Business Continuity Institute

地平線掃描報告 2018

HORIZON SCAN REPORT

Correct as of January 2018

bsi.

序言
英國營運持續協會
Business Continuity Institute (BCI)

在 BSI 英國標準協會的協助下，英國營運持續協會 (Business Continuity Institute,BCI) 完成第 7 個年度的地平線掃描調查 (Horizon Scan Survey)，調查內容針對企業組織所面臨的主要威脅，營運持續專業從業人員的觀點，以及他們將採取哪些方法加以克服...等提出研究發現。本調查報告出版至今，受到營運持續與韌性專業人員的高度推崇，被視為組織擬訂營運持續策略的重要資訊來源。

今年我們發現營運威脅的型式更具複雜性與多樣化。非實體性的威脅，如大規模的網路攻擊，仍然高居排行榜第一位，像是 WannaCry 與 NotPetya 等勒索病毒對營運的衝擊程度更勝以往。

同樣的，專家們也擔心實體性的營運中斷將會危及員工安全，並造成重大財務損失。無論是導致停電的颶風，或濫射殺人事件 (例如恐怖攻擊) 而導致建築物封鎖等，各組織都必須預先做好準備。回顧過去一年，美國的颶風哈維 (Harvey) 以及菲律賓的天秤 (Vinta) 颱風所造成的嚴重損失，還有遍及各區的恐攻威脅不斷，在在證明充分的準備是企業組織存續與成功之關鍵因素。

本調查報告同時針對一些被組織視為迫在眉睫的威脅，與實際造成的中斷程度相互比較。令人憂心的是，研究結果顯示，即使專家事先已經提出警告，在某些事件上，例如重大流行疾病卻是無法預先偵測到的。這再度顯示進行地平線掃描演練的重要性，能為營運持續專責人員清晰地勾劃出所面臨挑戰的具體概況。

從正向的角度來看，營運持續作業是建立組織韌性最關鍵的做法之一。無論是在營運持續計劃的實行，或是產業標準的採用，都呈現逐年成長的發展趨勢。此外，今年度的調查報告首度增加一項新的評量指標，顯示存續較久的組織是如何採用營運持續計畫，而這項計畫帶來的長期效益也使得他們更有意願維持資源的投入。

導入營運持續計畫，並且與跨領域 (例如風險、實體安全或災害復原) 的專業人員分享地平線掃描分析之結果，是建立韌性的關鍵。本調查報告目的在於彰顯個案成因，並且提升不同區域、行業與產業之專業人員對營運持續的認知。

David Thorp
BCI 執行總監

序言
英國標準協會
British Standards Institute (BSI)

2018 地平線掃描報告 (Horizon Scan report) 是 BSI 與英國營運持續協會 (Business Continuity Institute, BCI) 建立堅實夥伴關係的最佳成果，提供了精闢觀點與市場分析以作為企業組織營運持續管理的重要資源。BSI 與 BCI 連續 7 年合作製作此份報告，志在協助各組織瞭解當前所處的商業環境。

自從本報告發表以來，儘管商業環境發生巨幅波動與變化，但對企業最顯著的營運威脅類別卻始終如一。爆炸性發展的科技在全球上所扮演的角色，以及帶給企業組織的協助，讓科技成為企業組織的營運基礎。因此，毫無意外地，網路攻擊、資訊外洩以及無預警的資通訊中斷 仍然是當前經營的最重大威脅。如果這些威脅確實發生，將對組織的營運甚至聲譽造成重大衝擊。2017 年發生多起網路攻擊與資安頭條新聞事件，影響的層面從金融服務甚至橫跨到醫療服務產業，讓人感受到這些威脅已確確實實的存在現實生活當中。

隨著營運風險不斷攀高，以及更為精密複雜之智慧技術的持續發展，組織不能夠再故步自封。

對於大部分的組織而言，營運持續計畫依然是最為重要的。調查結果顯示連續 3 年組織導入 ISO 22301 營續持續管理系統的比例呈現持續成長，70% 的受調者表示積極地使用這項標準。加上營運持續管理計畫的投資增加，都清楚地顯示組織對於「預先準備」的重視。

然而，建立一個韌性的組織，最重要的不僅是擁有營運持續計畫，也需要一個更全面綜合的作法讓您掌握自身優勢與劣勢。

2017 年 BSI 發表了全世界第一份組織韌性指標報告。根據組織韌性 (BS 65000)、組織管理 (BS 13500)、風險管理 (ISO 31000) 與供應鏈風險管理 (PAS 7000) 這 4 個最佳綜合實踐標準中，我們鑑別歸納出 16 項關鍵的指標 (Index)，並由 1,260 位來自世界各地多家組織、部門的高階領導人依據績效與各個指標之重要性進行排名。

組織高階領導人針對 16 項關鍵指標重要性的排序，與地平線掃描報告的結論相互呼應。高階領導人認為所有的指標都很重要，但是聲譽風險則被視為其中最為重要的。而報告中指出企業組織增加對營運持續計畫與持續管理的投資，也證明了營運持續專業人員將地平線掃描與相關趨勢分析的專案工作視為維護組織聲譽的利器。

Howard Kerr
BSI 集團執行長

內容

1 報告摘要

報告摘要

657
參與調查的組織

76
國家

前 10 大威脅 (Threats)

1
網路攻擊
Cyber attack

2
資料外洩
Data breach

3
無預警的資訊與通訊中斷
Unplanned IT and telecom outages

4
公共服務中斷
Interruption to utility supply

5
惡劣氣候
Adverse weather

6
恐怖主義行動
Act of terrorism

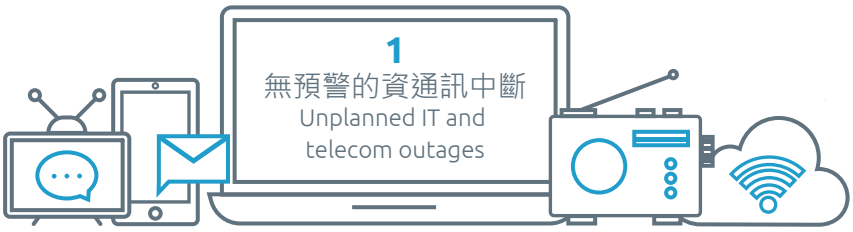
7
安全事故
Security incident

8
火災
Fire

9
供應鏈中斷
Supply chain disruption

10
運輸網路中斷
Transport network disruption

前 10 大衝擊 (Disruptions)

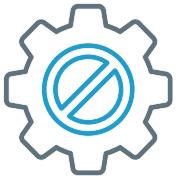


1
無預警的資通訊中斷
Unplanned IT and telecom outages

2
惡劣氣候
Adverse weather

3
公共服務中斷
Interruption to utility supply

4
網路攻擊
Cyber attack



5
人才 / 關鍵技術的取得
Availability of talents/key skills

6
安全事故
Security incident

7
運輸網路中斷
Transport network disruption

8
新頒布之法令或法規
New laws or regulations

9
火災
Fire

10
供應鏈中斷
Supply chain disruption

前 10 大趨勢 (Trends)

2
流失重要員工
Loss of
key employee

3
社群媒體的影響
Influence
of social media

4
新法規和更嚴謹的
監管審查
New regulations
and increased
regulatory scrutiny

5
互聯網相關服務的
普及和高度採用
Prevalence and high
adoption of internet
dependent services

6
政局變化
Political
change

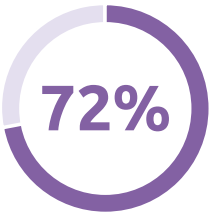
7
潛在的
全球大流行疾病
Potential
emergence of a
global pandemic

8
供應鏈複雜度提升
Increasing
supply chain
complexity

9
消費者態度與
行為改變
Changing consumer
attitudes and
behavior

10
氣候變遷
Climate
change

趨勢分析

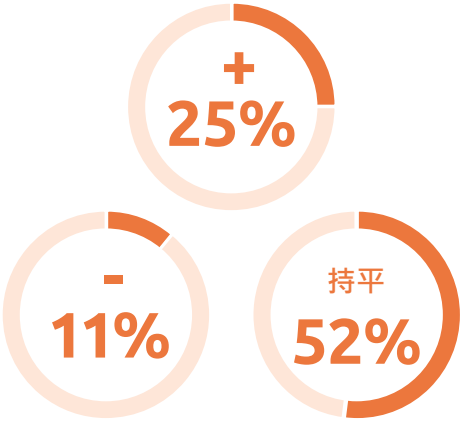


72% 的受訪者
進行較長期的趨勢分析，
作為其地平線掃描行動的一環

然而

29% 的受訪者未能獲得
趨勢分析的內容

對營運持續的投資程度



採用 ISO 22301

70% 受訪者使用 ISO 22301
作為做為其
營運持續計畫的指導原則

2

主要報告

引言

英國營運持續協會在 BSI 連續第 7 年的支持之下，推出 2018 地平線掃描報告，針對企業組織所面臨的短期與長期營運威脅提出調查結果與看法。本報告也評估了組織在面對營運中斷而預為因應的對策及作法，以展望營運持續工作的普及。

本報告的調查結果包含來自 76 個國家，共計 657 家受訪組織，以及相關的個案研究。這份報告發行至今，已經成為營運持續及組織韌性領域專業人員的重要產業資源。

衡量對特定威脅的關切程度

網路威脅持續成為營運持續與韌性專業人員最為關切的議題。網路攻擊居於首位，53% 的受訪者「極度關切」此議題 (圖 1)。資料外洩 (42%) 以及無預警的資訊與通訊中斷 (36%) 則分別位居第 2 與第 3 名，這就是前三大受到關切的議題。回顧過去一年發生多起網路資安事件，包括災情哀鴻遍野的勒索病毒 WannaCry 與 NotPetya，不難看出為何這類非實體性威脅這麼令人憂心了。

