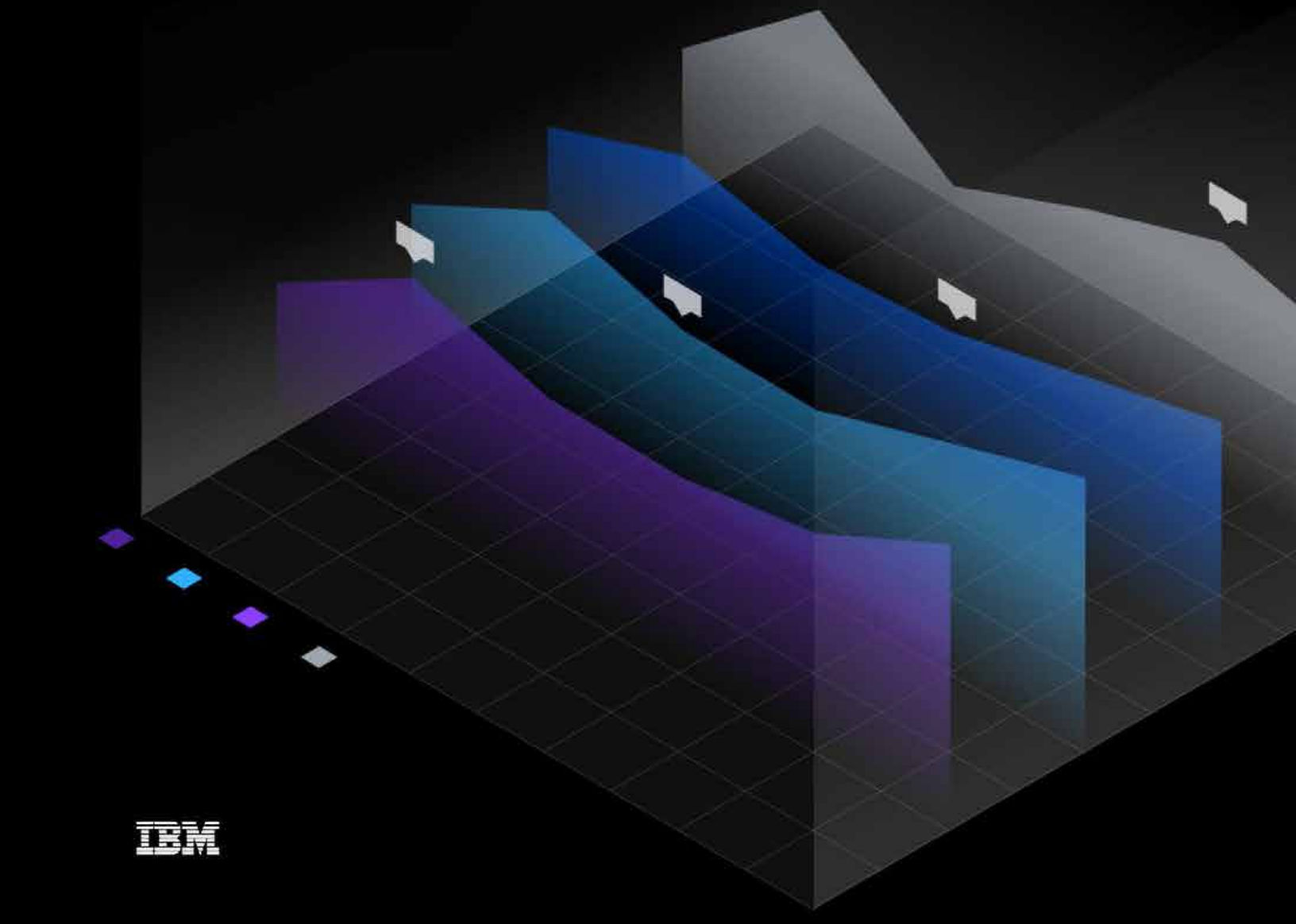
IBM Security

2020 年資料洩露成本報告



IBM

目錄

執行摘要

這是 Ponemon Institute 連續第 15 年開展研究發佈年度《*資料洩露成本報告*》，其中五年的報告由 IBM Security 贊助和發佈。我們希望企業可以利用此研究加速創新，同時也希望當不同類型和規模的組織在面臨資料洩露和網路安全事件風險時，也能留住客戶信任。

該報告已成為網路安全產業的主要基準工具之一，讓 IT、風險管理和安全領導者即時瞭解能夠規避或加劇資料洩露成本的因素。此報告還會展示我們分析過的成本中的一致性和波動性，協助我們洞悉資料洩露趨勢。

在 2020 年 *的資料洩露成本報告**中，Ponemon Institute 招募了 524 家在 2019 年 8 月至 2020 年 4 月期間經歷過資料洩露的企業。為確保研究儘可能涉及更多產業的公司，本研究甄選了來自 17 個國家/地區、涵蓋 17 個產業且規模各異的公司。我們的研究人員採訪了 3,200 多位知情人士，他們所在的企業都發生過資料洩露事件。

資料洩露成本報告數據

524

個發生洩露的組織

3,200

位接受訪問的個人

17

個國家和地區

17

個產業

*本報告中的年份是指發佈年份，而不一定是發生洩露的年份。2020 年報告中分析的是 2019 年 8 月至 2020 年 4 月期間發生的資料洩露。

在訪問的過程中，我們還提出了一些問題，以判斷企業在發現洩露和立即回應資料洩露等活動上的支出。還有一些問題也會影響成本，例如資料洩露的根本原因；組織用於發現和控制事件的時間以及因為洩露導致業務中斷並失去客戶造成的預計損失。我們還考察了其他一些成本因素，例如洩露之前實施的安全措施，組織及其 IT 環境的特徵等。

因此我們的報告可提供龐大的資料集、廣泛的分析和趨勢洞察。在後面的執行摘要中，我們簡要介紹了如何計算資料洩露成本以及本次研究的一些重要發現。為深入瞭解資料，完整的結果部分列舉了 49 張分析圖和人口統計圖。

基於研究得出的對組織而言最行之有效的措施，我們為 IT 領導者、網路安全戰略家和風險管理員提供安全措施建議，降低資料洩露可能帶來的財務損失和品牌損害。報告的最後詳細闡釋了我們的研究方法。

2020 年報告新增內容

我們希望每年更新報告提供分析，在既立足於往年報告又能找到突破點的基礎上，緊跟日新月異的技術和趨勢，以便企業更全面地瞭解風險和確保資料安全的標準。

2020 年注定是不平凡的一年。除了技術和威脅方面週而復始的變化之外，一場席捲全球的疫情讓世界各地的企業和消費者的生活有了翻天覆地的變化。

儘管本次研究在新冠疫情迅速蔓延之前數月便已啟動，但在研究的大多數洩露事件發生之後，我們仍然要求參與者回答一些補充性問題，這些問題都與新冠疫情之下開展遠端工作所帶來的潛在影響有關。我們發現，大多數組織 (76%) 都預計遠端工作會讓回應潛在的資料洩露面臨更嚴峻的考驗。

今年的報告中加入了新的研究，可更加深入地瞭解我們長期使用的資料類型 — 其中包括資料洩露每條記錄的成本以及資料洩露的根本原因。我們首次在研究中細分了被盜的每條記錄的成本，以便基於洩露的記錄類型來分析成本，這些記錄類型包括客戶個人身分資訊 (PII)、員工 PII 以及智慧財產權 (IP)。在分析資料洩露根本原因時，我們更加深入地探索了更具體的惡意洩露類型，其中包括憑證被盜和內部人員威脅等。

本次研究首次要求參與者識別被推定為對洩露負責的威脅主體類型，其中包括國家和受經濟利益驅動的攻擊者，我們的成本分析顯示，最常見的惡意洩露類型，即受經濟利益驅動的網路犯罪者攻擊導致的洩露，並非成本最高的類型。

隨著勒索軟體和破壞性惡意軟體的攻擊日益普遍，我們在今年的報告中新增了成本分析，結果發現，這些致命攻擊的平均洩露成本要高於資料洩露的整體平均水準。

資料洩露統計資訊

$3.86 百萬

平均總成本

美國

成本最高的國家

醫療保健

成本最高的產業

280 天

發現和控制所需的平均時間

今年的研究中還新增了幾項成本因素，例如漏洞和紅隊測試的影響（使用一種對抗方法進行滲透測試）以及遠端工作和安全技能短缺對這些成本的影響。毫不意外，在研究分析的 25 項可增加資料洩露平均成本的因素中，技能短缺排名前三，而紅隊測試則是可降低資料洩露平均成本排名前五的成本因素。

報告還審查了一些新的問題，例如深入探討了資訊安全官所發揮的作用以及網路安全保險涵蓋的成本類型。

值得注意的是，在今年的報告中，資料洩露的平均總成本略有下降，從去年的 392 萬美元下降至今年的 386 萬美元，這一現象讓一些人認為資料洩露成本已趨於飽和。

另一方面，我們的研究似乎顯示，擁有更先進的安全流程（如自動化和正式的事件回應團隊）的組織，與那些在這些領域的安全態勢不那麼先進的組織之間的資料洩露成本差距愈來愈大。

這是一份全球性報告，研究所涉及的範圍之廣，意味著我們不能在此次研究中強調所有國家/地區和產業的資料洩露成本的細微差別。正因為如此，我們開發了在線計算器和資料探索工具 (ibm.com/databreach)，方便您進行客製化並發現自己需要的內容。

我們希望您能從中得到對您的組織富有意義的洞察，並得出有用的結論，更好地保護您的企業取得成功所依賴的資料。

我們如何計算資料洩露的成本

為計算資料洩露的平均成本，本研究排除了極小和極大規模的洩露。2020 年研究考察的資料洩露中被破壞的記錄在 3,400 至 99,730 條不等。我們單獨分析了「大規模洩露」的成本，在報告的「完整的結果」部分會對此加以詳細說明。

本次研究使用了一種名為作業成本法 (ABC) 的會計方法，這種方法可識別活動並根據實際的使用分配成本。四項流程相關的活動造成了一系列與組織的資料洩露相關的支出：偵測和升級、通知、資料洩露後回應以及業務損失。

要更加深入地瞭解此報告使用的方法，請參閱研究方法部分。

下文詳細介紹了這四個成本中心。

偵測和升級

使公司能夠合理發現洩露的活動。

- 取證和調查活動
- 評估與稽核服務
- 危機管理
- 與管理層和董事會溝通

業務損失

可最大程度減少客戶流失、業務中斷和收入損失的活動。

- 因為系統停機造成的業務中斷和收入損失
- 客戶流失和獲取新客戶的成本
- 名譽受損和商譽降低

通知

讓公司能夠通知資料主體、資料保護監管機構及其他第三方的活動。

- 傳送給資料主體的電子郵件、信函、通話或一般通知
- 確定法規要求
- 與監管機構溝通
- 聯絡外部專家

事後分析回應

協助資料洩露受害者與公司溝通以及賠償受害者和繳納監管機構罰款的活動。

- 服務台和進線通訊
- 信用監控和身分保護服務
- 開設新帳戶或新信用卡
- 法律支出
- 產品折扣
- 監管機構罰款

重要發現

本文的重要發現以 IBM Security 對 Ponemon Institute 編纂的研究資料所作的分析為基礎。

-1.5%

平均總成本淨變化

（2019-2020 年）

儘管資料洩露平均總成本年成長率略有下降，但許多公司的成本卻不降反增。

表面來看，儘管成本從 2019 年研究中的 392 萬美元下降至 2020 年研究中的 386 萬美元，但最成熟的公司和產業的成本仍然較低，而那些在安全自動化和事件回應流程中落後一步的組織，其成本則要高出很多。更深入地分析單個遺失或被盜記錄的平均成本（每條記錄的成本）之後發現也普遍存在差異，具體視洩露中遺失或被盜的資料類型而異。

$150

每條記錄的客戶 PII 平均成本

在我們研究的資料洩露中，客戶的個人可識別資訊 (PII) 是最常受到破壞的記錄類型，其成本也最高。

在遭到攻擊的組織中，有 8% 的組織表示，資料洩露中被盜的客戶 PII 遠遠高於任何其他記錄類型。在所有資料洩露中，遺失或被盜記錄的平均成本為 146 美元，而那些包含客戶 PII 的被盜記錄的平均成本為 150 美元。

惡意攻擊引發的資料洩露中，客戶 PII 每條記錄的成本會增加至 175 美元。研究中有 24% 的資料洩露涉及到匿名客戶資料，每條記錄的平均成本為 143 美元，它將惡意攻擊引起的資料洩露中的每條記錄的成本增加至 171 美元。

+$137,000

遠端工作對平均總成本的影響

新冠疫情期間的遠端工作會增加資料洩露成本和事件回應時間。

在表示因為新冠疫情需要開展遠端工作的組織中，70% 的組織認為此舉會增加資料洩露的成本，76% 的組織認為會增加發現和控制潛在資料洩露的時間。遠端工作會使 386 萬美元的資料洩露平均總成本增加近 137,000 美元，增加後的平均總成本為 400 萬美元。

憑證被盜或洩露是導致惡意攻擊資料洩露的最昂貴的原因。

每五家遭受惡意資料洩露的公司中就有一家 (19%) 是由於憑證被盜或洩露而被滲透，使這些公司的洩露平均總成本增加了近 100 萬美元，達到 477 萬美元。整體而言，惡意攻擊是最常見的根本原因（占研究中之洩露的 52%），其次是人為失誤 (23%) 或系統故障 (25%)，平均總成本為 427 萬美元。

+14%

雲端錯誤配置對平均總成本的影響

雲端的錯誤配置是洩露的主要原因。

除了被盜或被破壞的憑證之外，錯誤配置的雲端伺服器也是惡意攻擊引起的資料洩露中最常見的初始威脅向量，占 19%。雲端錯誤配置導致的洩露平均成本增加了 50 多萬美元，達到 441 萬美元。

$1.52 百萬

業務損失平均總成本

業務損失仍然是最主要的成本因素。

業務損失的成本約占資料洩露平均總成本的 40%，從 2019 年的 142 萬美元增加至 2020 年的 152 萬美元。業務損失的成本中包括更高的客戶流失率，因為系統停機時間損失的收入以及因為聲譽受損而增加獲取新業務的成本。

358 萬美元

與未部署安全自動化的組織相比，全面部署了安全自動化的組織平均節省的成本

安全自動化對資料洩露成本的影響在過去三年間也有所增長。

全面部署了安全自動化（使用了人工智慧平台和自動化洩露編排）的企業，從 2018 年的 15% 增加到 2020 年的 21%。

同時，安全自動化在降低資料洩露平均成本方面的效力也在不斷增強。尚未部署安全自動化的企業的平均總成本為 603 萬美元，是全面部署安全自動化的企業的兩倍以上，後者的資料洩露平均成本為 245 萬美元。相比那些未部署安全自動化的公司，全面部署了安全自動化的公司節省的成本從 2018 年的 155 萬美元增長到了 358 萬美元。

100 倍

超過 5000 萬條記錄的洩露與普通洩露的成本倍數

大規模洩露成本飆升了數百萬美元。

在超大規模資料洩露的樣本中，洩露記錄數量超過 100 萬條的公司承擔的成本是整體平均成本的很多倍。涉及 100 萬條至 1000 萬條記錄的洩露的平均成本為 5000 萬美元，是記錄少於 10 萬條的洩露平均成本（386 萬美元）的 25 倍以上。在記錄超過 5000 萬條的洩露中，平均成本為 3.92 億美元，是平均值的 100 多倍。

國家主體導致的洩露成本最為高昂。

儘管大多數惡意洩露都由受經濟利益驅動的網路攻擊者發起，但國家主體發動的攻擊往往成本最為高昂。2020 年的研究中，大多數惡意洩露 (53%) 都由受經濟利益驅動的攻擊者發起，相比之下，國家威脅主體參與了 13% 的惡意洩露，駭客占 13%，還有 21% 的資料洩露由動機不明的攻擊者發起。但與受經濟利益驅動的洩露的 423 萬美元相比，推定為國家贊助的洩露的平均成本為 443 萬美元。

+$292,000

安全系統複雜性對平均總成本的影響

安全複雜性和雲端遷移給公司帶來了最高的成本。

在 25 個成本因素中，安全系統複雜性的成本最為高昂，它讓洩露的平均總成本增加了 292,000 美元，調整後的平均總成本為 415 萬美元。洩露時發生的大規模雲遷移讓洩露的平均成本增加了 267,000 美元，調整後的平均成本為 413 萬美元。

+96 天

醫療保健與金融產業洩露生命週期

發現和控制洩露的平均時間因產業、地域和安全成熟度而千差萬別。

在 2020 年的研究中，發現洩露的平均時間為 207 天，控制洩露的平均時間為 73 天，平均「生命週期」為 280 天。

醫療保健產業的平均洩露生命週期為 329 天，金融產業的平均生命週期比它短 96 天（233 天）。與未部署安全自動化的公司相比，全面部署安全自動化的公司的生命週期可縮短 74 天，從原來的 308 天縮短至 234 天。

$2 萬美元

與未組建 IR 團隊或開展測試的組織相比，組建了事件回應團隊並開展 IR 測試的組織平均節省的成本

事件回應 (IR) 準備狀態可為企業達到最大的成本節省。

組建了事件回應團隊並廣泛測試其事件回應計畫的組織，其資料洩露的平均成本為 329 萬美元。相比之下，未採取任一項措施的組織的平均總成本為 529 萬美元，二者相差 200 萬美元。在 2019 年的研究中，兩種類型的組織之間的成本差距為 123 萬美元。

16 個國家/地區中有 12 個

從 2019 年的研究以來，平均總成本有所增加的國家/地區

從 2019 年開始，地區和產業差異出現了較大的波動。

美國以 864 萬美元的資料洩露成本繼續高居榜首，中東以 652 萬美元緊隨其後。在 2019 年和 2020 年的研究中，16 個國家/地區中有 12 個的平均總成本都有所增加，其中斯堪地那維亞的增幅最大，為 12.8%。

醫療保健產業以 713 萬美元連續第十年高居平均洩露成本榜首，與 2019 年的研究相比增長了 10.5%。同樣，能源產業也比 2019 年增長了 14.1%， 在 2020 年的研究中平均成本為 639 萬美元。整體來看，17 個產業中有 13 個產業的平均總成本在逐年下降，降幅最高的分別是媒體、教育、公共部門和餐旅。

完整的結果

在本部分中，我們提供本次研究的詳細結果。

按照以下順序呈現主題：

1. 全球調查結果和重點
2. 資料洩露的根本原因
3. 影響資料洩露成本的因素
4. 安全自動化趨勢和效力
5. 發現並控制資料洩露的時間
6. 資料洩露的長尾成本
7. 新冠肺炎帶來的潛在影響
8. 大規模洩露的成本

全球調查結果和重點

*資料洩露成本報告*是一份全球性報告，它綜合了 17 個國家/地區和 17 個產業的 524 家組織的結果，得出了全球平均值。但在某些情況下，為進行比較，報告會按照國家/地區或產業對結果進行細分。儘管一些國家/地區和產業的樣本量較小，但研究中會儘量選擇一些有代表性的組織。

重要發現

$7.13 百萬

與 2019 年的研究相比，醫療保健產業資料洩露的平均成本增長了 10%

80%

記錄中含有客戶 PII 的洩露的比例，每條記錄的平均成本為 150 美元

$5.52 百萬

與員工人數不足 500 人的組織的 264 萬美元的成本相比，員工人數超過 25,000 人的企業的洩露平均總成本

圖 1

全球研究概覽

國家/地區	2020 年樣本	樣本百分比	貨幣	研究年數
美國	63	12%	美元	15
印度	47	9%	印度盧比	9
英國	44	8%	英鎊	13
德國	37	7%	歐元	12
法國	36	7%	歐元	7
巴西	35	7%	巴西雷亞爾	9
日本	33	6%	日元	11
中東*	29	6%	里亞爾	7
加拿大	26	5%	加元	6
韓國	24	5%	韓元 (KRW)	3
東協#	23	4%	新加坡元	2
澳大利亞	23	4%	澳元	11
斯堪地那維亞+	23	4%	冰島克朗	2
義大利	21	4%	歐元	9
拉丁美洲**	21	4%	比索	1
土耳其	20	4%	土耳其里拉	3
南非	19	4%	南非美元	5
總計	524			

今年的研究考察了 17 個國家或地區樣本中的洩露情況。

國家和地區包括美國、印度、英國、德國、巴西、日本、法國、中東、加拿大、義大利、韓國、澳大利亞、土耳其、東協、南非、斯堪地那維亞，還首次將拉丁美洲（墨西哥、阿根廷、智利和哥倫比亞）納入研究範疇。**圖 1** 顯示了樣本量、各國家/地區貨幣以及各國家/地區被納入研究的年數。

*中東是位於沙烏地阿拉伯和阿拉伯聯合大公國的公司集群地

#東協是位於新加坡，印度尼西亞，菲律賓，馬來西亞，泰國和越南的公司集群地

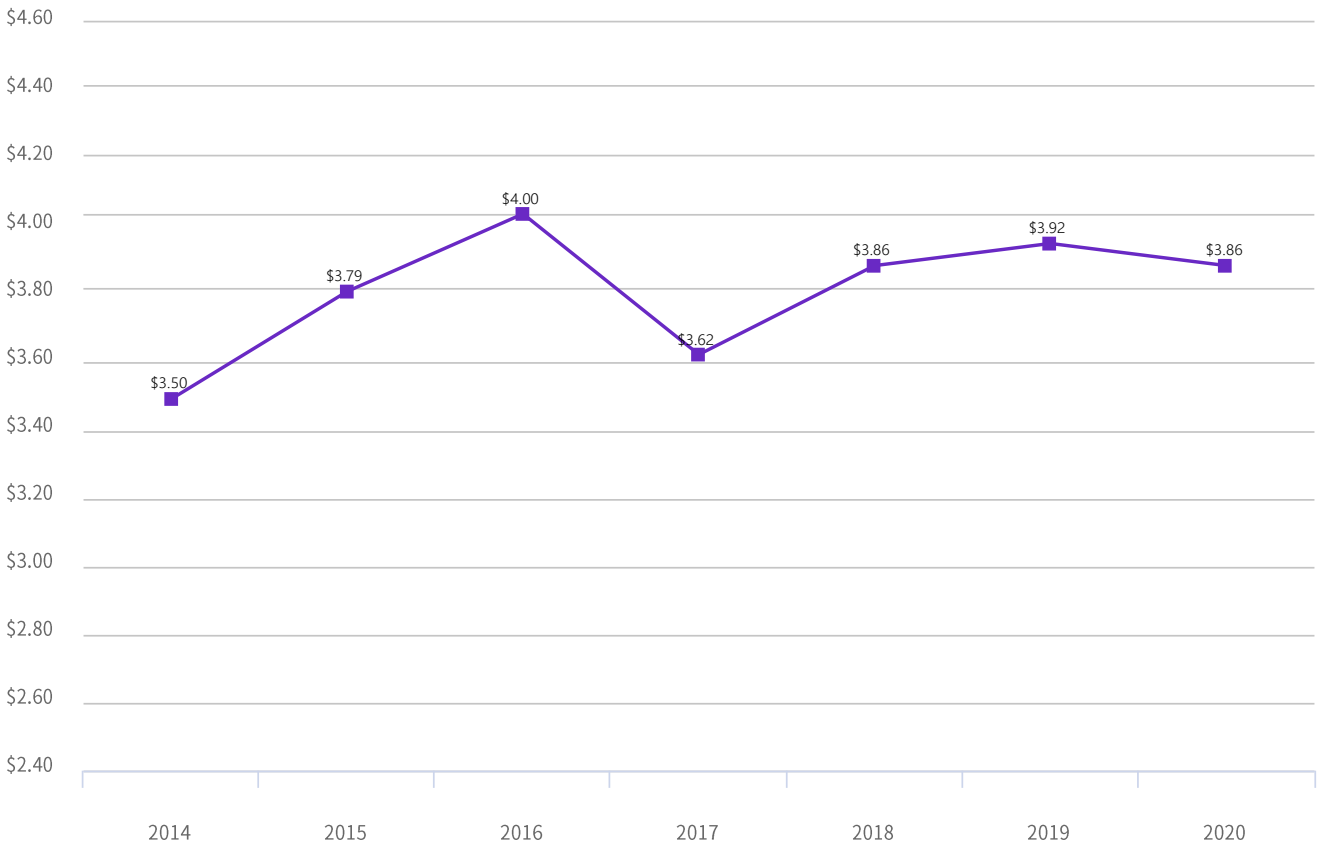
+斯堪地那維亞半島是位於丹麥，瑞典，挪威和芬蘭的公司集群地

** 拉丁美洲是位於墨西哥、阿根廷、智利和哥倫比亞的公司集群地

圖 2

資料洩露的平均總成本

以百萬美元為單位



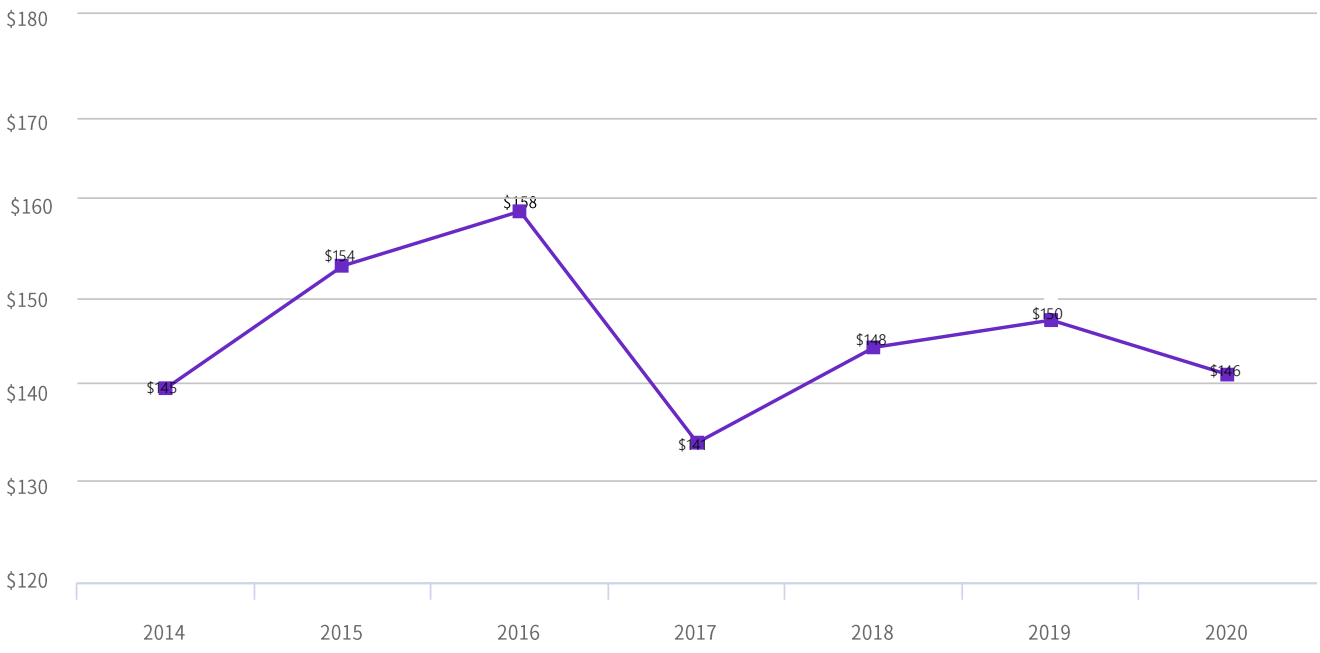
自 2014 年以來，資料洩露的平均總成本增長了 10%。

圖 2 顯示了七年來資料洩露的全球平均總成本。2020 年研究中的綜合平均總成本為 386 萬美元，與 2019 年的 392 萬美元相比略有下降。過去七年的加權平均值為 379 萬美元。

