サイバーセキュリティにおけるポジティブリスク

AWS 規範ガイダンス

AWS 規範ガイダンス: サイバーセキュリティにおけるポジティブリスク

Table of Contents

サイバーセキュリティにおけるポジティブリスク

Greg Bell (Amazon Web Services (AWS))

2022 年 5 月 (ドキュメント履歴)

ほとんどの人は、損失への露出や有害事象の管理など、リスクを否定的な観点から考えています。ただし、国際標準化機構 (ISO) は、リスクを「不確実性が目標に及ぼす影響」と定義します。この場合、その影響はプラスにもマイナスにもなり得ます。

実際のリスクは業界によって異なる場合がありますが、この標準的な定義はすべての業界に適用され、各業界にはマイナスのリスクとプラスのリスクがあります。サイバーセキュリティ業界において、ネガティブリスクは潜在的な損失を指し、ポジティブリスクは資産、知識、改善、またはデータの潜在的な利益を指します。

プロジェクト管理ドメインと ITドメインは、事業報告や事業上の意思決定におけるポジティブリスクを評価する戦略を導入しています。しかし、サイバーセキュリティ業界はまだこれを一般的な方法として導入しておらず、多くのリスク管理方法論は引き続きネガティブリスクに重きを置いています。ポジティブリスクについて議論するにしても、手短に済ませてしまいます。

従来、サイバーセキュリティはリスクをネガティブな観点からしか見ていませんでした。サイバーセキュリティにおける一般的なネガティブリスクには、次の 2 種類があります。

- ダウンサイドリスク — 脅威など外部要因による損失への露出。例えば、サイバー犯罪者はセキュリティインシデントを発生させたり、その可能性を高めたりする可能性があります。
- アップサイドリスク — 変化から生じる脆弱性など、利益を追求している間の損失への露出。例えば、IT 戦略を実施しているときに、セキュリティインシデントの可能性を不用意に高めてしまう可能性があります。アップサイドリスクはポジティブリスクと同じではありません。アップサイドリスクは利益を追求している間に発生するものの、損失の可能性に重きを置いています。

最近まで、サイバーセキュリティはネガティブリスクのみを考慮しており、リスクの定義は潜在的なマイナスの結果に重きを置いていました。ポジティブリスクは、リスクの特定を始めた時点での潜在的なプラスの結果に重きを置いています。ポジティブなリスクを除外すると、サイバーセキュリティにおけるプラスの結果を認識できなくなります。ネガティブなリスクに重点が置かれているため、一般的に経営幹部はサイバーセキュリティを予測的ではなく事後的であると認識し、サイバーセキュリティがビジネスに寄与するプラスの成果を過小評価しています。

このドキュメントでは、サイバーセキュリティ業界にとってのポジティブリスクを定義し、サイバーセキュリティ戦略にポジティブリスクを含めることのメリットと重要性について説明します。

ポジティブリスクのメリット

特に、潜在的な損失からビジネスを保護することに重点を置いているサイバーセキュリティのような業界では、リスクを否定的な観点から捉えるのは簡単です。潜在的な利益に基づいてサイバーセキュリティリスクを再構成することにより、ポジティブな成果の促進、組織のセキュリティ体制の強化、顧客の信頼度の向上を実現し、ビジネスに利益をもたらすことができます。

ポジティブな成果の促進

ポジティブリスクを採用することで、組織はある分野がポジティブなビジネス成果にどの程度貢献しているかを評価し、認識できるようになります。「経営幹部と役員室のサイバーセキュリティ」(エンタープライズ戦略グループの調査レポート) によると、

- ビジネスリーダーとテクノロジーリーダーの 69% は、サイバーセキュリティは全体または大部分がテクノロジー分野であり、ビジネスとはほとんど、またはまったく関係がないと考えています。
- ビジネスリーダーとテクノロジーリーダーの 11% は、サイバーセキュリティを規制コンプライアンスと同一視しています。
- 組織の 82% が、サイバー脅威の増加、企業内でのテクノロジー統合の進展、アタックサーフェスの拡大などの要因により、サイバーセキュリティリスクが過去 2 年間で増加したと回答しています。

サイバーセキュリティの幹部がポジティブリスクを会話や報告に盛り込むことで、社内の安全な IT 運用の価値を高めることができます。

例えば、ある企業が数年前にデータ漏えいに見舞われ、そのデータ漏えいはパッチ管理プロセスの欠如によって引き起こされたとしましょう。このインシデントは今でもメディアに取り上げられており、同企業に対する顧客の認識およびやり取りに影響を与えています。同企業はインシデントを乗り越え、提供するサービスを拡大したいと考えていますが、顧客の信頼度が販売を妨げています。サイバーセキュリティは、ポジティブリスクを利用して、アプリケーションを継続的に更新するパッチ管理プロセスに投資するよう経営陣を説得しました。新しいプロセスにより、データ漏えいのリスクは大幅に軽減され、同企業のセキュリティ体制が改善されました。最新のパッチ管理プロセスのニュースは、メディアや潜在的な顧客にも届きました。顧客は安心して同企業から購入できるようになり、売り上げは目覚ましいレベルにまで増加しました。