另一方面，實體安全也仍然是組織極度重視的議題。公共服務中斷 (18%) 以及惡劣氣候 (18%)，被專業人員視為第四與第五項重大威脅。這兩個議題經常相互相關，例如惡劣天氣事件，像是近 10 年來最強的大西洋颶風─艾瑪 (Irma) 重創加勒比海地區帶來嚴重災情，哈維 (Harvey) 颶風所降下的豪雨造成美國休士頓市區淹水與道路交通癱瘓，阻斷了基本民生服務。

安全事件 (16%) 下降 2 個名次，但是仍然穩居前 10 大威脅之內，與恐怖主義行動並列第 6 名。這充分反映出受訪者對於工作場所暴力行為的關切。根據英國營運持續協會先前的研究顯示，有越來越多組織正採取相關措施，以建立有效的緊急通訊系統來因應這類意外事件 [1]。

火災 (14%) 排名第 8，因火勢迅速蔓延造成 71 人死亡的英國倫敦住宅大廈 Grenfell Tower 大火事件，可能是此類威脅今年進入前 10 名的原因。最後，或許是因為實體破壞的威脅升高，供應鏈 (13%) 以及運輸網路中斷 (13%) 分別排名第 9 與第 10。此外，在英國營運持續協會的其他研究中，也指出恐怖主義為供應鏈的前 10 大擔憂議題之一 [2]。

1 BCI Emergency Communications Report 2017.
2 BCI Supply Chain Resilience Report 2017.

必須留意的還包括新頒布之法令或法規 (12%) 所帶來的挑戰，以及人才 / 關鍵技術 (11%) 的取得，為何從去年的第 9 與第 10 順位跌落到第 11 與 13 順位。鑒於當前全球政治動盪不安的浪潮，以及歐盟一般資料保護規範 (European General Data Protection Regulation, GDPR) 的正式實施日期即將來臨，將值得我們關注的是，組織如何投入更多心力來應對各種不同類型的營運威脅。

年份	前 5 大威脅
2016	**1.** 網路攻擊 **2.** 資料外洩 **3.** 無預警的資訊與通訊中斷 **4.** 恐怖主義行動 **5.** 安全事件
2017	**1.** 網路攻擊 **2.** 資料外洩 **3.** 無預警的資訊與通訊中斷 **4.** 安全事件 **5.** 惡劣氣候
2018	**1.** 網路攻擊 **2.** 資料外洩 **3.** 無預警的資訊與通訊中斷 **4.** 公共服務中斷 **5.** 惡劣氣候

表 1. 近年來組織面臨最重大的威脅

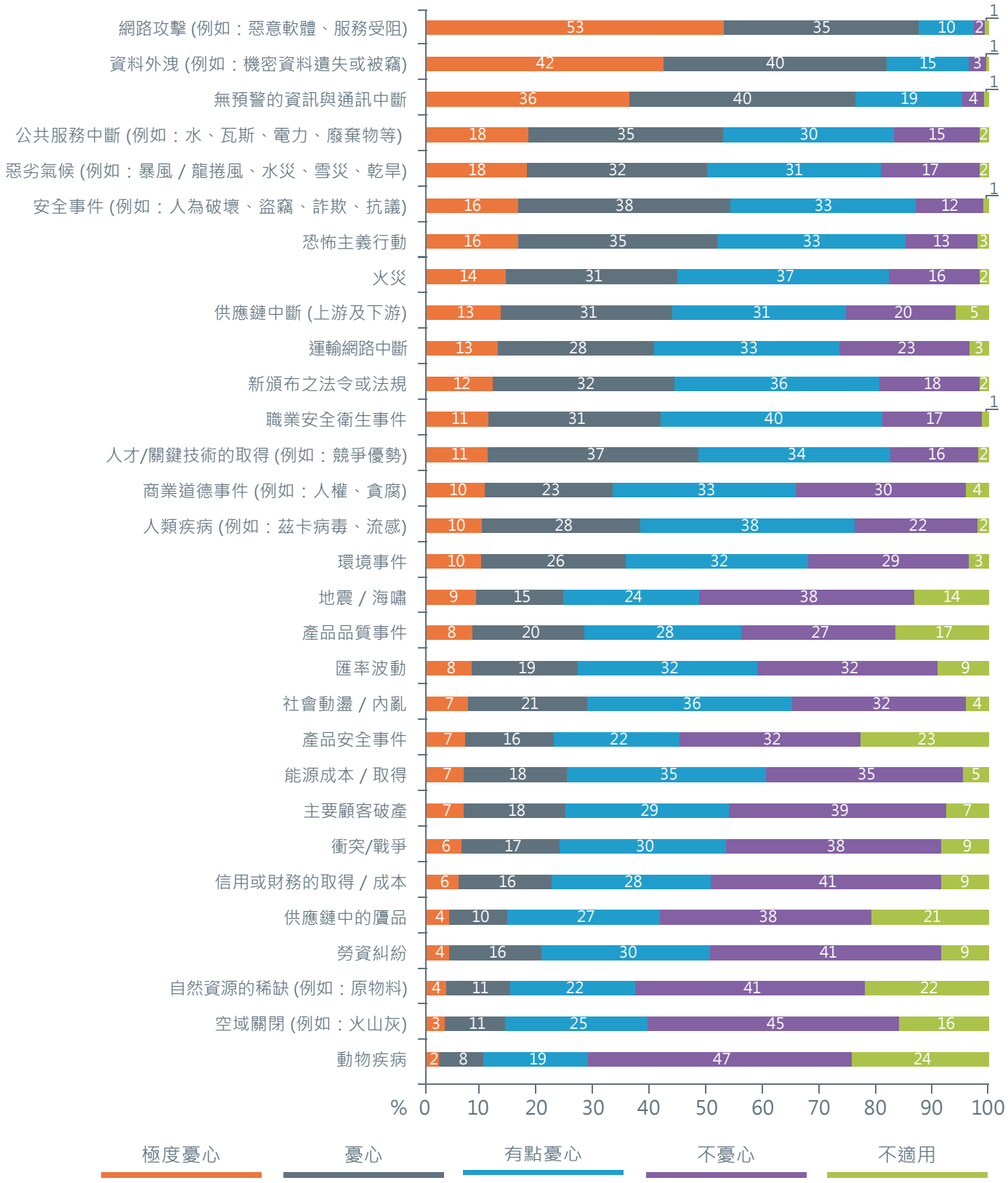


圖 1. 跟據您的分析，您的組織在 2018 年對下列威脅的擔憂程度為何?
(母體數=595，答題結果以百分比顯示，允許複選。)

個案討論

大流行疾病 (Pandemics)

過去 40 年以來，大流行疾病的數量增加了 3 倍。專家們已敲響下一次可能大爆發的疾病警鐘 - 即橫掃中國的 H7N9 禽流感病毒株。這病毒引發呼吸系統的嚴重問題，令感染者有極高比例最終需要進入加護病房。這僅是自西非的伊波拉 (Ebola)、南美洲茲卡 (Zika) 病毒之後到處肆虐的致命疾病之一，而這些威脅在未來似乎沒有減輕的趨勢 [3]。除此之外，未來危害人體健康的意外事件也可能是人為的。專家們認為恐怖組織可能試圖購買生化武器而大規模散布感染源。雖然目前看起來機率不大，但是如伊斯蘭國 (Islamic State, IS) 等恐怖組織已證實可能進行生化攻擊 [4]。

各國政府與國際組織都意識到這些威脅，並進行製作指南規章與建議以因應這些公共衛生緊急事件。營運持續計畫被視為此類因應計劃的重要環節之一，因為這將有助於組織確保其員工的安全以及營運的持續。

世界衛生組織 (The World Health Organizations, WHO) 指出，營運持續計畫是各種層級與社會族群因應緊急狀態的核心。世界衛生組織在所出版的大流行疾病指南 [5] 中，概述了處理公共衛生緊急危機事件時必須採取的主要行動。澳洲政府也針對「傳染疾病管理計劃」[6] 提供了範本，以供其國內組織作為營運持續計劃的一部分。加拿大公營事業也針對健康危害的營運持續計畫出版一份專門指南，這與一般的計畫是有所不同，因為這份指南的焦點著重在危機發生期間可應用的人力資源 (因為這可能更受影響) 而非建築物或資訊這類實體資產 [7]。

針對大流行疾病預做準備計畫，是面對未來嚴苛挑戰的關鍵。運用地平線掃描分析所提出的見解，將能協助專業人員擬定周全的決策，藉以了解組織在面對特定威脅當下的脆弱程度。

3 http://time.com/magazine/us/4766607/may-15th-2017-vol-189-no-18-u-s/

4 https://www.reuters.com/article/us-biological-weaons-commentary/commentary-the-next-super-weapon-could-be-biological-idUSKBN17L1SZ

5 http://www.who.int/influenza/preparedness/pandemic/PIRM_withCoverPage_201710_FINAL.pdf?ua=1

6 https://www.tisn.gov.au/Documents/Template+for+Pandemic+Plan.pdf

7 https://www.ccohs.ca/publications/PDF/businesscontinuity.pdf

評估實際衝擊程度

這是地平線掃描報告第二年將特定威脅所造成的衝擊，與該項威脅受到關切的程度進行比較，並透過圖表的方式來呈現 (如圖 1) ，目的是為了顯露出組織對某些特定衝擊的認知與實質上所受到的影響有何不同，從而說明為何風險評估應該成為營運持續計畫的一環 (圖 2)。

