DELL Technologies

5 イノベーションをもたらす安全な環境に向けての推奨事項

1	2	3	4	5
早い段階で頻繁にコミュニケーションをとる	**セキュリティ スタックを合理化しシンプルにする**	**サイバーセキュリティ ガードレールを確立する**	**柔軟性を保ち、創造力を発揮する**	**強固なセキュリティ文化を醸成する**
経営陣や主要なステークホルダーを関与させる	複雑さを緩和する	ポリシーを定義する	新しいセキュリティ手法を受け入れる	幅広い参加を促進する
イノベーションの計画を理解する	冗長性を排除する	アクセス制御を実装する	イノベーションに対応するセキュリティ手法に重点を置く	透明性を促進する
セキュリティ チームが会話を開始できるよう支援する	情報を一元管理する	論理システムと物理システム全体を統合する	イノベーションが生まれるのはセキュリティ オフィスであるということを念頭に置く	コラボレーションを促進する
	強力な調達評価プロセスを開発する			

イノベーションをもたらす安全な環境を作る

テクノロジーとデータ主導の世界でイノベーションを最大化するには、イノベーションをサポートするサイバーセキュリティを構築する必要があります。しかし、セキュリティを損なうことなく、成長、創造性、イノベーションを強化する環境を組織が構築するには、どうすればよいでしょうか。

そのような環境の実例を調査するために、Dellサイバーセキュリティ マーケティング担当のSameer　Shahは、アリゾナ州ギルバートの最高情報セキュリティ責任者(CISO)であるTony Bryson博士と面会し、革新的な「未来の都市」イニシアティブと、その推進においてセキュリティが果たす役割について対談しました。

ここではBryson博士の推奨事項の要約をご紹介します。全編は**dell.com/cybersecuritymonth**でご覧いただけます。

> 「（ステークホルダーが）何を目指しているのか、そしてテクノロジーとイノベーションをどのように活用してビジネスと顧客に利益をもたらす可能性があるのかを必ず把握してください」
>
> *Tony Bryson博士、最高情報セキュリティ責任者(CISO)*
> *ギルバート*

未来の都市

ギルバートの「未来の都市」イニシアティブは、データを活用して住民の生活を豊かにする、持続可能で回復力のあるインフラストラクチャを構築することを目的としていました。住民が請求書を支払うことから、交通運行、水の供給や水質まで、テクノロジーはサービスの提供に大きく関わっています。また、将来のサービスの利用状況とニーズを予測するためのデータ収集も含まれます。このイニシアティブに期限はなく、継続的な進歩を促進する反復的なプロセスとなります。

初代CISOとしてのBryson博士の使命は、サイバーセキュリティに対してより戦略的なアプローチを取ることでした。テクノロジーを駆使した近代的な都市サービスを提供するには、この町の意欲的な目標をサポートするように設計された強力なデータ保護、分類、および制御機能が必要でした。

このプロセスが順調に進む中で、Bryson博士は、成功を促進するとともに、安全に成長し革新するための適切な環境を作り出すのに役立つ重要な推奨事項を特定しました。

早い段階で頻繁にコミュニケーションをとる

Bryson博士が強調したのは、イノベーション プロセスの早い段階で経営陣やその他の主要なステークホルダーを関与させる必要性です。「彼らが何を目指しているのか、そしてテクノロジーとイノベーションをどのように活用してビジネスと顧客に利益をもたらす可能性があるのかを必ず把握してください」と博士は述べました。

早い段階でのコミュニケーションの延長線にあるものとして、イノベーション サイクルの開始時にサイバーセキュリティに関する会話を行うことが挙げられます。サイバーセキュリティ チームは、重要なパートナーとして、こうした話し合いのきっかけになることができます。

ギルバートのAI活用はその最たる例です。セキュリティ　オフィスは2年前にこうした話し合いを始め、AIが生成したデータを信頼する方法、そのデータを保存する方法、住民がAIの使用を正しく理解できるようにする方法など、重要な質問を投げかける上で主導的な役割を果たしました。これをきっかけに、部門横断的な委員会が設立され、ギルバートに常勤の最高人工知能責任者が採用されました。これも米国西部では初めてのことでした。

「もし私たちがこの特定のイノベーションの実現を妨げるような拒否反応を示していたら、このようなことは何も起きなかったでしょう」とBryson博士は言います。「イノベーションを起こし、正しい方法で物事を行おうとするとき、会話がその出発点となります」。

セキュリティ スタックを合理化しシンプルにする

Bryson博士の最初の仕事の1つは、製品やサービスそれぞれの用途を理解するために、セキュリティ スタックを棚卸しすることでした。それにより、過剰な冗長性が明らかになりました。削減と合理化はコストの節約につながりますが、さらに重要なことは、一元管理された情報と信頼できる情報源が小規模なセキュリティ チームに提供され、それに基づいてサイバーセキュリティ機能の管理と問題への対処できるようになることです。

Bryson博士は、「複雑さはサイバーセキュリティの敵である」という古い格言を繰り返しながら、「何が起きているのかを理解するために、システムからシステムへと動き回らなければならない状況は望ましくありません」と述べました。

適切なサイバーセキュリティ ガードレールを確立する

組織内のイノベーターは、システムとデータを安全に保つセキュリティ ガイド レールを理解し、遵守する必要があります。それはたとえば、ポリシーやアクセス制御、イノベーターが活動の場所を理解するのに役立つその他の考え方が含まれます。この活動の場所とは、セキュリティとイノベーターの間の効果的なパートナーシップによって生み出される、イノベーションのための安全な環境のことです。

柔軟性を保ち、創造力を発揮する

Bryson博士は、サイバーセキュリティ標準を制定して実施することが重要である一方で、イノベーションには時に流動性と創造性が必要であると指摘しました。博士は、「イノベーションはビジネス部門だけで起きるものではありません。多くの場合、イノベーションは情報技術内で起こり、さらには情報セキュリティ オフィス内でも起こります。ビジネスで起こるイノベーションに伴い、システムとデータを保護するための新しい独創的な方法を見つける必要があるかもしれません。そのための準備を万端にしておきましょう」と述べました。

DELL Technologies

強固なサイバーセキュリティ文化を醸成する

Bryson博士は、強力なセキュリティ文化を発展させることの重要性を次のように強調しました。「サイバーセキュリティに関して言えば、文化がほぼすべてです。社員がサイバーセキュリティを意識する文化がない場合は、脅威の対象領域を認識してください」。

強固なサイバーセキュリティ文化の基盤は、オープンで透明性のある対話、幅広い関与、明確に表現された基準、セキュリティ チームと社内外の顧客との間のコラボレーションの精神など、これまでに説明した多くの要素の上に構築されます。

成長が加速するにつれて、サイバーセキュリティは、防御に重点を置いた事後対応的な姿勢から、プラスの成果を促進することを優先するプロアクティブなアプローチに進化していく必要があります。

組織は、イノベーションを保護するだけでなく強化するという、セキュリティに対する新しい考え方を採用する必要があります。

これは、セキュリティ対策を開発プロセスに組み込んだコミュニケーションとコラボレーションを通じて実現できます。その目標は、セキュリティを損なうことなく創造性を発揮できる環境です。

dell.com/cybersecuritymonthで今日のサイバーセキュリティの重要な課題に対処する方法をご紹介しています

DELL Technologies