圖 3

資料洩露的每條記錄的平均成本

以美元為單位



資料洩露的每條記錄的成本小幅下降至 146 美元。

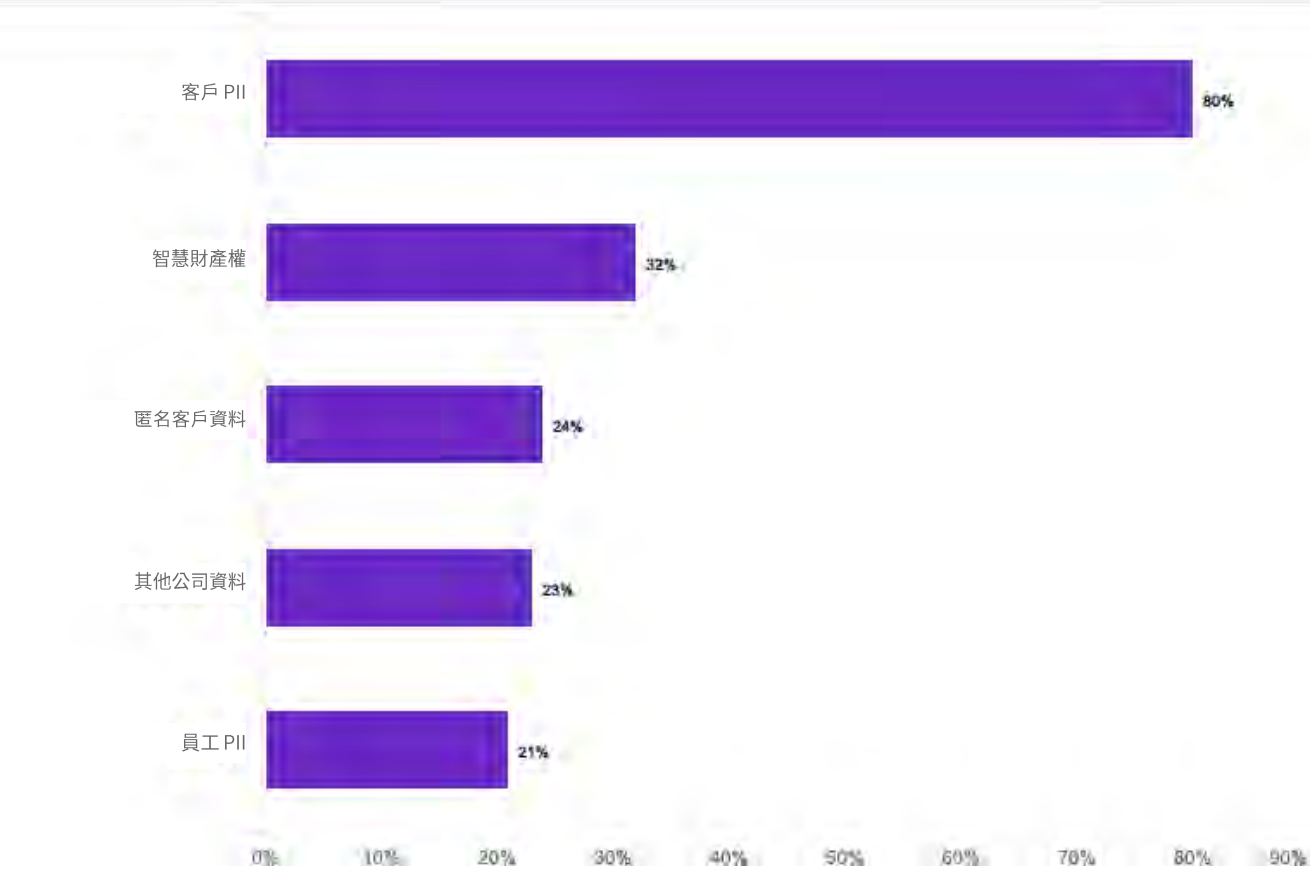
圖 3 顯示了過去七年來，每條被破壞記錄的平均資料洩露成本。

過去七年來，每條記錄的加權平均成本為 149 美元。

圖 4

被破壞的記錄類型

涉及各類資料的洩露百分比



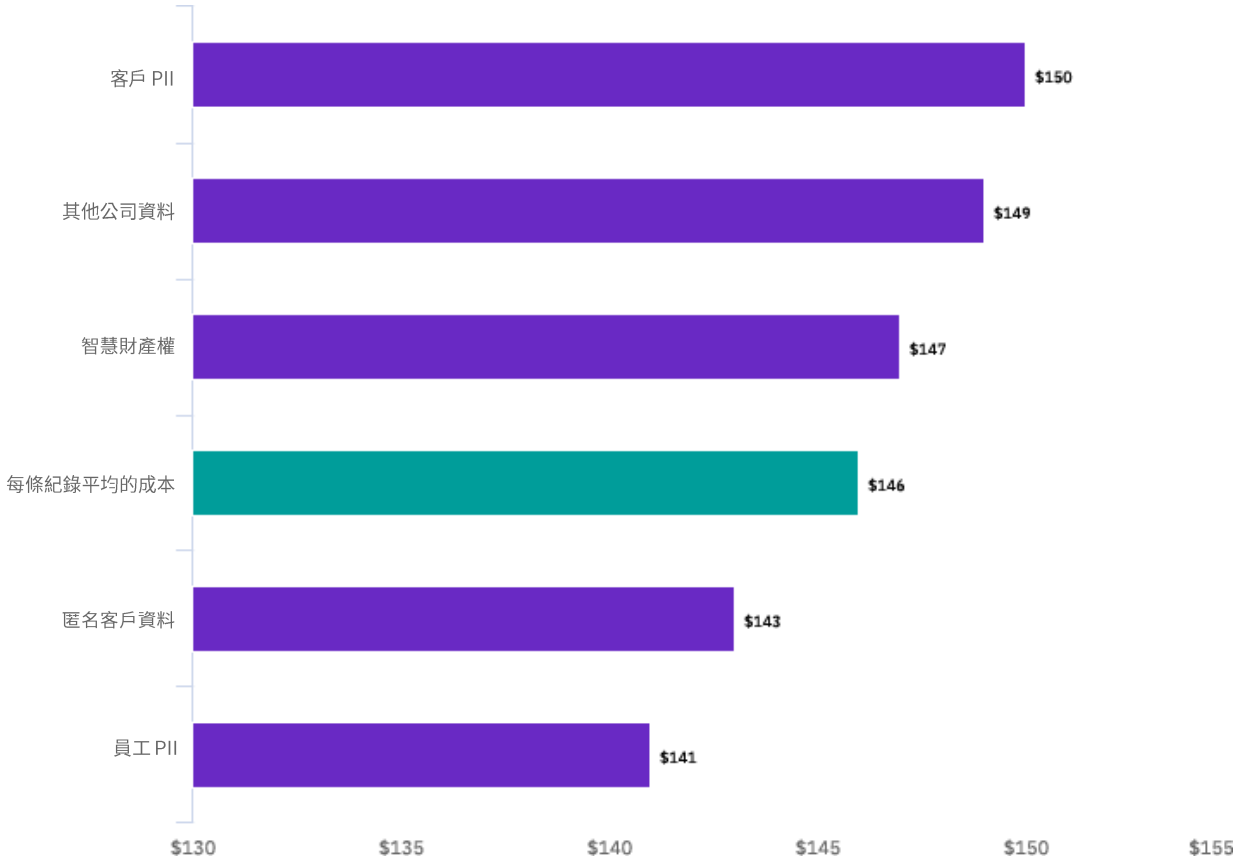
客戶 PII 是發生洩露時最常遺失或被盜的資料類型。

圖 4 顯示出，80% 的資料洩露中都有客戶 PII。32% 的資料洩露中都會發生智慧財產權被竊取，24% 的資料洩露中都會有匿名客戶資料被盜的情況發生。

圖 5

每條記錄的平均成本（按被破壞的資料類型劃分）

以美元為單位



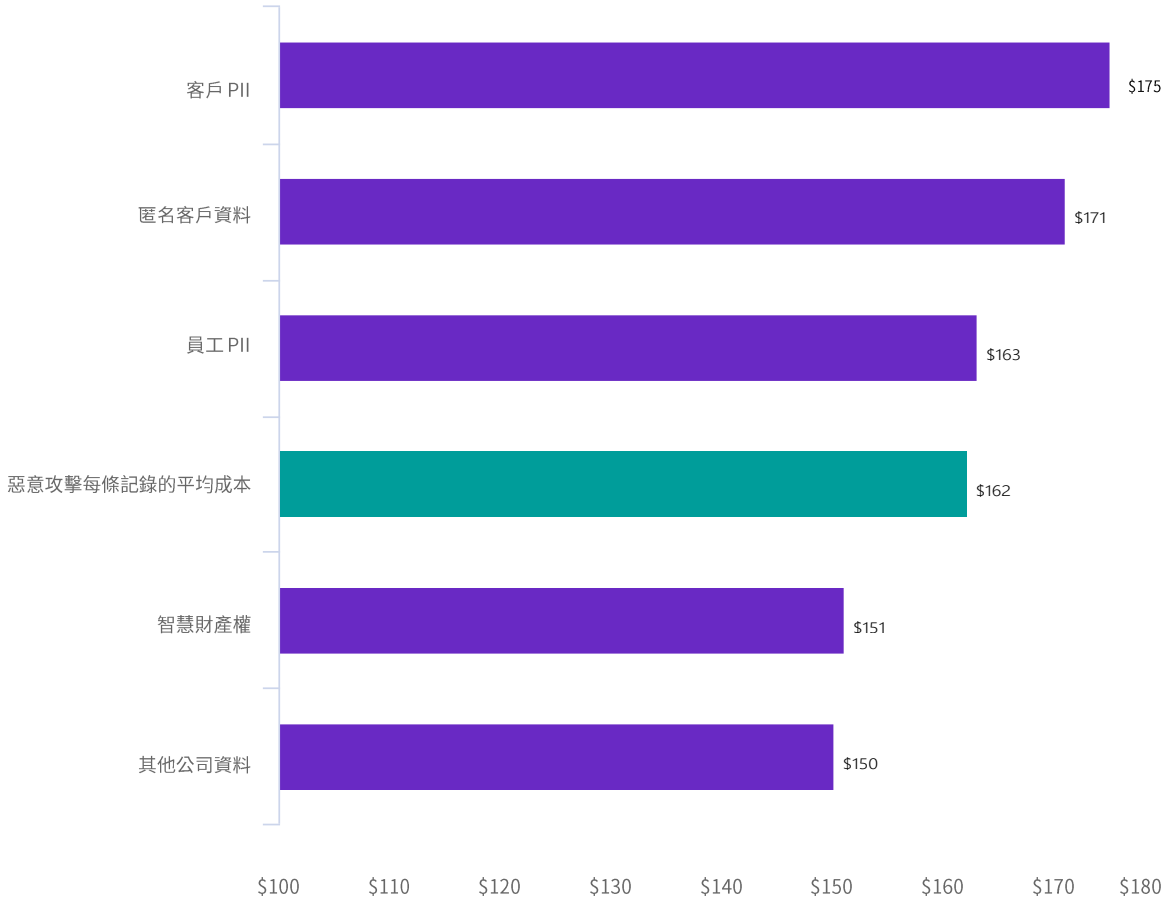
客戶 PII 是資料洩露中成本最高的被盜資料類型。

如圖 5 所示，每條遺失或被盜記錄的客戶 PII 平均成本為 150 美元，每條記錄的智慧財產權成本為 147 美元，每條記錄的匿名客戶資料（非 PII）成本為 143 美元，每條記錄的員工 PII 成本為 141 美元。

圖 6

惡意攻擊中每條記錄的平均成本（按被盜資料類型劃分）

以美元為單位



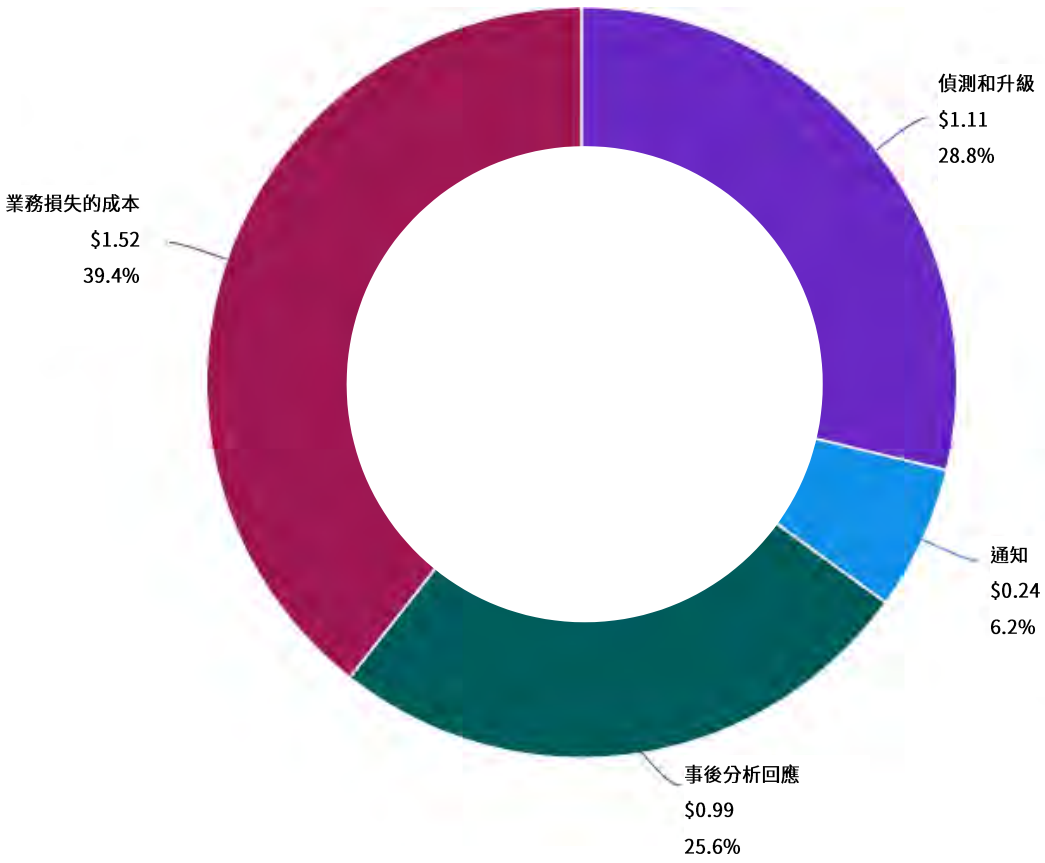
惡意攻擊導致的資料洩露的每條記錄的成本會更高。

如圖 6 所示，惡意攻擊中客戶 PII 的每條記錄的成本為 175 美元，比其他任何類型的洩露中受損的客戶 PII 的每條記錄平均總成本（每條記錄 150 美元）高出近 17%。

圖 7

資料洩露平均總成本分為四類

以百萬美元為單位



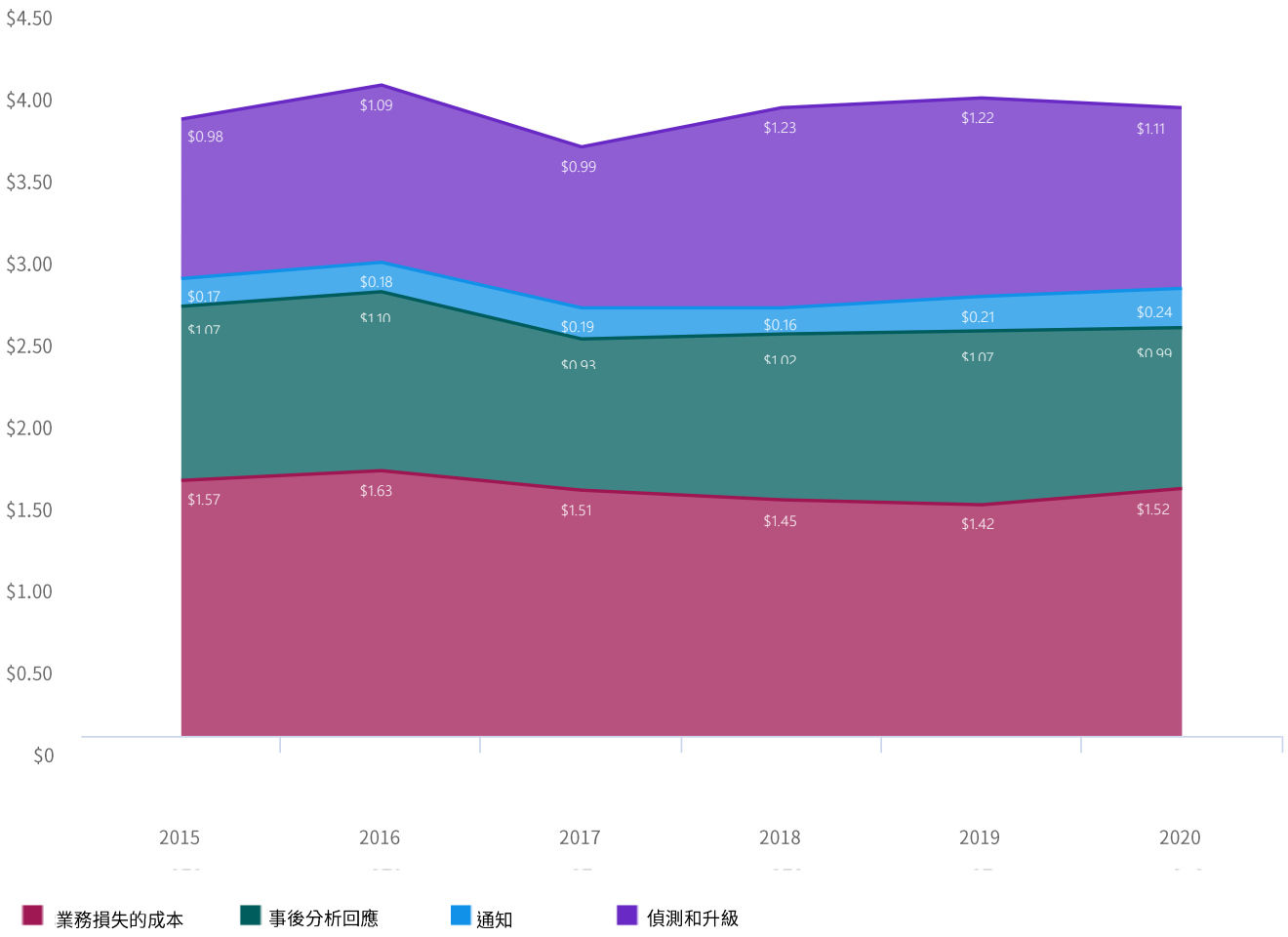
業務損失在資料洩露平均成本中占有最高比例。

圖 7 以美元為單位展示了四個成本部分以及各自所佔資料洩露總成本的百分比。業務損失的平均成本為 152 萬美元或總成本的 39%。最低的成本部分是通知資料洩露，為 240,000 美元或總成本的 6%。

圖 8

四類資料洩露平均成本的趨勢

以百萬美元為單位



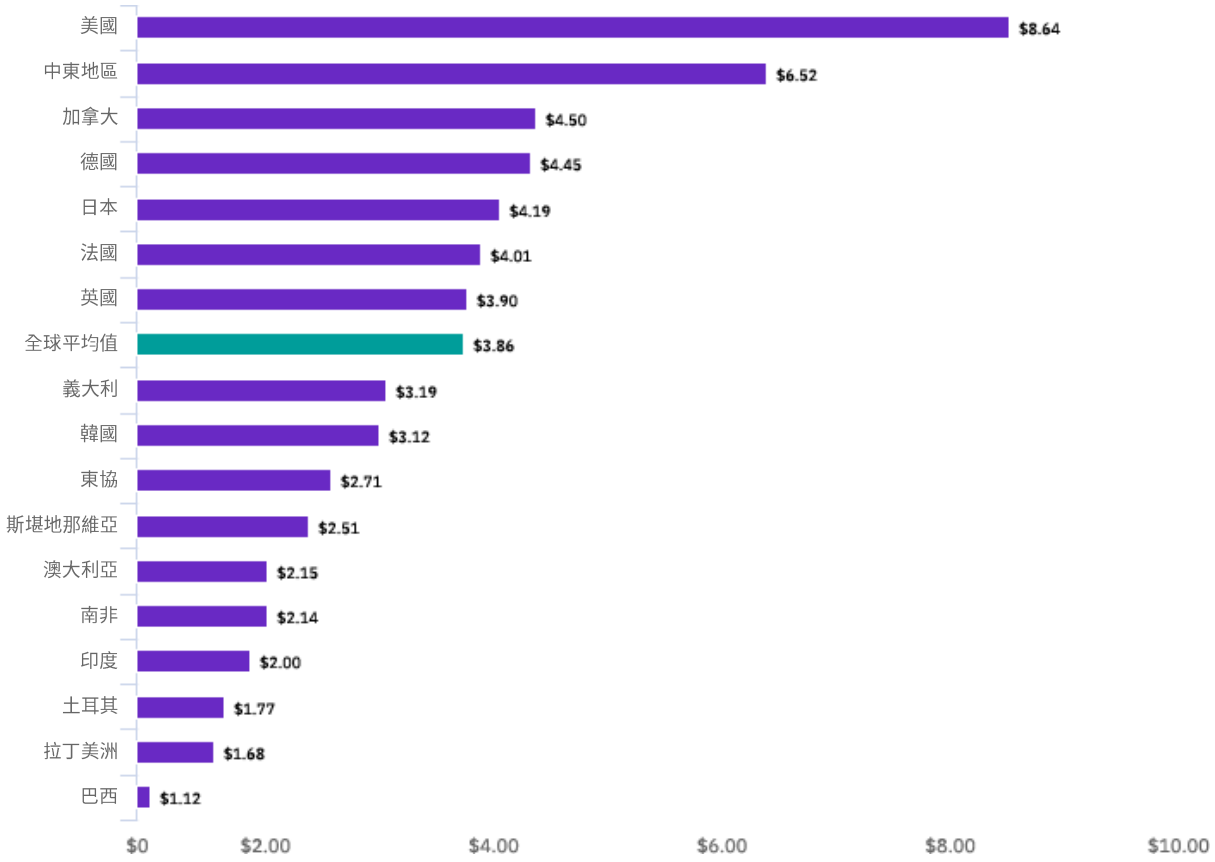
業務損失的成本年成長率略有增加。

圖 8 顯示了過去六年間業務損失、洩露後回應、通知和偵測和升級的成本趨勢。該模式顯示了這些成本的一致性。通知仍是最低的成本部分，而業務損失則是最高的成本部分。

圖 9

資料洩露的平均總成本（按國家或地區劃分）

以百萬美元為單位



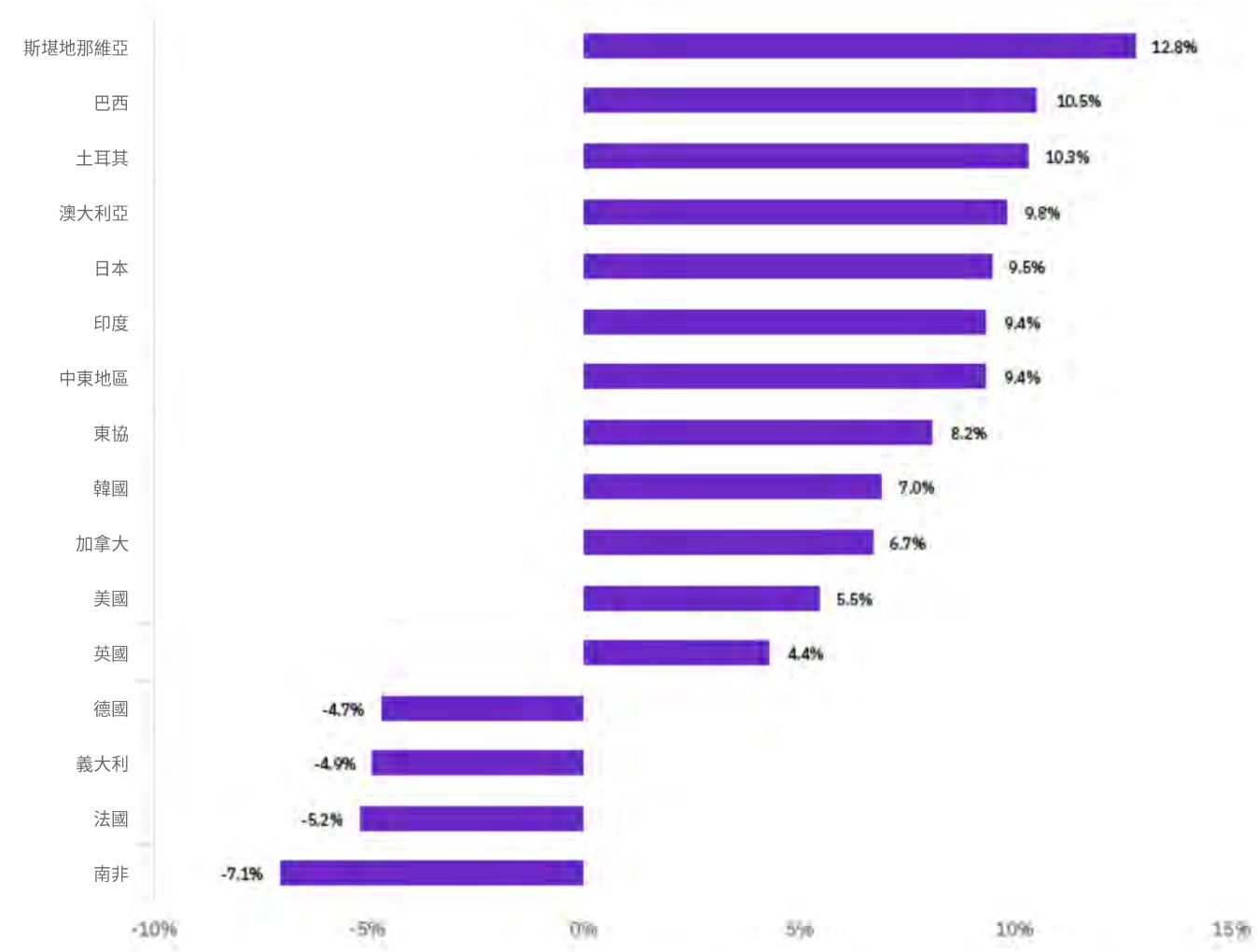
資料洩露的平均總成本因國家/地區而異。

圖 9 顯示了按國家/地區劃分的資料洩露平均總成本。美國的組織以 864 萬美元的總平均成本高居榜首，中東以 652 萬美元緊隨其後。相比之下，拉丁美洲和巴西的組織的平均總成本最低，分別為 168 萬美元和 112 萬美元。