受訪者所選的前 3 大衝擊分別是：無預警的資訊與通訊中斷 (67%)、惡劣氣候 (50%) 以及公共服務中斷 (43%)。有趣的是，當組織在衡量各種威脅造成的衝擊程度時，網路攻擊僅排名第 4 (37%)，但這卻是營運持續專業人員排名第一的憂心事件。這與去年的調查結果相符，原因可能在於即使是偶而發生，但網路攻擊所造成的嚴重損失與影響範圍廣闊，一如 WannaCry 勒索軟體事件，即牽動全球數個組織。人才 / 關鍵技術的取得 (22%) 在衝擊排行榜上名列第 5，反而未出現在營運持續專業人員的前 10 大關切議題中。

再繼續看到第 6 與第 7 名的安全事件 (20%) 與運輸網路中斷 (18%)，則與組織對於實體安全性的關切程度是一致的。英國營運持續協會之前針對緊急狀態通訊的研究中，也揭示了安全相關議題也是最具破壞性的問題 [8]。

有趣的是，即使新頒布的法令與法規 (16%) 並未列入前十大關切議題中，仍然被視為最常見衝擊問題的第 8 名。未能因應新頒布的法令規範進行必要的配合時，可能對組織造成嚴重影響，例如歐盟的一般資料保護規範 (GDPR) ，可能為全球企業帶來新的風險與挑戰，但也可能是組織評估與改善作業流程的機會。

火災 (16%)、供應鏈中斷 (14%) 以及職業安全衛生事件 (13%) 都列在前 10 大衝擊之內，與受訪者對於這些威脅之關切程度一致。

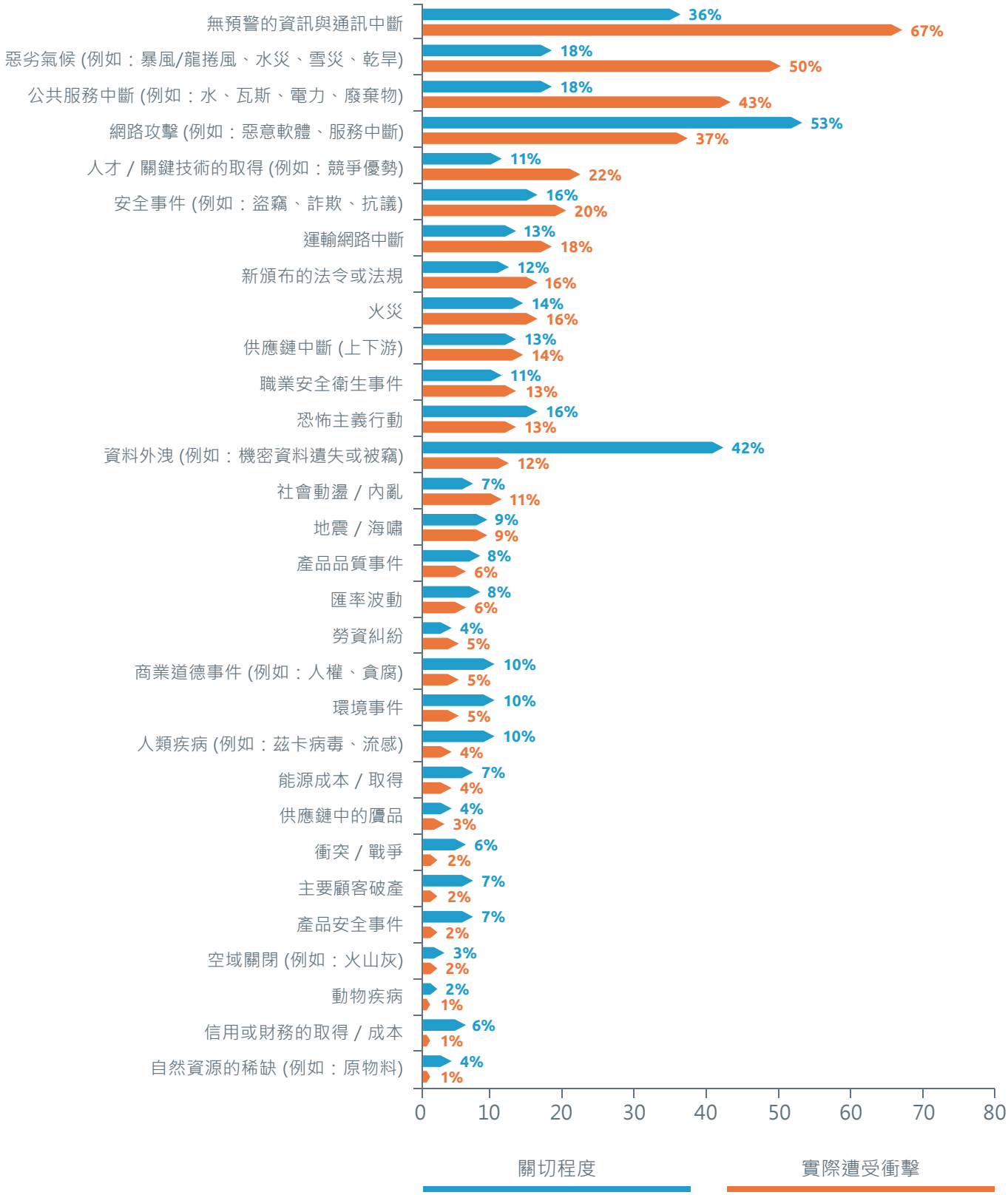


圖 2：您在過去 12 個月當中是否經歷過以下營運衝擊？
（母體數=538，答題結果以百分比顯示。允許複選）

新興趨勢與不確定性

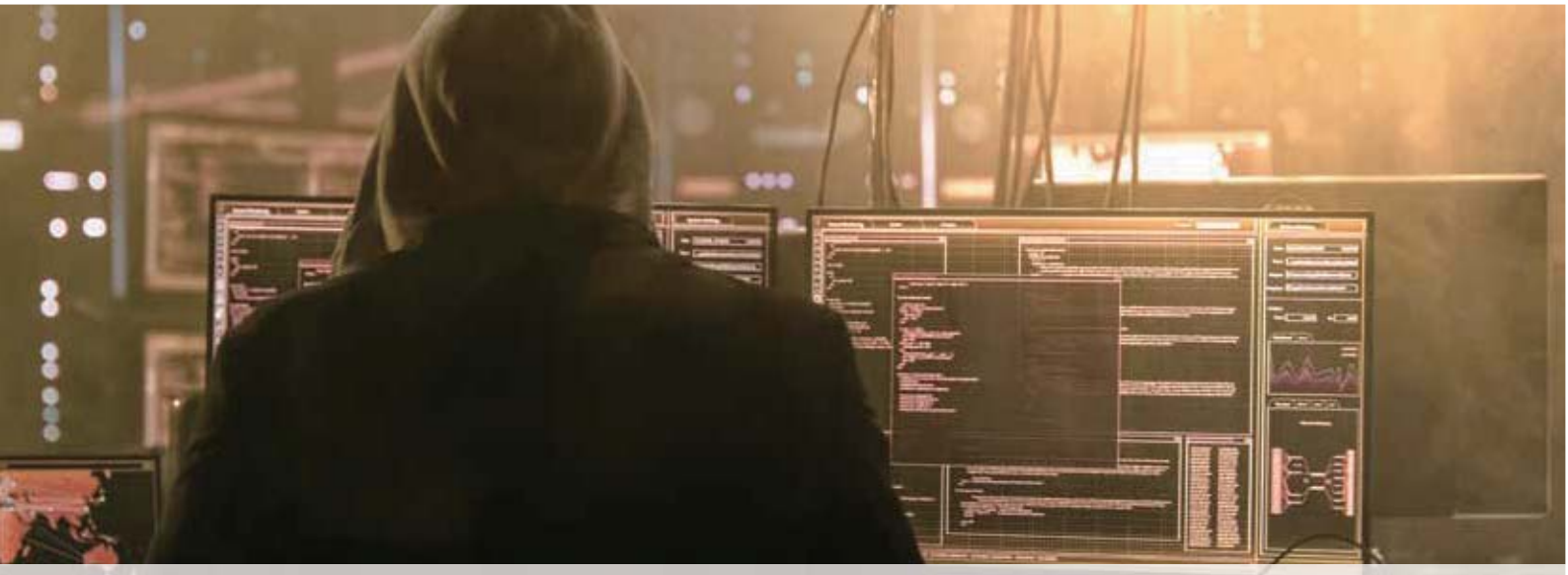
本報告也衡量了營運威脅的長期[9]發展趨勢與不確定性（圖 3）。使用網際網路進行的惡意攻擊（77%）仍然是第一大威脅，與去年度的報告結果一致。由於物聯網 IoT 裝置的佈署增加且成為駭客的新標靶，因此網路攻擊在未來確實有可能更為頻繁。關鍵人才的流失（51%）以及社群媒體的影響（50%）則分別排名第 2 與第 3，與去年排名順序互換。前 5 名當中還包括了新頒布之法令法規所增加的約束力（49%），以及互聯網相關服務的普及和高度採用（40%）。

此圖表所列出的網路攻擊、監管問題以及人力資本損失等議題組合，透露出專業人員認為未來的威脅是何等複雜。2017 全球風險評估報告（GRR 2017）[10] 也反映這部分的現象，其中更將網路攻擊與就業不足或失業都列在最具影響力的威脅之中。值得注意的是 GRR 2017 將這些威脅視為迫在眉睫而非未來之事，顯示出威脅情境的複雜度，以及不同角色或職務的人員對相同威脅的各別解讀。

政局變化（38%）與潛在的全球疫病傳播（34%）則分別位居第 6 與第 7 名。這兩個趨勢可能彼此相互關聯，例如當國家陷入政治動盪，缺乏管理時，傳染疾病便有機可乘，例如：伊波拉（Ebola）[11] 病毒在全球肆虐。

回顧 2017 英國國家風險報告（UK National Risk Register 2017），全球大流行疾病被視為短期內最迫在眉睫的威脅 [12]。有趣的是再度觀察到各個組織對於某些特定威脅的不同看法，實際上這些威脅遠比想像中來得更為迫近。

供應鏈複雜度提升（32%），消費行為改變（30%）以及氣候變遷（30%）均列在前 10 大的順位之中。氣候變遷的威脅性增高，印證了英國營運持續協會的研究，該研究發現組織已將其視為長期性的問題，並且必須適度的先期規劃 [13]。



9 For longer term it is usually meant a period of time beyond five years.
10 Global Risk Report 2017. World Economic Forum.
11 www.un.org/News/dh/infocus/HLP/2016-02-05_Final_Report_Global_Response_to_Health_Crises.pdf
12 www.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf
13 Continuity Planning for Climate Change. The BCI. 2017.

