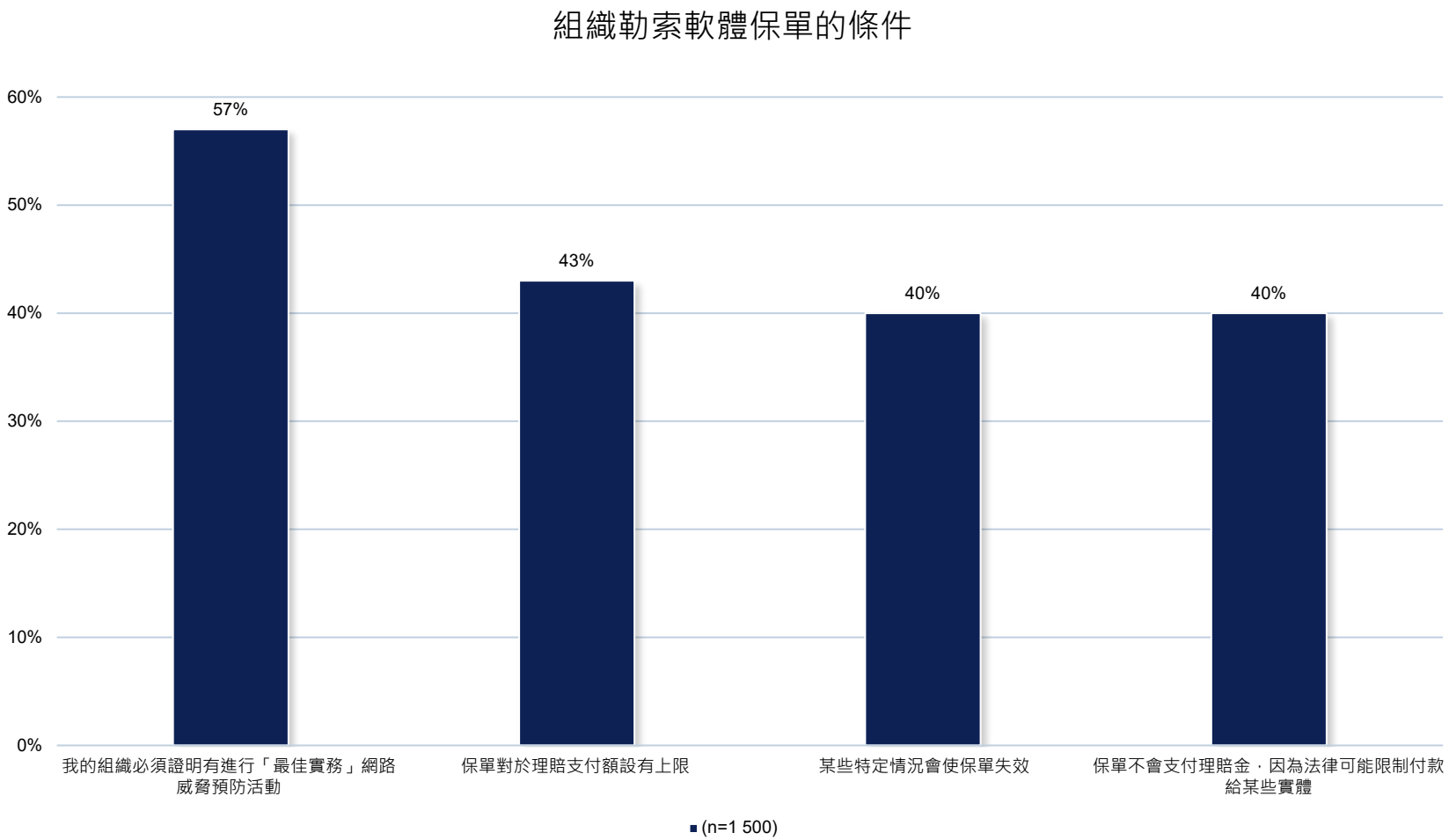
66%

同意，若組織遭受勒索軟體攻擊，只要支付贖金，**便不會再次被攻擊**

網路罪犯會鎖定各種進入點，而攻擊則較可能來自外部來源



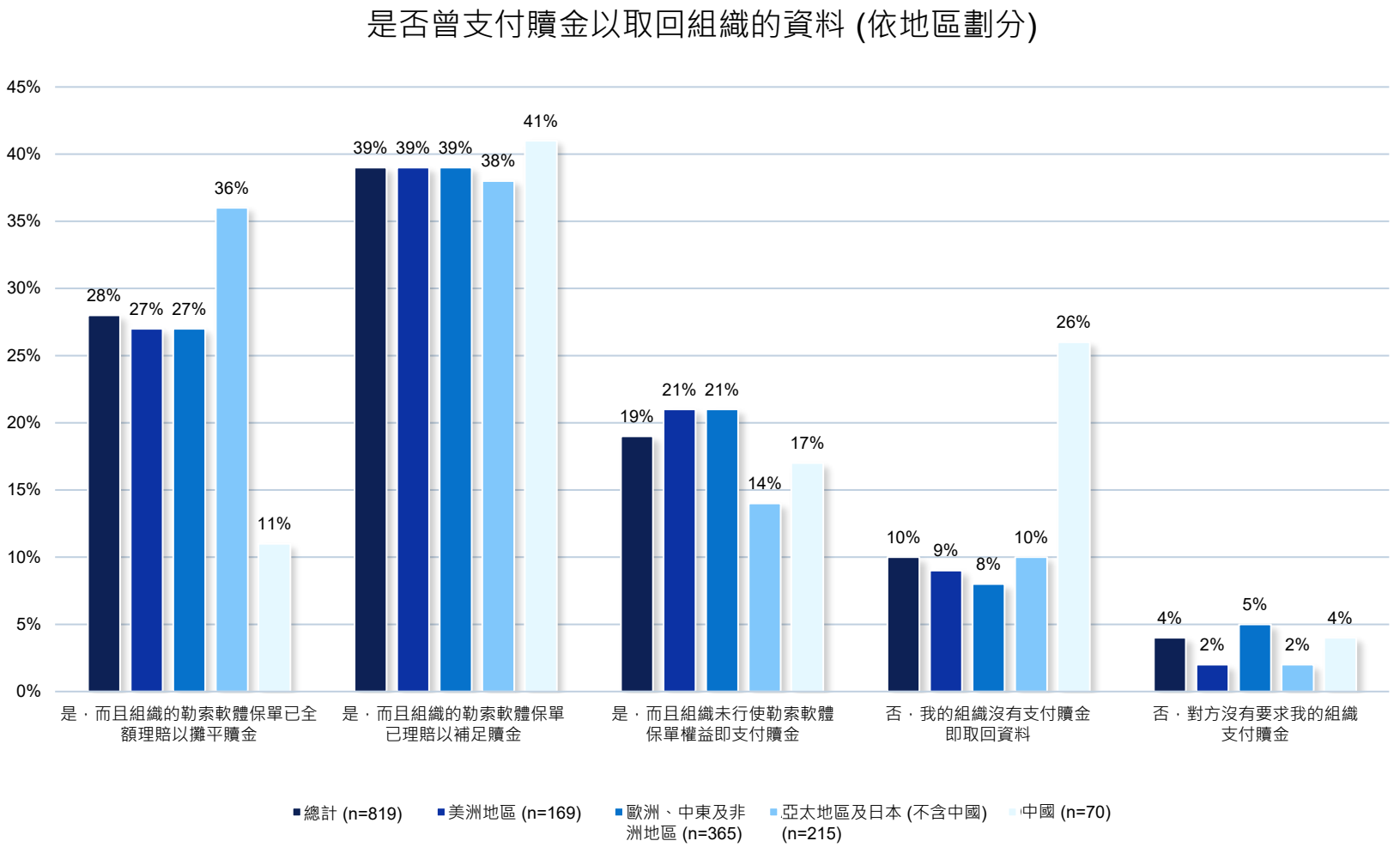
勒索軟體保單對於各組織而言很常見，但這也敲響了一道警鐘