圖 10

2019-2020 年間各國家或地區的平均總成本百分比變化

以本國貨幣計算



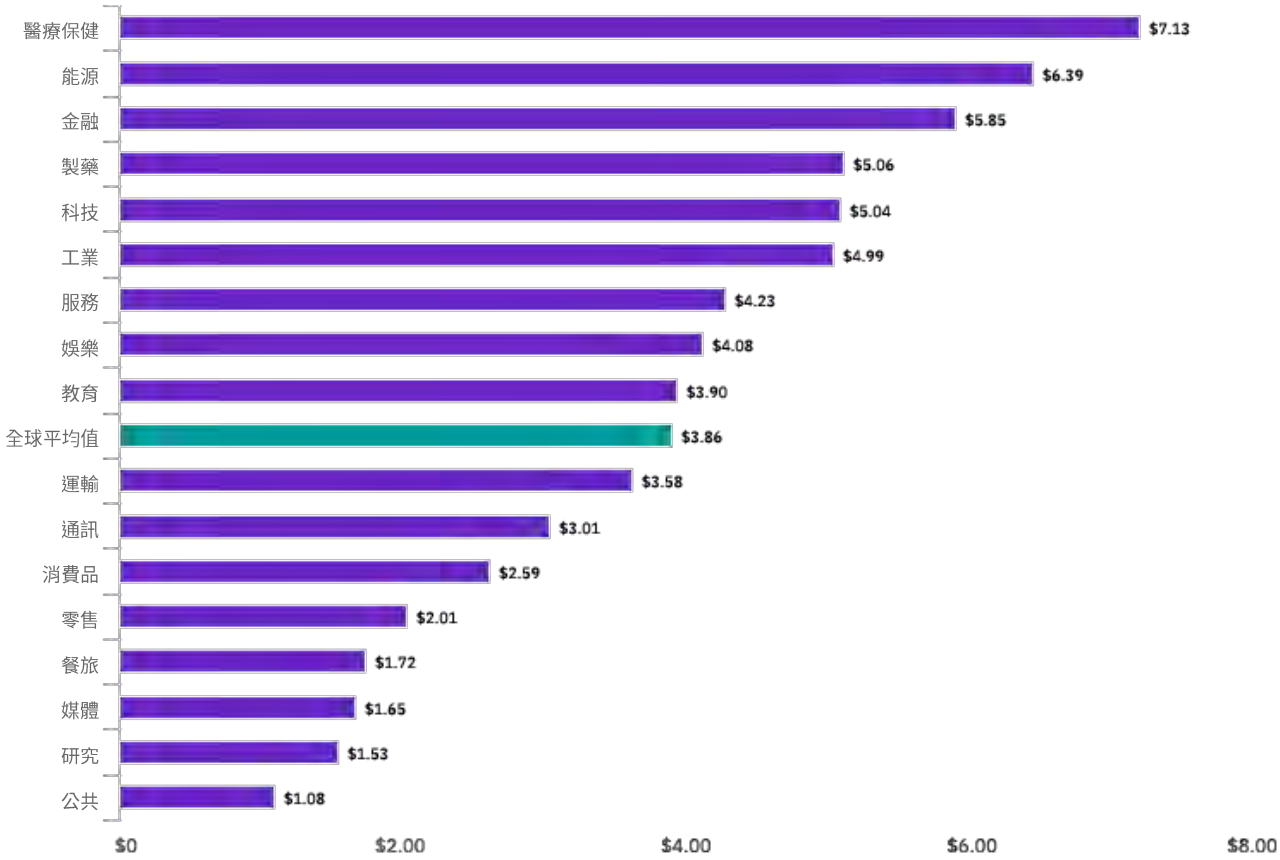
16 個國家或地區中，有 12 個國家或地區的資料洩露平均總成本有所增加。

如圖 10 所示，在 2019 年至 2020 年的研究中，斯堪地那維亞的資料洩露總成本增幅最大，法國和南非降幅最大。

圖 11

資料洩露的平均總成本（按產業劃分）

以百萬美元為單位

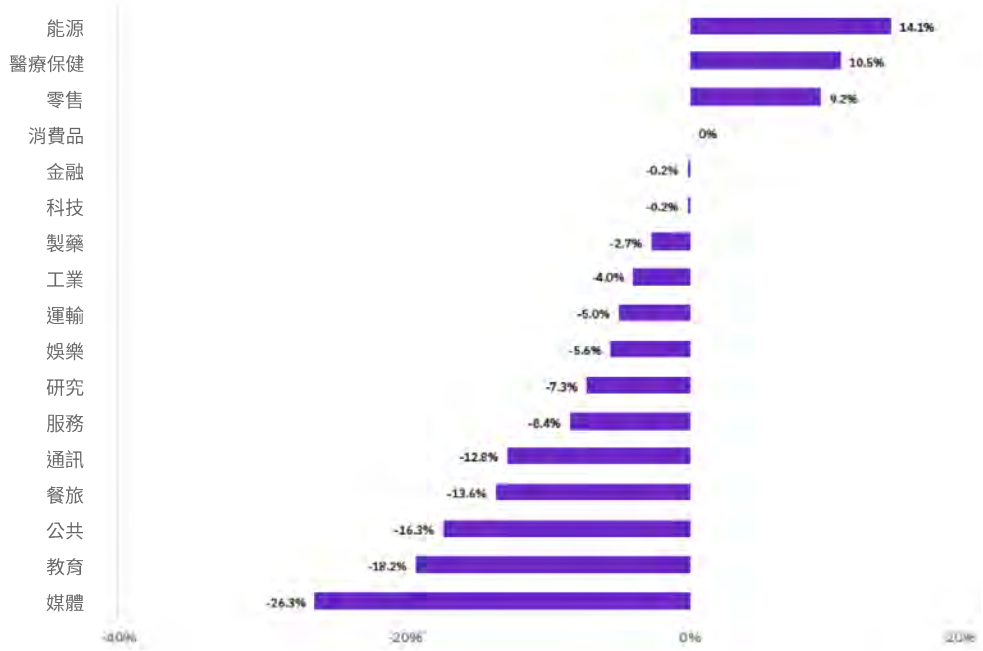


面臨更嚴格法規要求的組織承擔的資料洩露成本會更高。

如圖 11 所示，醫療保健、能源、金融服務和製藥產業發生的資料洩露平均總成本明顯高於監管力度較小的產業，例如餐旅、媒體和研究組織。在此研究中，公共部門組織的資料洩露成本一直處於末位，因為他們不太可能因為資料洩露而失去大量客戶。

圖 12

2019-2020 年間各產業平均總成本百分比變化



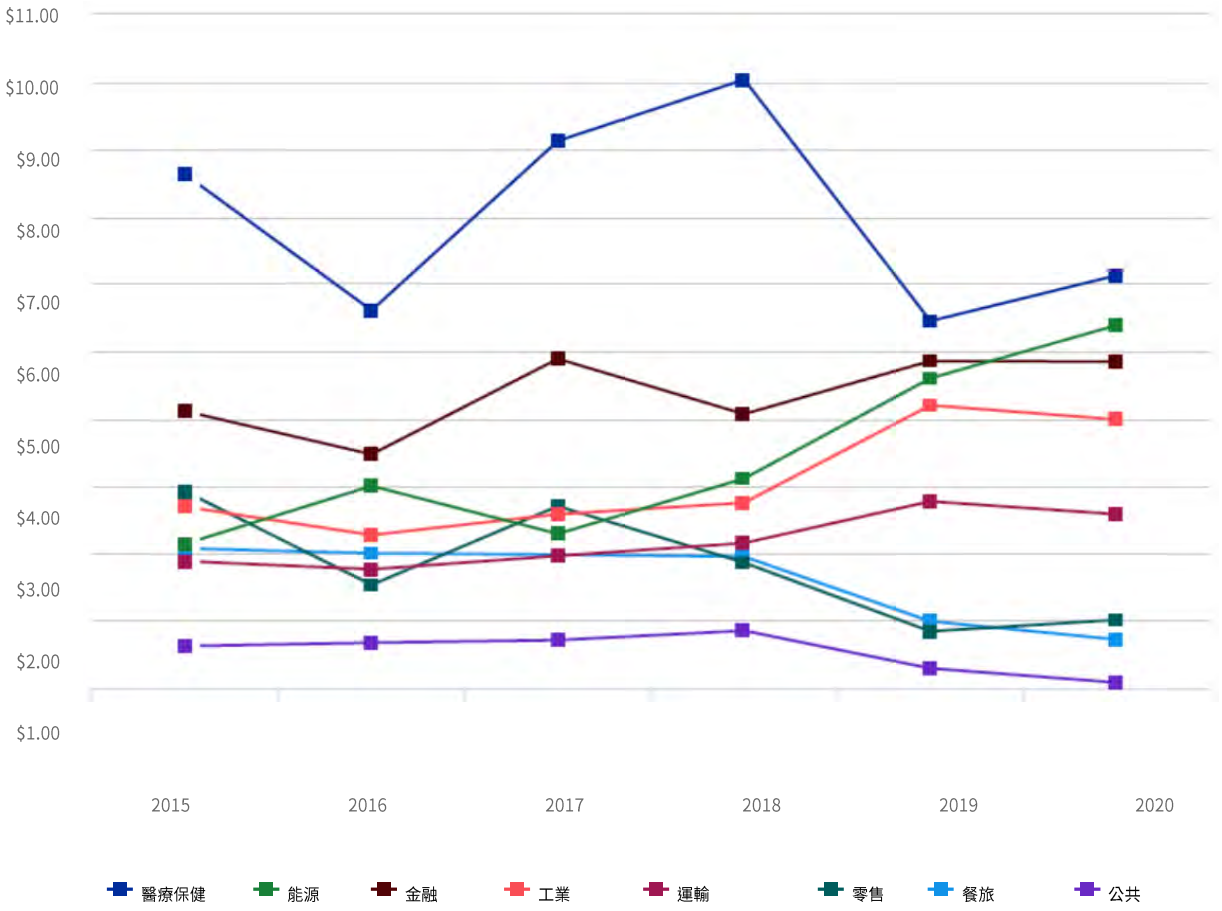
能源、醫療保健和零售產業資料洩露成本的增幅最高。

從圖 12 可以看出，在 2019 年和 2020 年研究中涵蓋的 17 個產業中，只有 3 個產業的資料洩露成本有所增加。能源、醫療保健和零售產業的平均總成本增幅最大，而公共部門、教育和媒體產業則出現了最大跌幅。

圖 13

八個行业的資料洩露平均總成本趨勢

以百萬美元為單位



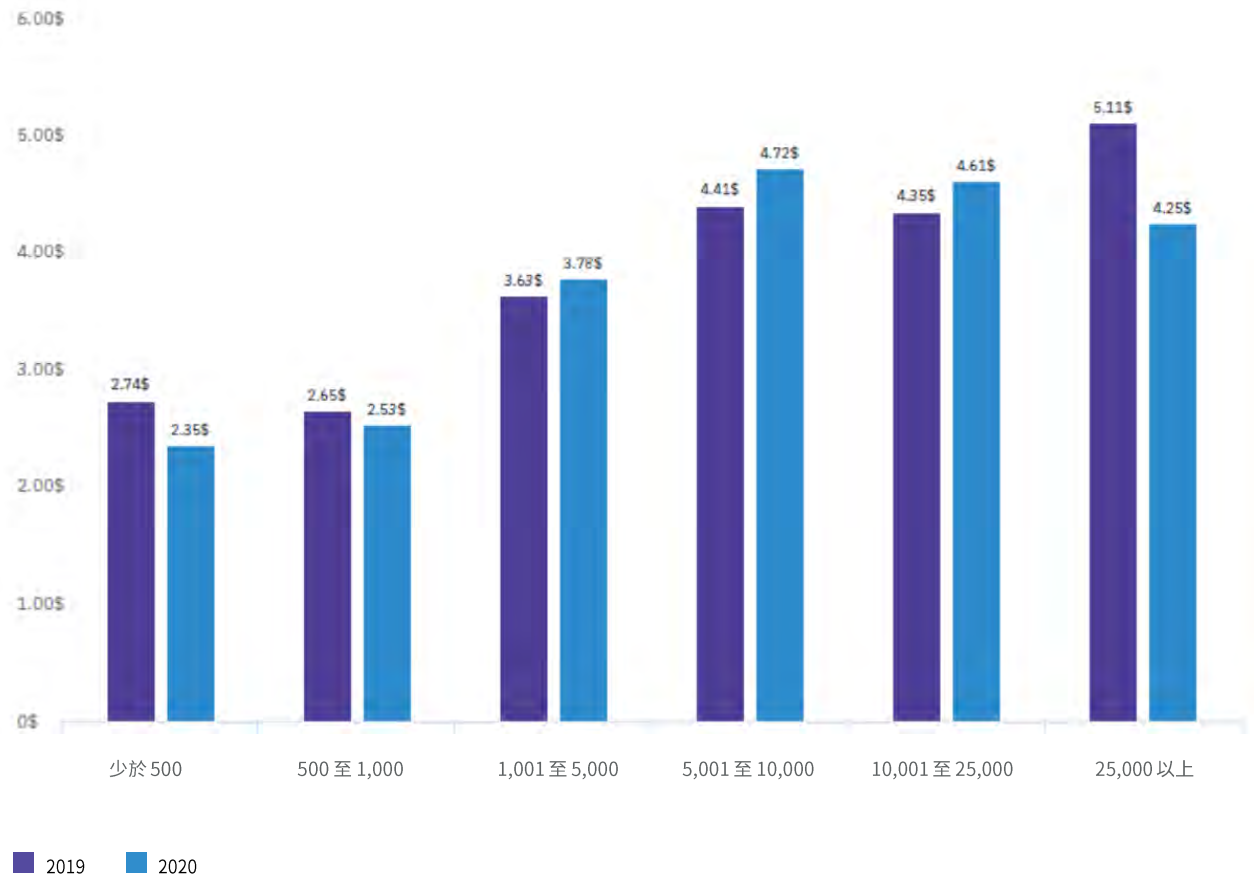
醫療保健和金融產業一直都是資料洩露成本最高的產業。

圖 13 顯示了過去六年間八個產業部門的線圖。醫療保健一直是成本最高的產業，而公共部門一直是成本最低的產業。

圖 14

按組織規模劃分的資料洩露平均總成本

以百萬美元為單位



中等規模組織的資料洩露平均成本有所增加。

從**圖 14** 可以看出，在 2019 和 2020 年的研究中，規模最小的組織（1,000 名員工或更少）和規模最大的組織（員工人數超過 25,000 人）的資料洩露平均總成本有所下滑。員工人數超過 25,000 人的組織，平均總成本從 2019 年的 511 萬美元下降到 2020 年的 425 萬美元，下降幅度為 16.8%。但對於中等規模的組織而言，洩露總成本平均起來卻有所增加。人數在 5,001 至 10,000 人的組織，洩露平均成本從 2019 年的 441 萬美元增加至 2020 年的 472 萬美元，增幅為 7%。從比例上看，越小的組織每位員工的平均成本反而更高。

資料洩露的根本原因

多年來，研究一直在透過參與者瞭解引起資料洩露的原因。前幾年的報告將這些根本原因分為三類：系統故障（IT 和業務流程故障）；人為失誤（玩忽職守的員工或承包商無意中引起資料洩露）；以及惡意攻擊（由駭客或犯罪的內部人士引起）。

今年的報告仍將這些洩露分為三類。但是在更加深入的分析中，我們要求參與者提供更詳細的與惡意攻擊原因有關的資訊，其中包括初始威脅向量和攻擊者類型。我們在本部分提供了這些分析的結果。

重要發現

52%

惡意攻擊引起的洩露的比例，平均成本為 427 萬美元

19%

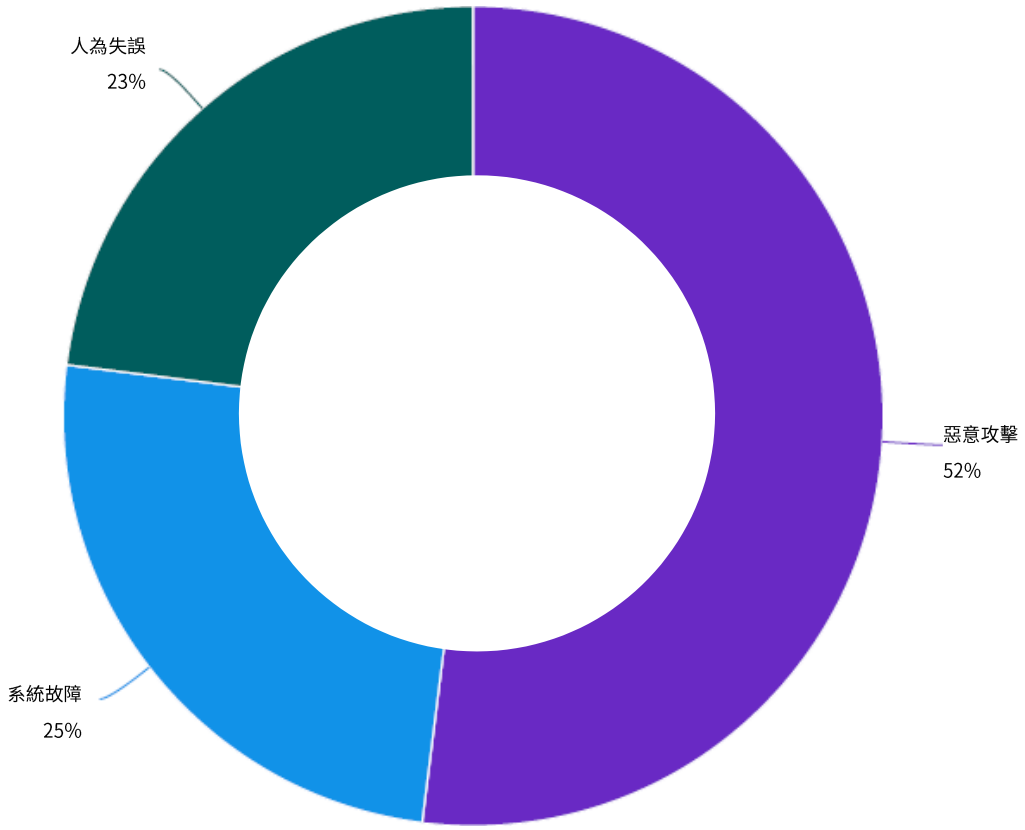
憑證被盜 (19%) 和雲端錯誤配置 (19%) 引起的惡意洩露的比例

$4.43 百萬

國家攻擊者引起的資料洩露的平均成本，13% 的惡意攻擊由國家主體發起

圖 15

資料洩露根本原因細分為三類



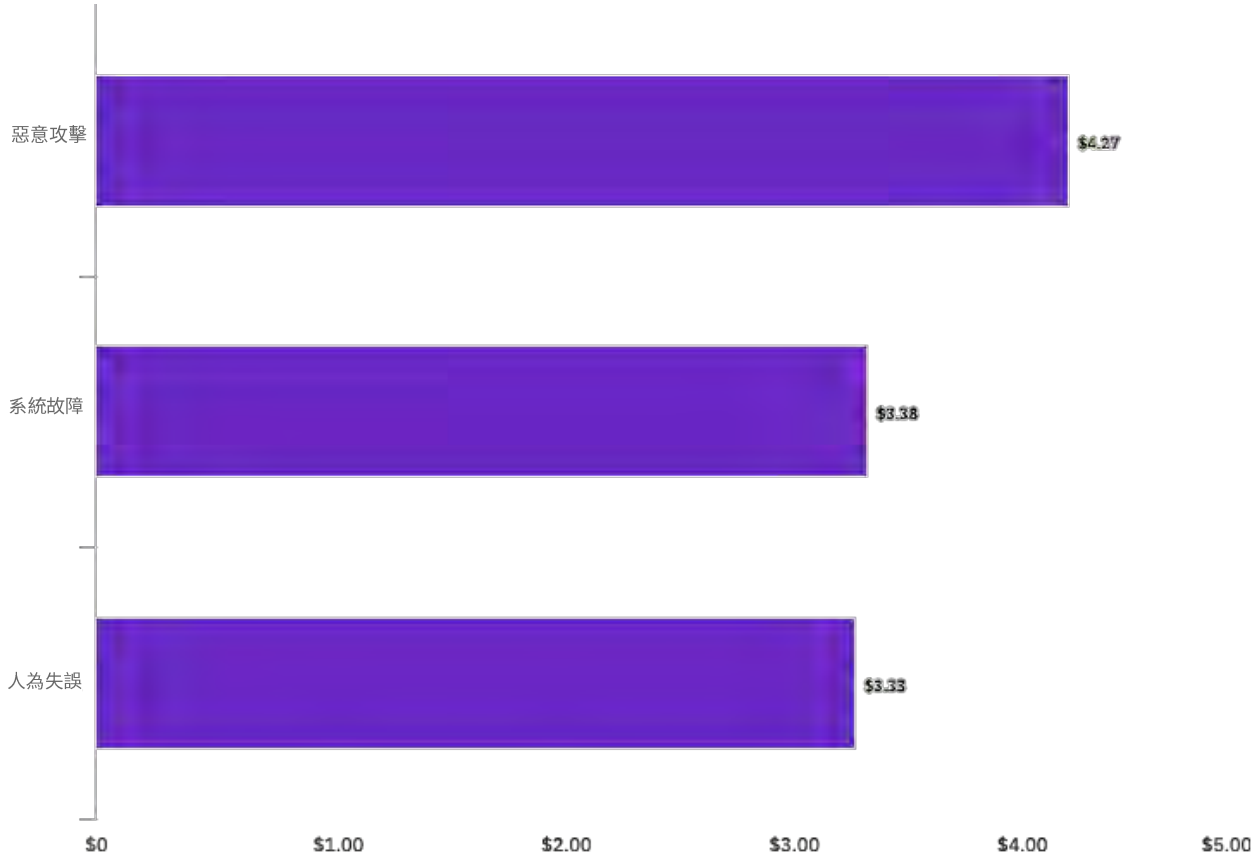
惡意攻擊是大部分資料洩露的罪魁禍首。

圖 15 匯總了三大類別的資料洩露根本原因。52% 的事件中涉及到惡意攻擊，系統故障和人為失誤的比例分別為 25% 和 23%。

圖 16

三種資料洩露根本原因的平均總成本

以百萬美元為單位



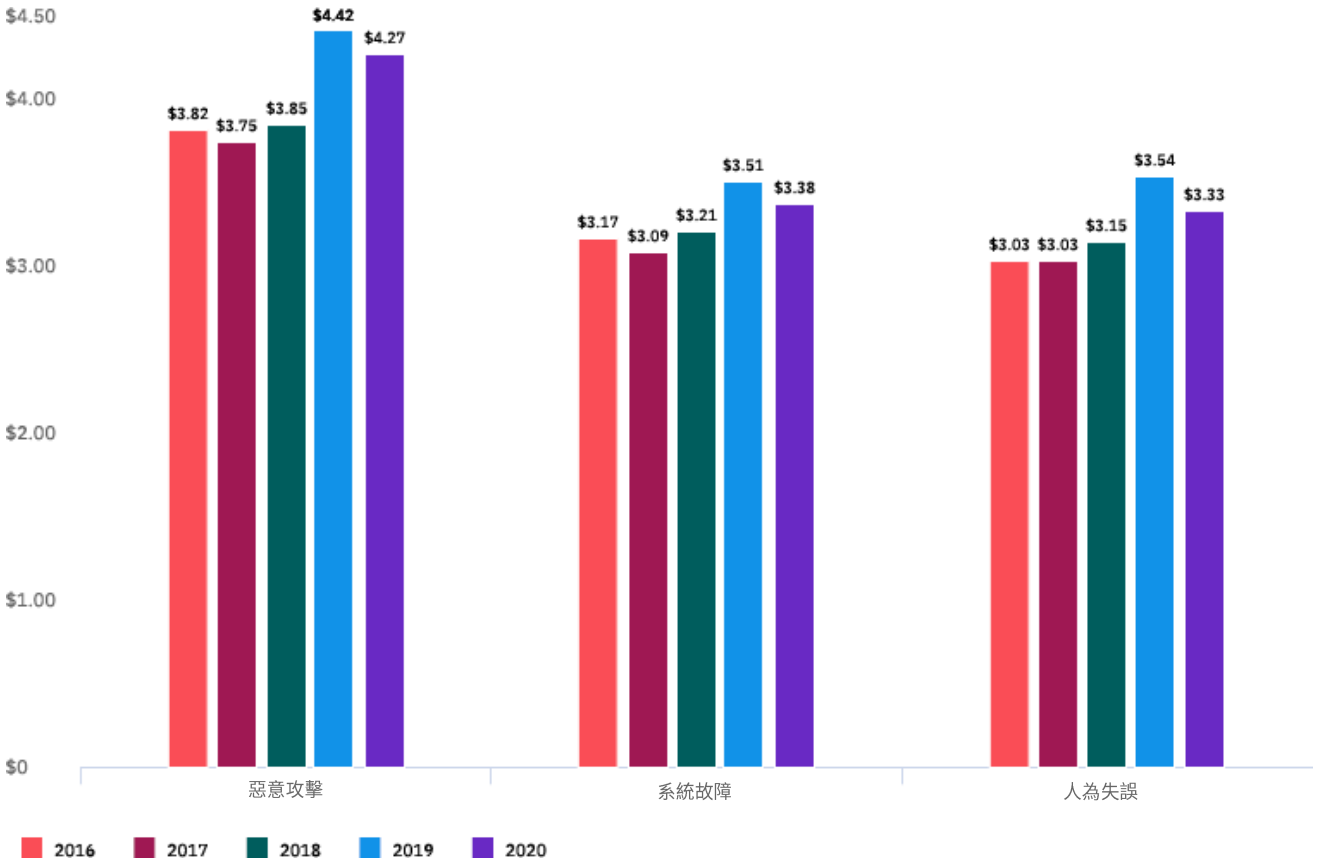
惡意攻擊是成本最為高昂的根本原因。

如圖 16 所示，在 2020 年的研究中，惡意攻擊導致的資料洩露的平均成本為 427 萬美元，比系統故障或人為失誤引發的資料洩露的成本高出近 100 萬美元。

圖 17

平均總成本的趨勢（按資料洩露的根本原因劃分）

以百萬美元為單位

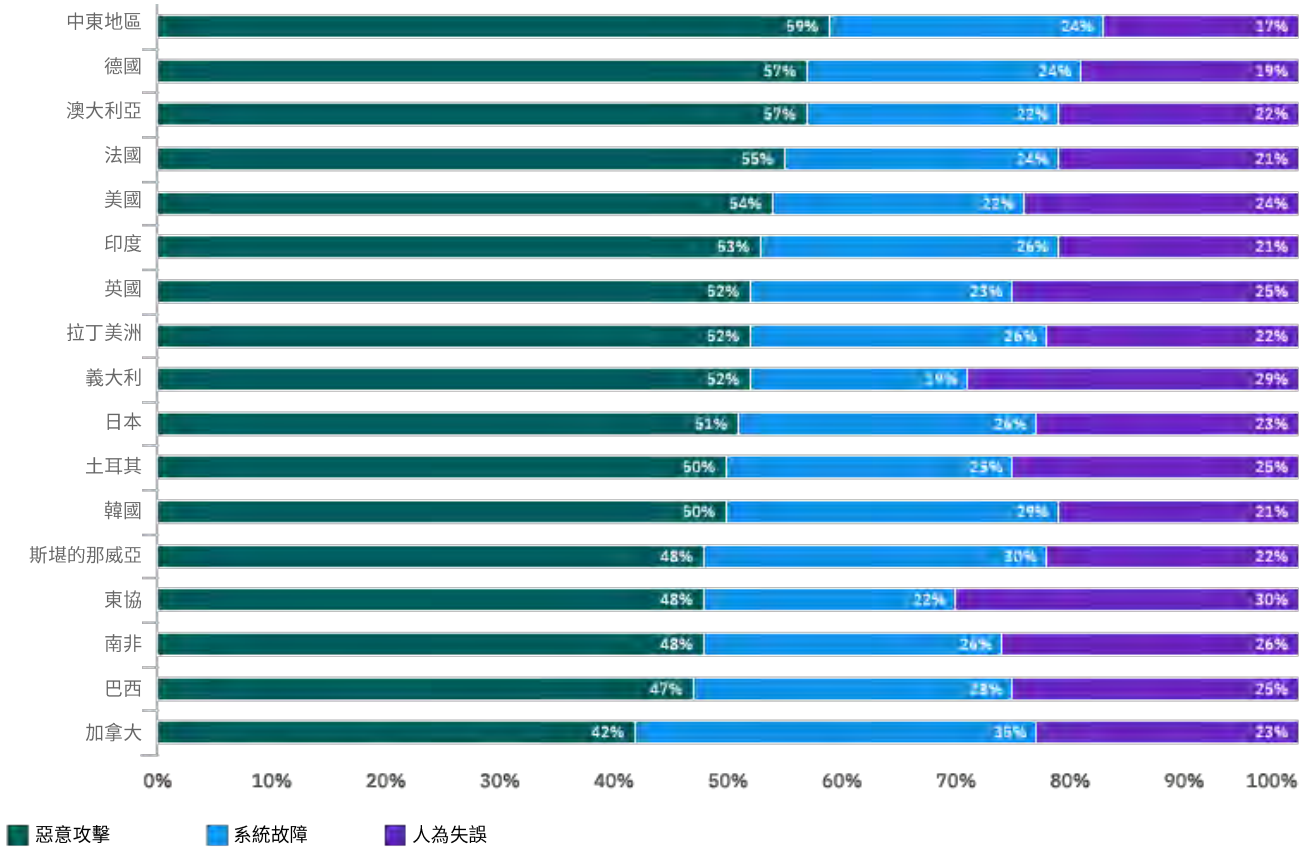


過去五年來，成本最為高昂的仍是惡意攻擊洩露。

圖 17 顯示了過去五年間三種資料洩露根本原因的平均總成本。從研究中可以得知，自 2016 年以來，根本原因的模式一直非常平穩，與 2019 年相比，2020 年的成本略有下降。自 2016 年以來，惡意洩露的平均總成本增長了近 12%。