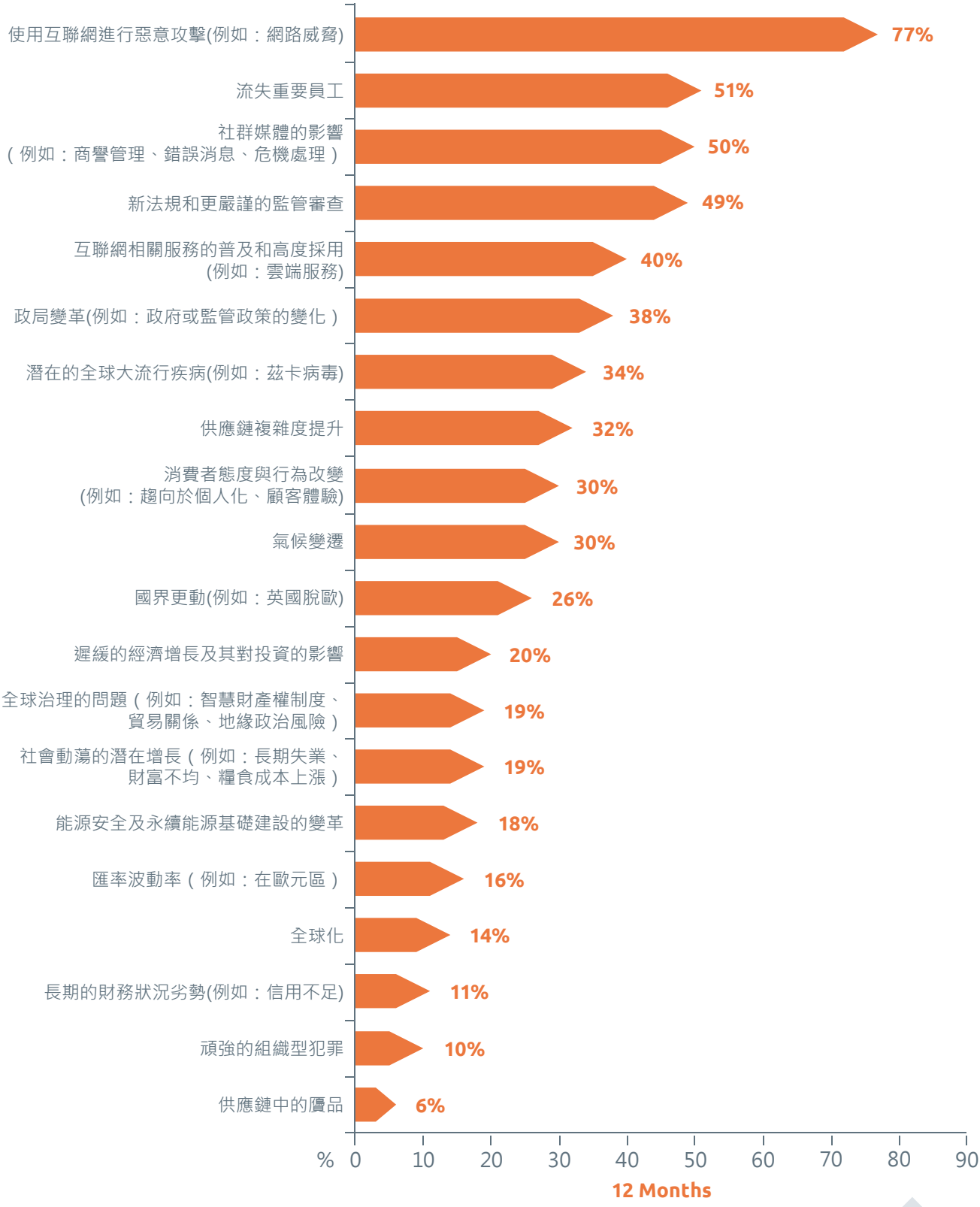


圖3：您評估營運持續性時，會考慮以下哪種趨勢或不確定性?
(母體數=564。答題結果以百分比顯示。允許複選)

個案討論

2017 的資料外洩

2017 年，美國信用報告巨擘 Equifax 遭遇嚴重的資料外洩事件，起因是由於某個未即時更新應用軟體的漏洞 [14]。這起資料外洩事件影響 1 億 4300 萬位消費者的個人資料，包括他們的姓名、社會安全卡號碼、生日、地址與駕照號碼。此外，駭客還竊取到 209,000 張美國信用卡資料，以及英國與加拿大居民的財務狀況 [15]。

依據該公司 2017 年最後一季發布的展望報告，其獲益低於產業的預期水準。報告中顯示資料外洩導致 6000 萬至 7500 萬美元的損失。而 Equifax 說明此項損失是因為與其他組織及政府機構的簽約延遲所導致，他們也試圖贏回信賴並平反商譽。該公司也重新調整第四季的獲利預測，從平均每股 $1.42 美元跌至 $1.38~$1.32 美元 [16]。

在美國，每年因資料外洩導致聲譽損害、法律成本、直接的財務損失以及復原工作，平均造成組織多出 700 萬美元的營運成本 [17]。 近期一項針對全世界資料外洩成本的研究顯示，可能影響到這類營運衝擊成本的因素包括了預料之外的顧客流失、外洩資料的規模、花費在確認與遏止的時間，事件發生後的通知，以及造成外洩的根本原因 [18]。

因此，除了擁有完善的網路安全作業以外，只要組織與其成員能夠對網路緊急應變與災難復原等作業充分瞭解，並且接受完整的訓練，似乎就能夠在網路安全事件發生期間與其後降低相關成本。就這個案例而言，雖然軟體開發商早已發佈露漏洞補丁，但未進行電腦的更新仍屬於人為失誤。因此，組織必須時時留意網路的人為因素，因為這可能是資料外洩的原因，而非純屬技術問題。

14 http://www.itpro.co.uk/data-leakage/29418/equifax-data-breach-hack-costs-equifax-875-million-as-income-plummets

15 O'Brien, S.A. Giant Equifax data breach: 143 million people could be affected. CNN Money. 2017 Sept 8. [cited 2018 January 4]. Available from http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html

16 Reuters. Equifax Warns About Impact of Data Breach on its Business. Fortune. 2017 Nov 10 [cited 2018 January 4]. Available from http://fortune.com/2017/11/10/equifax-warns-data-breach-business/

17 Puzas, D. Data breaches cost US businesses an average of $7 million – here's the breakdown. Business Insider. 2017 Apr 27 [cited 2018 January 4]. Available from www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4

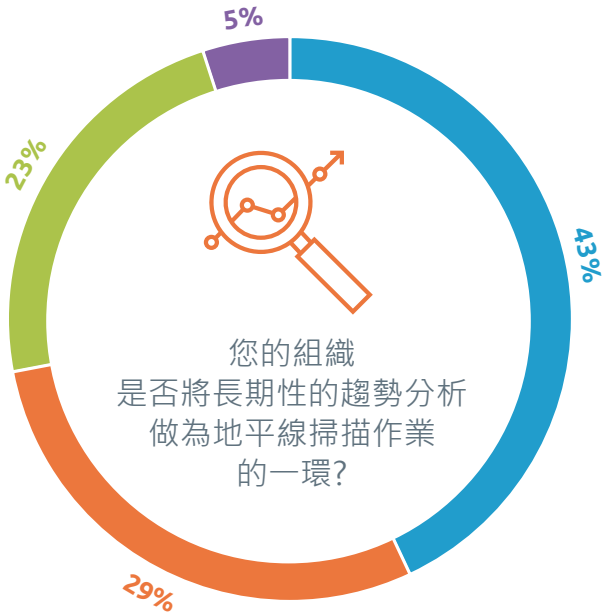
18 Ponemon Institute. 2017 Cost of Data Breach Study: Global Overview. 2017 June. [cited 2018 January 4]

長期性趨勢分析之執行評效

年份	執行趨勢分析的組織比例
2016	70%
2017	69%
2018	72%

表 2：長期性趨勢分析

即使相較前一年，今年有更多組織表示執行趨勢分析 (從 69% 增加至 72%)，但仍有幾乎四分之一的組織 (23%) 毫無行動。組織執行趨勢分析的比例增加，也意味著組織對這項分析的重要性認同度上升，這是因為當各種營運阻礙都能被逐條列舉，且不同部門之間能夠分享這項分析的結果，便可創造出長期性趨勢分析的真正價值。



43%
是的，這項分析是經由組織的核心幕僚單位進行 (例如：策略或風險部門)