93%

的組織**有勒索軟體保單**

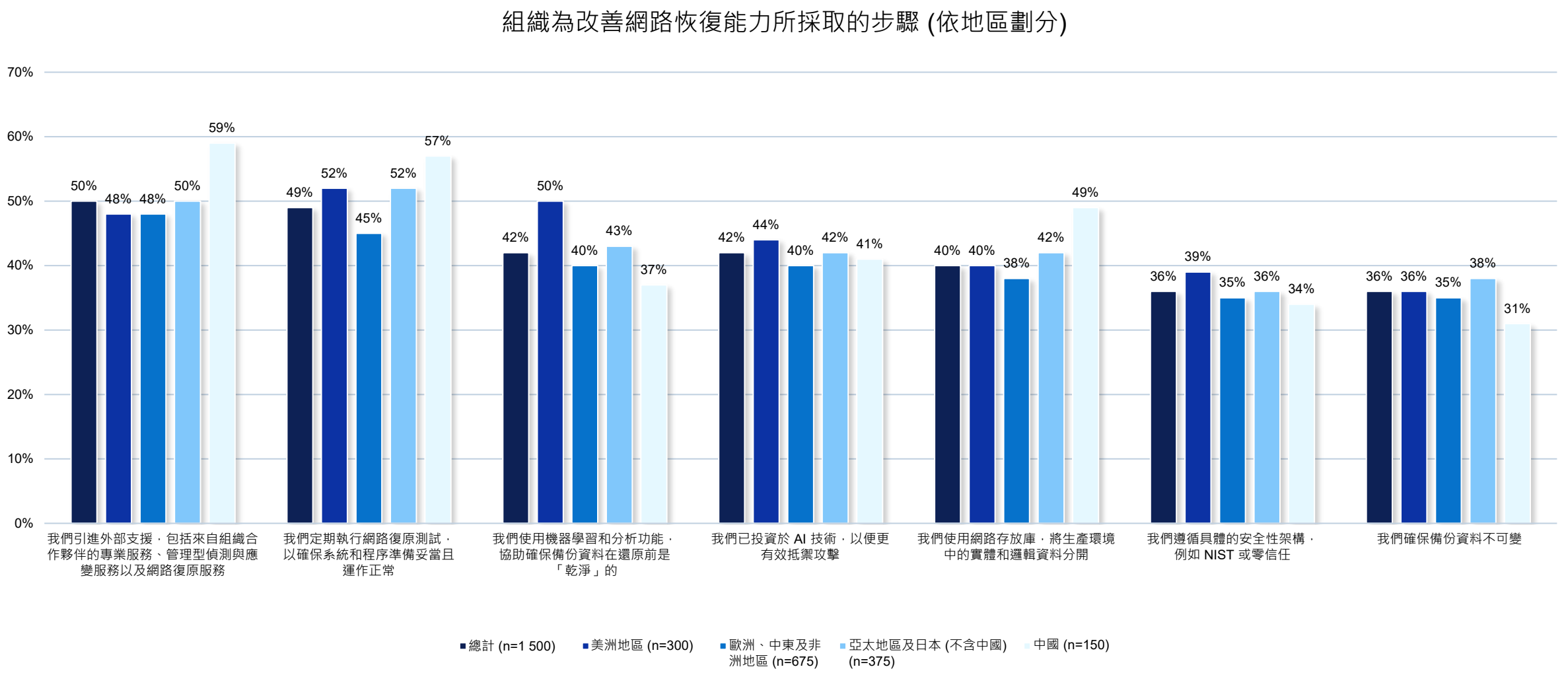
儘管許多組織都有勒索軟體保單，但仍發現在財務方面不堪一擊



1.92

百萬美元──過去 12 個月裡因**網路攻擊及其他網路相關**事件而衍生的組織平均成本

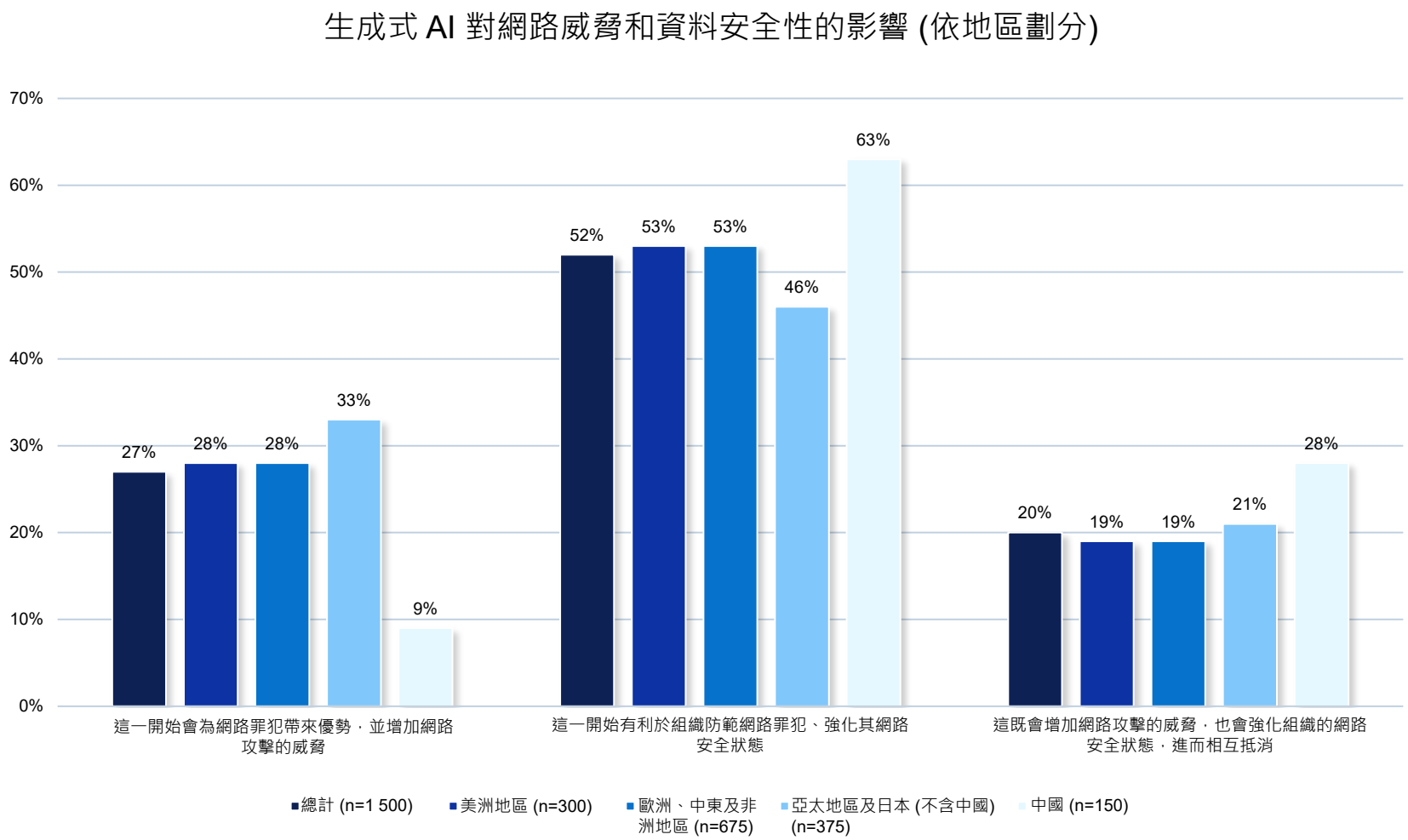
