資通安全管理之資訊揭露

一、資通安全管理策略與架構：

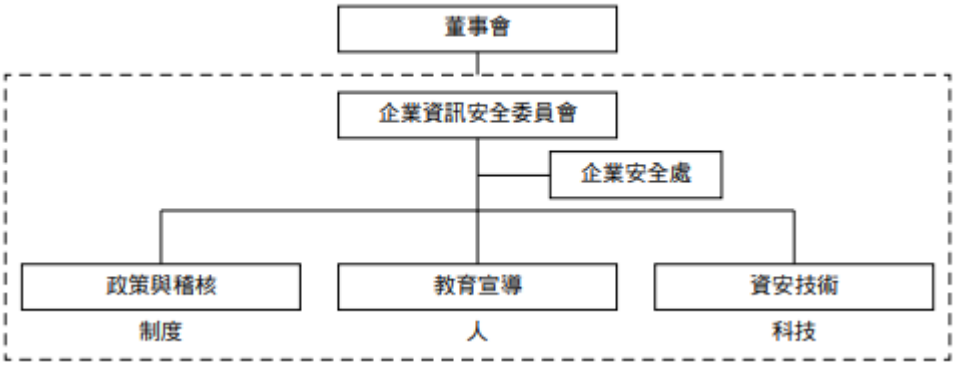
敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。(法規依據：年報準則第 18 條第 6 款第 1 目)

範例一：

（一） 資通安全風險管理架構

X 公司在民國九十二年成立「企業資訊安全委員會」負責執行資訊作業安全管理規劃，建置與維護資訊安全管理體系，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核。企業資訊安全委員會由總經理擔任主席，並由數位功能組織 A 副總經理擔任督導暨資訊安全長，公司內各單位（包含法務、人力資源、研發、工程、生產等）主管均為委員會成員；另也成立了「企業安全處」，專責公司資訊安全及實體安全規劃與相關的稽核事項，亦主導此委員會運行。

企業資訊安全委員會透過每半年管理審查會議，審核資安風險分析結果及 X 公司採取對應的防護措施與方策，確保資訊安全管理體系持續運作的適用性、適切性及有效性。委員會每年向董事會彙報資安管理成效及資安策略方向，由具有資安領域相關背景的 B 獨立董事督導資訊安全及網路安全策略，定期檢討修正。B 獨董曾任 OO 部長及 OO 協會理事長，於任內領導多項資安專案，包括 OO 會報擔任副召集人及 OO 委員會發起及成立計畫。



（二） 資通安全政策

X 公司的資訊安全政策涵蓋本公司及海內外子公司，是以「一、建立符合法規與客戶需求之資訊安全管理規範；二、透過全員認知，達成資訊安全人人有責的共識；三、保護公司與客戶資訊的機密性、完整性與可用性；四、提供安全的生產環境，確保公司業務之永續營運」為指導準則。並以防毒、防駭、防漏三大資安防護主軸為目標，建立防火牆、入侵偵測、防毒系統及諸多內控系統，以提升公司在防禦外部攻擊以及確保內部機密資訊防護的能力。

X 公司已導入並建立完整的資訊安全管理系統（ISMS, Information Security Management System），從系統面、技術面、程序面降低企業資安威脅，建立符合客戶需求的資訊安全保護環境，並不斷地進行「計劃－實施－查核－行動」（PDCA, Plan-Do-Check-Act）循環以持續改善。

「計劃階段」著重資安風險管理，為了強化資訊安全，X 公司自民國九十六年導入 ISO27001 資訊安全管理體系的認證，使資訊系統皆能在標準的管理規範下運作，降低因人為疏失所造成的安全漏洞及生產異常，也透過年度的複審作業，不斷持續改善。另在民國一〇三年公司決定投入 ISO15408 共通準則認證，這是一個特別針對生產安全產品的認證，不但注重安全產品在接收、處理及銷毀等安全程序，也對實體門禁管制有很高的要求，以達到生產全線之安全目的。相關認證訊息詳公司網站 https://www.XXX.com。