圖 18

資料洩露根本原因細分（按國家或地區劃分）

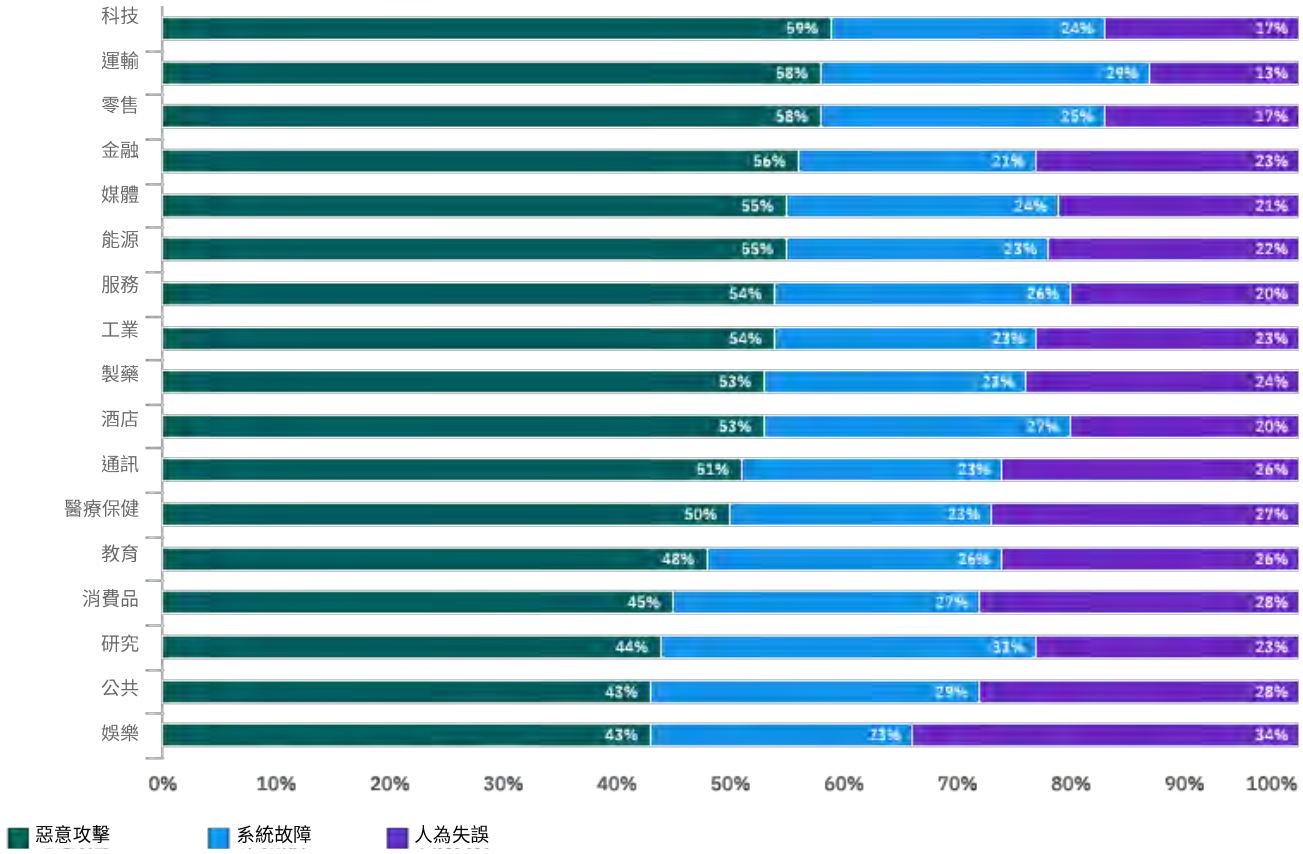


洩露的根本原因會因地域而異。

從圖 18 可以看出，中東、德國和澳大利亞因為惡意攻擊引起資料洩露的比例最高，而南非、巴西和加拿大因為惡意攻擊引起資料洩露的比例最低。加拿大因為系統故障引起資料洩露的比例最高。東協和義大利因為人為錯誤導致資料洩露的比例最高。

圖 19

各產業資料洩露根本原因細分



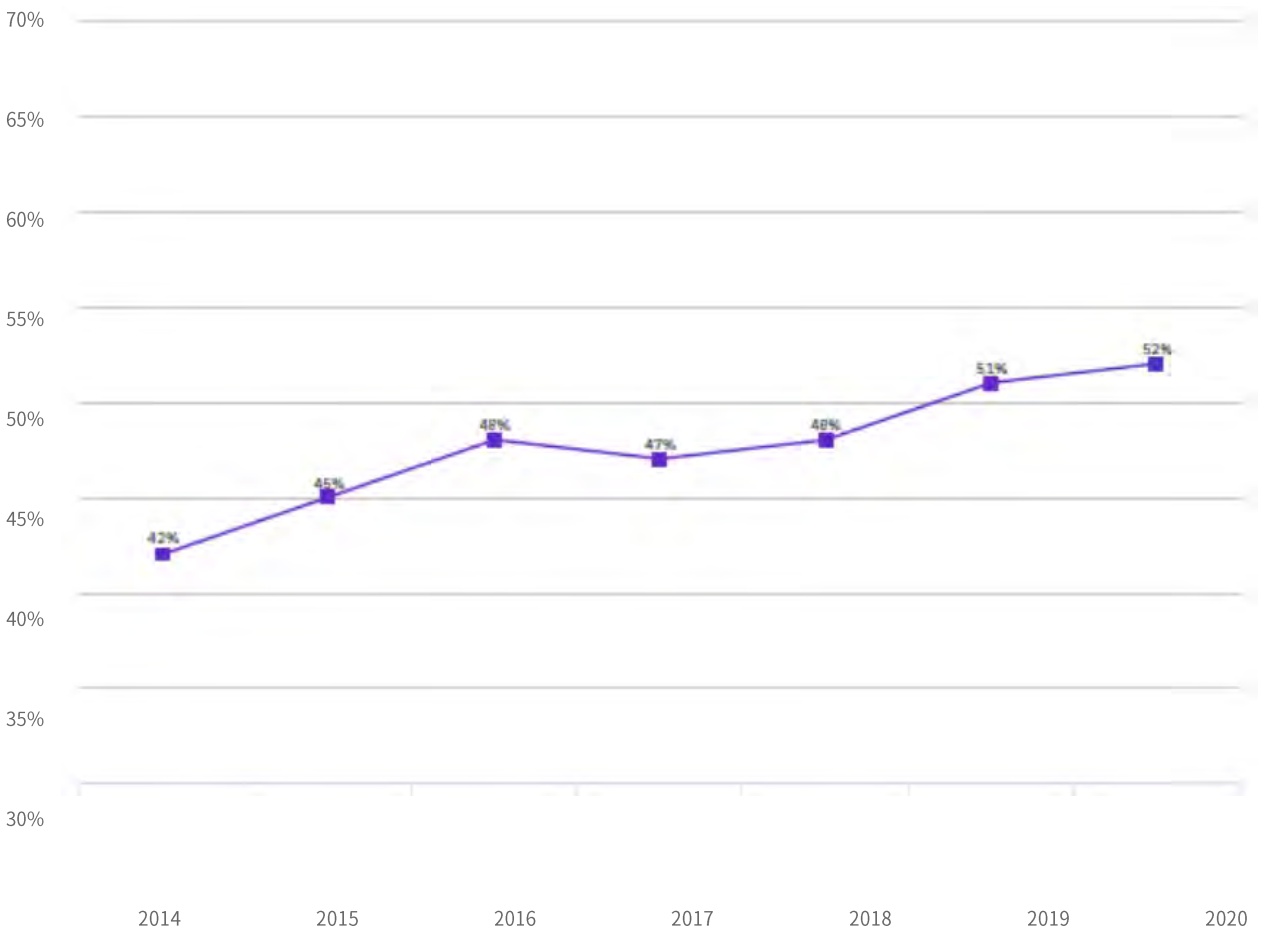
不同產業資料洩露根本原因的細分也各不相同。

如圖 19 所示，科技、運輸、零售和金融產業受到惡意攻擊的比例最高。娛樂、公共部門和消費品產業因人為失誤導致資料洩露的比例最高。系統故障是在研究、公共部門和運輸產業更為常見的資料洩露根本原因。

圖 20

惡意攻擊導致的資料洩露的趨勢

所有洩露的百分比



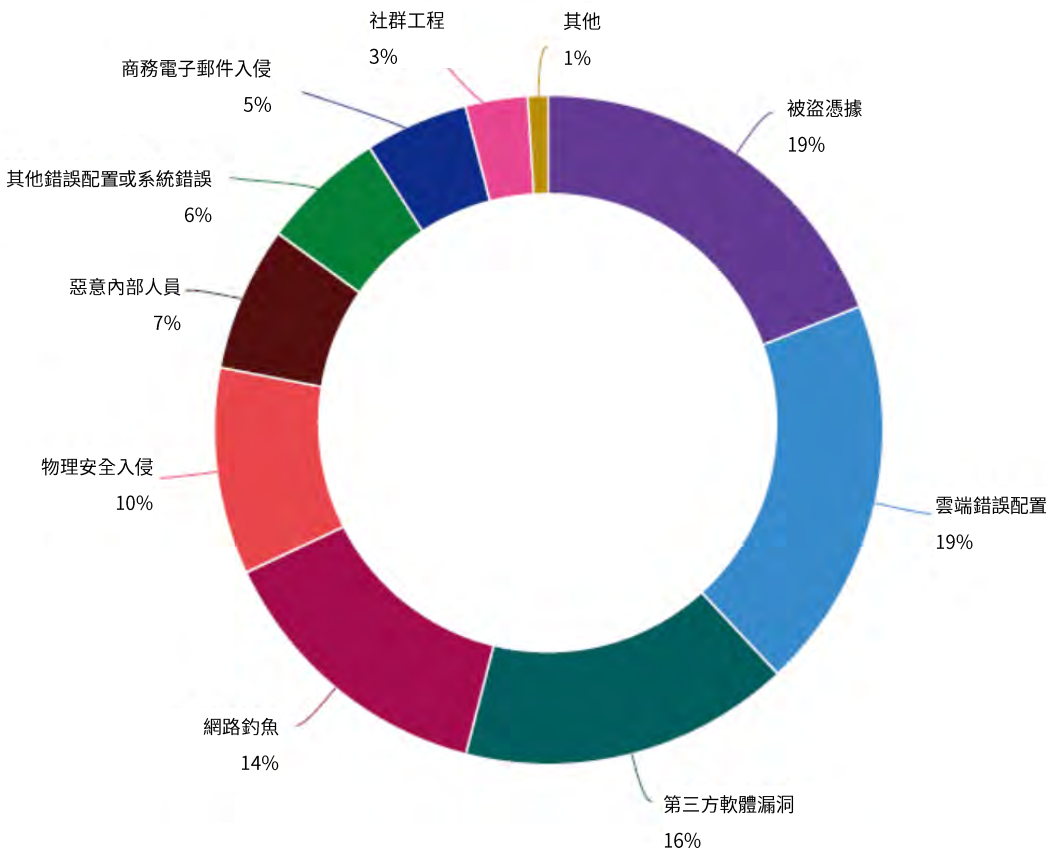
惡意攻擊引起的洩露比例一直在穩步上升。

從**圖 20** 可以看出，報告中的惡意攻擊資料洩露的比例從 2014 年的 42% 上升至 2020 年的 52%。增加的 10 個百分點表示惡意攻擊引發洩露的比例增長了近 24%（增長率）。

圖 21

惡意攻擊資料洩露根本原因細分（按威脅向量劃分）

惡意攻擊引起的洩露的百分比

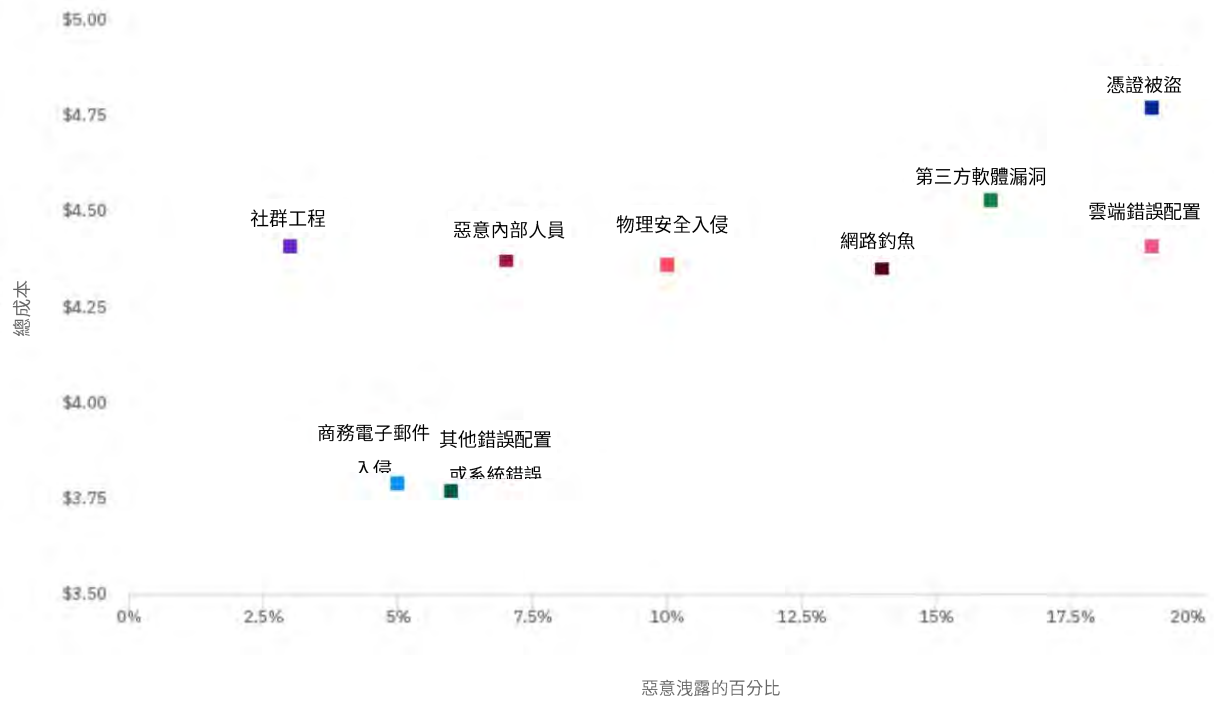


憑證被盜、雲端錯誤配置或第三方軟體漏洞，是引起大部分惡意洩露的三大原因。

被盜用/洩露的憑證和雲端配置錯誤是主要的初始威脅向量，分別占到惡意洩露的 19%。如圖 21 所示，第三方軟體漏洞也是主要的初始威脅向量，在惡意洩露中占 16%。

圖 22

惡意攻擊資料洩露的平均成本和頻率（按根本原因向量劃分）

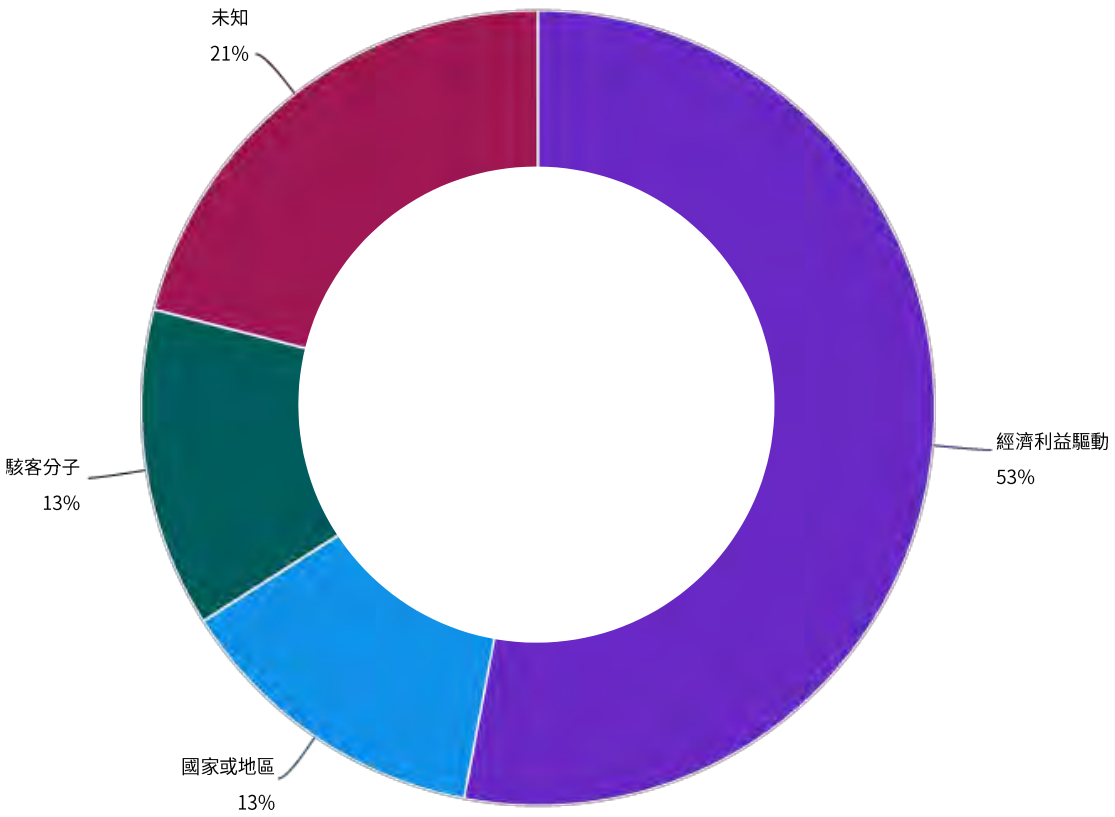


憑證被盜是成本最高也是最常見的威脅向量。

圖 22 利用散點圖顯示了惡意洩露中的九個初始威脅向量，X 軸上顯示了洩露的百分比，Y 軸上顯示了平均總成本。憑證被盜是圖中右上方最遠的威脅向量，這表示它的頻率和成本在惡意資料洩露中都占有很高的比例。

圖 23

按威脅向量類型歸納的惡意攻擊資料洩露



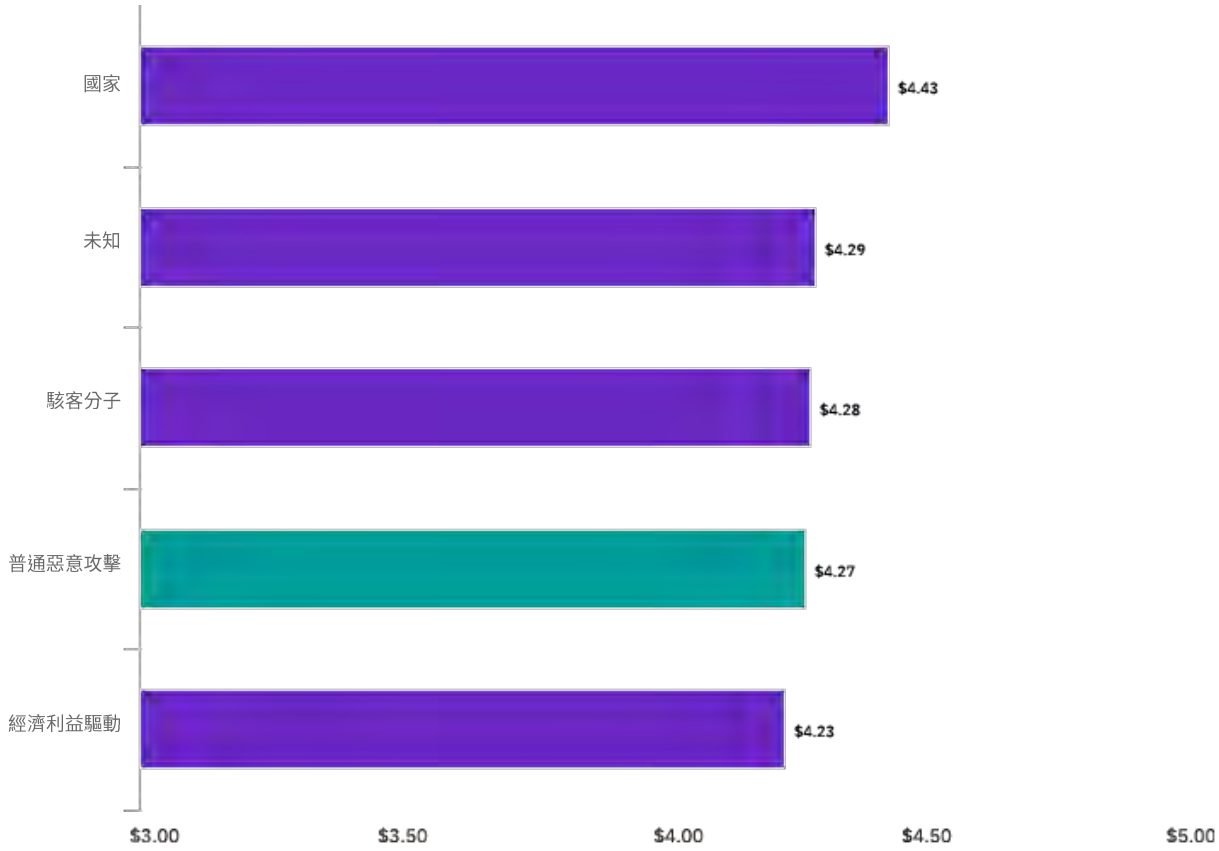
受經濟利益驅動的攻擊者是大多數惡意資料洩露的始作俑者。

如圖 23 所示，大多數惡意洩露 (53%) 都由經濟利益驅動的攻擊者發起。國家威脅主體參與了 13% 的惡意洩露，駭客占 13%， 還有 21% 的此類資料洩露由動機不明的攻擊者發起。

圖 24

惡意攻擊資料洩露的平均成本（按威脅主體類型劃分）

以百萬美元為單位



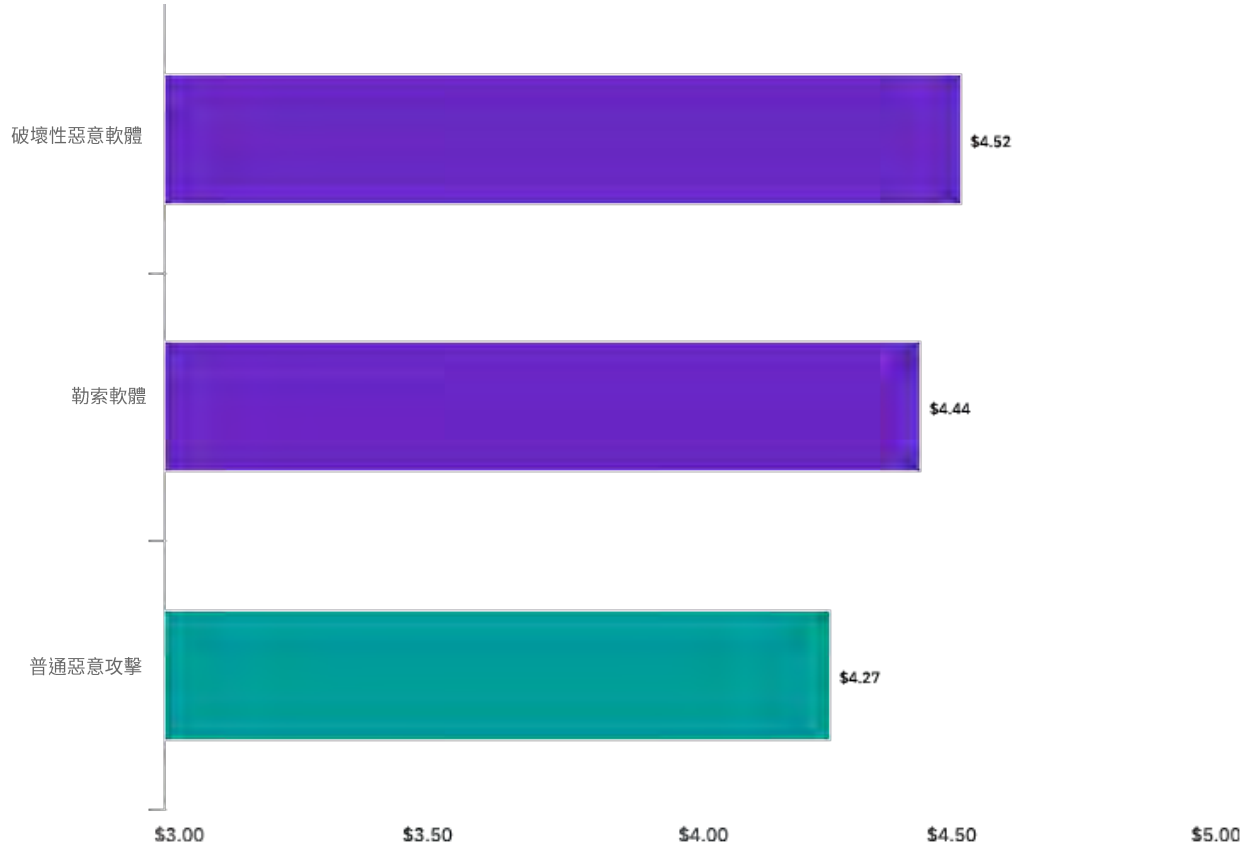
國家攻擊者發起的惡意洩露造成的成本最為高昂。

圖 24 按威脅主體類型顯示了資料洩露的成本。成本最高的惡意洩露由國家主體發起，平均成本為 443 萬美元。駭客發起的惡意洩露的平均成本為 428 萬美元，受經濟利益驅動的網路犯罪者發起的惡意洩露的平均成本為 423 萬美元。

圖 25

勒索軟體或破壞性惡意軟體漏洞的平均成本

以百萬美元為單位



勒索軟體和破壞性的惡意軟體漏洞比普通的惡意攻擊成本更高。

如圖 25 所示，以破壞性/Wiper 式攻擊破壞資料的惡意攻擊（平均成本為 452 萬美元）和勒索軟體攻擊（444 萬美元），其成本比普通的惡意洩露（427 萬美元）或普通的資料洩露（386 萬美元）成本更高。

影響資料洩露成本的因素

本部分更加深入地探討了影響資料洩露的多個因素，其中包括不同類型的安全技術和實務、IT 環境以及第三方介入。今年的研究分析了 25 個獨特的成本因素，它們可以緩解影響（降低洩露的平均總成本）或放大影響（增加洩露的平均總成本）。