所幸，各組織正採取各種步驟來增加網路韌性



然而，並非所有組織都認為生成式 AI 對其網路恢復能力有益

81%

同意，新興科技 (例如 AI、IoT、邊緣) **會為資料保護帶來風險**



事實上，由於各組織已經對資料保護有所顧慮，許多人認為生成式 AI 將帶來新的難題

88%

同意，生成式 AI 將產生大量新資料，而這些資料**需要受到妥善保護**

88%

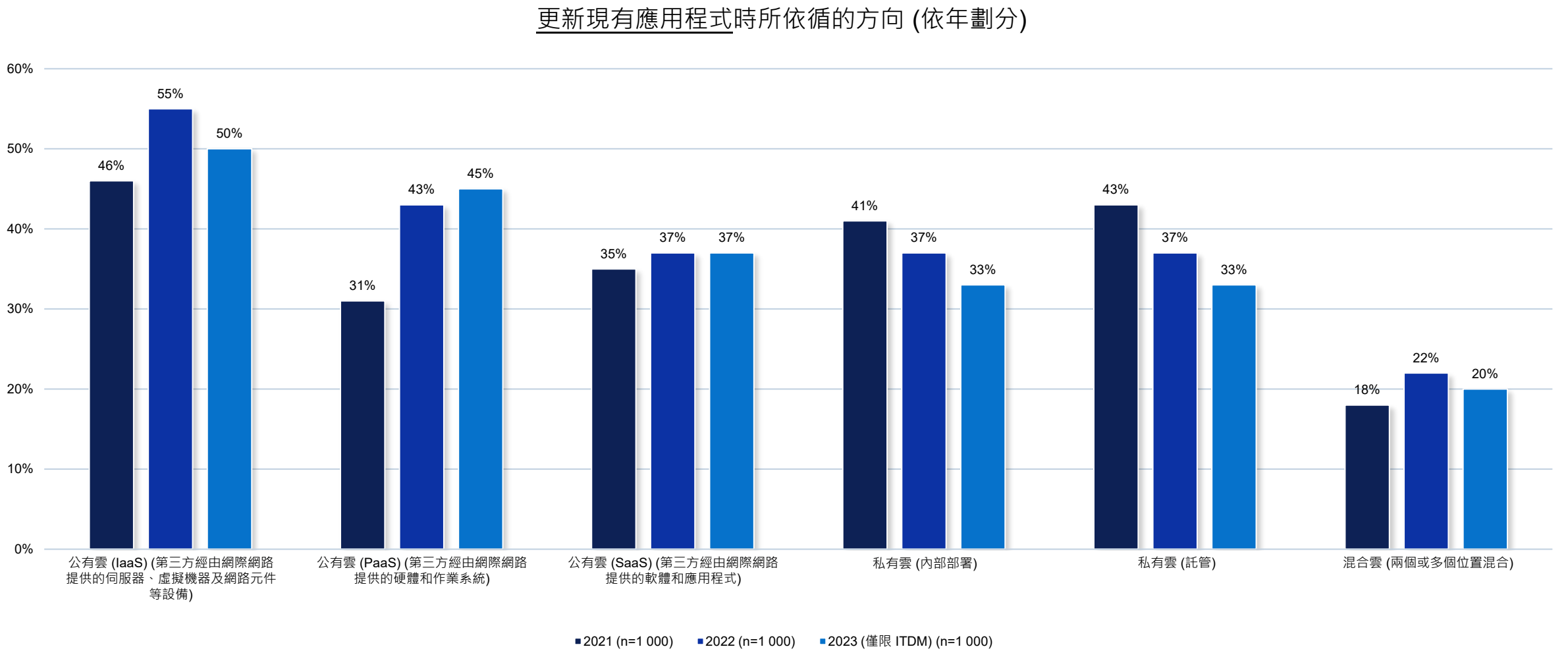
同意，生成式 AI 會提高特定資料類型的價值，而這類資料需要**更高的資料保護服務等級**

85%

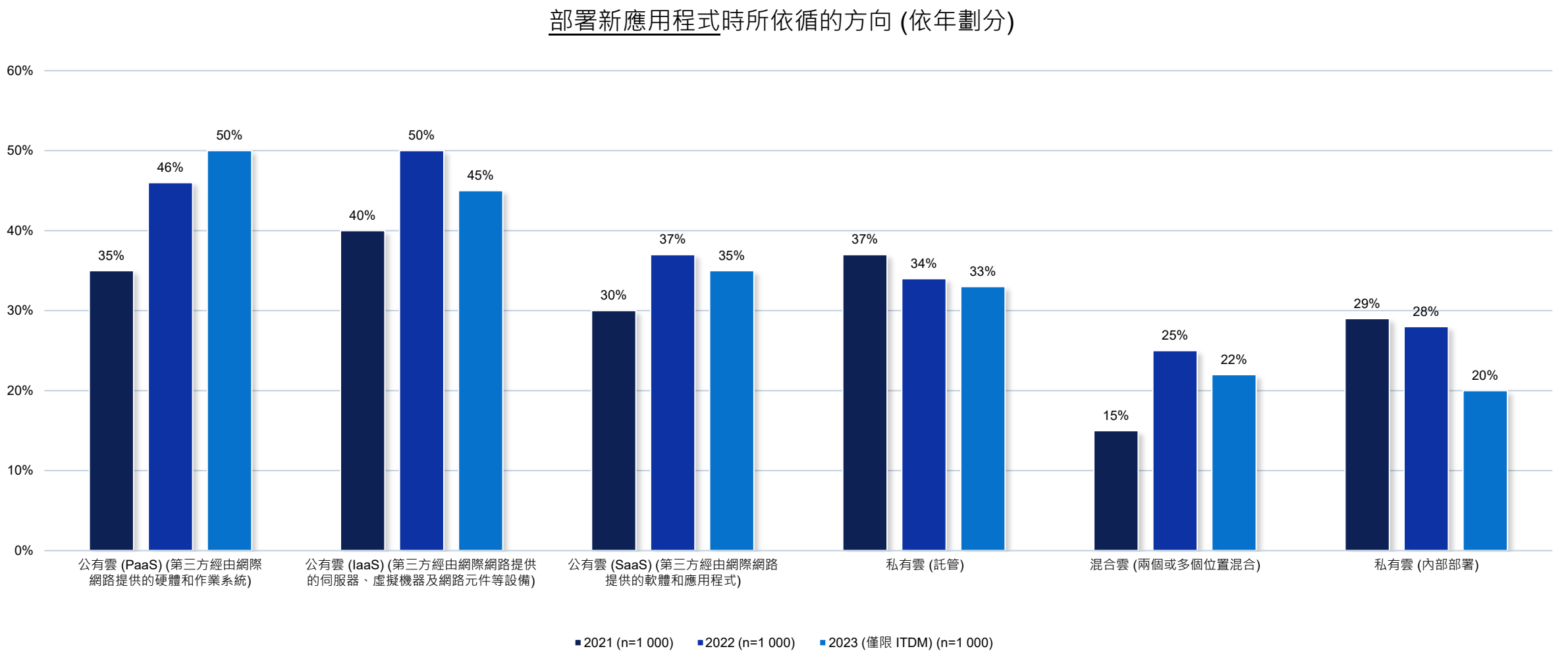
同意，如果用於生成式 AI 的資料集**損毀**，將會**影響生成式 AI 輸出**