「執行階段」建構多層資安防護機制，持續導入新資安風險控管技術，以智慧化／自動化機制提升各類資安事件之偵測及回應處理程序的效率，並強化資訊安全及網路安全保護流程，以維護公司重要資產的防護。

「查核階段」定期監控資安管理指標成效，及上述管理系統每年第三方複審稽核，另委由知名的資安廠商進行滲透測試，以確保持續提升資安管理及防禦能力。

「行動階段」檢討與持續改善，當員工及承商違反資安相關規範及程序時，依據規定進行懲處，並持續進行全員資安教育訓練以提升資安意識。

（三） 具體管理方案

為達資安政策與目標，建立全面性的資安防護，推行的管理事項及具體管理方案如下：

- 提升資安防禦能力：定期進行資安系統脆弱度分析及滲透測試，並加以補強與修護，以降低資安風險。建立網路安全事件應變計畫，依事件嚴重度等級進行影響和損失評估，採取對應的通報及復原行動。

- 精進資安管理程序：不斷強化資安防禦能力外，在管理程序及意識認知上也須並重。依據 NIST（National Institute of Standards and Technology）標準建立企業資安框架，設置對應的度量指標。員工應遵守資安規定（如嚴格管制行動儲存裝置）、遵循 SOP 作業，並不斷地進行 PDCA 循環以持續改善。

- 增進網路、端點及應用安全：提升端點設備的異常偵測及防護能力，包含應用程式白名單（Application Whitelisting）機制與端點偵測與回應（EDR, Endpoint Detection and Response）機制。整體資訊系統網路安全區域優化，增加重要主機特權帳號登入多因子認證防護。

- 法令遵循及導入國際資安認證標準：X 公司已符合資訊安全相關的 ISO27001、ISO15408、ISO22301 及美國沙氏法案（Sarbanes-Oxley Act, SOX404）等認證標準及法規，作為達成各項風險管理的方法與檢驗依據。公司內部亦成立對應的風險管理委員會，專責推動各項標準化作業，降低生產營運的風險。

- 風險控制：與國際資安大廠合作，透過其專業服務進行整體資安體檢，以公正第三方驗證之客觀結果，作為進階資安強化的依據。X 公司已投保資安險作為企業解決資安威脅風險

的方法之一，保護公司於發生網路攻擊時，能將潛在損失降至最小的範圍。

- 教育訓練：進行全員資安教育訓練與不定期社交工程釣魚郵件測試，以提升資安意識，使資安的運作在高階主管與各部門的支持下，落實到每一位員工身上。
- 疫情管制：因應全球 COVID-19 疫情，強化在家工作（WFH）的防毒駭及資訊安全保護措施，宣導勿使用公共電腦與網路作為工作使用，善盡保護公司資訊之責任。

（四） 投入資通安全管理之資源

資訊安全已為公司營運重要議題，對應資安管理事項及投入之資源方案如下：

- 專責人力：設有專職之企業組織「企業安全處」，負責公司資訊安全規劃、技術導入與相關的稽核事項，以維護及持續強化資訊安全。
- 認證：通過 ISO27001 資訊安全認證及 ISO15408 廠區認證，相關資安稽核無重大缺失。
- 客戶滿意：無重大資安事件，無違反客戶資料遺失之投訴案件。
- 教育訓練：所有新進員工到職前皆完成資訊安全教育訓練課程；全體員工皆完成兩次線上資訊安全教育訓練及考核；年度共計執行四次社交工程釣魚郵件測試。
- 資安公告：製作超過十份資安公告，傳達資安防護重要規定與注意事項。
- 供應鏈：所有新進承商均完成 X 公司資安規定之教育訓練。
- 資安險：X 公司自民國一〇八年起每年投保資安險，作為面對資安威脅之風險管理解決方案之一，保額為一千萬美元。