今年的報告中新增了多個因素：紅隊測試、漏洞測試以及安全托管服務（緩解成本的因素）和安全技能短缺以及遠端工作（放大成本的因素）。

本部分還深度解析了三個可緩解資料洩露成本影響的領域：CISO 的角色、網路保險和事件回應團隊。

重要發現

$291,870

增加與複雜安全系統相關的資料洩露的平均總成本

51%

利用網路保險索賠支付諮詢和法律服務成本的組織的比例

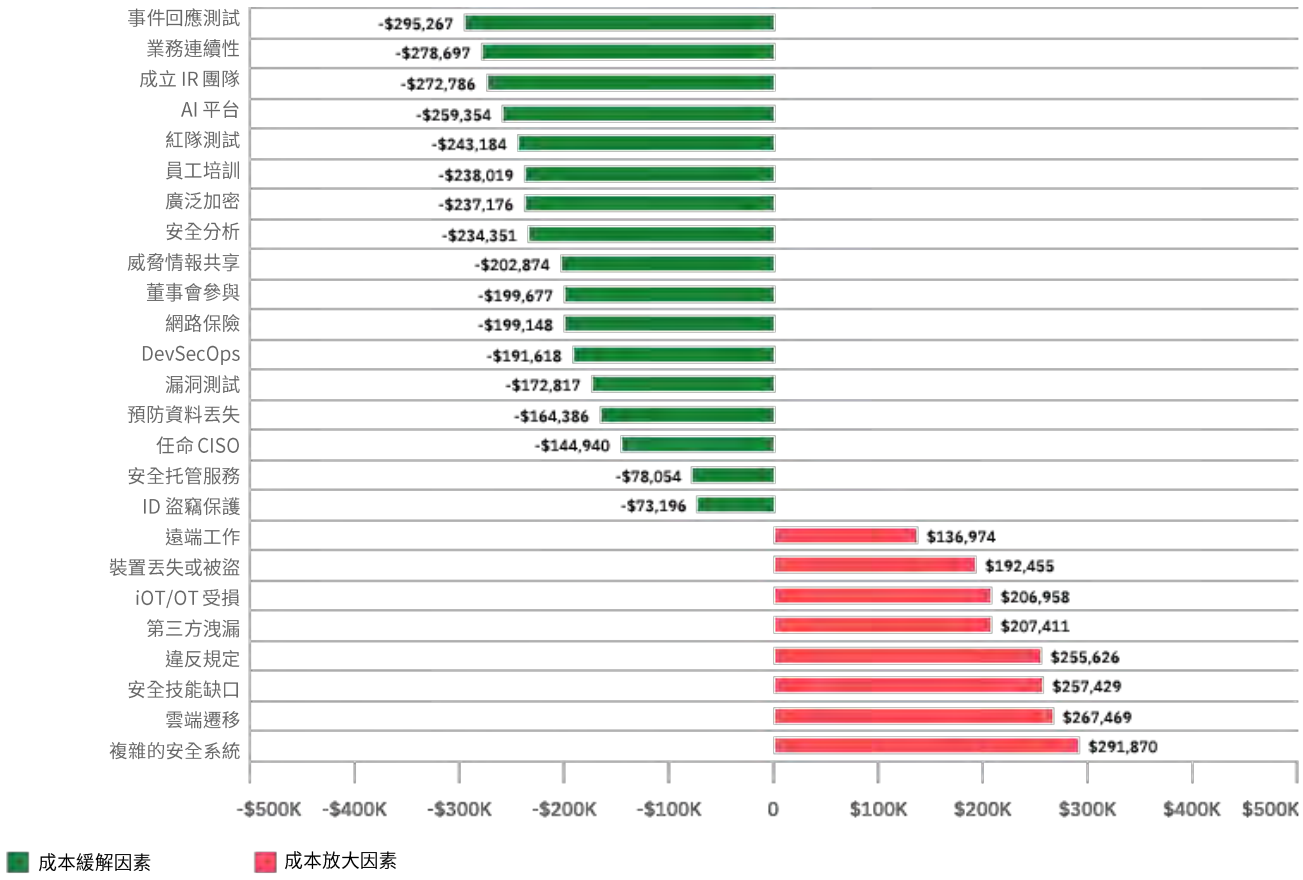
46%

表示 CISO 最應該對資料洩露負責的受訪者的比例

圖 26

25 個重要因素對資料洩露平均總成本的影響

美國 386 萬美元平均總成本的變化



安全系統複雜性和事件回應計畫測試，對資料洩露的總成本影響最大。

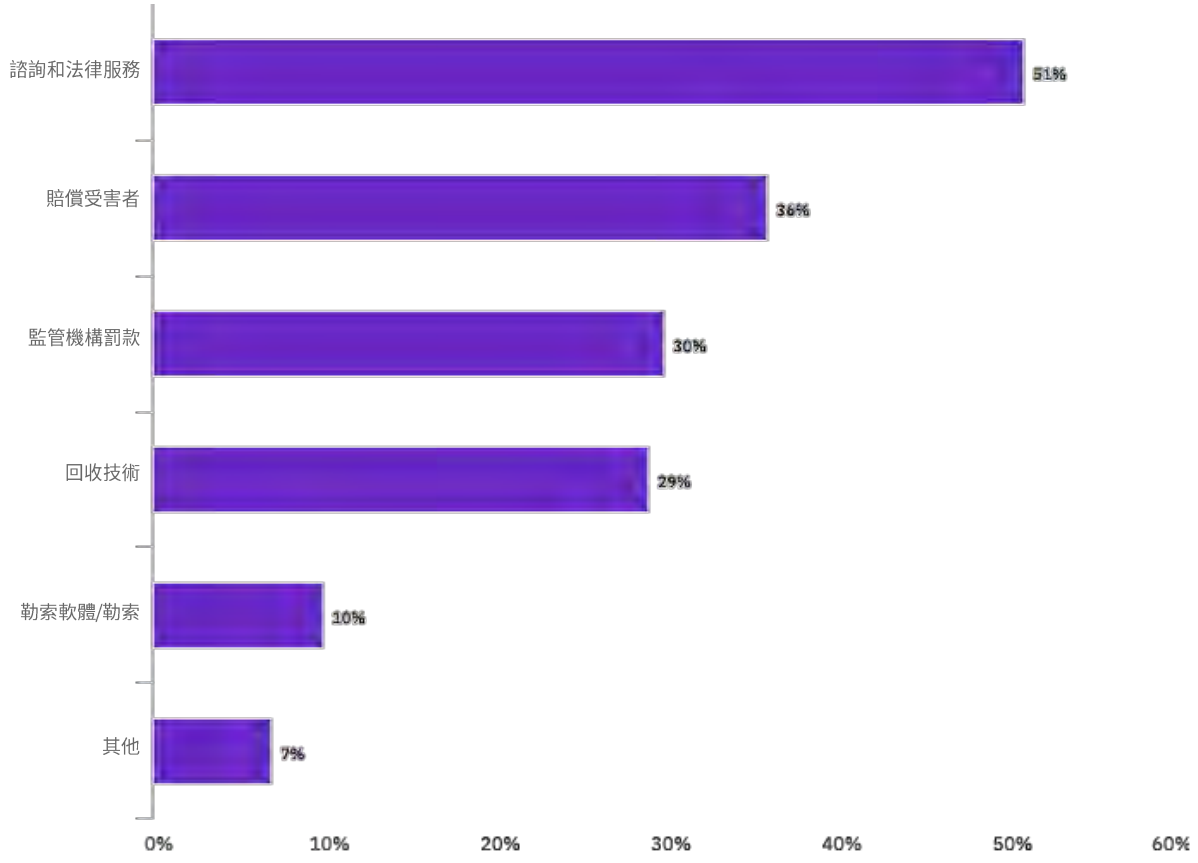
從圖 26 可以看出 386 萬美元的資料洩露平均總成本中 25 個因素的各自平均成本影響。各種可用技術和內部專業知識不足導致的安全系統複雜性，使資料洩露的平均總成本平均增加了 291,870 美元。向雲端遷移產生了更高的資料洩露平均成本，平均成本增加了 267,469 美元。

可降低資料洩露平均總成本的因素包括廣泛測試事件回應計畫和業務連續性管理，這兩項因素分別將平均成本降低了 295,267 美元和 278,697 美元。

圖 27

使用網路安全保險索賠支付的成本類型

回應的百分比，允許多個回應



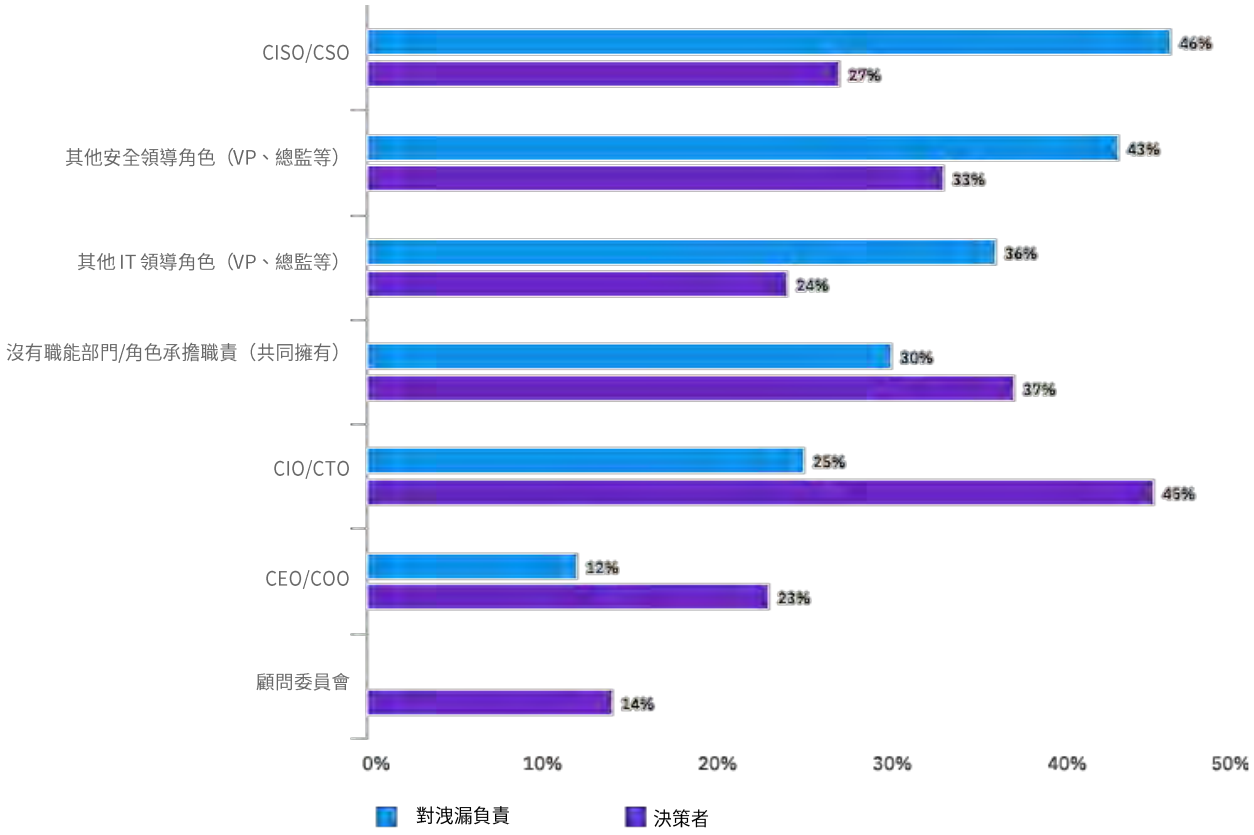
網路保險通常可涵蓋第三方服務和受害者賠償的費用。

從圖 27 可以看出，51% 的組織會利用網路保險索賠來支付第三方諮詢和法律服務的費用。36% 的組織利用網路保險向受害者支付賠償費用。只有 10% 的組織利用網路保險索賠支付勒索軟體或勒索的費用。

圖 28

誰對資料洩露、網路安全政策和技術決策負有最大責任？

回應的百分比，允許多個回應



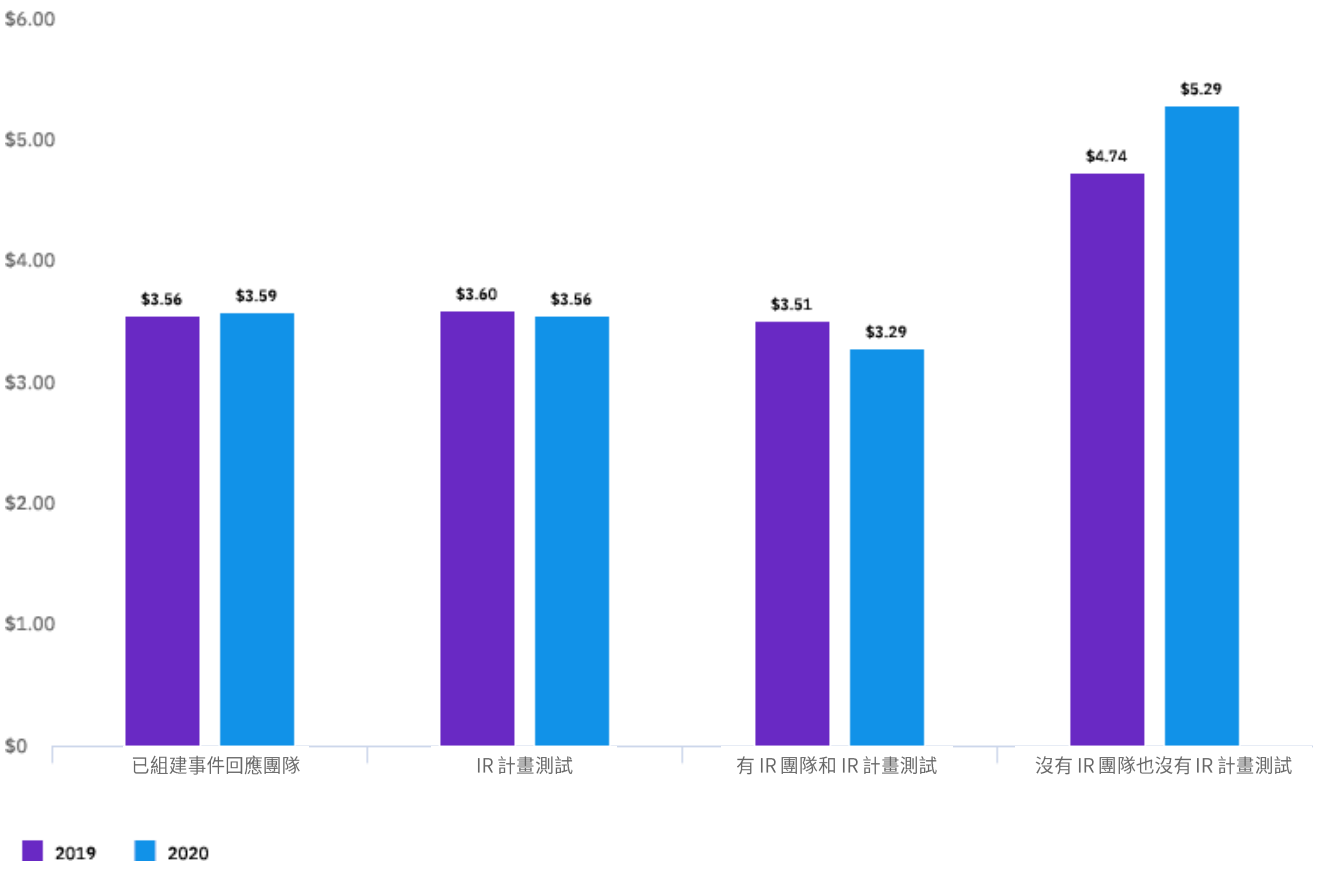
CISO 最有可能對資料洩露承擔最終責任。

如圖 28 所示，46% 的受訪者表示，CISO/CSO 應該對資料洩露負責，但只有 27% 的受訪者表示 CISO/CSO 最應該對網路安全政策和技術決策負責。CEO 和 COO 對資料洩露負責的可能性最小，而 CIO/CTO 通常被認為是網路安全政策和技術的最終決策者。

圖 29

有事件回應團隊和 IR 規劃測試的資料洩露平均總成本

以百萬美元為單位



事件回應團隊和事件回應計畫測試雙劍合璧，可顯著降低資料洩露的成本。

如圖 29 所示，組建了事件回應團隊並廣泛測試其事件回應計畫的組織，其資料洩露的平均成本為 329 萬美元。相比之下，未採取任一項措施的組織的平均總成本為 529 萬美元，二者相差 200 萬美元。

安全自動化趨勢和效力

這是我們第三年審視資料洩露成本與安全自動化之間的關係。在本報告中，安全自動化是指在發現和控制網路漏洞利用或漏洞時加大或替代人為干預的安全技術。此類技術依賴人工智慧、機器學習、分析和自動編排。

重要發現

21%

2020 年全面部署安全自動化的組織比 2018 年的 15% 有所上升

$3.58 百萬

沒有部署安全自動化的組織與全面部署自動化的組織在資料洩露平均總成本方面的差異

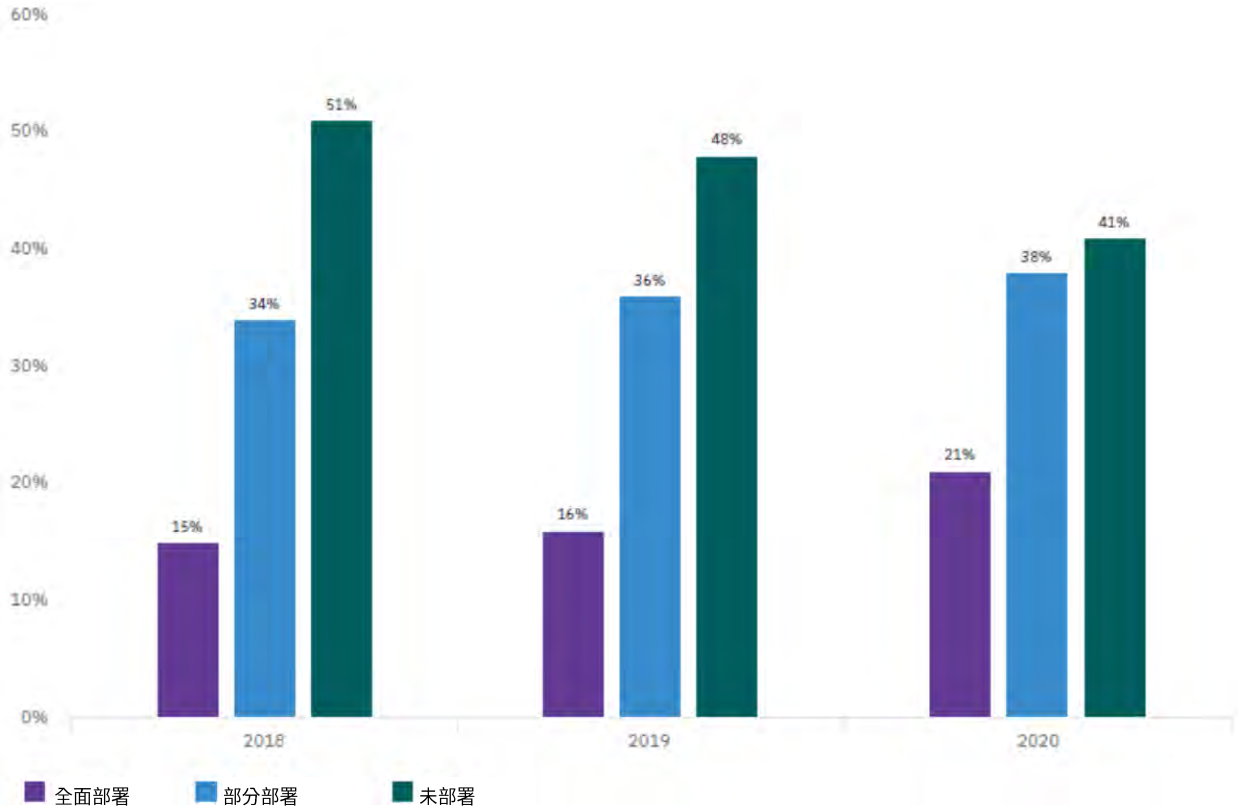
30%

德國全面部署安全自動化的組織的比例在所有國家中排名最高

圖 30

比較三個部署水準的安全自動化狀態

每種自動化水準的組織所占的百分比



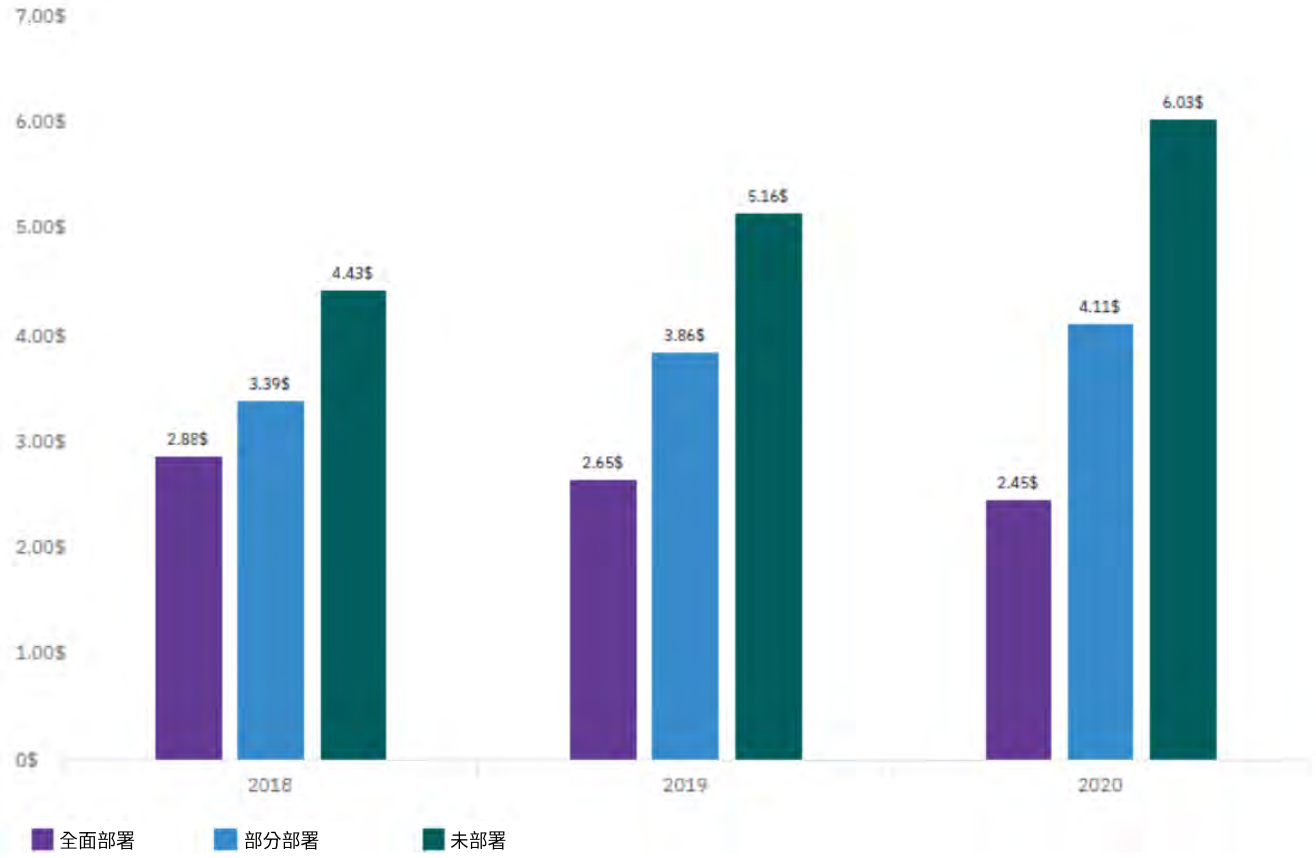
全面部署自動化的比例在過去三年間有所增加。

如圖 30 所示，在 2020 年的研究中，只有 21% 的公司全面部署了安全自動化，2018 年這一比例為 15%，2019 年為 16%。在 2020 年的研究中，還有 38% 的公司部分部署了自動化，41% 的公司尚未部署自動化。

圖 31

各安全自動化部署水準的資料洩露平均總成本

以百萬美元為單位



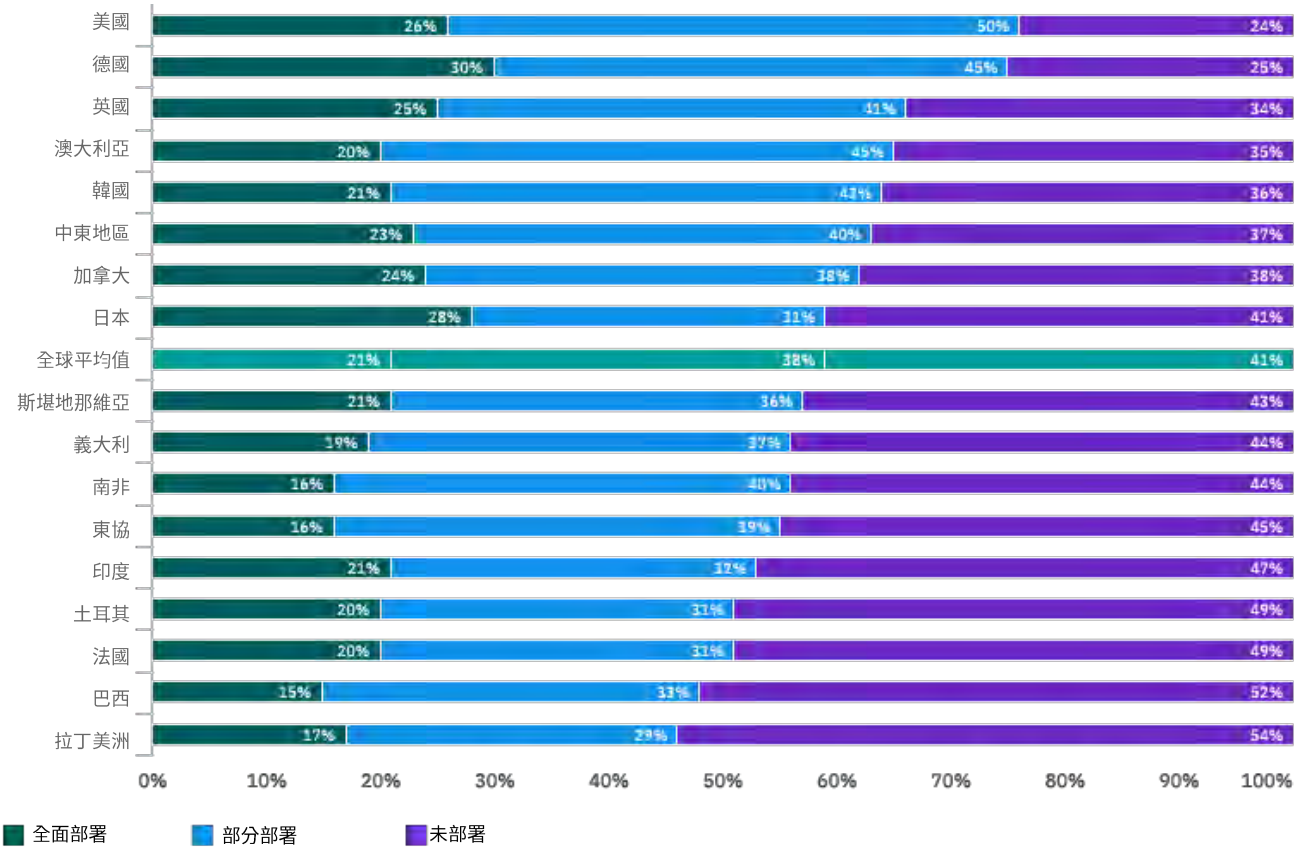
安全自動化對資料洩露成本的影響在過去三年間有所增加。

如圖 31 所示，在 2020 年的研究中，全面部署了安全自動化的組織的資料洩露平均總成本為 245 萬美元，比尚未部署安全自動化的組織的平均成本少 358 萬美元。在 2018 年的研究中，全面部署了自動化的組織與未部署自動化的組織，二者的資料洩露平均成本差距為 155 萬美元，2019 年這一差距為 251 萬美元。