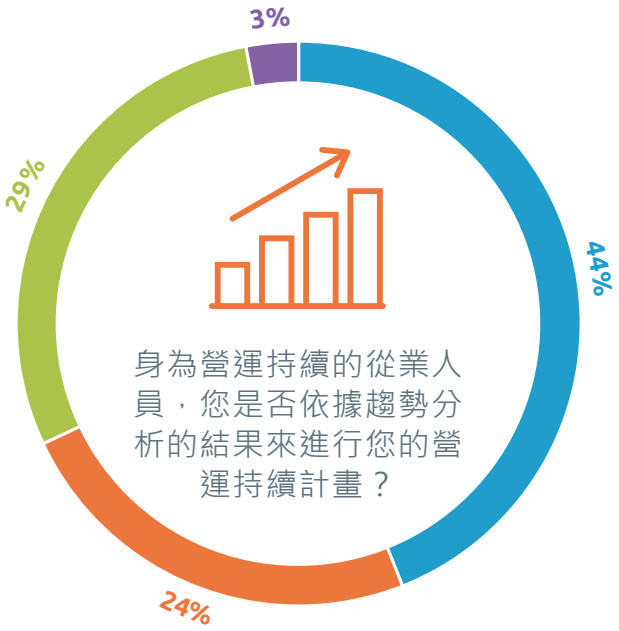
29%
是的，但這項分析是由各部門依據個別需求而進行

23%
不，我們不會進行

5%
我不清楚

圖 4：您的組織是否將長期性的趨勢分析做為地平線掃描作業的一環？
(母體數=579)

在本項調查中，每 10 個受訪者有 7 個表示會借鑒於趨勢分析的結果 (68%)，而無法獲得趨勢分析結果的受訪者比例則與去年相同 (29%)。這顯示在許多組織內部中，資訊壁壘的現象仍然存在，這也將是建構組織韌性的潛在障礙。



44%
是的，我瞭解趨勢分析的結果並且加以運用

24%
是的，我一開始就協助進行趨勢分析

29%
不，我未曾掌握到這些資訊

3%
不，我看不出這些資訊的價值

圖 5：身為營運持續的從業人員，您是否依據趨勢分析的結果來進行您的營運持續計畫？(母體數=573)

近五分之四的受訪者 (77%) 表示 2018 年會增加或維持對營運持續計畫的投資。這顯示無論組織規模大小，對於營運持續計畫的效益皆有更多的認知。事實上，中小企業與大企業都傾向維持營運持續計畫的適度投資，僅有 6% 的中小企業與 12% 的大型企業計畫削減預算，這與去年所調查的 7% 與 16% 相比，已分別有所進步。

25%
增加投資預算，以滿足營運持續計畫的擴展或其它新需求

52%
在組織的營運周期內，維持適當的營運持續計畫範圍與定位

11%
減少投資預算，縮減營運持續計畫的影響範圍

12%
我不清楚

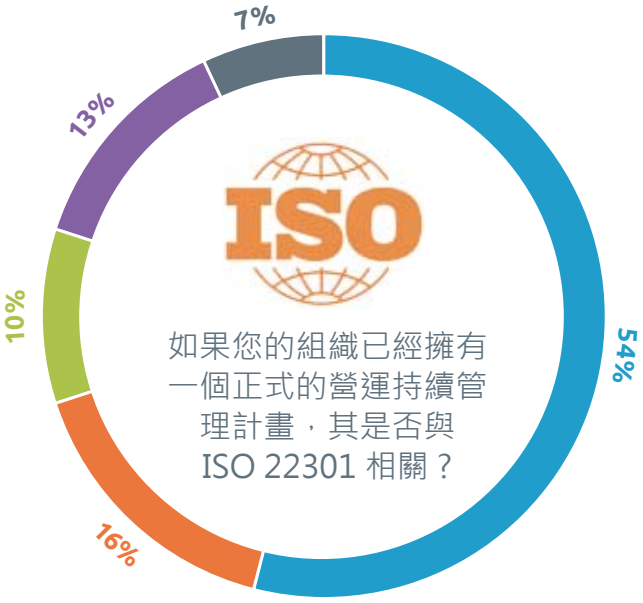
圖 6：如果您的組織現在已經有營運持續計畫，2018 年將投入的預算與 2017 年相比，會如何調整？(母體數 =571)

ISO 22301 持運持續管理系統之採用

年份	採用 ISO 22301
2016	51%
2017	63%
2018	70%

表 3：組織採用 ISO 22301 的近期統計

我們在今年的調查結果可以觀察到，組織採用相關標準，例如 ISO 22301，有相當大比例的成長 (63% → 70%)，而不計劃使用此標準之組織的比列也降低 (18% → 13%)。進一步來看，資通訊業 (86%)、能源與公共事業 (74%) 以及專業服務業 (74%) 是高度採用 ISO 22301 標準的產業。儘管今年金融與保險業未進入採用 ISO 22301 標準的前 3 名產業中，但其採用的比例仍然高達 70%。



54%
使用 ISO 22301 做為營運持續計畫的框架，但未驗證

16%
使用 ISO 22301 做為營運持續計畫的框架，並且通過驗證

10%
目前並未使用 ISO 22301 做為營運持續計畫的框架，但在2018年有此打算

13%
未使用 ISO 22301，且 2018年也無此打算

7%
無答覆

圖 7：如果您的組織已經擁有一個正規的營運持續管理計畫，其是否與 ISO 22301 相關? (母體數=642)

今年度的報告首次衡量組織內部營運持續管理計畫的成熟度。令人感到鼓舞的結果是，有 44% 的受訪者採用營運持續計畫已經長達 5 年之久。如果把這項資訊細分來看，可以觀察到經營年數較久的組織，對營運持續計畫的投資也越多。在擁有營運持續管理計劃超過 5 年以上的組織中，有 86% 表示他們在 2018 年將維持或增加對這項計畫的投資，而採用營運持續計畫少於 5 年者，則有 71% 表示他們也將會增加資源的投入。可能是因為當營運持續計畫的執行時間越長，專業人員將開始看到投資的回饋效益，而這項結論也在其他的研究報告中被證實 [19]。

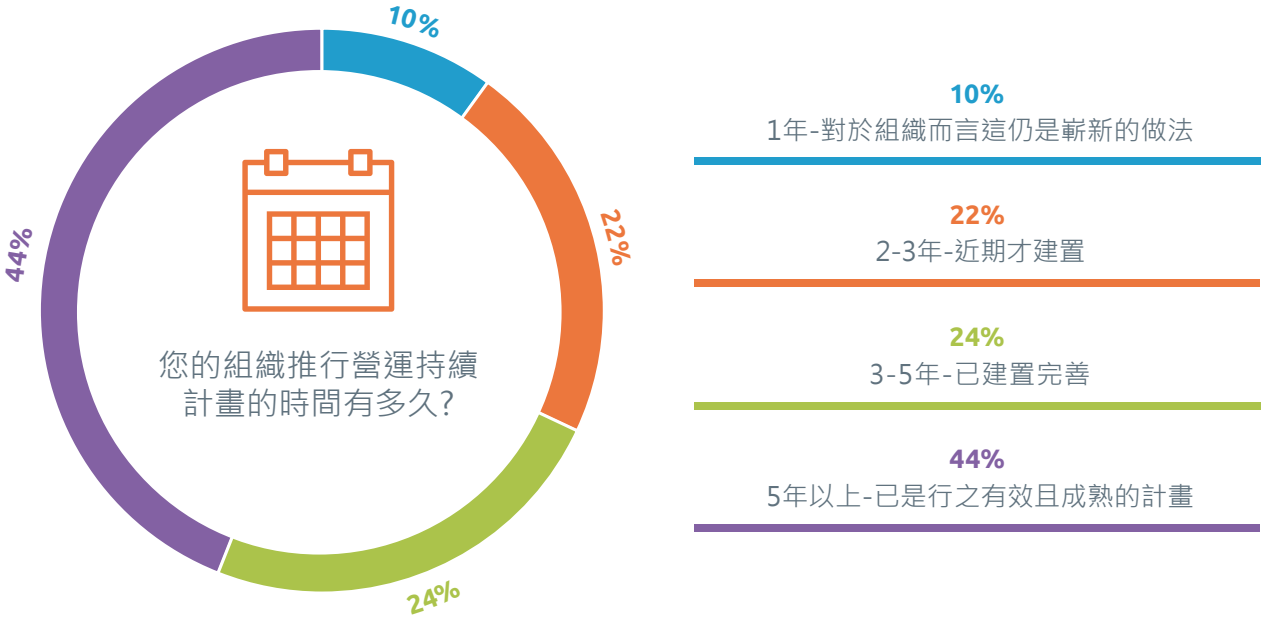
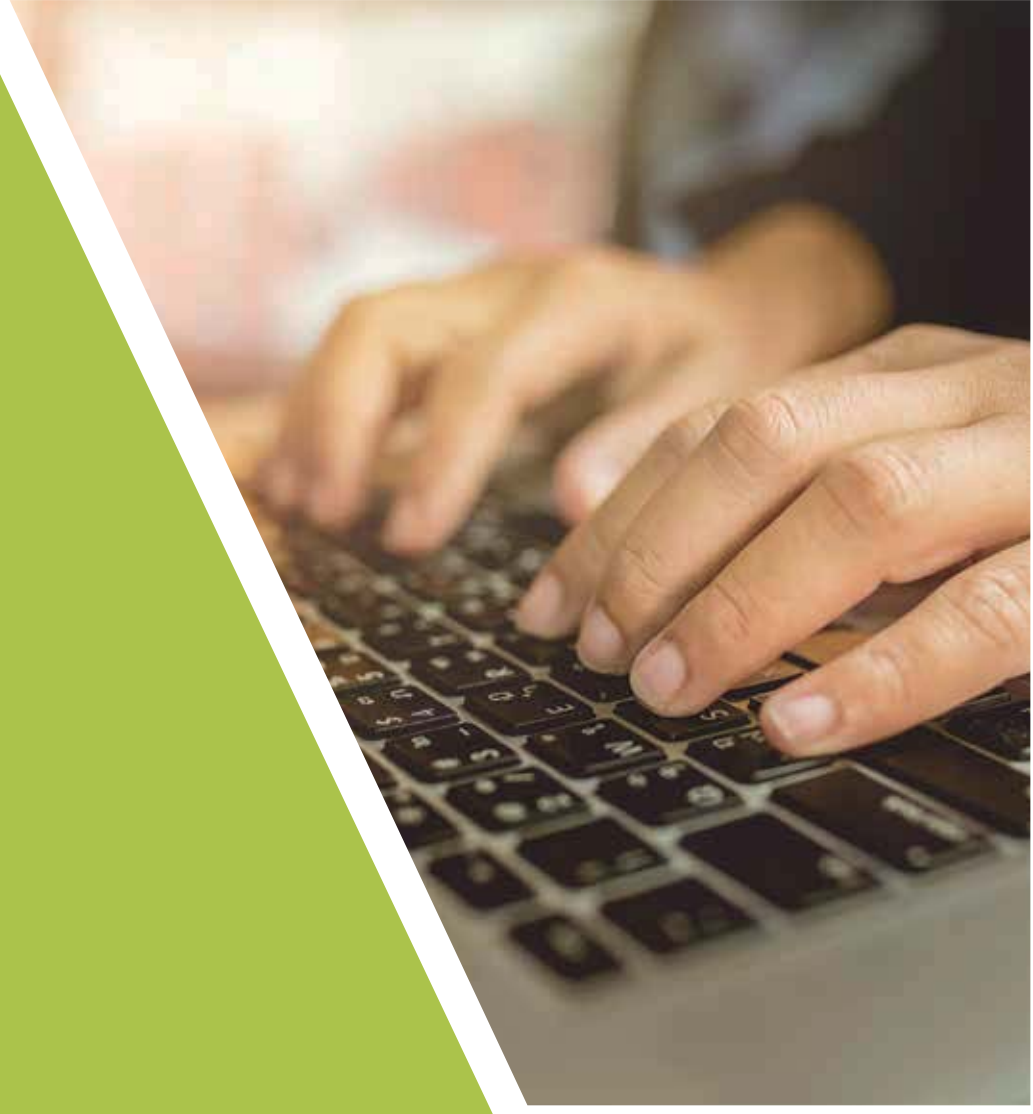


