DELL Technologies

5

有关搭建适合创新的安全环境的建议

1	2	3	4	5
尽早并经常沟通	**合理化和简化安全堆栈**	**建立网络安全保护框架**	**保持灵活，发挥创意**	**培养坚实的安全文化**
与高管和关键利益相关者接洽	降低复杂性	定义策略	接纳新的安全方法	推动广泛参与
了解创新计划	消除冗余	实施访问控制	专注于包含创新的安全方法	提高透明度
鼓励安全团队开展对话	创建单一管理平台	跨逻辑和物理系统进行集成	请记住，安全办公室也可以孕育创新	促进协作
	制定强大的采购评估流程			

搭建适合创新的安全环境。

为了在这个由技术和数据驱动的世界中更大限度地提高创新能力，必须建立网络安全来支持创新。但问题是，组织如何才能打造一个既能促进发展、发挥创造力、实现创新又不影响安全性的环境呢?

为了调查此类环境的真实案例，戴尔网络安全营销部的 Sameer Shah 会见了亚利桑那州吉尔伯特市的首席信息安全官 (CISO) Tony Bryson 博士，讨论了未来城市创新计划以及安全性在推动该计划方面发挥的作用。

请继续阅读 Bryson 博士的建议摘要。如需观看完整对话，请访问 **dell.com/cybersecuritymonth。**

> 确保您了解 [利益相关者] 要实现的目标，以及他们可能如何利用技术和创新来使企业和客户受益。”
>
> ***Tony Bryson** 博士，吉尔伯特市首席信息安全官 (CISO)*

未来之城

吉尔伯特市的未来之城计划旨在构建可持续且富有弹性的基础架构，利用数据丰富市民的生活。从居民支付账单到交通运营，再到水供应和质量，各项服务的提供都很大程度上使用了技术。此外，它还涉及收集数据，以预测未来的服务使用情况和需求。该计划拥有无线终点，是一个迭代过程，会推动持续进展。

作为首位 CISO，Bryson 博士的任务是采取更具战略性的网络安全方法。要提供现代化、由技术提供支持的城市服务，需要强大的数据保护、分类和控制功能，来为该市的宏伟目标保驾护航。

随着这一过程的不断推进并取得成功，Bryson 博士提出了一些关键建议，这些建议推动实现成功，并营造了合适的环境，以供安全地发展和创新。

尽早并经常沟通

Bryson 博士强调，在创新过程的早期，需要让高管和其他关键利益相关者参与进来。“确保您了解他们要实现的目标，以及他们可能如何利用技术和创新来使企业和客户受益。”他说。

说到尽早沟通，很自然地可以想到在创新周期开始时进行网络安全对话，而作为关键合作伙伴，网络安全团队在这些讨论中可以发挥催化剂的作用。

吉尔伯特市对 AI 的使用就是一个很好的例子。安全办公室两年前就开始了这些对话，并引领着提出了关键问题：如何信任 AI 生成的数据，如何存储这些数据，以及如何确保居民正确理解对 AI 的使用。这促成了跨职能委员会的成立，进而为吉尔伯特市迎来了全职首席人工智能官，这在美国西部尚属首例。

“如果我们划出一道安全界限来阻止这种特定创新的发生，这一切都将无法实现，”Bryson 博士说，“因此，说到尝试创新和尝试正确的实现方法，对话是一切的起点。”

合理化和简化安全堆栈

Bryson 博士的首要任务之一是清点安全堆栈，以了解各种产品和服务的用途。这项工作让他发现了严重的冗余。精简和合理化可以节省资金，但更重要的是，它将为小型安全团队提供单一管理平台和单一信息源，以便管理网络安全功能和解决问题。

Bryson 博士说：“我不希望人们在不同系统间来回切换，而只为了弄清楚发生了什么。”他的话与一句老格言不谋而合 — 复杂性是网络安全的敌人。

建立正确的网络安全保护措施

组织中的创新者需要了解并遵守安全准则，以确保系统和数据安全。这些规则可以是策略、访问控制或其他可帮助创新者了解应用场景的原则。这种应用场景代表了安全的创新环境，是安全团队和创新者之间通过有效合作搭建的。

保持灵活，发挥创意

Bryson 博士指出，虽然制定和执行网络安全标准很重要，但创新有时还需要变通性和创造力。他指出：“创新不仅仅发生在业务部门，在信息技术领域，甚至在信息安全办公室也时有发生。随着您的企业围绕您进行创新，您可能必须找到新的、有创造性的方法来保护您的系统和数据。所以，一定要做好准备。”

DELL Technologies

培养坚实的网络安全文化

Bryson 博士强调了培养坚实安全文化的重要性。“在网络安全方面，文化几乎无处不在...如果不培养起人人都重视网络安全的文化，就要认清面临的威胁面。”

坚实的网络安全文化基于众多已经探讨过的元素，包括开放透明的对话、广泛的参与、明确的标准，以及安全团队与内部和外部客户之间的协作精神。

随着发展的不断加速，网络安全必须与时俱进，从以防御为主的被动态势转为积极促成优化成果的主动方法。

组织应接纳现代化的安全思维，不仅要为创新保驾护航，还要不断推动创新。

要实现这一点，必须通过沟通和协作，将安全措施集成到开发流程中。目的是营造一个既能激发创造力又不影响安全性的环境。

了解如何应对当今一些主要的网络安全挑战：**dell.com/cybersecuritymonth**

DELL Technologies