圖 32

各國家/地區的安全自動化部署平均水準

三種自動化水準的組織所占的百分比



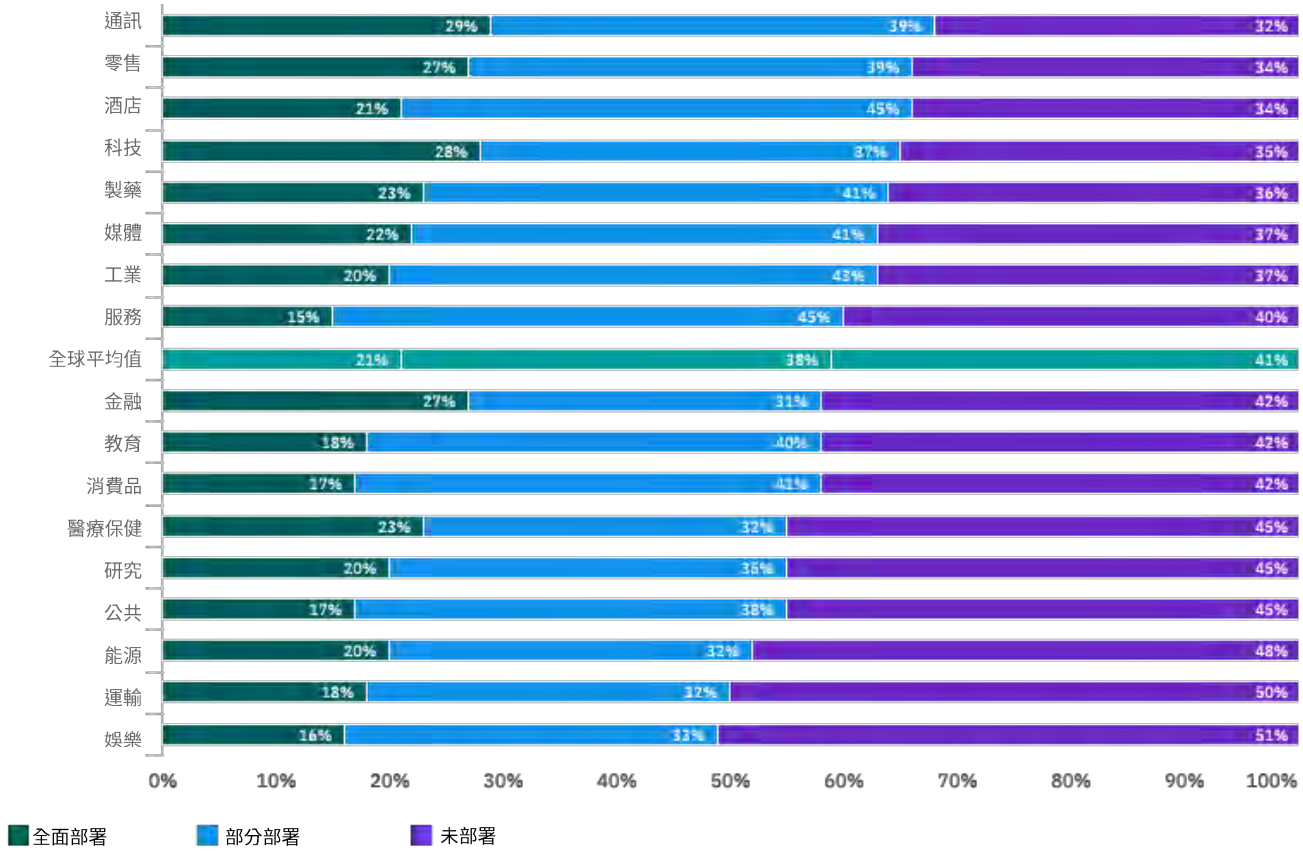
安全自動化的狀態因國家和地區而異。

從圖 32 可以看出，美國和德國全面部署或部分部署自動化的組織比例更高（美國為 76%，德國為 75%）。美國全面部署安全自動化的比例為 26%，德國為 30%。在未部署自動化的國家中，拉丁美洲和巴西所占的比例最高，分別為 54% 和 52%。

圖 33

各產業的安全自動化部署平均水準

三種自動化水準的組織所占的百分比



部署的安全自動化水準因產業而異。

從圖 33 可以看出，通訊、科技和零售產業的組織全面或部分部署自動化的比例最高。金融產業的組織全面部署安全自動化的比例 (27%) 高於組織的平均比例。但是在金融產業裡，部分部署自動化的組織所占比例相對較低 (31%)，這意味著金融產業裡全面和部分部署自動化的綜合比例低於全球平均水準（58%，全球平均水準為 59%）。娛樂和運輸產業沒有部署自動化的組織比例最高。

發現並控制資料洩露的時間

前幾年的研究結果發現，發現和控制資料洩露的速度越快，成本就越低。發現的平均時間是偵測到已發生事件所需的時間。控制時間是指組織在偵測到事件並最終恢復服務所需的時間。

從初次偵測出洩露到控制洩露之間經歷的時間，我們稱之為資料洩露生命週期。這些指標可用於判斷組織事件回應和控制流程的效力。本次研究首次考察了安全自動化對資料洩露生命週期方向的影響。

重要發現

280 天

發現並控制資料洩露的平均時間

315 天

發現和控制惡意攻擊引起的資料洩露的平均時間

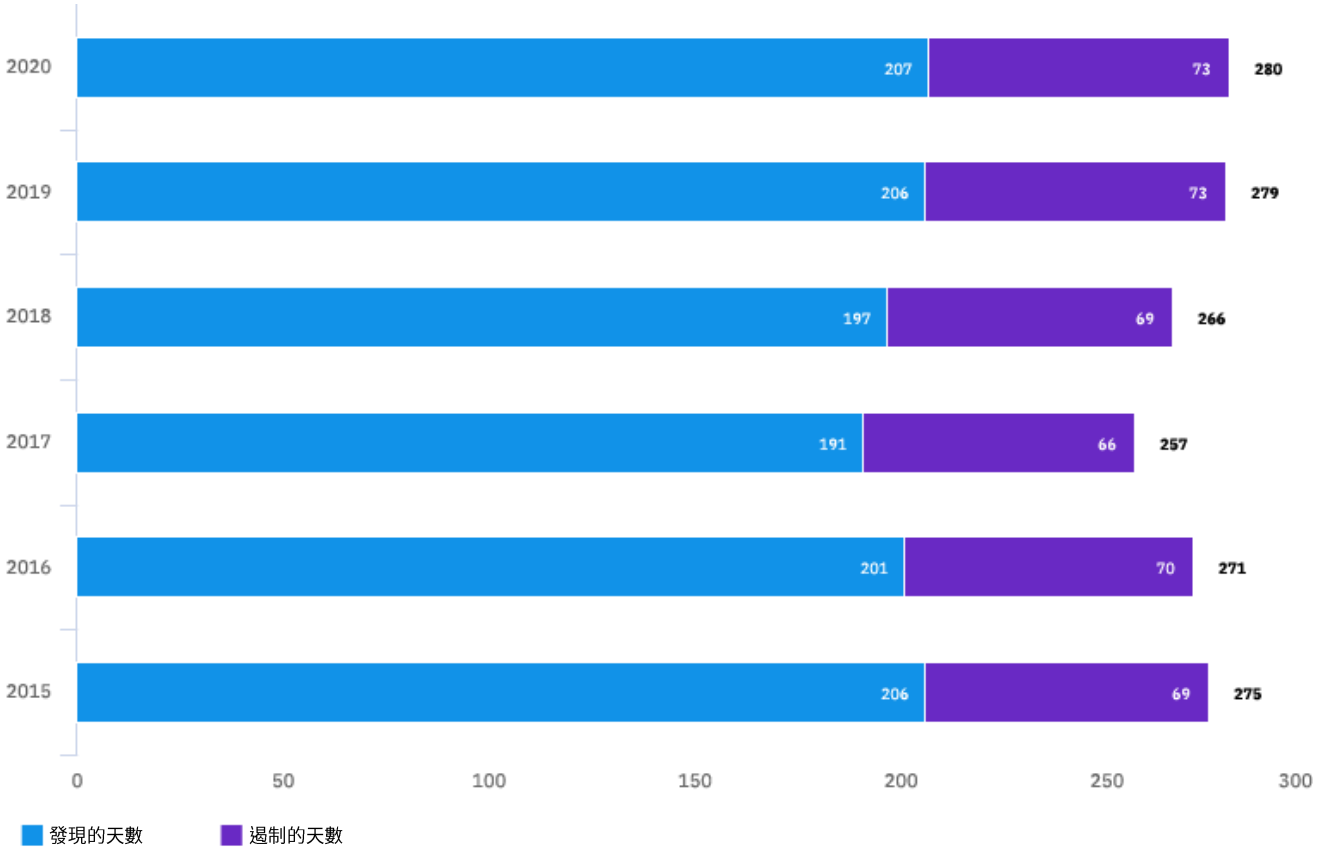
$1.12 百萬

與 200 天以上相比，在 200 天以內控制資料洩露所節省的平均成本

圖 34

發現並控制資料洩露的平均時間

以天為單位



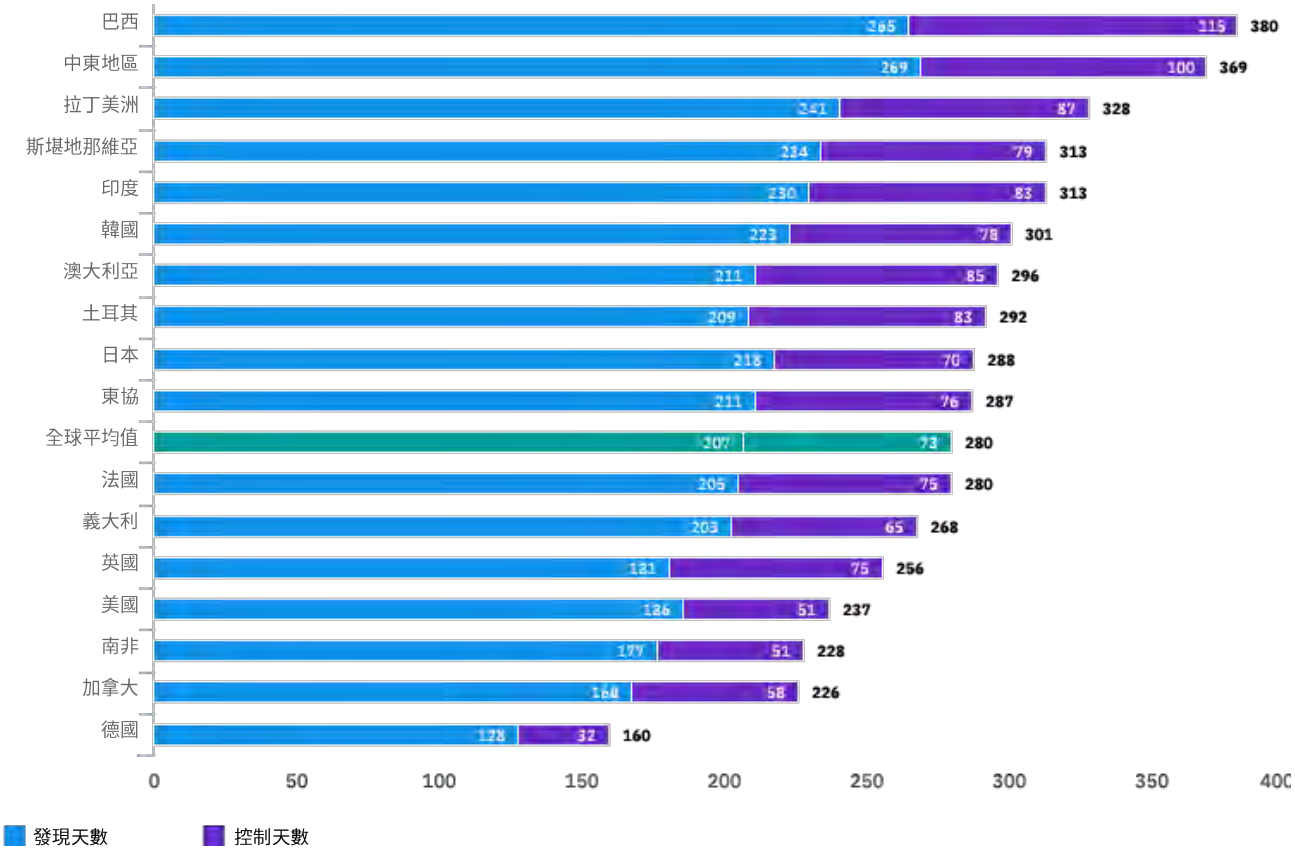
發現和控制洩露的平均時間一直較為平穩。

如圖 34 所示，在過去的幾份報告中，發現和控制資料洩露的時間變化不大。在 2020 年的研究中，發現洩露的平均時間為 207 天，控制洩露的平均時間為 73 天，共計 280 天。2019 年，資料洩露生命週期為 279 天。

圖 35

發現和控制資料洩露的平均時間（按國家或地區劃分）

以天為單位



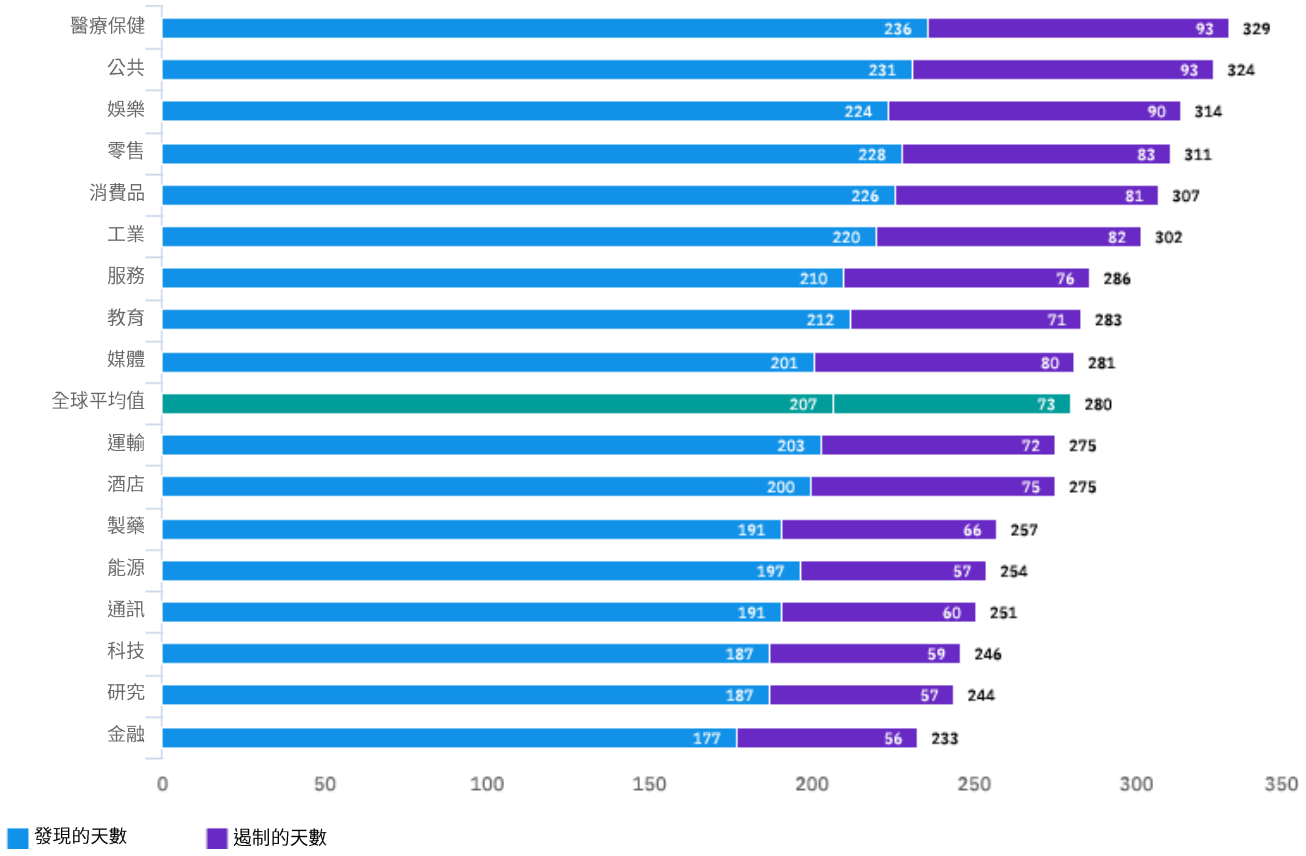
各國家/地區在平均洩露生命週期方面存在顯著差距。

如圖 35 所示，巴西和中東發現和控制資料洩露所需的平均時間遠遠高於平均值，分別為 380 天和 369 天。南非、加拿大和德國的資料洩露生命週期較短，德國的組織平均只需 160 天即可控制洩露。

圖 36

各產業發現並控制資料洩露的平均時間

以天為單位



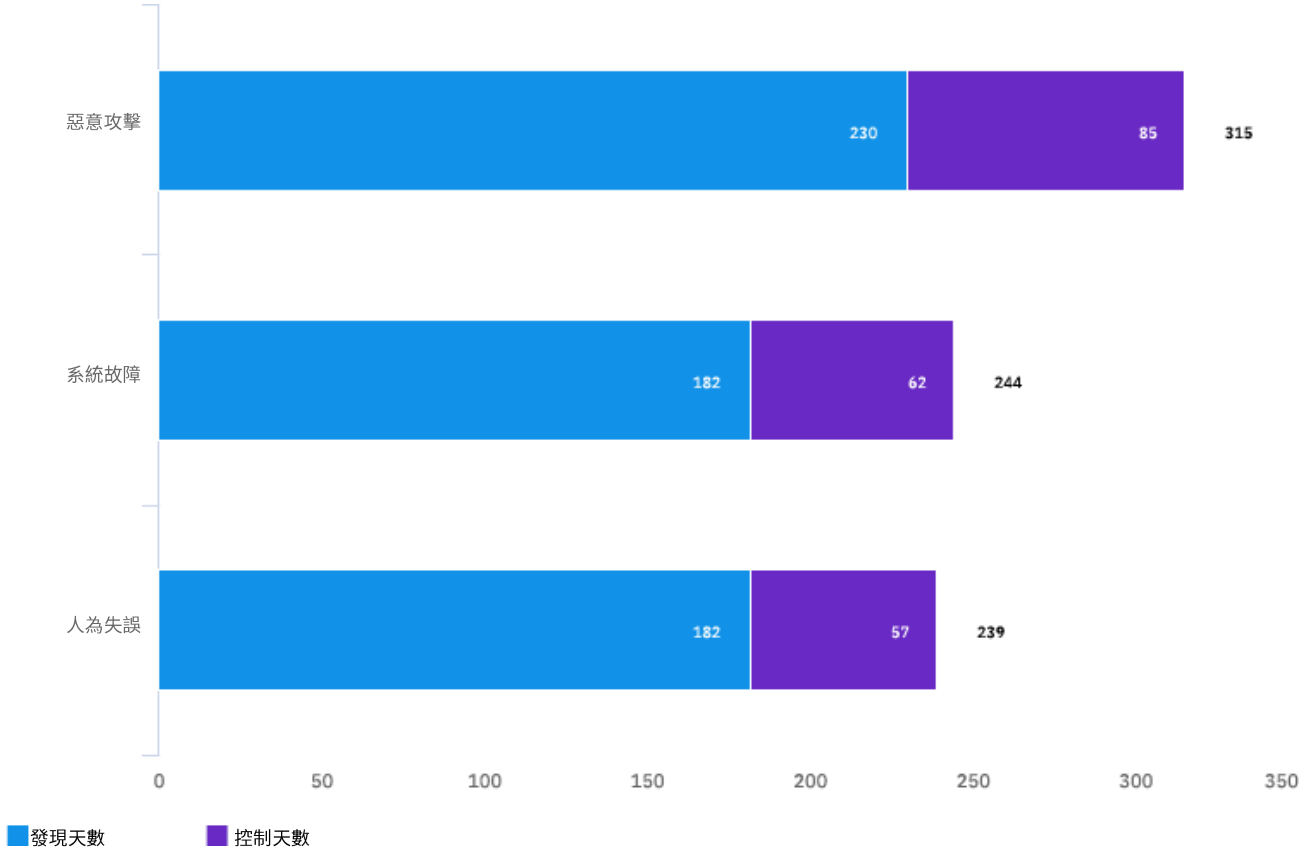
金融產業與醫療保健產業在控制洩露方面的時間相距甚遠。

如圖 36 所示，醫療保健產業發現和控制洩露的平均時間最長，達 329 天。金融產業發現和控制洩露的平均時間最短，為 233 天。九個產業高於 280 天的全球平均洩露生命週期，另八個產業低於此水準。

圖 37

發現並控制資料洩露的平均時間（按根本原因劃分）

以天為單位



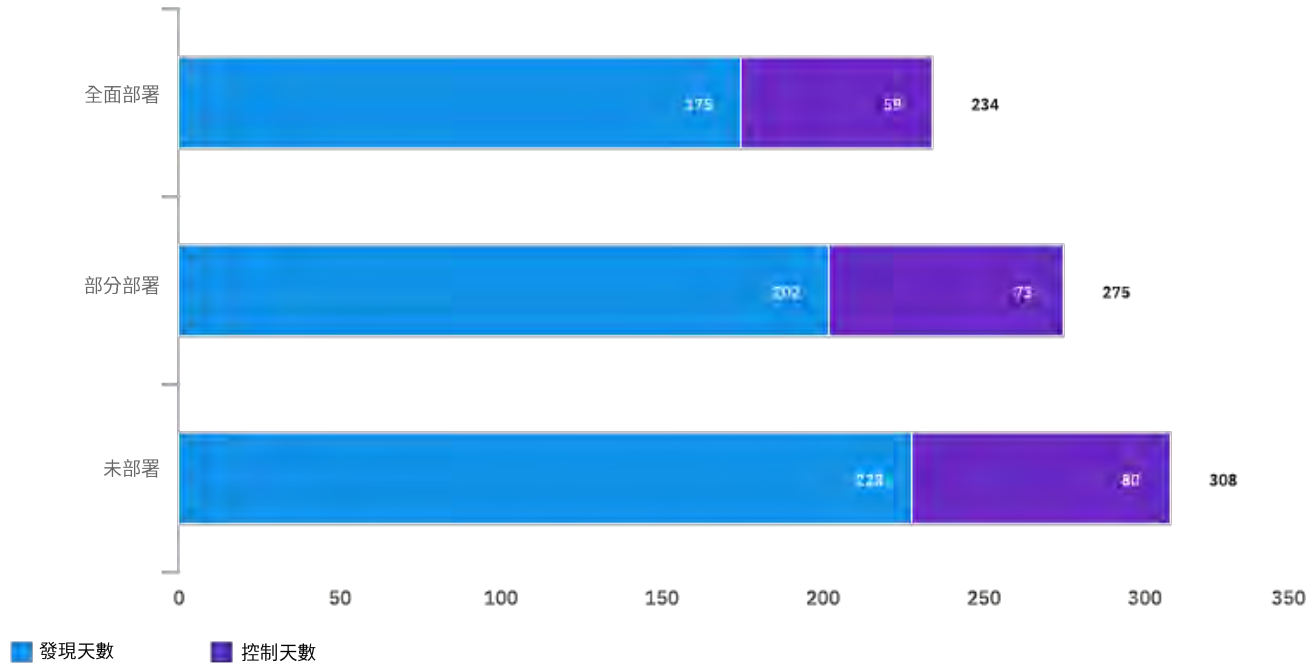
惡意攻擊導致的資料洩露所需的發現和控制時間最長。

如圖 37 所示，在 2020 年的研究中，與其他根本原因導致的洩露相比，發現和控制惡意洩露的平均時間為 315 天。發現和控制系統故障引發的洩露平均需要 244 天，發現和控制人為失誤引發的洩露平均需要 239 天。與普通的資料洩露相比，發現惡意洩露的時間要長 23 天。發現惡意洩露的平均時間為 230 天，而總體平均需要 207 天。

圖 38

發現並控制資料洩露的平均時間（按安全自動化水準劃分）

以天為單位



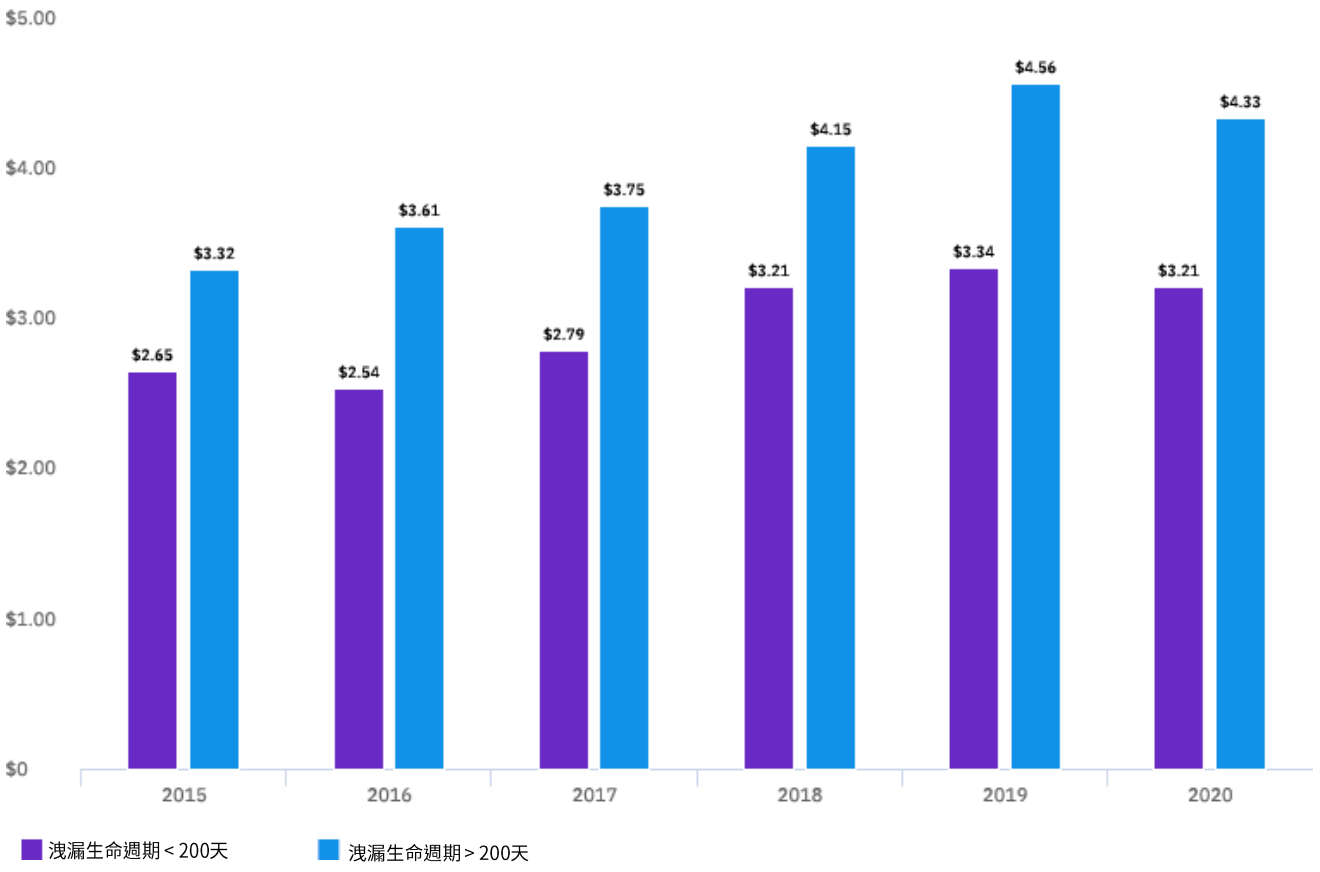
安全自動化縮短了發現和控制資料洩露的時間。

本次研究首次考察了自動化對資料洩露生命週期的影響。從圖 38 可以看出，全面部署自動化之後，發現洩露的平均時間為 175 天，控制洩露的平均時間為 59 天。若未部署自動化，發現洩露的平均時間會大幅增加至 228 天，控制洩露的時間會增加至 80 天，總計 308 天。

圖 39

基於資料洩露平均生命週期的資料洩露平均總成本

以百萬美元為單位



資料洩露生命週期影響了洩露的平均成本。

過去六年的研究得出了一致的結果，即生命週期（發現洩露的時間與控制洩露的時間之和）在 200 天以上的資料洩露成本遠遠高於生命週期不到 200 天的資料洩露。如**圖 39** 所示，在 2020 年的研究中，生命週期超過 200 天的洩露的平均成本比不到 200 天的洩露平均要高出 112 萬美元（200 天以上為 433 萬美元，不到 200 天為 321 萬美元）。