3. 多雲端的使用

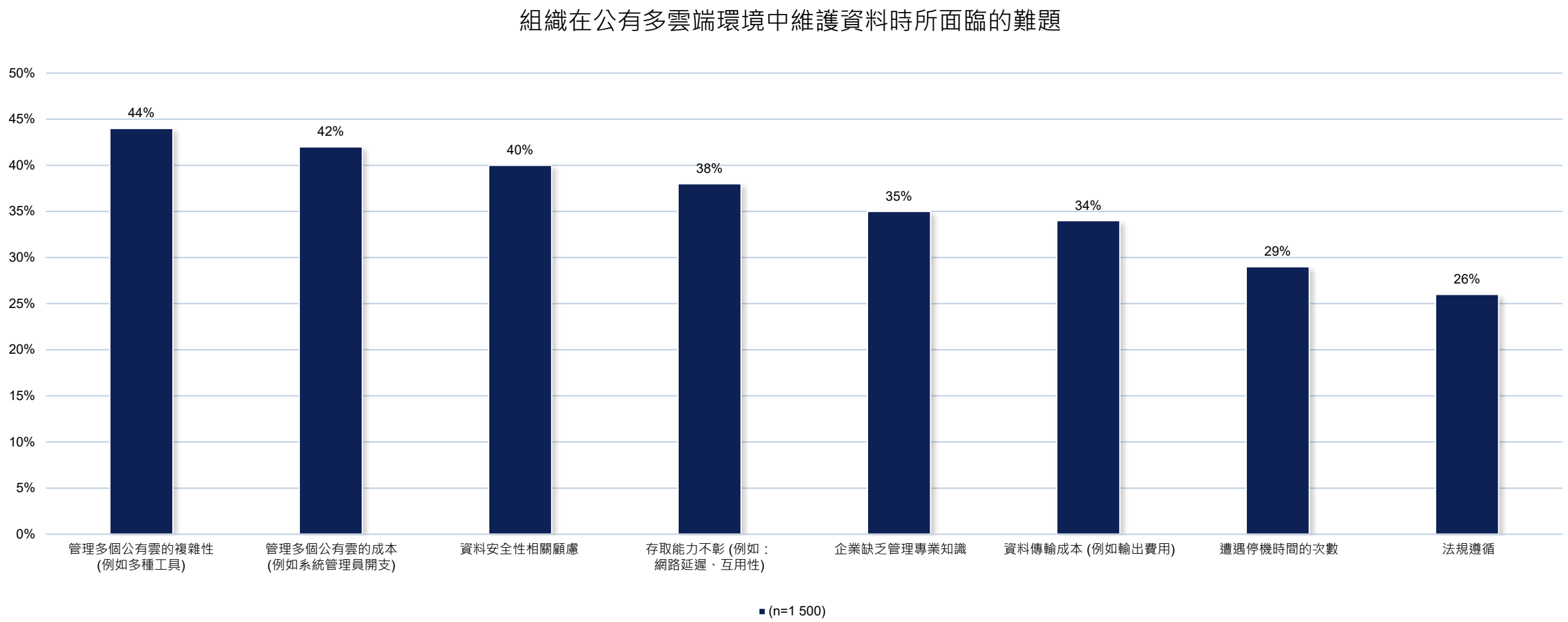
在更新現有應用程式時，公有雲仍是熱門選擇，而對於私有雲的偏好則正在減少



公有雲也是部署新應用程式的熱門選擇，但支援可能正在減少

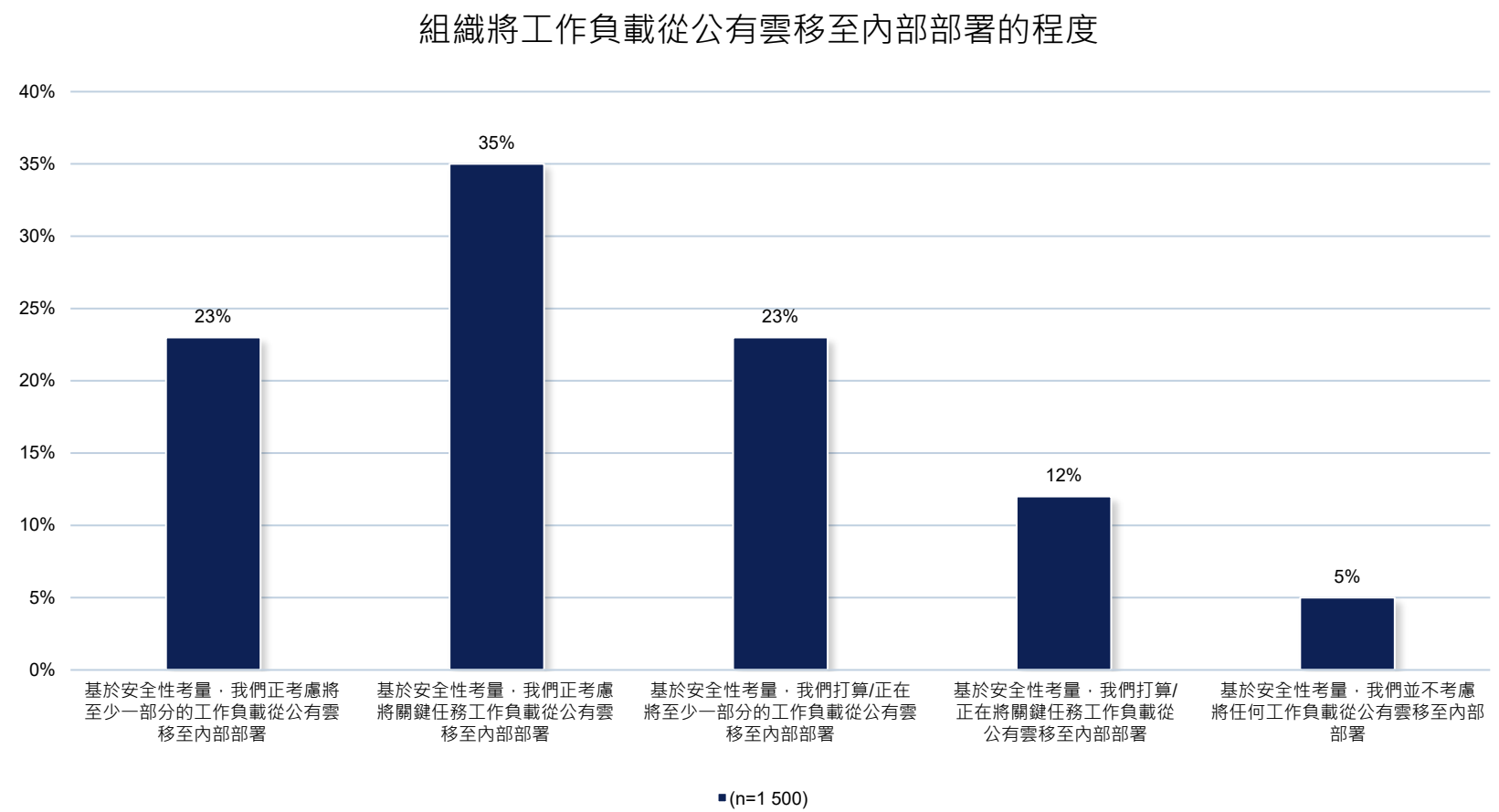


儘管公有雲相當受歡迎，但許多組織在維護資料時仍面臨諸多難題



篩選條件：資料 劃分：地區 = 總計

基於安全性考量，許多組織正在將部分工作負載從公有雲移至內部部署，或考慮這樣做

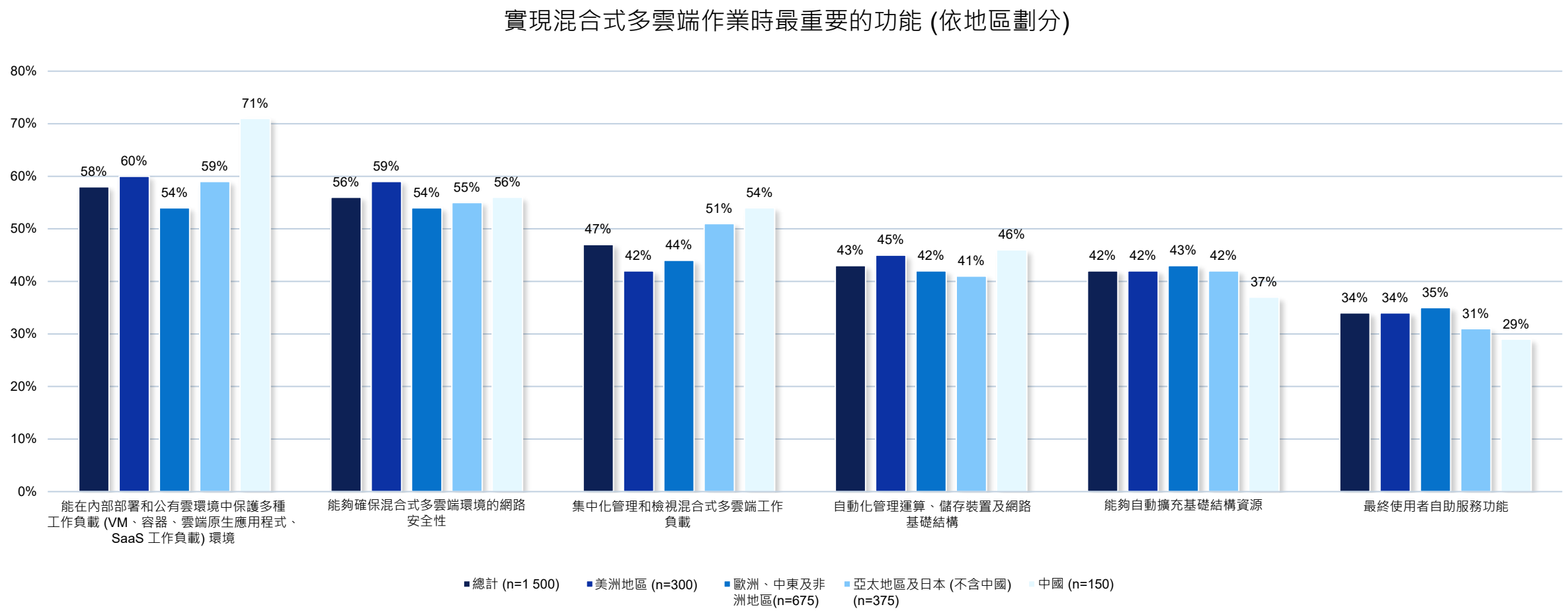


79%

對於其組織能否在公有雲環境中**保護其所有資料沒有多大信心**

