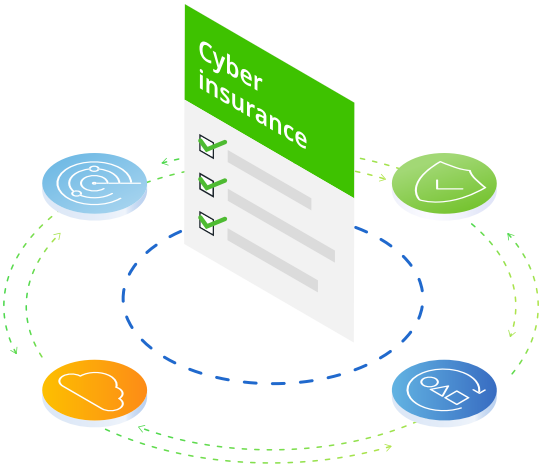
COHESITY

ヒントシート

サイバー保険に関する5つの重要な質問

ランサムウェアが急増する中で知っておくべきこと



ランサムウェアが蔓延し、民間企業や公的機関のあらゆる業界に影響を与えていることは周知の事実です。多くの企業がすでにサイバー保険に加入していますが、攻撃の可能性がかなり高いことから、より広範に関心が高まっています。

主な課題

- 保険の補償の制限と除外
- リスクの定量化の難しさ
- 標準化の欠如
- 補償内容の混乱
- 低い採用率

サイバー保険とは?

サイバー保険とは、サイバー攻撃、データ侵害、その他サイバー関連の事故の結果として生じる損失に対して金銭的な保護を提供する保険です。売上損失、弁護士費用、データ復旧費用、企業ブランドに対するダメージコントロールのために雇うPR会社の費用など、関連する費用が保険の対象となります。サイバー保険は通常、売上損失やデータ復旧費用といったファーストパーティ (直接) 損失と、訴訟費用や和解金などのサードパーティ損失の両方をカバーします。

しかし、保険会社は現在、ランサムウェアの蔓延と、その焦点がバックアップシステムになったことで、保険会社の責任が大幅に増加したことを認識しています。このため、サイバー保険に加入する、あるいは保険を維持する方法が変わってきています。

ここでは、サイバー保険に関する5つの重要な質問と、保険会社が被保険者として適格であると判断するため、バックアップと復旧システムにどのような機能を求める可能性があるかについて説明します。

1. サイバー保険の標準的な適格性検討事項とは?

- **データセキュリティ対策:** 保険会社は、パスワードポリシー、データバックアップ手順、インシデント対応計画など、企業のデータセキュリティ対策を審査し、補償の対象かどうかを判断することがよくあります。
- **データ侵害の履歴:** 保険会社は、通常、企業のデータ侵害の履歴とそれを防止するための取り組み、企業が収集/保存しているデータの種類について質問します。
- **売上規模:** 保険会社によっては、保険の対象とする企業に対して最小または最大の売上要件を設定している場合があります。
- **地理的場所:** 保険会社によっては、特定の国や地域に所在する企業に対してのみ保険を提供する場合があります。
- **ビジネスの種類:** 保険会社によっては、医療や金融など特定の業種に特化した保険を提供し、その業種に特化した資格を設定している場合があります。

これらの資格やその他資格は、保険会社や保険契約によって異なる可能性があるため、すべての保険契約の条件を注意深く確認することが重要です。また、サイバー保険の経験を持つ信頼できる保険仲立人と協力し、あなたのビジネスに適した補償を見つけることも良い考えです。

2. サイバー保険の適用を受けるには、どのような内部セキュリティコントロールが必要ですか?