圖 8：您的組織推行營運持續計畫的時間有多久? (母體數=575)

19 Business Continuity delivers return on investment. BCI. 2016.

3 結論



結論

1

網路意外事件仍然是長短期內最受關切的議題。過去一年以來發生的大規模網路攻擊以及越來越多的網路安全相關事件，再度印證了組織建立網路韌性的必要性。根據英國營運持續協會的相關研究顯示，營運持續計畫將在其中扮演舉足輕重的角色。

2

各種不同型態的實體安全問題也是對組織的威脅。極端氣候與所造成的影響，如停電，也是今年專業人員特別擔心的。然而，工作場所的暴力事件，例如恐怖攻擊，也被視為主要的憂心事情之一。工作場所復原計畫有助於組織為各種實體安全事件做好準備，確保員工的安全，並且減低衝擊對營運造成的影響。

3

新頒布的法令與法規在短期內並未被組織視為重大的挑戰。但是隨著 GDPR 將於 2018 年 5 月實施，監管議題似乎也將在不久的將來開始影響到各組織。進行完善的地平線掃描分析，絕對有助於專業人員瞭解未來的威脅樣貌。

4

潛在的全球大流行疾病被視為長期議題。然而，近期西非的伊波拉 (Ebola) 病毒與肆虐南美洲的茲卡 (Zika) 病毒 顯示出這類威脅已經出現，並且可能持續存在，因為過去 60 年來，病數量每 10 年就增加 4 倍 [20]。

5

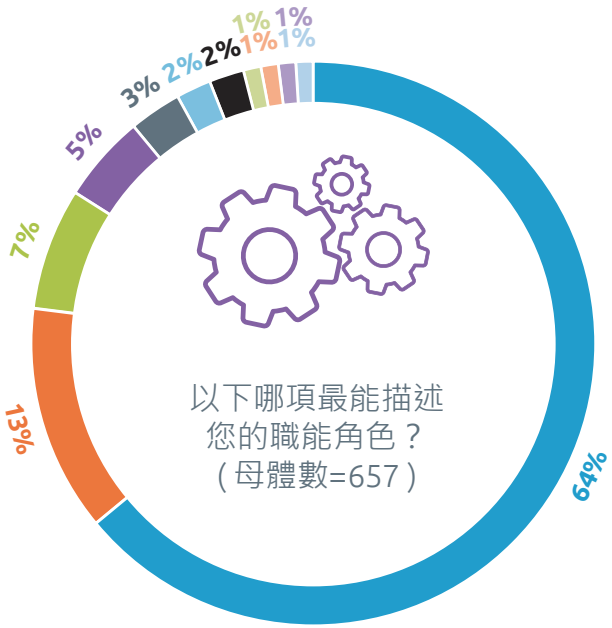
越來越多專業人員已經體認到營運持續計畫的優點。採用 ISO 22301 的人數持續增加，對於營運持續管理計畫的投資也是如此。此外，組織採用並且深耕營運持續計畫的時間越久，便越能維持對此計畫的資源投入，顯示出兩者存在正相關的關係。

20 time.com/4766624/next-global-security/

4 附錄

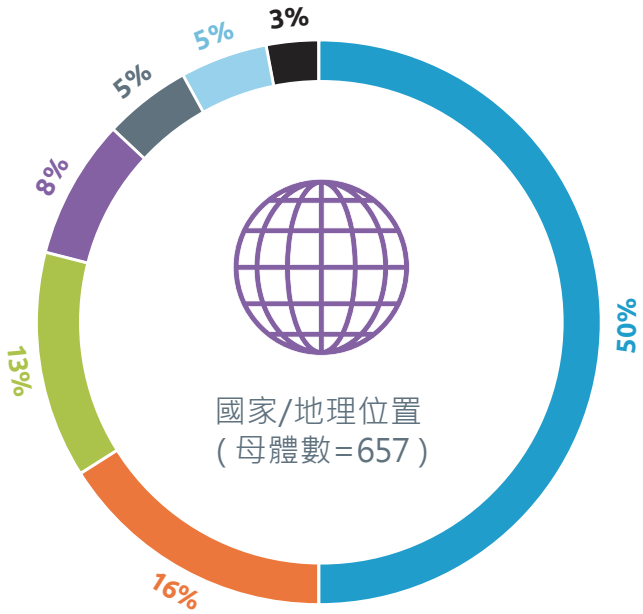
1. 人口統計資訊

a. 受訪者的職能角色



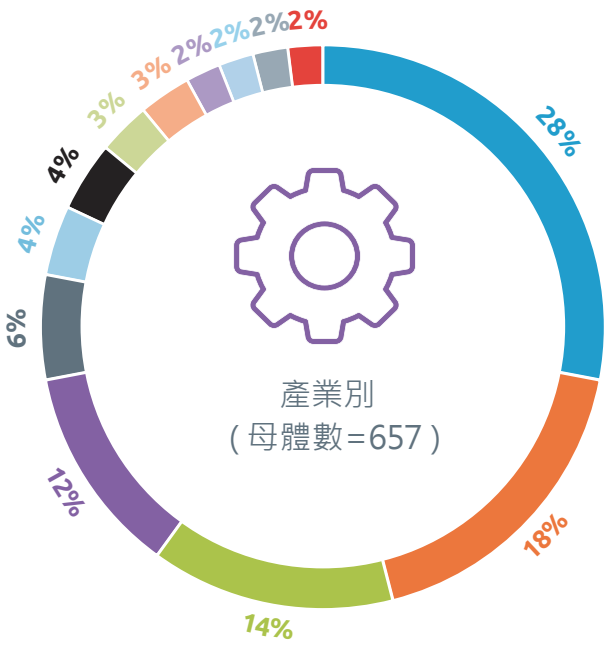
- **64%** 營運持續
- **13%** 風險管理
- **7%** IT 災難復原/ IT 服務持續性
- **5%** 緊急應變規劃
- **3%** 品質 / 營運改善
- **2%** 安全 (實體 / 虛擬)
- **2%** 內部稽核
- **1%** 職業安全與衛生管理
- **1%** 供應鏈 / 物流 / 採購 / 採購顧問
- **1%** 營運 / 服務之高階管理者
- **1%** 供應鏈 / 物流 / 採購 / 採購顧問

b. 地理分佈



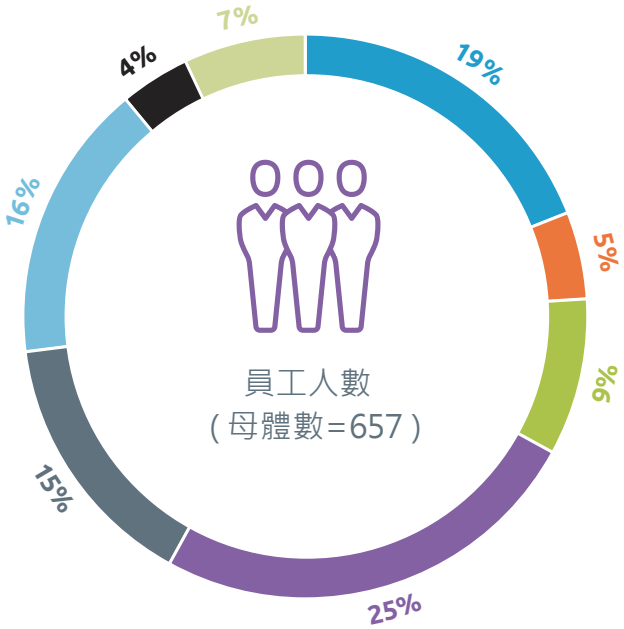
- **50%** 歐洲
- **16%** 北美洲
- **13%** 亞洲
- **8%** 澳大拉西亞
- **5%** 薩哈拉以南的非洲地區
- **5%** 中東與北非 (MENA)
- **3%** 中美及拉丁美洲 (CALA)