リスクを特定する際にポジティブリスクを考慮しないと、評価が不完全になり、ビジネス上の意思決定に影響を与える可能性があります。ビジネス上の意思決定に影響を与える可能性のあるポジティブリスクの具体例については、「ポジティブリスクの例」を参照してください。

セキュリティ体制の強化と顧客の信頼度の向上

サイバーセキュリティは企業のセキュリティ体制に不可欠です。データ漏えいは顧客の信頼度に悪影響を及ぼす可能性がありますが、強固なセキュリティ体制と評判は顧客の信頼度を高め、ビジネスチャンスを拡大する可能性があります。

ポジティブな成果の促進 で説明したように、調査によると、経営幹部はサイバーセキュリティに関連するネガティブリスクは理解しているが、往々にしてポジティブリスクやビジネス価値を理解していないことが明らかになっています。しかしながら、サイバーセキュリティ分野のリーダーは、強固なセキュリティ体制が組織にもたらすメリットを理解しているという調査結果が出ています。

Vodafone は「Cyber Security Research: The Innovation Accelerator」(Vodafone ホワイトペーパー) で、サイバーセキュリティに関する世界中の意思決定者 1,434 人にインタビューを行いました。彼らのデータによると、

- 回答者の 73% は、強力なセキュリティが新たなビジネスチャンスを生み出すと考えています。
- 89% は、セキュリティを強化することで顧客のロイヤルティと信頼度が高まると回答しています。
- また、90% は、イメージを改善し、新しい潜在顧客にアプローチして、実顧客に転換できたと回答しています。
- 89% は、効果的なサイバーセキュリティをもつことは競争上の優位性であり、競合他社との差別化に役立つと考えています。
- 24% は、クラウドテクノロジーとモノのインターネット (IOT) を使用し、対象を絞った IT セキュリティ制御を採用することで収益が増加したと報告しています。
- 経営幹部とのコミュニケーションにおいて、ネガティブな結果を招きかねないことを伝える代わりに、ポジティブリスクを利用して、顧客の信頼度向上がもたらすビジネス価値を伝えることができます。経営幹部は、プログラムへの資金提供に関して慎重になることがあります。場合によっては、サイバーセキュリティは運用に必要最低限なものになることもあります。社内で資金提供を依頼する際にポジティブリスクを伝えることで、経営陣はサイバーセキュリティのビジネス価値を理解しやすくなります。その結果、サイバーセキュリティへの資金提供が増え、企業の収益が増加する可能性があります。

サイバーセキュリティリスク言語の変化

サイバーセキュリティにポジティブリスクを導入する場合の課題の 1 つは、技術用語やドメイン固有の用語が脅威、脆弱性、およびセキュリティコントロールなどのネガティブリスクに集中している点です。サイバーセキュリティ業界は、サイバーセキュリティがビジネスにもたらすポジティブなビジネス成果 (またはポジティブリスク) を強調する言語を含むように、その語彙を進化させ、拡大する必要があります。ビジネス上の利点、メリット、ビジネス価値といった用語は、組織に対するサイバーセキュリティの貢献を強調するものです。

サイバーセキュリティの言語を変えることは、サイバーセキュリティは脅威と脆弱性にのみ焦点を当てた技術分野であり、ビジネスから切り離されているという認識を変えるのに役立ちます。ビジネスリーダーは一般的に、サイバーセキュリティがビジネス成果に及ぼすプラスの影響を過小評価しています。経営陣のサイバーセキュリティに対する認識についての詳細は、「ポジティブな成果の促進」を参照してください。

関連分野での導入の増加

ポジティブリスクを含めることへの関心は多くの分野で高まっています。その理由として、ポジティブリスクはそのドメインが寄与するビジネスの成果を認識しているからです。ポジティブリスクの概念は最近、一般的なプロジェクト管理プロセスおよび定義に導入されました。

2013 年、プロジェクトマネジメント協会 (PMI) は、ポジティブリスク (機会とも呼ばれる) の定義をプロジェクトマネジメント知識体系 (PMBOK) の第 5 版に含めました。PMBOK は個人のリスクを「発生した場合、1つまたは複数のプロジェクト目標にプラスまたはマイナスの影響を与える不確実な事象または状態」と定義しています。また、全体的なプロジェクトのリスクを、「不確実性がプロジェクト全体に及ぼす影響は…プロジェクト内の個々のリスクの合計よりも大きくなります。なぜなら、不確実性にはプロジェクトの不確実性の原因がすべて含まれており…ステークホルダーがプロジェクト結果のばらつき (プラスとマイナスの両方) の影響にさらされていることを表しているからです」と定義しています。