範例二：

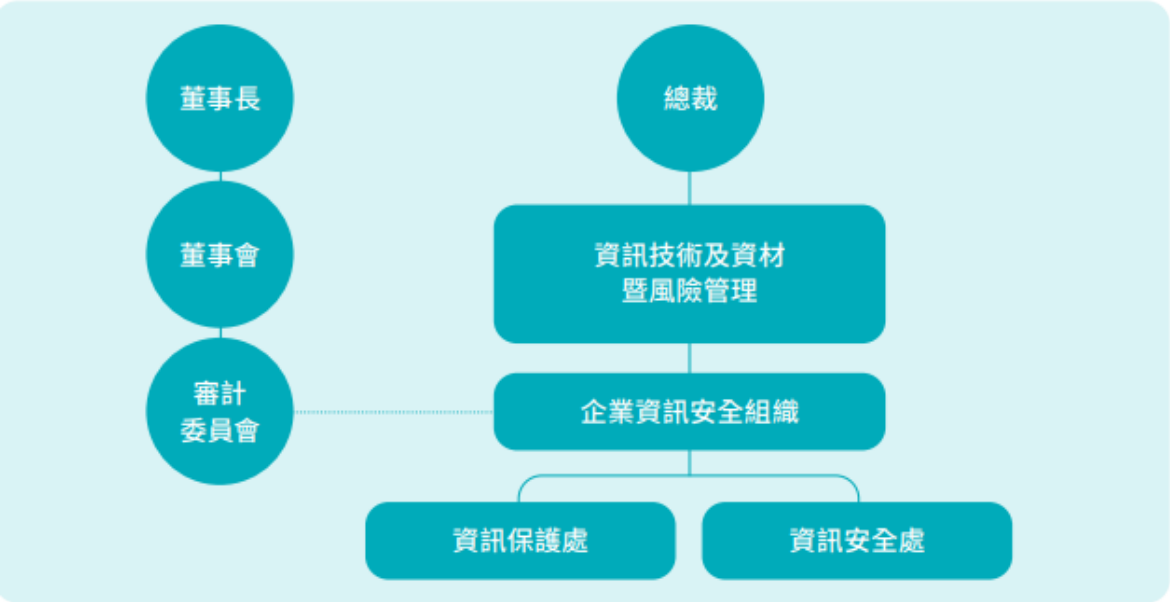
（一） 資通安全風險管理架構

1. 企業資訊安全治理組織

Y 公司民國 XX 年設立「企業資訊安全組織」，下轄資訊安全處與資訊保護處，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核，由企業資訊安全組織最高主管每半年向董事會審計委員會彙報資安管理成效、資安相關議題及方向。Y 公司審計委員會肩負監督治理企業資訊安全之責，由具有資安領域相關背景的審計委員 A 監督評核 Y 公司資訊與網路安全管理機制及方向。

Y 公司為執行企業資訊安全組織訂定的資安策略，確保內部遵循資安相關準則、程序與法規，特別成立「Y 公司專屬資訊保護委員會」，由資訊技術及資材暨風險管理資深副總經理擔任主席，法務、人力資源、研究發展、營運組織副總經理擔任委員會成員，並設置企業資訊安全組織最高主管為執行秘書、內部稽核最高主管為觀察員，每季召開會議，檢視及決議資訊安全與資訊保護方針及政策，落實資訊安全管理措施的有效性。

2. Y 公司企業資訊安全組織架構



3. Y 公司專屬資訊保護委員會架構

（二） 資通安全政策

1. 企業資訊安全管理策略與架構

企業資訊安全組織為有效落實資安管理，透過涵蓋台灣廠區與海外子公司各單位的「資訊保護工作推動團隊」，每月召開例行會議，依據規畫、執行、查核與行動（Plan-Do-Check-Act, PDCA）的管理循環機制，檢視資訊安全政策適用性與保護措施，並定期與專屬資訊保護委員會回報執行成效。

「規畫階段」著重資安風險管理，建立完整的資訊安全管理系統（Information Security Management System, ISMS)，推動各廠區持續通過國際資安管理系統認證（ISO/IEC27001、ISO/IEC15408），從系統面、技術面、程序面降低企業資安威脅，建立符合客戶需求、最高規格的機密資訊保護服務。「執行階段」則建構多層資安防護，持續導入將資安防禦創新技