資料洩露的長尾成本

資料洩露的成本影響在事件發生之後持續多年。在去年的研究中，我們首次考察了資料洩露在兩年或兩年多之後對組織的影響。研究結果顯示，洩露發生後的第一年成本最高，但在兩年多之後又會捲土重來。

我們還考察了受到高度監管的產業的組織與資料保護法規較為寬鬆的產業在「長尾成本」方面的差異。我們定義的接受高度監管的產業包括：能源、醫療保健、消費品、金融、科技、製藥、通訊、公共部門和教育。零售、工業、娛樂、媒體、研究服務和餐旅產業的組織所在的監管環境較為寬鬆。在對監管嚴厲和監管寬鬆的產業所作的分析中，我們得出了以下結論：監管和法律成本可能是導致洩露發生多年之後成本上升的原因。

在 2020 年的研究中，我們以 101 家公司為樣本，這些公司承擔了兩年或兩年以上的資料洩露成本。

重要發現

61%

第一年發生的資料洩露成本的平均比例

44%

受到嚴厲監管的產業第一年發生的資料洩露成本的平均比例

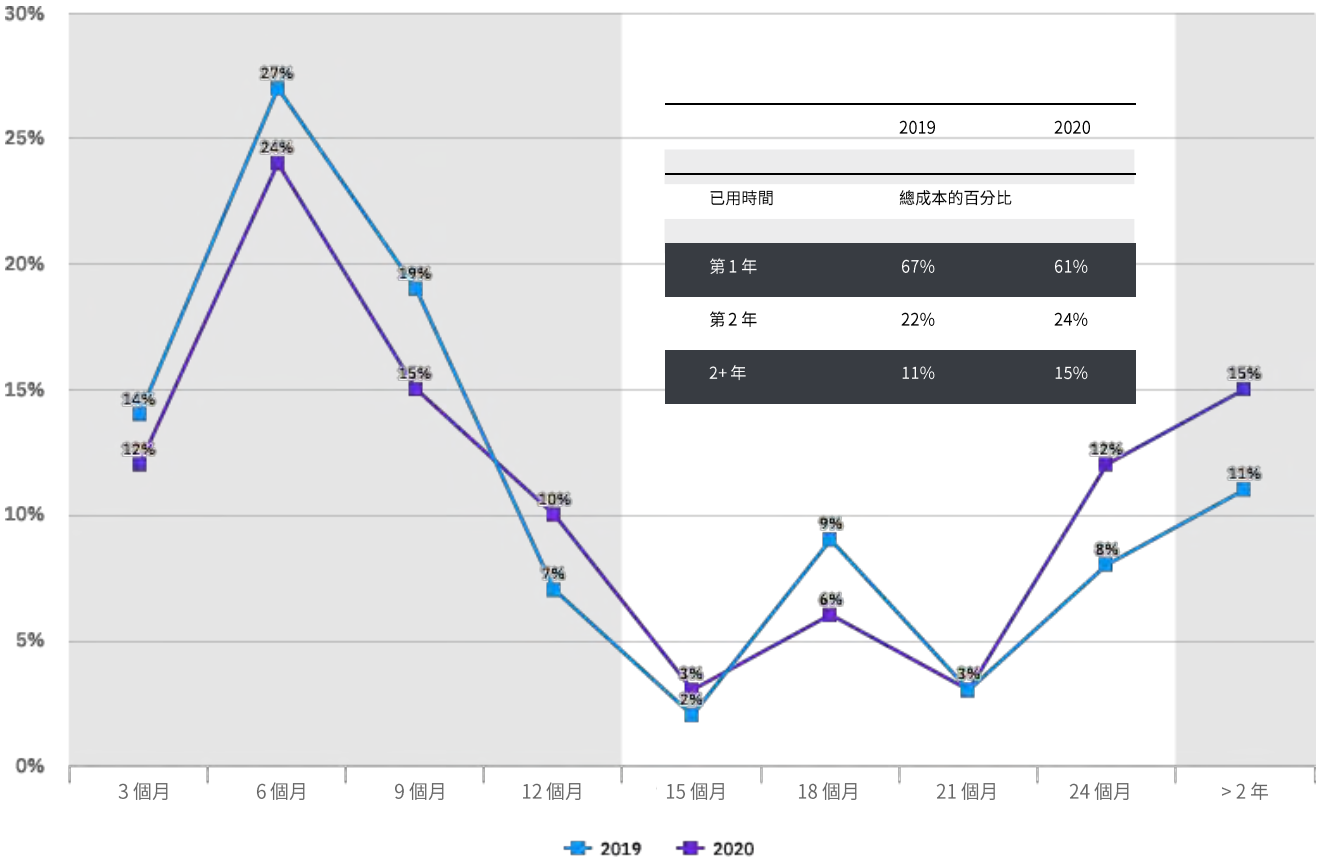
92%

監管寬鬆的產業前兩年發生的資料洩露成本的平均比例

圖 40

兩年多之後資料洩露平均成本的分佈情況

以三個月為間隔發生的成本百分比



已用時間	總成本的百分比 2019	2020
第 1 年	67%	61%
第 2 年	22%	24%
2+ 年	11%	15%

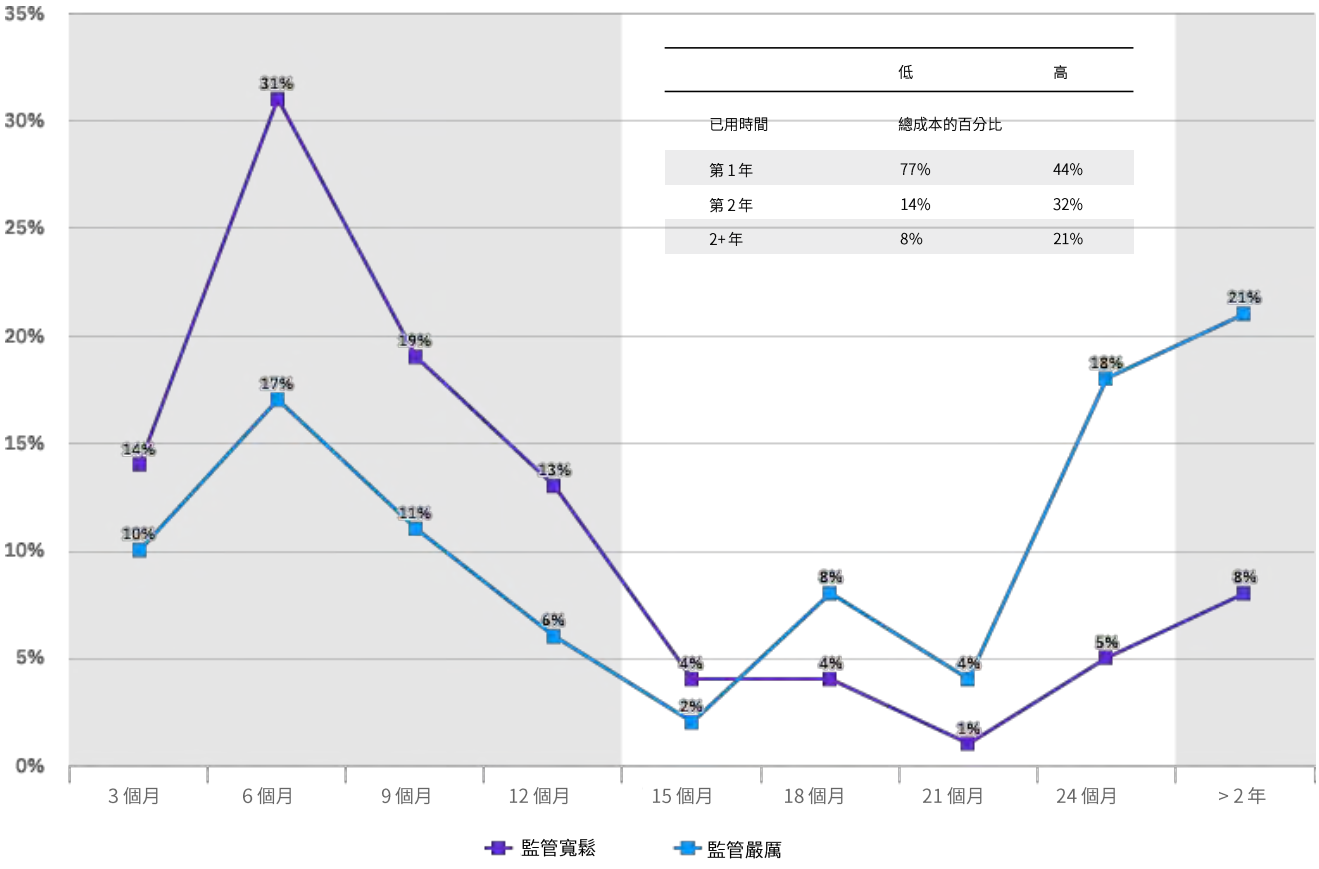
在 2020 年的研究中，兩年後發生的洩露成本的比例有所增加。

如圖 40 所示，長尾成本分析發現，資料洩露的成本平均有 61% 發生在第一年，24% 發生在第二年，還有 15% 發生在兩年後。與 2019 年分析中的 11% 相比，洩露發生兩年多之後的成本略有增加。

圖 41

寬鬆和嚴厲監管環境下資料洩露平均成本的分佈情況

以三個月為間隔發生的總成本百分比



	低	高
已用時間	總成本的百分比	
第 1 年	77%	44%
第 2 年	14%	32%
2+ 年	8%	21%

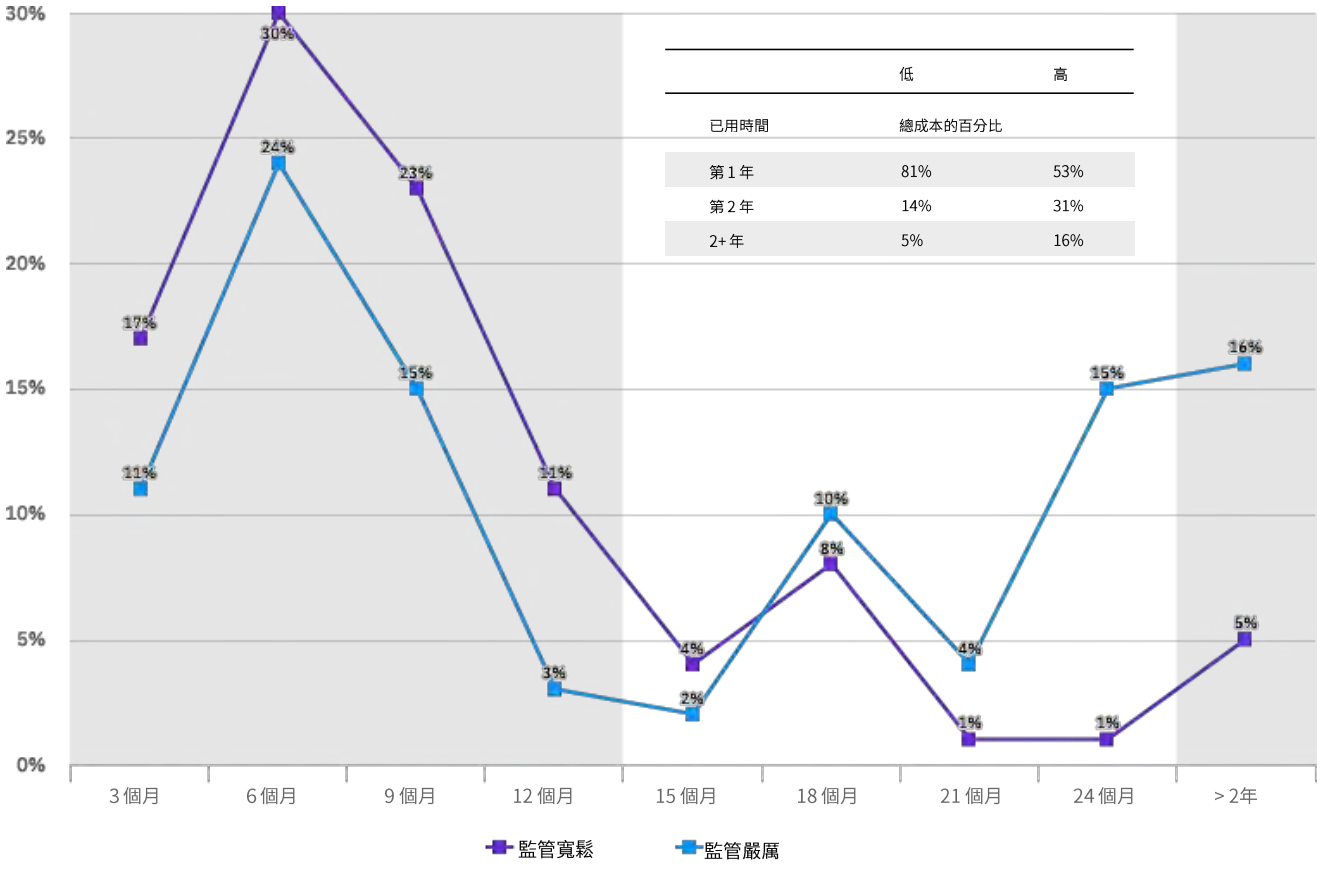
受到高度監管的產業，在洩露發生一年之後承擔了大部分成本。

如圖 41 所示，較為寬鬆的監管環境下的組織更有可能在第一年承擔資料洩露的全部成本。在監管較為寬鬆的產業中，平均有 77% 的成本發生在第一年，而在監管較為嚴厲的組織內，平均有 44% 的洩露成本發生在第一年。

圖 42

寬鬆和嚴厲監管環境下資料洩露平均成本的分佈情況（2019 年報告）

以三個月為間隔發生的總成本百分比



從 2019 年對嚴厲監管環境和寬鬆監管環境的分析看出，洩露發生兩年多之後產生的成本比例有所下滑。

圖 42 顯示了 2019 年研究中，寬鬆的資料保護監管環境與嚴厲的資料保護監管環境下的長尾洩露成本。在 2019 年的研究中，受到高度監管的產業平均有 16% 的成本發生在兩年之後。而在 2020 年的研究中，受到高度監管的產業平均有 21% 的成本發生在兩年之後（參閱圖 41）。

新冠肺炎帶來的潛在影響

新冠肺炎疫情極大改變了組織的經營方式，大量員工在家辦公，增加了對視訊會議、雲端應用和網路資源的需求。為瞭解這一新的態勢，我們在研究中增加了幾個問題，以收集研究參與者對新冠疫情對資料洩露成本潛在影響的看法。

重要發現

54%

因應新冠疫情需要遠端工作的組織的百分比

76%

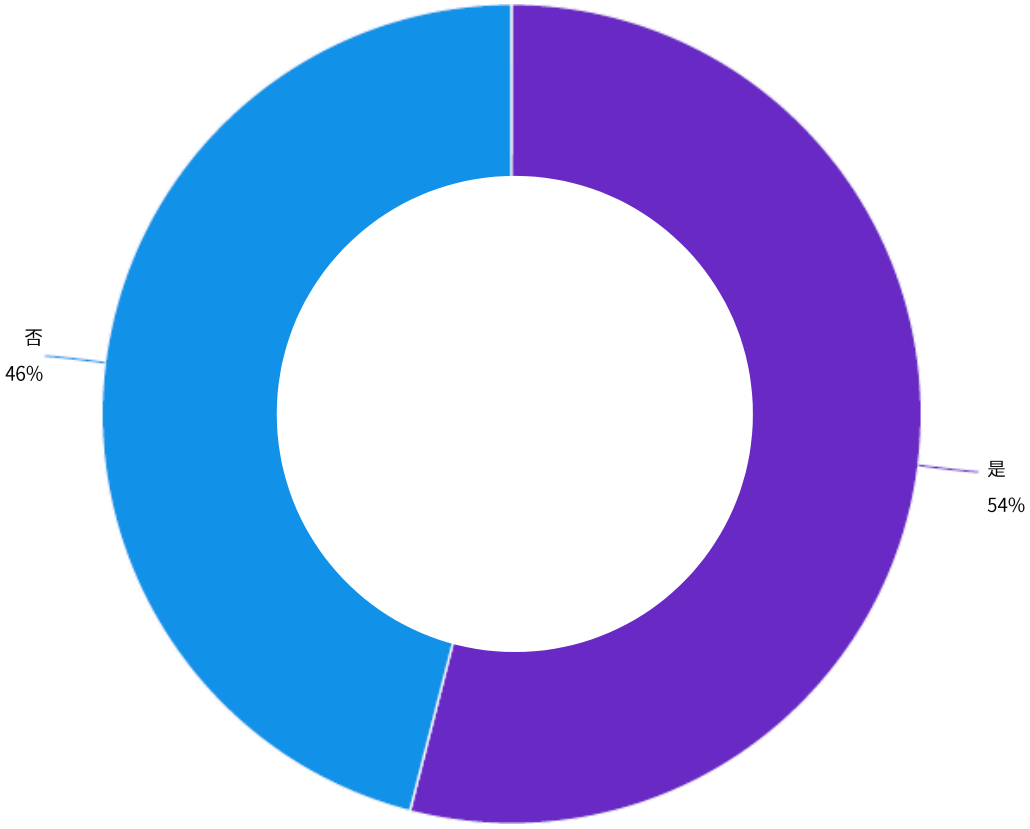
認為遠端工作會增加發現和控制資料洩露時間的參與者比例

70%

認為遠端工作會增加資料洩露成本的參與者比例

圖 43

您的組織是否因為新冠疫情而要求員工遠端工作？



新冠疫情之下，大多數組織都需要遠端工作。

如圖 **43** 所示，為因應新冠疫情，研究中的大多數組織 (54%) 都需要遠端工作。

圖 44

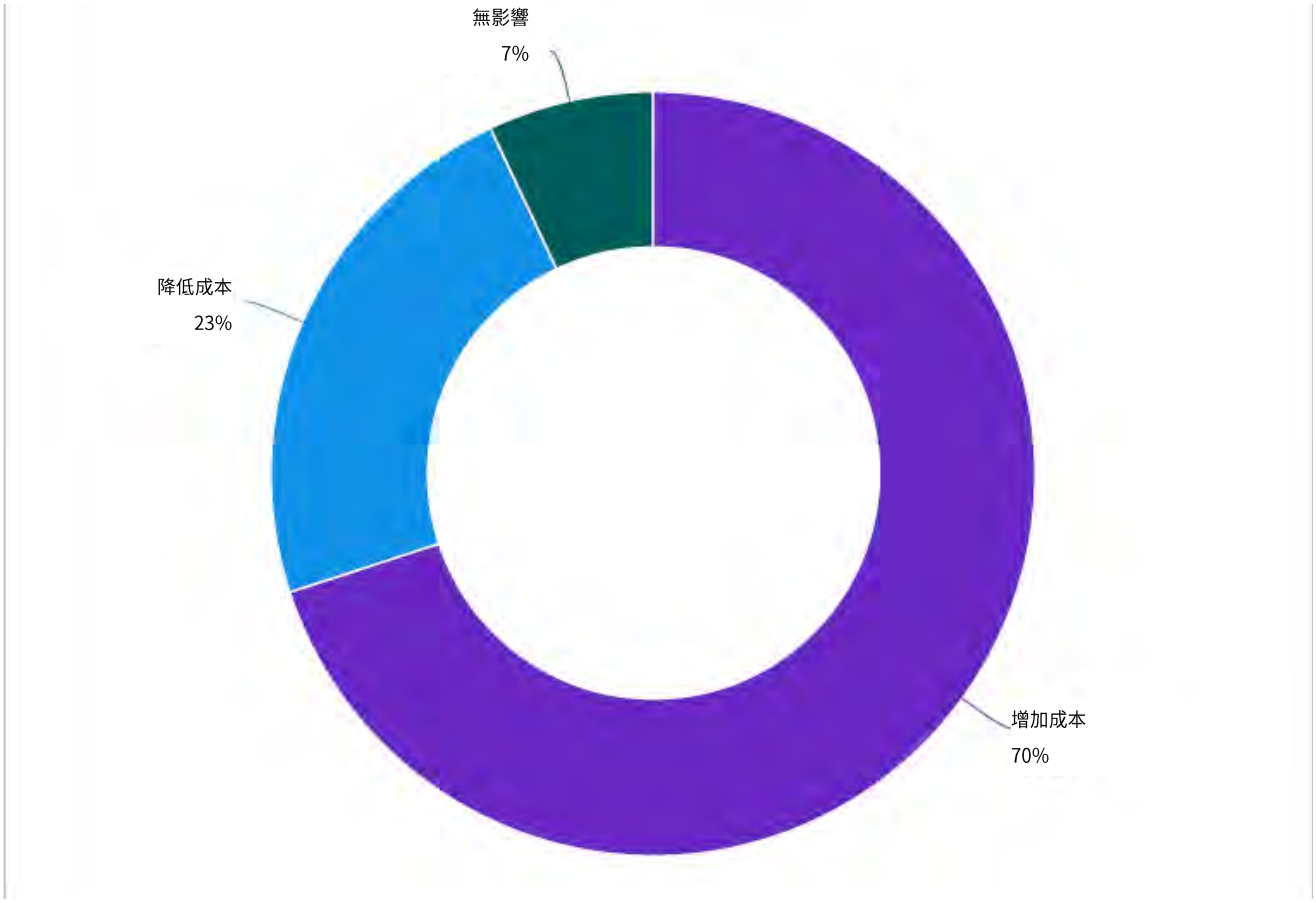
遠端工作對您回應資料洩露的能力有何影響？

四分之三的受訪者預計可能需要更長的時間才能發現和控制資料洩露。

從**圖 44** 可以看出，在表示組織因為新冠疫情需要開展遠端工作的受訪者中，有超過四分之三 (76%) 的受訪者認為此舉會增加發現和控制資料洩露的時間，20% 的受訪者認為會縮短發現和控制洩露的時間，還有 4% 表示不會有任何影響。

圖 45

遠端工作如何影響資料洩露的成本？



遠端工作會增加潛在資料洩露的成本。

如圖 **45** 所示，在表示組織因為新冠疫情需要開展遠端工作的受訪者中，70% 的受訪者認為此舉會增加潛在資料洩露的成本。還有 23% 的受訪者表示會降低資料洩露的成本，另外 7% 的受訪者則表示不會有任何影響。

大規模洩露的成本

今年是我們第三年評估破壞記錄達 100 多萬條的資料洩露的成本，也就是我們所說的大規模資料洩露。這種大規模洩露在大多數企業都並不常見，但一旦發生大規模洩露，就會對消費者和產業產生巨大的影響。自我們在 2018 年的研究中對它進行分析以來，大規模洩露的平均成本一直在增加。

今年的調查分析了 17 家公司，這些公司都遭遇了 100 萬條甚至更多記錄遺失或被盜的資料洩露。為全面闡釋我們的方法，請參閱此報告末尾處的資料洩露成本常見問題。

重要發現

$392 百萬

超過 5,000 萬條記錄的洩露的平均成本

100 倍

涉及 5,000 萬條以上的記錄與普通資料洩露在平均成本方面的差異

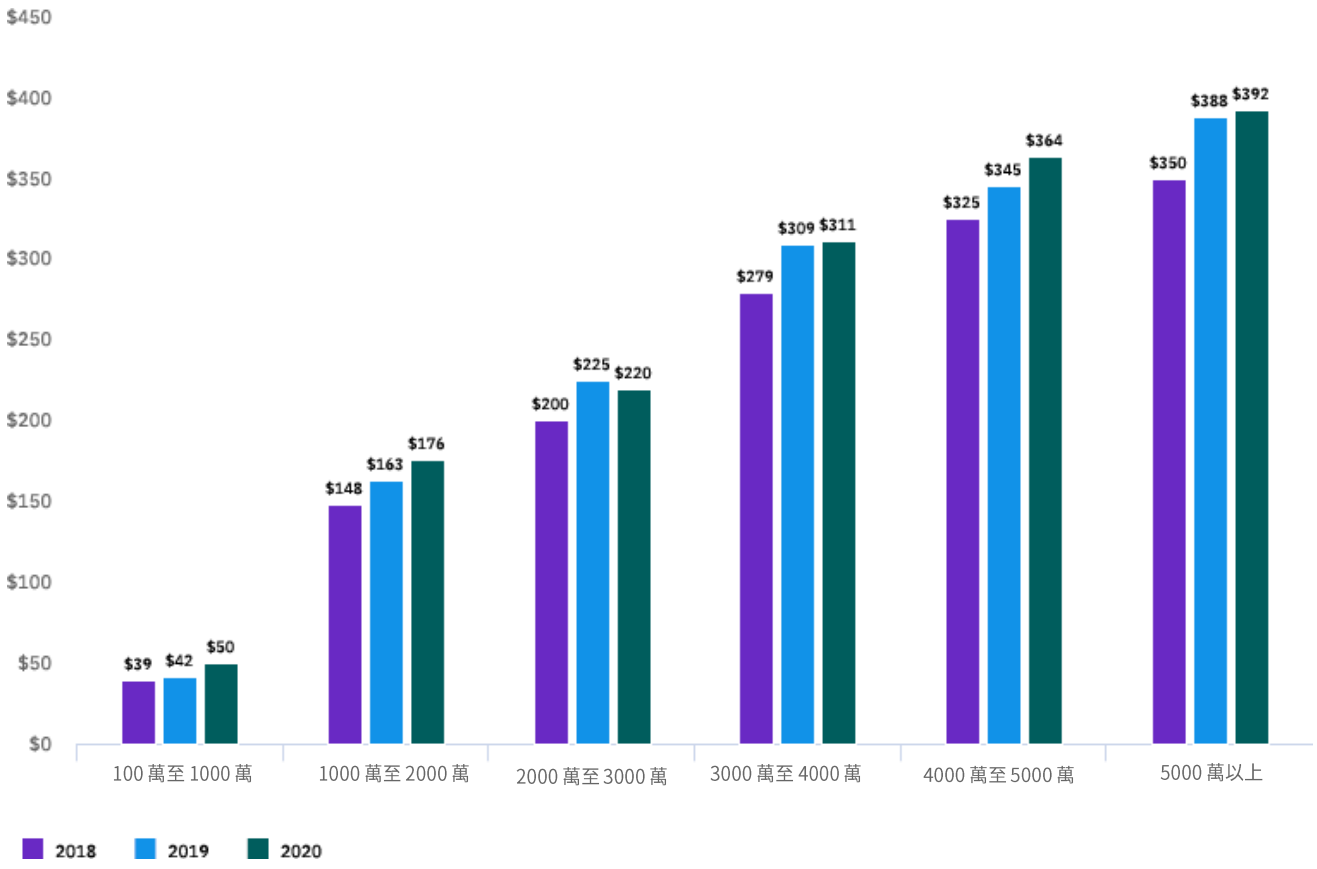
$19 百萬

在 2019 年至 2020 年的研究中，涉及 4,000 萬至 5,000 萬條記錄的洩露的平均成本有所增加

圖 46

大型洩露的平均總成本（按遺失的記錄數量計算）

以百萬美元為單位



大規模洩露的成本屢創新高。

如圖 46 所示，涉及 100 萬條至 1,000 萬條記錄的洩露的平均成本為 5,000 萬美元，是記錄少於 10 萬條的洩露平均成本（386 萬美元）的 25 倍以上。規模在 100 萬至 1,000 萬條記錄的洩露增長速度最快，已從 2018 年的 3,900 萬美元 (22%) 增長至 2020 年的 5,000 萬美元。

記錄超過 5,000 萬條的洩露的平均成本為 3.92 億美元，是資料洩露平均成本的 100 多倍。絕對成本增幅最大的是超過 5,000 萬條記錄的洩露，已從 2018 年的平均 3.5 億美元增加到 2020 年的 3.92 億美元。