PMI はリスクの定義にポジティブな結果を含めていますが、残念ながらサイバーセキュリティ業界ではまだ適用されていません。

ポジティブリスクの例

テクノロジー、プロジェクト管理、サイバーセキュリティにおけるポジティブリスクの例を以下に示します。

テクノロジーにおけるポジティブリスク

テクノロジーにおけるポジティブリスクの一例として、テクノロジーの導入による賃金コスト削減の可能性が挙げられます。例:

1. テクノロジーの導入は、業務効率の向上につながる可能性があります。
2. 業務効率の向上は、労力の削減につながる可能性があります。
3. 労力の削減は、賃金コストの削減につながる可能性があります。

プロジェクト管理におけるポジティブリスク

プロジェクト管理におけるポジティブリスクの一例として、プロジェクト予算の計算ミスがコスト削減や追加プロジェクトへの資金提供につながる可能性が挙げられます。例:

1. テクノロジープロジェクトを早期に実施すると、プロジェクトマネージャーがプロジェクトコストを誤って計算する可能性があります。
2. プロジェクトコストの計算を誤ると、過剰なプロジェクト資金につながる可能性があります。
3. 過剰なプロジェクト資金は、コスト削減や追加プロジェクトへの資金提供につながる可能性があります。

サイバーセキュリティのポジティブリスク

サイバーセキュリティにおけるポジティブリスクの一例として、パッチ管理の導入により顧客の信頼度が高まる可能性が挙げられます。例:

1. パッチ管理を実装することで、アプリケーションの脆弱性を低減することができます。
2. 脆弱性を低減することで、アプリケーションのリスクを軽減し、アプリケーションの安全性を高めることができます。
3. アプリケーションのセキュリティが向上すれば、データ損失を減らすことができます。

4. データ損失を減らすことで、顧客の信頼度が高まる可能性があります。

サイバーセキュリティにおけるポジティブリスクのもう 1 つの例としては、インシデントレスポンスの導入による従業員の生産性向上の可能性が挙げられます。例:

1. インシデントレスポンスを導入することで、ネットワークトラフィックの増加を検出できる可能性があります。
2. ネットワークトラフィック増加の検出は、音楽やビデオのストリーミングサービスなど、従業員が業務に関係のないコンテンツにアクセスすることで発生する、リソースの悪用を検出することにつながります。これらの悪用はネットワーク帯域幅を消費し、ネットワークやアプリケーションのパフォーマンスに悪影響を及ぼす可能性があります。
3. 従業員による会社のリソースの悪用を検出することで、これらのサービスのブロックにつながる可能性があります。
4. これらのサービスをブロックすると、ネットワーク帯域幅の消費が減り、従業員の生産性が向上する可能性があります。

最後に、サイバーセキュリティにおけるポジティブリスクの例として、インシデント対応計画を実施することでビジネスチャンスが増え、プライバシー法の遵守につながる可能性が挙げられます。例:

1. インシデント対応計画を実施することで、マルウェアやランサムウェアを迅速に検出して特定できる可能性があります。
2. マルウェアやランサムウェアを特定することで、影響を最小限に抑え、会社のリソースへの脅威を軽減することができます。
3. 会社のリソースへの脅威を軽減することで、新たなビジネスチャンスが生まれ、企業がプライバシー法の遵守を継続できる可能性があります。

サイバーセキュリティのリスク対応

ポジティブリスクとネガティブリスクとでは、対応が大きく異なります。ネガティブリスクの場合は、結果への影響を最小限に抑えるための措置を講じますが、ポジティブリスクの場合は、結果への影響を最大化するための措置を講じます。次の表は、ポジティブリスクとネガティブリスクに対して、考えられる対応策を示しています。

リスクタイプ	レスポンス	定義
ポジティブリスク	攻撃	リスクが発生する確率または可能性を最大化して、そのプラスの効果を実現します。
	共有	リスクの所有権または責任の一部を他の当事者に割り当てます。これはネガティブリスクの場合と同じアプローチで、潜在的な損失や利益を抑えようとします。
	強化	機会を最大化するために、リスクを生み出す条件を増やします。
	Ignore (無視)	リスクの可能性を無視し、何の対策も講じません。このような反応は、リスクの可能性が非常に低い場合や、プラスの結果から得られるメリットが最小限である場合によく見られます。
ネガティブリスク	軽減	リスクが発生する確率または可能性を最小限に抑えます。
	転送	保険ポリシーを購入して保険会社にリスクを譲渡するな