術，將資安控管機制整合內化於軟硬體維運、供應商資安管理等平日作業流程，系統化監控資訊安全，維護 Y 公司重要資產的機密性、完整性及可用性。「查核階段」積極監控資安管理成效，依據查核結果進行資安指標衡量及量化分析，並透過定期模擬演練資安攻擊進行資訊安全成熟度評鑑。「行動階段」則以檢討與持續改善為本，落實監督、稽核確保資安規範持續有效；當員工違反相關規範及程序時，依據資安違規處理流程進行處置，並視違規情節進行人事處分（包括員工當年度考績或採取必要的法律行動）；此外，亦依據績效指標及成熟度評鑑結果，定期檢討及執行包含資訊安全措施、教育訓練及宣導等改善作為，確保 Y 公司重要機密資訊不外洩。

2. 企業資訊安全風險管理與持續改善架構

（三） 具體管理方案

多層資安防護

網路安全
- 導入先進技術執行電腦掃描及系統與軟體更新
- 強化網路防火牆與網路控管，防止電腦病毒跨機台及跨廠區擴散

裝置安全
- 建置機台入廠掃毒機制，防止內含惡意軟體的機台進入公司
- 依電腦類型建置端點防毒措施，強化惡意軟體行為偵測

應用程式安全
- 制定開發流程應用程式安全自檢表、評核標準及改善目標
- 持續強化應用程式安全控管機制，並整合於開發流程及平台

供應鏈資訊安全
- 建構供應商資安保護自我檢核機制
- 定期傳達　　公司最新的資安規定及注意事項

資料安全保護技術強化
- 開發先進資訊保護工具，藉由資料標籤加強文件機密分類及資料保護
- 文件及資料加密控管及有效追蹤
- 郵件外寄控管

檢討與持續改善

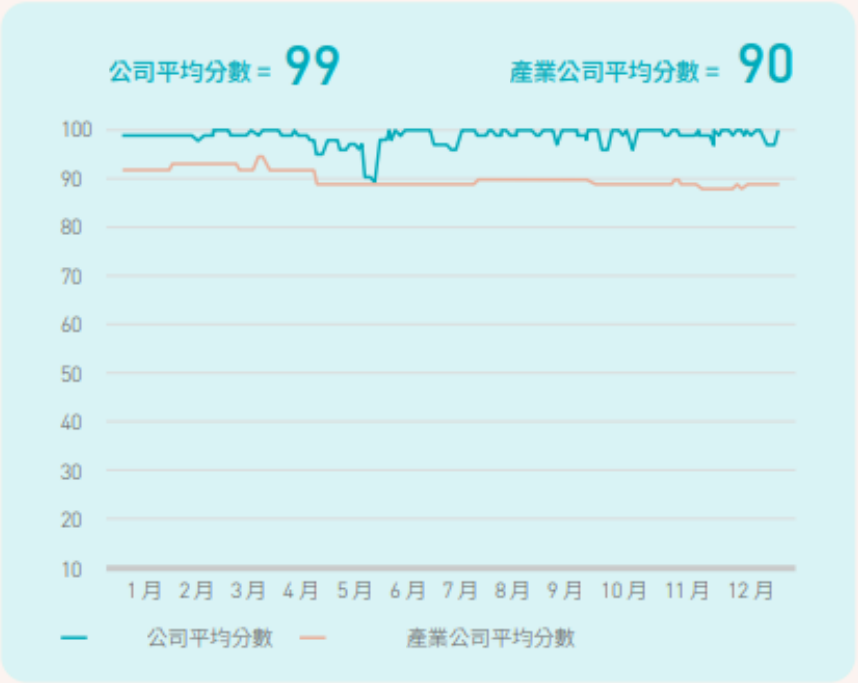
教育訓練與宣導
- 加強員工對郵件社交工程攻擊的警覺性，執行釣魚郵件防禦偵測
- 定期舉辦員工辨識能力演練，提升員工資安意識