c. 產業別



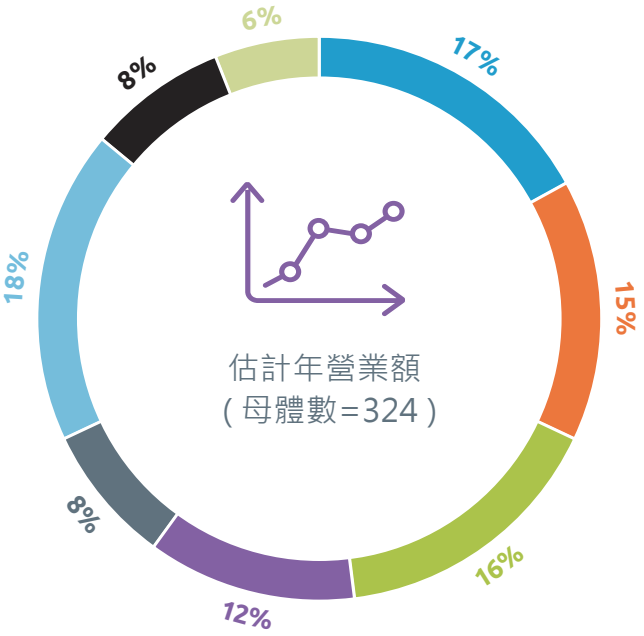
- **28%** 金融與保險服務
- **18%** 專業服務
- **14%** 資訊與通訊
- **12%** 公共行政與國防 (例如：地方/ 中央政府及緊急應變機構)
- **6%** 健康與社會照護
- **4%** 能源與公共事業服務
- **4%** 製造
- **3%** 運輸與倉儲
- **3%** 零售與批發
- **2%** 教育
- **2%** 媒體與娛樂
- **2%** 支援服務
- **2%** 工程與建築

d. 員工人數



- **19%** 0 - 250
- **5%** 251 - 500
- **9%** 501 - 1,000
- **25%** 1,001 - 5,000
- **15%** 5,001 - 10,000
- **16%** 10,001 - 50,000
- **4%** 50,001 - 100,000
- **7%** 100,000 以上

e. 估計年營業額



單位：歐元

17% 低於 100 萬	15% 100 萬 - 1000 萬
16% 1100 萬 - 1 億	12% 1.01 億 - 5 億
8% 5.01 億 - 10 億	18% 10 億 - 100 億
8% 110 億 - 500 億	6% 大於 500 億

2. 依地區/國家比較

	歐洲	北美洲	亞洲	大洋洲
前 3 大威脅	1. 網路攻擊 (55%) 2. 資料外洩 (42%) 3. 無預警的資訊與通訊中斷 (36%)	1. 網路攻擊 (53%) 2. 資料外洩 (44%) 3. 無預警的資訊與通訊中斷 (30%)	1. 網路攻擊 (55%) 2. 資料外洩 (44%) 3. 惡劣氣候 (42%)	1. 網路攻擊 (47%) 2. 無預警的資訊與通訊中斷 (43%) 3. 資料外洩 (40%)
前 3 大衝擊	1. 無預警的資訊與通訊中斷 (73%) 2. 公共服務中斷 (45%) 3. 網路攻擊 (40%)	1. 惡劣氣候 (81%) 2. 無預警的資訊與通訊中斷 (56%) 3. 公共服務中斷 (44%)	1. 惡劣氣候 (65%) 2. 無預警的資訊與通訊中斷 (56%) 3. 網路攻擊 (36%)	1. 無預警的資訊與通訊中斷 (85%) 2. 惡劣氣候 (54%) 3. 網路攻擊 (41%)
前 3 大趨勢	1. 使用互聯網進行惡意攻擊 (80%) 2. 新法規和更嚴謹的監管審查 (52%) 3. 社群媒體的影響 (51%)	1. 使用互聯網進行惡意攻擊 (80%) 2. 社群媒體的影響 (54%) 3. 互聯網相關服務的普及和高度採用 (47%)	1. 使用互聯網進行惡意攻擊 (65%) 2. 新法規和更嚴謹的監管審查 (52%) 3. 流失重要員工 (50%)	1. 使用互聯網進行惡意攻擊 (78%) 2. 流失重要員工 (69%) 3. 互聯網相關服務的普及和高度採用 (56%)
已進行趨勢分析	77%	60%	69%	70%
採用 ISO 22301	69%	61%	76%	85%
營運持續計畫投資程度	增加 20% 刪減 8% 持平 58%	增加 33% 刪減 7% 持平 47%	增加 39% 刪減 10% 持平 43%	增加 11% 刪減 26% 持平 57%

	中東和北非	中美洲和拉丁美洲	撒哈拉以南的非洲地區	英國
前 3 大威脅	1. 網路攻擊 (44%) 2. 資料外洩 (34%) 3. 無預警的資訊與通訊中斷 (28%)	1. 網路攻擊 (43%) 2. 資料外洩 (38%) 3. 火災 (33%)	1. 網路攻擊 (37%) 2. 無預警的資訊與通訊中斷 (33%) 3. 資料外洩 (30%)	1. 網路攻擊 (53%) 2. 資料外洩 (39%) 3. 無預警的資訊與通訊中斷 (33%)
前 3 大衝擊	1. 無預警的資訊與通訊中斷 (69%) 2. 網路攻擊 (46%) 3. 公共服務中斷 (38%)	1. 惡劣氣候 (53%) 2. 公共服務中斷 (42%) 3. 無預警的資訊與通訊中斷 (32%)	1. 無預警的資訊與通訊中斷 (60%) 2. 公共服務中斷 (56%) 3. 惡劣氣候 (32%)	1. 無預警的資訊與通訊中斷 (73%) 2. 公共服務中斷 (48%) 3. 惡劣氣候 (39%)
前 3 大趨勢	1. 使用互聯網進行惡意攻擊 (66%) 2. 社群媒體的影響 (59%) 3. 流失重要員工 (50%)	1. 使用互聯網進行惡意攻擊 (61%) 2. 新法規和更嚴謹的監管審查 (56%) 3. 社群媒體的影響 (56%)	1. 使用互聯網進行惡意攻擊 (68%) 2. 政局變化 (64%) 3. 社群媒體的影響 (48%)	1. 使用互聯網進行惡意攻擊 (80%) 2. 社群媒體的影響 (54%) 3. 流失重要員工 (51%)
已進行趨勢分析	66%	65%	77%	76%
採用 ISO 22301	79%	54%	72%	70%
營運持續計畫投資程度	增加 38% 刪減 13% 持平 41%	增加 33% 刪減 22% 持平 33%	增加 21% 刪減 13% 持平 50%	增加 20% 刪減 7% 持平 58%

	美國	加拿大	澳洲	印度
前 3 大威脅	1. 網路攻擊 (58%) 2. 資料外洩 (48%) 3. 無預警的資訊與通訊中斷 (30%)	1. 網路攻擊 (41%) 2. 無預警的資訊與通訊中斷 (32%) 3. 資料外洩 (32%)	1. 網路攻擊 (46%) 2. 資料外洩 (43%) 3. 無預警的資訊與通訊中斷 (43%)	1. 網路攻擊 (63%) 2. 惡劣氣候 (50%) 3. 資料外洩 (48%)
前 3 大衝擊	1. 惡劣氣候 (77%) 2. 無預警的資訊與通訊中斷 (50%) 3. 公共服務中斷 (35%)	1. 惡劣氣候 (94%) 2. 無預警的資訊與通訊中斷 (78%) 3. 公共服務中斷 (72%)	1. 無預警的資訊與通訊中斷 (91%) 2. 惡劣氣候 (57%) 3. 網路攻擊 (46%)	1. 惡劣氣候 (69%) 2. 無預警的資訊與通訊中斷 (55%) 3. 社會動盪 / 內亂 (35%)
前 3 大趨勢	1. 使用互聯網進行惡意攻擊 (81%) 2. 互聯網相關服務的普及和高度採用 (51%) 3. 社群媒體的影響 (51%)	1. 使用互聯網進行惡意攻擊 (75%) 2. 氣候變遷 (65%) 3. 社群媒體的影響 (65%)	1. 使用互聯網進行惡意攻擊 (76%) 2. 流失重要員工 (65%) 3. 社群媒體的影響 (56%)	1. 使用互聯網進行惡意攻擊 (65%) 2. 新法規和更嚴謹的監管審查 (53%) 3. 流失重要員工 (53%)
已進行趨勢分析	59%	64%	71%	67%
採用 ISO 22301	66%	46%	89%	81%
營運持續計畫投資程度	增加 34% 刪減 8% 持平 42%	增加 27% 刪減 5% 持平 59%	增加 14% 刪減 29% 持平 54%	增加 36% 刪減 4% 持平 51%