可最大程度降低資料洩露帶來的財務損失和品牌影響的措施

*在本部分中，IBM Security 概述了參與研究的組織為降低資料洩露帶來的財務成本和名譽損失，所採取的措施。**

投資安全編排、自動化和回應 (SOAR) 以縮短發現和回應時間。

在資料洩露成本研究中，安全自動化可顯著降低發現和回應洩露的平均時間以及平均成本。SOAR 軟體和服務可協助您的組織利用自動化、流程標準化以及與現有安全工具的整合加速事件回應。人工智慧、分析和自動編排等自動化技術都可降低資料洩露平均成本。

採用零信任安全模型，以防止在未經授權的情況下存取敏感資料。

研究結果顯示，遺失、憑證被盜以及雲端錯誤配置是資料洩露最常見的三大根本原因。隨著組織逐漸向遠端工作和更少連接的混合多雲環境轉變，零信任策略讓員工在適當的情境下對相關資訊進行有限存取，進而保護資料和資源。

對回應計畫開展壓力測試以增強網路彈性。

與那些既未組建 IT 團隊又未測試任何 IR 計畫的組織相比，研究中既有事件回應 (IR) 團隊又測試了事件回應計畫的組織，其資料洩露平均總成本降低了 200 萬美元。我們常說「像實戰一樣訓練，像訓練一樣實戰」，就意味著要制定並測試事件回應方案，以最佳化企業高效迅速回應攻擊的能力。

·安全實務建議僅供參考，並不能保證結果。

使用有助於保護和監控端點與遠端員工的工具。

在因為新冠疫情需要開展遠端工作的組織中，70% 的組織認為此舉會增加資料洩露的成本。統一的端點管理 (UEM) 以及身分和存取管理 (IAM) 產品和服務，可讓安全團隊更加深入地瞭解公司以及自帶 (BYO) 筆記型電腦、桌上型電腦、平板電腦、行動裝置和 IoT（其中包括組織沒有物理存取連接的端點）的可疑活動，進而縮短調查和回應時間以隔離並控制破壞。

投資治理、風險管理與合規計畫。

偵測和升級成本僅次於損失業務的成本，是研究中排名第二的洩露成本類別。可評估企業風險並追蹤政府要求合規性的內部稽核框架，有助於增強組織偵測資料洩露並加大控制力度的能力。

最大程度降低 IT 和安全環境的複雜性。

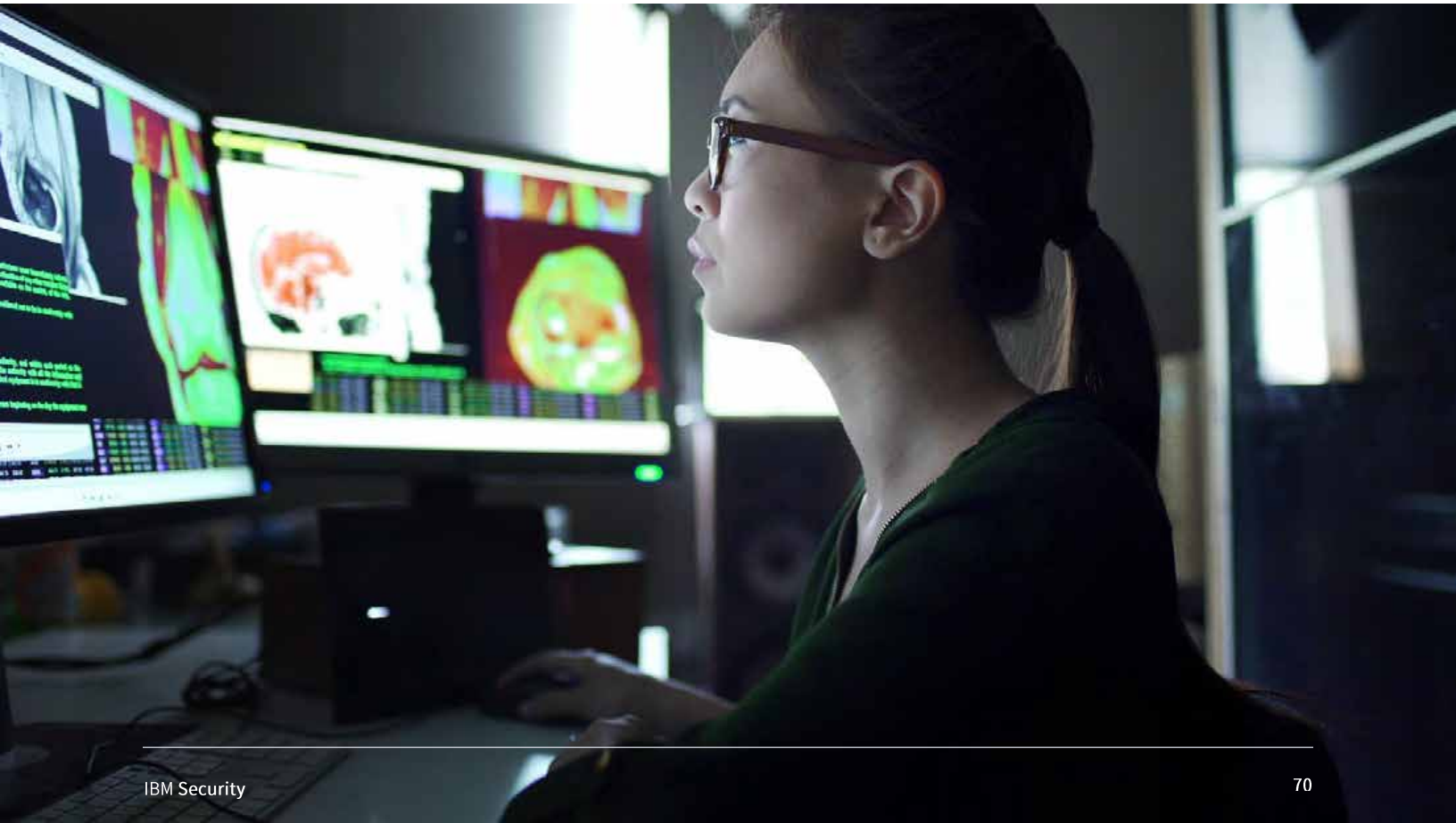
在今年的研究中，在列舉的 25 個因素中，安全系統的複雜性是導致資料洩露平均成本增加的頭號因素。第三方引起的資料洩露，廣泛的雲端遷移和 IoT/OT 環境也推高了資料洩露成本。能夠在分散的系統之間共享資料的安全工具，可協助安全團隊偵測複雜的混合多雲環境中的事件。

利用政策和技術保護雲端環境中的敏感資料。

隨著雲端環境中托管的資料量和價值不斷增加，組織應該採取措施保護雲端托管的資料庫。資料分類方案和保留計畫有助於瞭解容易被破壞的敏感和機密資訊，並透過加密保護敏感資訊。漏洞掃瞄、滲透測試和紅隊測試有助於發現雲端托管的資料庫漏洞風險和錯誤配置。研究發現，所有這些解決方案都可降低資料洩露平均成本。

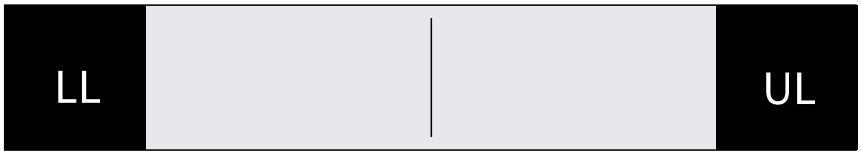
使用托管的安全服務有助於縮小安全技能差距。

研究中的組織發現，安全技能短缺是導致資料洩露成本增加的主要原因之一，而安全托管服務則有助於降低資料洩露平均成本。安全托管服務供應商利用持續的監控和整合的解決方案與服務簡化安全與風險。



研究方法

為確保充分的機密性，基準工具不會擷取任何公司特定的資訊。資料收集方法不包含實際的會計資訊，而是依賴各位參與者在數軸上標記範圍變數來預估直接成本。參與者需要在每個資料洩露成本類別的上限和下限範圍之間的一個點處標記一條數軸。



從數軸而不是各個已展示成本類別的點估計值來獲得數值，保持了機密性，並確保較高的回應率。基準工具還要求參與者分別對直接成本和機會成本進行第二次預估。

為方便管理基準流程，我們儘量只預估我們認為是測量資料洩露成本必不可少的成本活動中心。在與眾多專家探討之後，最終確定的項目中包含固定的成本活動。收集基準資訊之後，會重新仔細檢查每件工具以確保一致性和完整性。

基準工具中包含的資料洩露成本項目的範圍僅限於已知的成本類別，它們適用於各種處理個人資訊的業務操作。我們相信，側重於業務流程而非資料保護或隱私合規活動的研究會產生更高品質的結果。

資料洩露成本常見問題

什麼是資料洩露？

資料洩露定義如下：電子格式或紙制形式的個人姓名和醫療記錄和/或財務記錄或金融卡面臨潛在風險。本研究涉及的洩露中被破壞的記錄在 3,400 至 99,730 條不等。

什麼是被破壞的記錄？

我們將記錄定義為可以識別自然人（個人）的資訊，該自然人的資訊因為資料洩露而遺失或被盜。我們以資料庫為例，其中儲存了個人的姓名、信用卡資訊及其他身分識別資訊 (PII)，另一個示例是健康記錄，其中儲存了投保人的姓名和付款資訊。

如何收集資料？

我們的研究人員對 524 家在 2019 年 8 月至 2020 年 4 月期間經歷過資料洩露的公司開展了 3,200 多次單獨訪談，從中收集了大量深入的定性資料。我們從 2019 年 10 月開始招募組織，2020 年 4 月 21 日訪談正式結束。

受訪者中有 IT 專家也有合規和資訊安全從業人員，他們對組織的資料洩露以及解決洩露問題所花費的成本都瞭如指掌。出於隱私考慮，我們沒有收集組織特定的資訊。

如何計算成本？

要計算資料洩露的平均成本，我們收集了組織發生的直接和間接支出。直接支出包括聘請司法鑑定專家、外包熱線電話支援，以及為將來的產品和服務提供免費的信用監控訂閱和折扣。間接成本包括內部調查和溝通，以及營業額或客戶獲取率下降而造成客戶流失的外推值。

本次研究只呈現了與資料洩露經歷直接相關的事件。例如，組織可能因為《一般資料保護規則》(GDPR) 和《加州消費者隱私法案》(CCPA) 等新法規而決定加大對網路安全治理技術的投資，但這些投資並未直接影響本次研究中呈現的資料洩露成本。

為與前幾年的研究保持一致，我們使用了相同的貨幣換算方法，而沒有調整會計成本。

基準研究與調查研究有何不同？

資料洩露成本報告中的分析單位是組織。調查研究中的分析單位是個人。我們招募了 524 家組織來參與本次研究。

每條記錄的平均成本能否用於計算涉及數百萬份記錄遺失或被盜的資料洩露的成本？

我們研究中的資料洩露平均成本不適用於災難性的大型資料洩露，例如 Equifax、Capital One 或 Facebook。這些都不是許多組織會經歷的常見洩露。

因此，要透過瞭解資料洩露成本行為來得出有用的結論，我們把不超過 10 萬份記錄的資料洩露事件作為我們的研究目標。本研究中使用每條記錄的成本來計算單條紀錄洩漏事件的成本和總數量達數百萬之巨的多條紀錄洩露事件的成本得出的結果是不一致的。但今年的研究使用了模擬框架，它以 17 個規模相近的巨量資料洩露為樣本，衡量涉及 100 萬份甚至更多記錄（大型洩露）的資料洩露事件的成本影響。

為什麼使用模擬方法來估算大規模資料洩露的成本？

17 家遭遇大型洩露的公司樣本量太小，無法使用作業成本法執行有統計顯著性的分析。為解決這一問題，我們部署了蒙特卡羅模擬法，利用它透過反覆試驗預估一系列可能（隨機）的結果。

我們一共執行了 15 萬多次試驗。所有樣本均值的總均值提供了各種規模（被破壞的記錄從 100 萬份到 500 萬份不等）的資料洩露最有可能的結果。

是否每年都追蹤相同的組織？

每年的研究都會涉及不同的公司樣本。為了與之前的報告保持一致，我們每年招募的樣本公司都有類似的特徵，例如產業、員工人數、地理區域和資料洩露的規模等。從 2005 年起至今，我們已經研究了 3,940 家組織的資料洩露事件。

組織特徵

今年的研究涉及到 524 個來自不同地域和產業且規模各異的組織。2020 年的研究抽樣調查了 17 個國家或地區的 17 個產業。

今年的研究首次審查了位於拉丁美洲的組織集群地，其中包括墨西哥、阿根廷、智利和哥倫比亞。

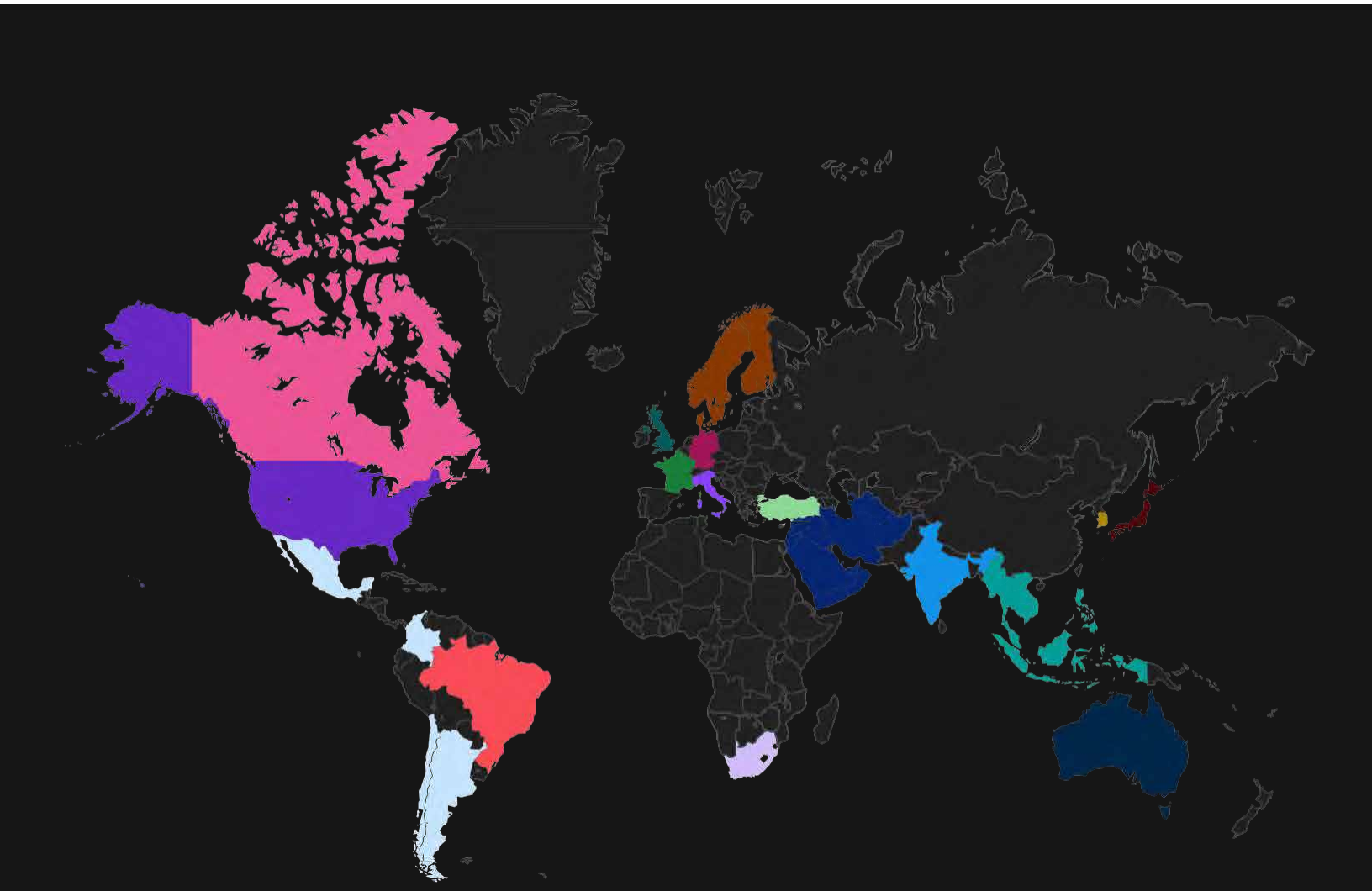


圖 47

樣本分佈（按國家或地區）

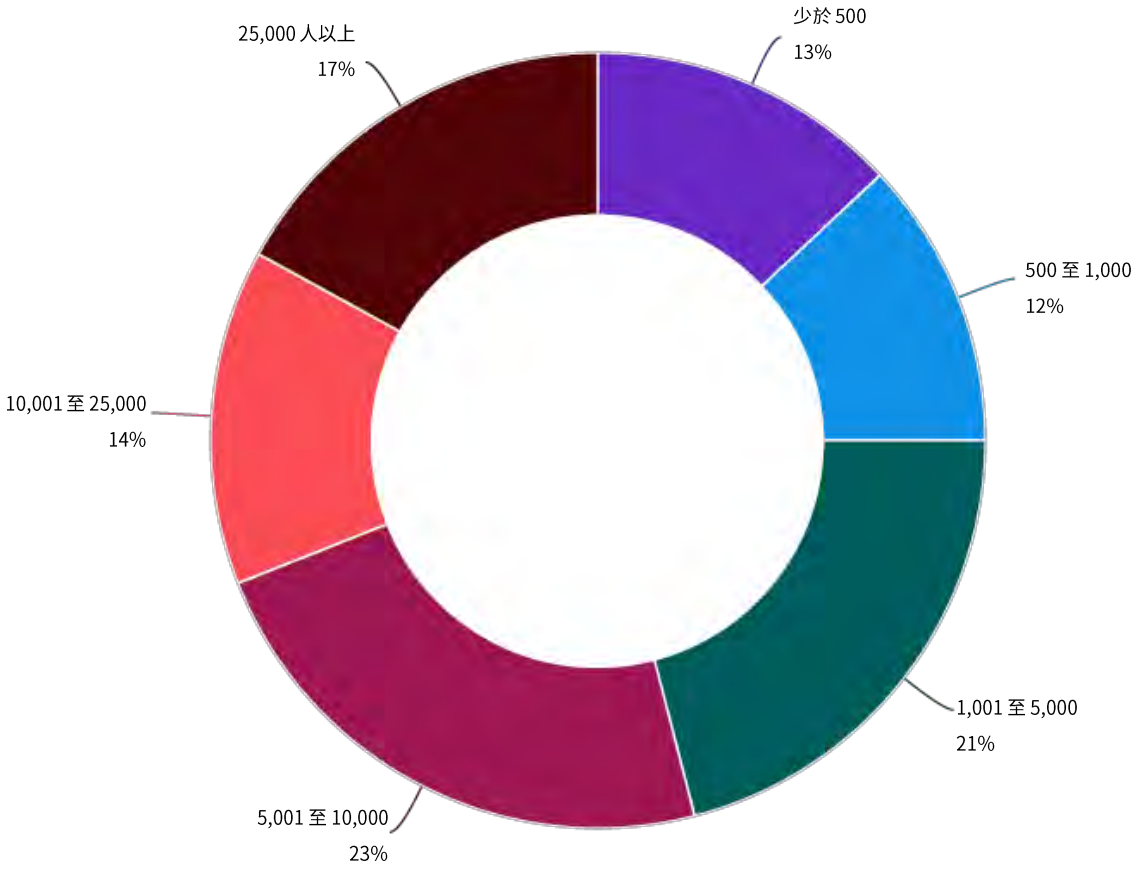
本次研究呈現了來自六大洲的國家/地區。

圖 47 顯示了基準組織的分佈情況（按國家或地區劃分）。美國以 12% 的代表比例高居榜首，印度和英國分別以 9% 和 8% 的比例緊隨其後。代表比例最低的國家/地區是東協、澳大利亞、斯堪地那維亞、義大利、拉丁美洲、土耳其和南非。

圖 48

按公司規模劃分的樣本分佈情況

按員工人數測量

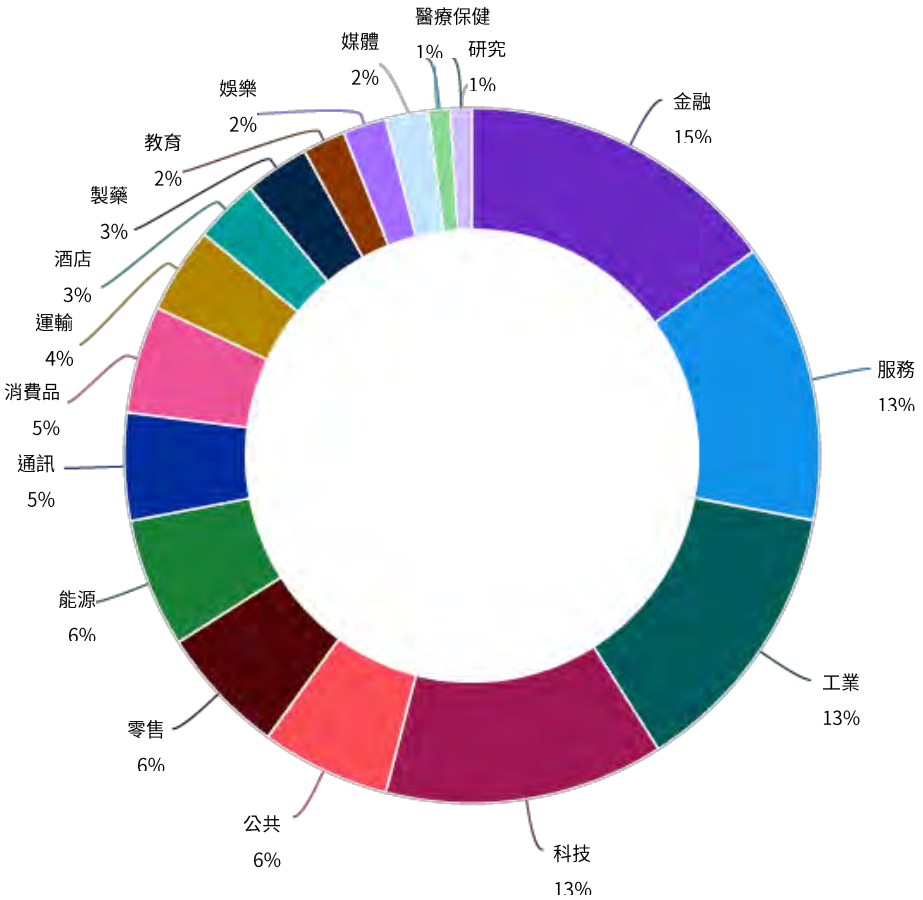


涵蓋了大中小型組織。

圖 48 顯示了樣本中 524 個按員工數量劃分的組織的分佈情況，員工數量代表著公司規模。該樣本略偏重於中等規模的組織，有 58% 的組織員工人數在 1,001 至 25,000 人之間，有 25% 的組織員工人數少於 1,000 人，還有 17% 的組織超過 25,000 人。

圖 49

各產業的樣本分佈情況



產業代表傾向於幾個較大的產業。

圖 49 顯示了基準組織的分佈情況（按產業劃分）。今年的研究涉及十七個產業。最大的產業是金融、服務、工業和科技。我們單獨解釋了工業的定義。

產業的定義

醫療保健
醫院，診所

金融
銀行、保險、投資公司

能源
石油和天然氣公司，公用事業，替代能源製造商和供應商

製藥業
製藥，包括生物醫學生命科學

工業
化學工藝、工程和製造公司

科技
軟體和硬體公司

教育
公立和私立大學和學院，培訓和發展公司

服務
專業服務，例如法律、會計和諮詢公司

娛樂
電影製作、體育、遊戲和娛樂場

運輸
航空、鐵路、卡車和運輸公司

通訊
報紙、圖書出版商、公共關係和廣告公司

消費品
消費品製造商和分銷商

媒體
電視、衛星、社群媒體和網際網路

餐旅服務
飯店、聯鎖餐廳、遊船公司

零售
實體店和電子商貿

研究
市場研究、智囊團、研發

公共
聯邦、州和地方政府機構以及非政府組織

研究限制

我們的研究利用了專有的機密基準方法，在之前的研究中都得到了成功部署。但是這種基準研究也存在固有的限制，在從研究結果中得出結論之前必須認真考慮這些限制。

非統計結果

我們的研究對象是全球實體的代表性非統計樣本。考慮到我們的取樣方法不夠科學嚴謹，因此統計推論、誤差幅度和置信區間不能用於這些資料。

非回應

無反應偏差未經測試，因此未參與研究的公司可能在潛在資料洩露成本方面有本質上的不同。

抽樣框架偏差

我們的抽樣框架帶有評判性，框架在多大程度上代表了被研究公司的群體，會影響到結果的品質。我們認為當前的抽樣框架偏向於制定了更成熟的隱私或資訊安全計畫的公司。

公司特定的資訊

基準不會擷取可識別公司身分的資訊。個人可利用它使用類別回應變數揭露關於公司和產業類別的地理資訊。

未測量的因素

我們在分析中省略了一些變數，例如主要的趨勢和組織特徵等。省略的變數可以在多大程度上說明基準結果，這一點我們無法確定。

外推成本結果

儘管可以將某些制衡原則納入基準流程，但受訪者仍有可能不提供準確或真實的回答。此外，使用成本外推方法而不是實際的成本資料也可能造成誤差和不準確性。

外推成本結果

今年美元表現強勢，極大地影響了全球成本分析。從本幣換算成美元降低了每項記錄的成本和平均總成本預估。為了與前些年保持一致，我們決定繼續使用與先前相同的會計方法而不是調整成本。

Ponemon Institute 和 IBM Security 簡介

*資料洩露成本報告*由 Ponemon Institute 和 IBM Security 聯合發佈。本次研究由 Ponemon Institute 單獨開展，IBM Security 對結果提供了贊助、分析並予以報告和發佈。

Ponemon Institute 致力於開展獨立研究和培訓，在企業和政府內部推廣負責任的資訊和隱私管理實務。對影響個人和組織敏感資訊管理和安全的重要問題開展高品質的實證研究，是我們肩負的使命。

Ponemon Institute 遵從嚴苛的資料機密性、隱私和道德研究標準，不會從個人那裡收集個人身分資訊（也不會在我們的業務研究中收集可識別公司身分的資訊）。此外，Ponemon Institute 還遵從嚴格的品質標準，確保受試者不會被問及不相關或不恰當的問題。

IBM Security 是最先進的整合式企業安全產品與服務組合之一。得益於享譽世界的 IBMR X-Force® 研發團隊的支援，該產品組合提供安全解決方案，協助組織將安全融入其業務流程，在充滿不確定的環境中也能蓬勃發展。

IBM 是全球最廣泛、最深入的安全研發和交付組織之一。IBM 每月監控 130 多個國家/地區的兩萬多億起事件，並擁有 3,000 多項安全專利。欲瞭解更多資訊，請造訪：ibm.com/security。

如果您對本研究報告有任何問題或意見（包括引用或重用此報告的權限），請透過信函、電話或電子郵件與我們聯絡：

Ponemon Institute LLC

收件人：研究部門 2308

US 31 NorthTraverse City, Michigan 49686 USA

1.800.887.3118

research@ponemon.org

如您有任何問題，請隨時聯繫我們

1. 免費專人諮詢熱線：0800-016-888 按 1

2. 郵件聯繫 IBM

3. 洞悉情報、智能管理：訪問 IBM Security 官網

採取後續行動

網路安全服務

藉助諮詢、雲端和托管安全服務降低風險瞭解更多 →

身分和存取管理

將每位使用者、API 和裝置安全地連接至每款應用程式瞭解更多 →

資料安全性

發現、分類並保護敏感的企業資料

瞭解更多 →

安全資訊和事件管理

獲得可見性，及時偵測、調查並回應威脅

瞭解更多 →

安全編排、自動化和回應

藉助編排和自動化加速事件回應

瞭解更多 →

雲端安全

將安全性整合到您的混合多雲之旅

瞭解更多 →

IBM Corporation
New Orchard Road
Armonk, NY 10504

美國印製 2020 年 7 月

IBM Security