資安成效監控

資安成熟度評鑑

- 委託外部專家（包括資訊安全稽核組織、網路資安風險評核機構）定期執行公司網路與資訊安全評鑑
- 整合第三方驗證之客觀結果與威脅情資，進行風險分析，資安管理體制進階強化

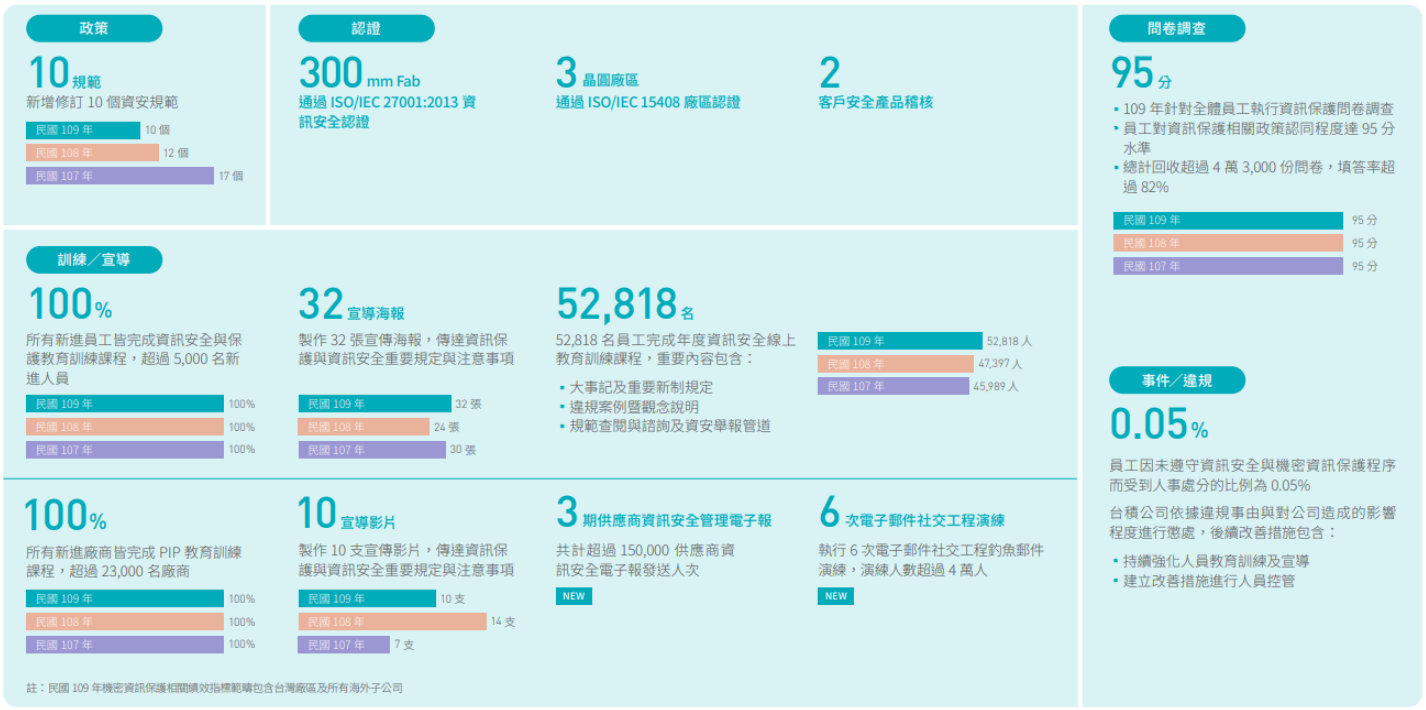
民國　　年　　公司資安體檢第三方評核結果



民國　　年，　　公司通過資安相關稽核無重大缺失，亦無違反資訊安全、造成客戶資訊洩漏及罰款等重大資安事件發生。此外，不論是由第三人或主管機關因為　　公司違反客戶個人資料保護或客戶資料遺失而向公司投訴，並且導致司法行動之投訴案件數為零。

（四） 投入資通安全管理之資源

民國 XX 年企業資訊安全措施推動執行成果



二、重大資通安全事件：

列明最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實。(法規依據：年報準則第 18 條第 6 款第 2 目)