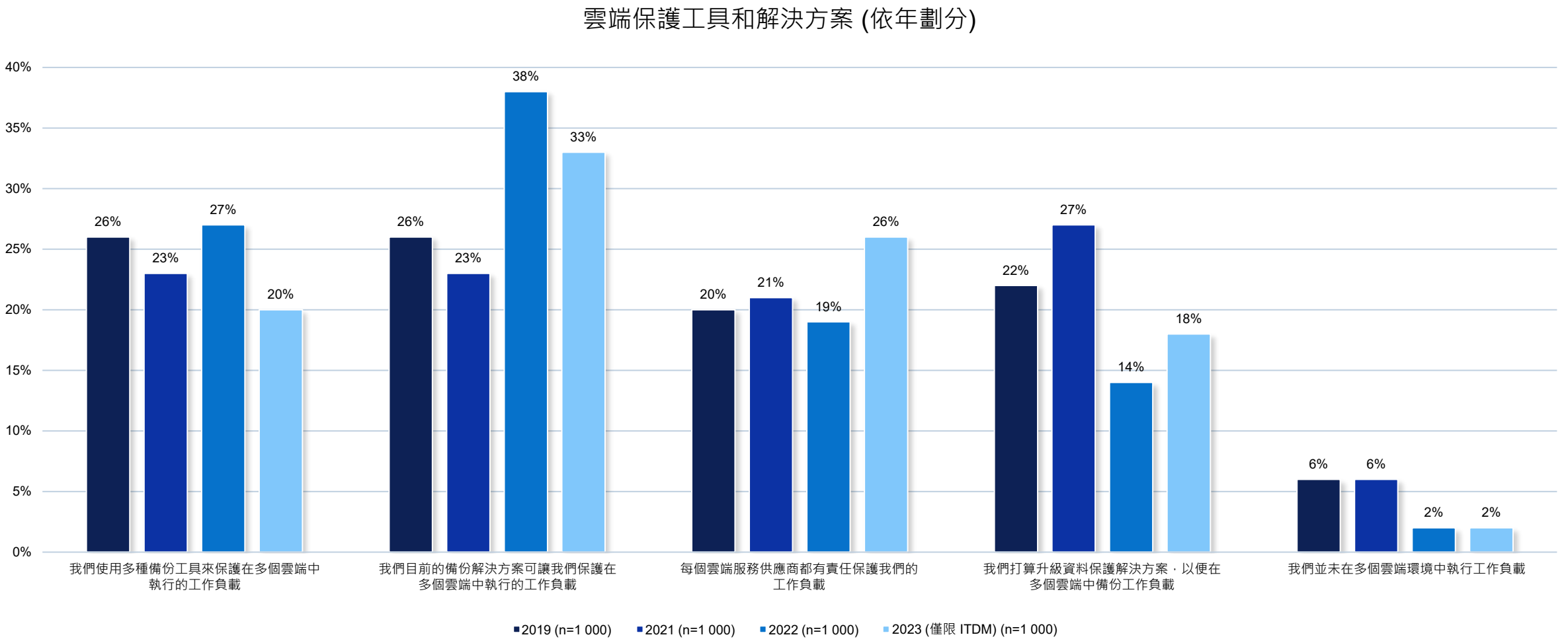
篩選條件：資料 劃分：地區 = 總計

有鑑於網路相關事件逐漸增加，而對於資料保護策略的信心亦不足，許多人認為安全機制是實現混合式多雲端作業時最重要的功能



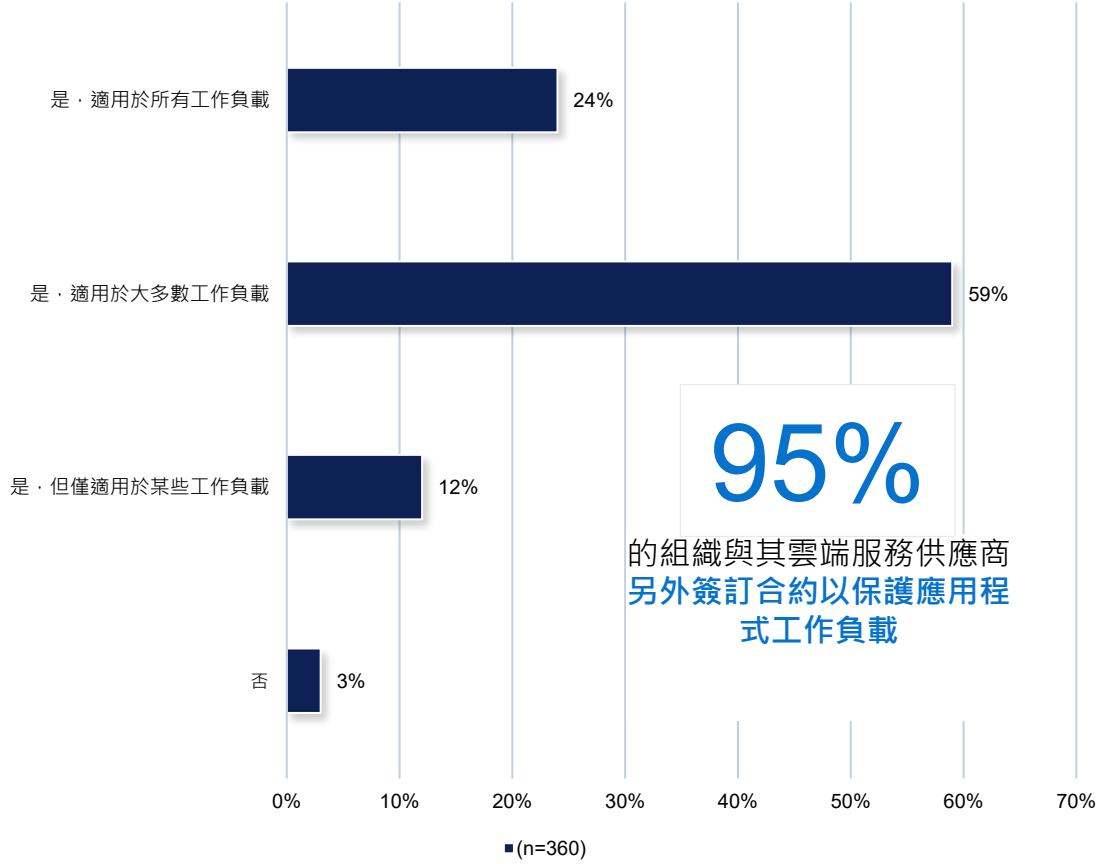
4. 保護雲端環境

各組織目前使用多種備份工具和解決方案來保護其工作負載，但同時也注意到升級的需求



組織日漸仰賴雲端服務供應商來保護跨雲端環境的工作負載

與 CSP 另外簽訂合約以保護應用程式工作負載

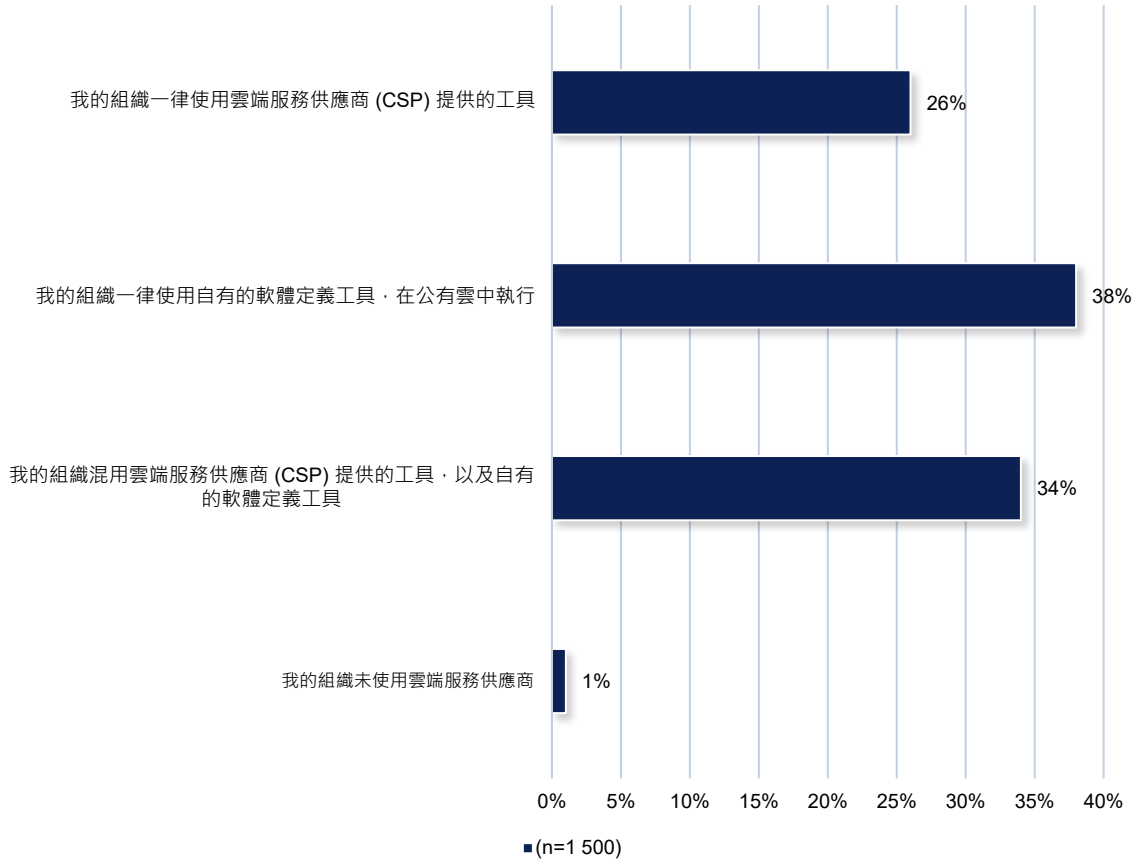


95%

的組織與其雲端服務供應商**另外簽訂合約以保護應用程式工作負載**