リスクタイプ	レスポンス	定義
		ど、リスクに対する責任や義務を他の当事者に移します。
	回避	リスクを生む条件を排除します。
	Accept	リスクの存在は認めますが、何の対策も講じません。

ネガティブリスクの場合、組織はリスク許容度およびリスク選好度に基づいてリスクを回避、転送、軽減、または許容します。リスクの発生を未然に防ぎ、発生した場合はミッション全体への影響を最小限に抑えようとします。

ポジティブリスク対応を理解する最善の方法は、例を挙げて説明することです。

- 攻撃 — あるセキュリティ担当者が最近、有能なセキュリティ専門家が新しい仕事を探すことを決めたと知り、新入社員候補として自分のチームに引き入れるために多額の契約ボーナスを手配しました。
- 共有 — ある事業ユニットのリーダーは、特権アクセス管理製品を使用してセキュリティを向上させたいと考えていますが、現在の会計年度にツールやサービスを購入するだけの予算がありません。リーダーは、パイロットプロジェクトとしてツールの購入· 実装を予定している別の事業ユニットのリーダーと協力し、しばらくして両方の事業ユニットをサポートするように導入を拡大します。
- 強化 — ある従業員が、サイバーセキュリティの脅威を軽減するために既存のビジネスプロセスを自動化する機会を特定しましたが、それには時間と設備への投資が必要です。このようなプロセスにはプラスのメリットがあると考えたマネージャーは、残業時間を承認して能力を開発し、プロジェクトを進めるために既存のハードウェアとソフトウェアのリソースを再利用します。
- 無視 — ある財務担当役員は、営業部門で働く従業員が、面倒で手間のかかるタスクを自動化する新しいアプリケーションを開発したことを知ります。このアプリケーションは最近、営業部門内に限って使用が承認されました。財務担当役員は、明示的な許可なしに新しいアプリケーションのコピーを入手して、自分の部署でも同様の利点を得ています。

次のステップ

テクノロジーやプロジェクト管理のドメインでは、リスク評価プロセスにポジティブリスクを導入してきましたが、サイバーセキュリティ業界はこれまでポジティブリスクを除外してきました。ポジティブリスクはビジネスにプラスの成果をもたらす可能性があり、サイバーセキュリティ業界ではポジティブリスクを受け入れ、そのメリットを実現するための移行が必要となります。

すべてのコミュニケーションにおいて、ポジティブリスクをすぐに伝え始めることができます。たとえば、リスク評価、セキュリティ評価、ステータスレポートには、ポジティブリスクに関するセクションを含める必要があります。経営幹部への資金提供要請にはポジティブリスクを盛り込み、事業への潜在的なメリットを伝え、申請を承認することで得られる潜在的なビジネス上の利点を強調する必要があります。

よくある質問

アップサイドリスクとポジティブリスクの違いは?

アップサイドリスクとポジティブリスクは同じように思えますが、実際には大きく異なります。リスクの中にはポジティブな結果とネガティブな結果があり、ネガティブな結果の中にもプラス面とマイナス面があります。

ポジティブリスクとは、アセット、知識、改善、データの潜在的な利益です。例えば、パッチ管理と、脆弱性を迅速に (1 週間以内に) 削除するプロセスを実装したとします。翌年には、セキュリティインシデントは発生しません。

アップサイドリスクは、利益を追求している間に損失にさらされるリスクです。例えば、ある企業が新しいアプリケーションをデプロイし、パッチ管理と、脆弱性を迅速に (1 週間以内に) 削除するプロセスを実装したとします。損失にさらされる可能性 (脆弱性を除去する期間) は、利益 (より安全なアプリケーション) を追求するためのものなので、これはアップサイドリスクとみなされます。脆弱性を除去するプロセスを 1 日に短縮することで、アップサイドリスクを増やすことができ、期間を 1 か月に延長することで、アップサイドリスクを減らすことができます。基本的にアップサイドリスクとは、損失を最小限に抑えながら利益を得る、不確実な可能性のことです。

サイバーセキュリティにポジティブリスクを含めることの重要性とは?

サイバーセキュリティのリスク評価や会話にポジティブリスクを組み込むことで、ビジネスにおけるサイバーセキュリティの価値を高めることができます。詳細については、「ポジティブリスクのメリット」を参照してください。

リソース

- Cybersecurity In The C-Suite and Boardroom (Enterprise Strategy Group 調査報告書)
- Cyber Security Research: The Innovation Accelerator (Vodafone のホワイトペーパー)
- Integrating Cybersecurity and Enterprise Risk Management (ERM) (NIST 出版物)
- Clarifying “Upside” and “Positive” Risk (FAIR institute ブログ投稿)

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
初版発行	—	2022 年 5 月 27 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。