範例一：

X 公司於民國 XX 年度未有重大資安事件之發生。近年來較為重大的資安事件為民國 XX 年發生的勒索病毒（Wanna Cry）事件，計有 42 台在 OA 區使用的 Server／PC／NB 受到感染而需重置，所幸因為及早發現及處置得當，並未擴展到產線電腦。公司除了立即更新以行為偵測的新版防毒軟體外，並落實資訊設備攜入之管理，也制定產線電腦須更新重大安全修補程式，以強化對此類攻擊系統漏洞的蠕蟲型病毒的防禦能力。在產線網路則設定存取控制清單（ACL, Access Control List），一旦發生病毒感染，也能將影響侷限在較小的範圍而不致於大幅擴散。

X 公司也在民國 XX 年加入半導體產業協會資安工作小組，共同研討制定機台電腦的安全性標準，善盡在地企業捍衛資安的責任。

以資安業界的一句名言作為補充說明：「There is no such thing as 100% security.」。當新的攻擊手法不斷翻新且防禦體系面臨有時間差的系統風險，過去的防禦成果不代表未來不會發生，企業對於資訊安全的要求也必須與時俱進，面對瞬息萬變且日益增長的資安威脅，資訊安全是一條任重而道遠持續精進的任務。X 公司將秉持著「正實迅慧」的企業文化，善盡資訊安全應當的注意及勤勉盡責之管理責任，提供客戶安全的生產環境，降低公司的營運風險，回饋股東最大的投資價值與利益。

範例二：

Y 公司於民國 X 年 X 月受到電腦病毒感染，影響部分電腦系統及廠房機台，致相關生產亦受波及。此次病毒感染的原因為內含 Y 公司未知的惡意軟體之新機台在○○員工安裝的過程中操作失誤。Y 公司網路防火牆亦未能有效地防止病毒擴散。雖然資料的完整性和機密資訊皆未受到影響，此次電腦病毒感染造成出貨延誤，本公司已於 X 年第 X 季認列電腦病毒感染相關損失新台幣 X 元（美金 X 元），帳列營業成本項下。Y 公司已採取改善措施，例如實施自動化系統以防止安裝無保護的機台；強化網路防火牆與網路控管以防止電腦病毒跨機台及跨廠區擴散；進一步

改進Y公司惡意軟體防護的措施也已在進行中。Y公司已額外編列適當的預算強化資訊技術安全，但仍無法保證公司免於惡意軟體的攻擊。

三、資通安全風險與因應措施：

科技改變（包括資通安全風險）及產業變化對公司財務業務之影響及因應措施。(法規依據：年報準則第20條第6款第5目)

範例一：

依據民國一一〇年世界經濟論壇風險報告，「網路安全失效（Cybersecurity failure）」列為關鍵科技風險。因網路安全失效而對網路攻擊（Cyber Attack）防禦能力不足，不僅可能使公司暴露於資料外洩及勒索風險外，更可能面臨生產系統中斷而造成嚴重營運損失，影響企業的優良商譽。許多全球與知名企業因發生勒索病毒事件造成重大損失，面對外部日新月異且多樣化的威脅，企業資安強化刻不容緩，如何運用有限資源，正確應對多變環境是一項重要的任務。

X公司在民國XX年成立「企業風險管理委員會」，協同公司內風險管控之關鍵組織，管理公司內外部風險。依照公司企業風險管理委員會管理流程，評估資安相關風險等級並採取應對風險管理方案及定期檢討。

X公司特別重視資安與網路風險之防範，故建構了一套完整的多層次防禦網，由外而內包含防火牆、入侵偵測、防毒系統、弱點掃描及修補程式管理等，並定期委由知名的資安廠商進行滲透測試，以確保持續提升資安防禦能力。在民國XX年也再次與國際資安大廠合作，透過其專業服務進行整體資安體檢，以公正第三方驗證之客觀結果，作為進階資安強化的依據。茲節錄該資安體檢評量總結為：「整體而言，X公司已落實資訊安全管理制度，依照現有的管理制度及控制措施，病毒、木馬及蠕蟲等傳統的惡意程式及傳統的駭客外部攻擊不易對X公司的資訊系統造成損害。」