3. 依產業別比較

	金融與保險服務	專業服務	公共行政與國防	資訊與通訊
前 3 大威脅	1. 網路攻擊 (62%) 2. 資料外洩 (54%) 3. 無預警的資訊與通訊中斷 (48%)	1. 網路攻擊 (42%) 2. 資料外洩 (35%) 3. 無預警的資訊與通訊中斷 (22%)	1. 網路攻擊 (45%) 2. 資料外洩 (38%) 3. 無預警的資訊與通訊中斷 (34%)	1. 網路攻擊 (58%) 2. 資料外洩 (47%) 3. 無預警的資訊與通訊中斷 (35%)
前 3 大衝擊	1. 無預警的資訊與通訊中斷 (75%) 2. 惡劣氣候 (53%) 3. 網路攻擊 (39%)	1. 無預警的資訊與通訊中斷 (63%) 2. 公共服務中斷 (44%) 3. 惡劣氣候 (40%)	1. 無預警的資訊與通訊中斷 (78%) 2. 惡劣氣候 (52%) 3. 公共服務中斷 (48%)	1. 無預警的資訊與通訊中斷 (58%) 2. 惡劣氣候 (51%) 3. 網路攻擊 (45%)
前 3 大趨勢	1. 使用互聯網進行惡意攻擊 (78%) 2. 新法規和更嚴謹的監管審查 (58%) 3. 社群媒體的影響 (55%)	1. 使用互聯網進行惡意攻擊 (70%) 2. 社群媒體的影響 (49%) 3. 流失重要員工 (44%)	1. 使用互聯網進行惡意攻擊 (84%) 2. 流失重要員工 (63%) 3. 社群媒體的影響 (49%)	1. 使用互聯網進行惡意攻擊 (82%) 2. 新法規和更嚴謹的監管審查 (56%) 3. 流失重要員工 (50%)
已進行趨勢分析	81%	63%	66%	78%
採用 ISO 22301	72%	74%	68%	86%
營運持續計畫投資程度	增加 29% 刪減 7% 持平 60%	增加 24% 刪減 11% 持平 49%	增加 15% 刪減 25% 持平 44%	增加 30% 刪減 8% 持平 54%

	健康與社會照護	製造	零售與批發	能源與公共事業服務
前 3 大威脅	1. 網路攻擊 (62%) 2. 無預警的資訊與通訊中斷 (54%) 3. 資料外洩 (38%)	1. 網路攻擊 (41%) 2. 供應鏈中斷 (41%) 3. 產品品質事件 (41%)	1. 網路攻擊 (60%) 2. 資料外洩 (33%) 3. 無預警的資訊與通訊中斷 (27%)	1. 網路攻擊 (62%) 2. 資料外洩 (46%) 3. 無預警的資訊與通訊中斷 (42%)
前 3 大衝擊	1. 無預警的資訊與通訊中斷 (70%) 2. 網路攻擊 (51%) 3. 公共服務中斷 (49%)	1. 供應鏈中斷 (52%) 2. 惡劣氣候 (48%) 3. 公共服務中斷 (43%)	1. 無預警的資訊與通訊中斷 (87%) 2. 惡劣氣候 (60%) 3. 人才 / 關鍵技術的取得 (53%)	1. 惡劣氣候 (56%) 2. 無預警的資訊與通訊中斷 (56%) 3. 公共服務中斷 (44%)
前 3 大趨勢	1. 使用互聯網進行惡意攻擊 (71%) 2. 社群媒體的影響 (66%) 3. 流失重要員工 (46%)	1. 使用互聯網進行惡意攻擊 (75%) 2. 供應鏈複雜度提升 (70%) 3. 新法規和更嚴謹的監管審查 (60%)	1. 使用互聯網進行惡意攻擊 (73%) 2. 流失重要員工 (67%) 3. 供應鏈複雜度提升 (60%)	1. 使用互聯網進行惡意攻擊 (84%) 2. 流失重要員工 (48%) 3. 潛在的全球大流行疾病 (44%)
已進行趨勢分析	64%	73%	86%	77%
採用 ISO 22301	68%	58%	35%	74%
營運持續計畫投資程度	增加 31% 刪減 6% 持平 42%	增加 29% 刪減 10% 持平 57%	增加 13% 刪減 13% 持平 60%	增加 19% 刪減 15% 持平 54%

4. 依營運規模比較

	中小型企業 (SMEs)	大型企業
前 3 大威脅	1. 網路攻擊 (35%) 2. 資料外洩 (29%) 3. 無預警的資訊與通訊中斷 (24%)	1. 網路攻擊 (57%) 2. 資料外洩 (45%) 3. 無預警的資訊與通訊中斷 (39%)
前 3 大衝擊	1. 無預警的資訊與通訊中斷 (57%) 2. 公共服務中斷 (41%) 3. 惡劣氣候 (32%)	1. 無預警的資訊與通訊中斷 (69%) 2. 惡劣氣候 (53%) 3. 公共服務中斷 (43%)
前 3 大趨勢	1. 使用互聯網進行惡意攻擊 (71%) 2. 流失重要員工 (49%) 3. 社群媒體的影響 (45%)	1. 使用互聯網進行惡意攻擊 (78%) 2. 新法規和更嚴謹的監管審查 (52%) 3. 社群媒體的影響 (52%)
已進行趨勢分析	55%	76%
採用 ISO 22301	68%	70%
營運持續計畫投資程度	增加 23% 刪減 6% 持平 55%	增加 26% 刪減 12% 持平 52%

作者介紹

Gianluca Riglietti CBCI
(BCI 研究與洞察經理)

Gianluca 畢業於倫敦國王學院，取得地緣政治、領土與安全的碩士學位，曾為擔任歐盟理事會主席的義大利總理工作。他具備撰寫學術與產業刊物的經驗，並且在國際論壇發表，亦替 BSI、Everbridge 與 Transputec 等企業進行專案工作。

他的聯絡方式 gianluca.riglietti@thebci.org

Lucila Aguada
(BCI 研究與洞察分析員)

Lucia 擁有計量心理學專家執照，專精於量化與質化研究，為菲律賓大學心理學準碩士。她協助非營利機構、製藥與健康照護客戶進行研究，同時也是一名合格教師，擁有 7 年以上的經驗，專精於兒童與特殊教育。

她的聯絡方式 lucila.aguada@thebci.org

致謝

BCI 感謝 BSI 連續 7 年支持此項研究。

關於 英國營運持續協會 (BCI)

英國營運持續協會 (BCI) 成立於 1994 年，旨在打造適應力佳、復原力強的世界；創立至今，已成為協助各企業維持營運持續與打造組織韌性的國際性領導協會。BCI 也是營運持續與組織韌性運作專家心目中的首選會員認證組織，在全球超過 100 個國家 / 地區擁有 8,000 名以上的會員，估計來自 3,000 個私人、公家與第三方部門組織。

BCI 擁有廣大的會員與合作夥伴關係網路，提供各種不同的體驗服務，包括世界級的教育課程、持續性的專業進修以及交流活動。每年有超過 1,500 人選擇參加 BCI 訓練課程，課程內容從認知提升工具的應用，到完整學位資格的取得，皆提供線上與課堂進修管道。

BCI 擁有卓越的韌性建置專業能力與全球知名的認證標準，能夠提供技術與專業能力保證。BCI 為尋求提升組織韌性的專業人士提供各種不同資源；此外也透過見多識廣的領導團隊與研究計劃協助促進產業提升。BCI 在全球擁有約 120 名合作夥伴，各企業可與本協會攜手合作，一同努力推廣營持續與組織韌性的最佳實務。

BCI 歡迎任何對組織韌性工作有興趣的人士，無論您是新手、經驗老道的專家或各行各業的企業組織，我們都竭誠歡迎您加入我們的行列。

聯絡 BCI

Marianna Pallini
Communications Executive, 10-11 Southview Park
Marsack Street, Caversham, RG45AF, United Kingdom
+44 118 947 8215 | research@thebci.org

關於 英國標準協會 (BSI)

英國標準協會 (BSI) 為全球性機構，專門提供企業必要的解決方案，將最佳標準實務轉換成卓越的日常表現。

BSI 成立於 1901 年，為全球第一個國家標準機構，也是國際標準組織 (ISO) 的創始會員。BSI 影響力跨足航太、汽車、營造、食品、金融、健康照護、IT、及零售等產業等。BSI 與全球 181 個國家超過 85,000 位客戶合作，BSI 制定的各種標準帶動了全球卓越發展。

成立一世紀以來，BSI 持續協助全球企業進行改革，國際上多數採用 BSI 所創始之標準，來協助客戶穩定成長、妥善管理並降低風險、並且更具韌性。

請造訪 bsigroup.tw 瞭解更多資訊

關於 BSI 訓練學苑

BSI 訓練學苑講師團隊每位均累積了豐富的稽核及講師經驗，並取得國際認可。BSI 身為百年國家標準制定機構，經驗及知識的累積，是無與倫比的。在營運持續方面的課程，目前已規劃了 BS 10012 個人資訊管理系統、ISO/IEC 27001 資訊安全管理系統、ISO/IEC 20000 IT 服務管理系統及 ISO 22301 營運持續管理系統。

企業組織可依據員工執掌內容，安排課程做完整的訓練規劃，以培養並提升員工在風險管控與建構組織韌性的能力。進一步開課日期，可連絡 BSI 訓練學苑 training.taiwan@bsigroup.com 或來電洽詢。

聯絡 BSI

簡慧伶 (Julia Chien)
行銷部協理 BSI台灣分公司
台北市內湖區基湖路39號5樓
+886 (0)2 2656 0333 | julia.chien@bsigroup.com

Business Continuity Institute

Business Continuity Institute

10-11 Southview Park, Marsack Street,
Caversham, Berkshire, UK, RG4 5AF

bci@thebci.org
www.thebci.org

bsi.