# 企業使用雲端的5個安全提示

對組織而言，安全性是現今不容忽視的重要議題，在今年的「2017 歐洲資訊安全科技展（Infosecurity Europe 2017）」，雲端安全也是受到熱烈討論的主題。由於網路攻擊的複雜性與頻率日漸增高，企業紛紛尋求保護自己的新方法。運用雲端的企業數量已達空前之多，一般普遍認為網路攻擊也比其他平台所造成的影響層面更為廣泛。因此，組織必須針對任何可能的意外狀況預作因應。

## 1 留意針對雲端的勒索軟體

大部份的組織都不知道勒索軟體不僅會讓實體的伺服器停擺，也可能會攻擊雲端。由於無法以傳統的安全機制進行防護，因此組織必須針對勒索軟體做好準備，並且備妥正確的系統與作業流程，以保護自己與企業。

## 2 組織須投資自動化工具

雲端攻擊的複雜度漸增，使得組織越來越難自保。自動化工具則可以提供協助，尤其今日的自動化工具常針對無法預測的攻擊而特別設計。此展會中也展示了許多高智慧工具，能夠提供即時的警示與回應，儘量降低內部與外部威脅所帶來的風險。

## 3 組織須提高在網路安全方面的支出

組織必須把網路安全視為決策的前提，而非事後的追悔。通常當組織從實體為主轉向運用雲端時，往往理所當然地認為供應商將會承擔起安全性防護之責。實際上，全球的雲端供應商，提供的是以敏捷操控功能與改善績效為主，安全性通常不是首要議題，因此組織必須考量到自身的安全需求，必要時就應該提高在網路安全性方面的支出。

## 4 軟體開發者將承擔更多雲端安全的責任

在傳統的基礎設施中，各個角色與責任都有明確的定義，但是使用雲端的企業則並非如此。雲端難以抵擋來自網路的攻擊，因此所有的軟體開發商，不僅包括從事資通訊安全者，都必須負起維護工作系統安全之責。

## 5 為雲端建立重要的管理系統與驗證

由於越來越多的組織將應用程式移到雲端，也因此催生許多新驗證。組織可以運用重要的安全管理系統（management system），以及靠追蹤驗證的生命週期（certificate lifecycle），來適當地管理自己的系統。

bsi.