有鑑於台灣及全球近年來資料外洩、病毒感染及駭客入侵的事件頻傳，造成重大的營運中斷損失（BI ,Business Interruption），資安威脅已然變本加厲。企業資安防護做得好，也無法保證不會成為受攻擊的目標。X公司自民國XX年起每年投保資安險作為面對資安威脅之風險管理解決方案之一，於民國XX年X月生效並追溯可能已潛伏在公司內的攻

擊，包括台灣、新加坡及日本所有廠區為承保範圍，保額為一千萬美元，保護公司於發生網路攻擊時，能將潛在損失降至最小的範圍。

範例二：

Y 公司已建立全面的網路與電腦相關資安防護措施，但無法保證其控管或維持公司製造營運及會計等重要企業功能之電腦系統能完全避免來自任何第三方癱瘓系統的網路攻擊。這些網路攻擊以非法方式入侵 Y 公司的內部網路系統，進行破壞公司之營運及損及公司商譽等活動。在遭受嚴重網路攻擊的情況下，Y 公司的系統可能會失去公司重要的資料，生產線也可能因此停擺。Y 公司透過持續檢視和評估其資訊安全規章及程序，以確保其適當性和有效性，但不能保證公司在瞬息萬變的資訊安全威脅中不受推陳出新的風險和攻擊所影響。網路攻擊也可能企圖竊取公司的營業祕密及其他機密資訊，例如客戶或其他利害關係人的專有資訊以及 Y 公司員工的個資。

惡意的駭客亦能試圖將電腦病毒、破壞性軟體或勒索軟體導入 Y 公司的網路系統，以干擾公司的營運、對 Y 公司進行敲詐或勒索，取得電腦系統控制權，或窺探機密資訊。這些攻擊可能導致公司因延誤或中斷訂單而需賠償客戶的損失；或需擔負龐大的費用實施補救和改進措施，以加強公司的網路安全系統；也可能使 Y 公司因涉入公司對其有保密義務之員工、客戶或第三方資訊外洩而導致的相關法律案件或監管調查，而承擔重大法律責任。

Y 公司過去曾經因購買及安裝內含惡意軟體的設備而遭受攻擊，未來也可能面臨類似的攻擊。為了預防及降低此類攻擊所造成的傷害，Y 公司落實相關改進措施並持續更新，例如建置機台入廠掃毒機制以防止內含惡意軟體的機台進入公司；強化網路防火牆與網路控管以防止電腦病毒跨機台及跨廠區擴散；依電腦類型建置端點防毒措施；導入先進的解決方案以偵測與處理惡意軟體；設計開發資安強化個人電腦供員工使用；設計開發雲端應用安全政策；導入新技術加強資料保護；加強釣魚郵件偵測；建立一個整合的自動化資安維運平台，並定期執行員工警覺性測試及委託外部專家執行資安評鑑。雖然 Y 公司持續加強資訊安全防護措施，但仍無法保證公司免於惡意軟體及駭客攻擊。

此外，Y 公司需要分享高度敏感及機密的資訊給部分其雇用提供 Y 公司及其全球關係企業服務的第三方廠商，以使其能提供相關服務。儘管

Y 公司在和第三方服務廠商簽訂之服務合約中，要求其遵守保密及／或網路安全規定，但不能保證每個第三方服務廠商都將嚴守這些義務。由上述服務廠商及／或其承攬商所維護的內部網路系統及外部雲端運算網路（例如伺服器），亦會有遭受網路攻擊的風險。若 Y 公司或其服務廠商無法及時解決這些網路攻擊所造成的技術性問題，或確保 Y 公司（及屬於本公司客戶或其他第三方）的數據完整性及可用性，或控制住公司或其服務廠商的電腦系統，皆可能嚴重損及 Y 公司對客戶和其他利害關係人的承諾，而公司營運成果、財務狀況、前景及聲譽亦可能因此遭受重大不利影響。