篩選條件：資料 劃分：地區 = 總計

雲端服務供應商提供的備份與還原工具



篩選條件：資料 劃分：地區 = 總計

重要調查結果 – 摘要

資料保護風險態勢

- 各組織對於資料保護措施的顧慮逐漸擴大，而且缺乏信心，因而發現自己處於易受攻擊的處境
- 幾乎所有組織均面臨資料保護方面的難題，且在過去 12 個月裡，許多組織也因資料遺失及/或無預警系統停機時間，而面臨重大的服務中斷情形
- 過去 12 個月裡，外部安全性威脅是造成資料遺失及/或無預警系統停機時間最常見的原因
- 儘管資料保護面臨各種難題和顧慮，但仍有少數組織已完全實行零信任安全機制

網路攻擊的威脅與日俱增

- 過去 12 個月裡，遭遇網路攻擊或事件的組織數量持續增加，平均讓企業付出 192 萬美元的成本
- 許多組織擔心其備份資料可能會被勒索軟體攻擊感染或損毀
- 讓風險再增加的因素是，對於勒索軟體攻擊造成的後果，有被誤導的過度自信情形
- 儘管勒索軟體保單很常見，但這也敲響了一道警鐘，意味著組織在財務上不堪一擊

多雲端的使用

- 在更新現有及部署新應用程式時，公有雲仍是熱門選擇，但對於資料安全性也有所顧慮
- 基於安全性考量，許多組織正在將部分工作負載從公有雲移至內部部署，或考慮這樣做
- 有鑑於網路相關事件逐漸增加，而對於資料保護策略的信心亦不足，許多人認為安全機制是實現混合式多雲端作業時最重要的功能

保護雲端環境

- 各組織目前使用多種備份工具和解決方案來保護其工作負載，但同時也瞭解到需要升級
- 組織日漸仰賴雲端服務供應商來保護跨雲端環境的工作負載