DELL Technologies

5 關於安全創新環境的建議

1	2	3	4	5
儘早並經常溝通	**合理化並簡化安全堆疊**	**建立網路安全護欄**	**保持彈性，發揮創意**	**培養強大的安全文化**
讓高階主管和關鍵利益關係人參與	降低複雜度	定義原則	對新的安全方法持開放態度	促進廣泛參與
瞭解創新計畫	消除冗餘步驟	實施存取控制	著重可適應創新的安全方法	提高透明度
授權安全性團隊展開對話	建立單一窗口	跨邏輯和實體系統整合	請記住，創新可以在安全性辦公室進行	促進協同合作
	制定強大的採購評估流程			

版權所有 © 2024 Dell Inc. 或其子公司。保留所有權利。

為創新建立安全的環境。

為了在技術和資料導向的世界中最大限度地實現創新，必須建立網路安全以支援創新。但是，組織要如何營造一個能在不影響安全性的前提下，增進成長、創造力和創新的環境？

為了調查此類環境的真實範例，Dell 網路安全行銷部門的 Sameer Shah 與亞利桑那州吉爾伯特鎮資訊安全長 (CISO) Tony Bryson 博士會面，討論創新的「未來之城」計畫，以及安全性在推動計畫上所扮演的角色。

請繼續閱讀 Bryson 博士的建議摘要，並造訪 **dell.com/cybersecuritymonth** 觀看整場對談。

> 「務必掌握『利益關係人』的目標，以及他們可能會如何利用技術和創新，讓企業和客戶受益。」
>
> ***Tony Bryson** 博士，吉爾伯特鎮資訊安全長 (CISO)*

未來之城

吉爾伯特鎮的「未來之城」計畫旨在建立永續且有韌性的基礎結構，利用資料豐富居民的生活。在為居民提供從支付帳單、交通運輸到水源可用性和水質等服務方面，涉及大量技術。還涉及資料收集，以預測未來的服務使用和需求。這項計畫並沒有一個限定的終點，而是一個持續推動進步的反覆過程。

作為第一任資訊安全長，Bryson 博士的任務是採取更具策略性的方法解決網路安全問題。提供現代化、技術支援的城市服務需要強大的資料保護、分類和控制功能，以支援該鎮的宏大目標。

隨著該過程的持續進行和成功，Bryson 博士指出了幾個關鍵建議，這些建議促進了成功，並為安全成長和創新創造了合適的環境。

儘早並經常溝通

Bryson 博士強調，在創新過程中，有必要讓高階主管和其他關鍵利益關係人及早參與。他表示：「你必須知道他們的目標，以及他們可能會如何利用技術和創新，讓企業和客戶受益。」

早期溝通的自然延伸，是在創新週期開始時進行網路安全對話，而網路安全團隊作為關鍵合作夥伴，可以成為這些討論的催化劑。

吉爾伯特鎮對 AI 的使用就是一個很好的例子。兩年前，安全性辦公室就開始進行這些對話，並在提出關鍵問題方面發揮了領導作用：如何信任 AI 生成的資料、如何儲存資料，以及如何確保居民正確理解 AI 的使用。這促進了跨部會委員會的成立，而吉爾伯特鎮也為此聘請了全職的人工智慧長，這也是美國西部地區的首例。

Bryson 博士表示：「如果我們畫出一個安全圍欄來阻止這類特定的創新發生，就不會有這一切。因此，當涉及到嘗試創新和嘗試以正確的方式行事，對話就是起點。」

合理化並簡化安全堆疊

Bryson 博士的首要任務之一是清點安全堆疊，以瞭解每種產品和服務的用途。透過這項工作發現了大量的冗餘措施。減少和合理化這些冗餘措施將可節省資金。但更重要的是，這將為小型安全團隊提供單一窗口和單一資訊來源，以管理網路安全功能和解決問題。

Bryson 博士回應了那句古老的格言，即複雜性是網路安全的敵人，他說：「我不希望看到人們不得不從一個系統跳到另一個系統，試圖弄清楚發生了什麼事。」

建立正確的網路安全護欄

組織中的創新者必須瞭解並遵守確保系統和資料安全的安全性指南。這些規則可以是政策、存取控制或其他原則，幫助創新者瞭解作業環境。這個作業環境代表了安全的創新環境，透過安全性與創新者之間的有效合作關係而建立。

保持彈性，發揮創意

Bryson 博士提到，雖然制定和執行網路安全標準很重要，但創新有時需要流動性和創造力。他指出：「創新不僅僅發生在業務單位。很多時候，創新發生在資訊科技甚至資訊安全性辦公室。隨著業務不斷進行創新，你可能需要尋找有創造性的新方法來保護你的系統和資料。因此，請為此做好準備。」

版權所有 © 2024 Dell Inc. 或其子公司。保留所有權利。

DELL Technologies

培養強大的網路安全文化

Bryson 博士強調了發展強大安全文化的重要性。「在網路安全方面，文化幾乎就是一切。如果人們具有網路安全意識的文化不存在，就要體認威脅面的存在。」

強大的網路安全文化的基礎，建立在已經討論過的許多要素之上：公開透明的對話、廣泛的參與、清晰明確的標準，以及安全團隊與其內部和外部客戶之間的協作精神。

隨著成長加速，網路安全必須從著重防禦的被動立場，演變為優先考量促進積極成果的主動做法。

組織應採用現代化的安全性思維模式，不僅要保護、還要增強創新能力。

這可以透過將安全措施整合到開發過程中的通訊和協作來實現。目標是營造一個在不影響安全性的情況下，讓創造力得以蓬勃發展的環境。

造訪 **dell.com/cybersecuritymonth**，瞭解如何解決當今一些主要的網路安全挑戰

版權所有 © 2024 Dell Inc. 或其子公司。保留所有權利。

DELL Technologies