内部セキュリティコントロールは、サイバー攻撃のリスクを低減し、データ侵害の際の復旧を成功させる可能性を高めるために不可欠です。ここでは、保険会社が企業の保険加入資格を評価する際に注目する内部統制をいくつかご紹介します:

- **強固なアクセスコントロールポリシー:** 強力なパスワードや二要素認証の導入、アクセスログの定期的な監視により、機密データへの不正アクセスを防止することができます。
- **強力なデータ暗号化:** 転送時も保管時もデータを暗号化することで、盗難や不正アクセスから機密情報を保護することができます。
- **定期的なソフトウェアの更新とパッチの適用:** 最新のセキュリティパッチを適用してソフトウェアを最新の状態に保つことで、サイバー犯罪者に脆弱性を悪用されることを防ぐことができます。
- **包括的なインシデント対応計画:** サイバー攻撃や災害復旧に備え、データ復旧計画を含む包括的なインシデント対応計画を策定しておくことで、データ侵害やデータ損失の際に、タイムリーかつ効率的な対応を行うことができます。
- **継続的な従業員教育:** 従業員に対して定期的にセキュリティトレーニングを実施することで、フィッシング詐欺やその他のサイバー脅威を認識し、機密データのセキュリティを維持するためのベストプラクティスを理解することができます。
- **脆弱性評価と侵入テスト:** 脆弱性評価と侵入テストを定期的に実施することで、攻撃者に悪用される前に、潜在的なセキュリティ上の弱点を特定し対処することができます。

このようなセキュリティコントロール体制を整え、定期的に見直し、更新することで、保険会社に対して、企業がサイバーセキュリティを重視し、侵害のリスクを低減しようとしていることを示すことができます。

3. サイバー保険を申請する際に、優れたバックアップと復旧ポリシーの重要な要素になるものは何でしょうか?

サイバー攻撃の脅威が高まり、企業がサイバー攻撃から身を守る必要性が高まる中、保険会社はバックアップと復旧を含むセキュリティ対策にますます力を入れるようになってきています。強固な内部セキュリティコントロールに加えて、以下のような最新のバックアップと復旧機能を備えていることを示すよう保険の申請者に要求し、審査することがあります:

- **複数のバックアップコピー:** 複数のバックアップコピーを異なる場所に保管することで、サイバー、自然、人為的な災害が発生した場合にデータ損失を防ぐことができます。
- **不変のバックアップスナップショット:** サイバー犯罪者は巧妙化し、現在ではバックアップそのものをターゲットにしています。バックアップの更新や削除が可能な従来のシステムとは対照的に、バックアップスナップショットを変更できないようイミュータブルにすることが重要です。ソフトウェアベースのネイティブのイミュータブルバックアップスナップショットは、データの安全なコピーを提供し、データの損失や破損が発生した場合にシステムを復元するために使用することができます。また、フォレンジック調査、規制遵守、復旧前のデータのインテグリティ(完全性)を確保するためにも有効です。
- **強力なアクセス制御:** 役割ベースのアクセス制御 (RBAC) と多要素アクセス (MFA) を使用すると、許可されたユーザーだけが機密情報にアクセスできるようになります。強力なアクセス制御の目的は、貴重なデータへの不正アクセス、変更、または盗難を防ぐことです。そのため、最新のシステムでは、MFAに加えてクォーラム制御が提供されています。クォーラムは、複数のユーザーが意思決定プロセスに関与することを保証し、不正アクセスや誤使用のリスクを低減するために、追加のセキュリティレイヤーを提供します。

- **エアギャップ方式で隔離されたバックアップコピー:** ガートナー社の戦略的計画の予測では、2025年までに少なくとも75%のIT組織がサイバー攻撃に1回以上直面するとしています[1]。そのため、一部の保険会社では、エアギャップ方式のバックアップを求めるようになっています。サイバー保管庫など、別のネットワークのエアギャップ方式で隔離された場所にバックアップコピーを保管することで、攻撃後にバックアップデータを確実に復旧させることができます。
- **バックアップの完全性スキャン:** バックアップデータの完全性をチェックすることで、リストアするデータが完全で正確であり、マルウェアがないことを確認します。これは、本番データやエンドポイントをスキャンするセキュリティソリューションへの補完的機能です。バックアップをスキャンすることで、新しいマルウェアが確認された場合でも、復旧プロセス中にマルウェアが組織内に侵入することがないようにすることができます。サイバー保険では、バックアップにマルウェアがないことをテストする機能について質問されることがあります。Tenableのようなサイバーセキュリティプロバイダーと連携した最新のシステムでは、ITが脆弱性を特定し、復旧中に本番環境にマルウェアが再導入されないよう支援します。
- **インスタントマスリストア:** インスタントマスリストアのような機能を活用することで、複数のシステムを同時に迅速に復旧させることができ、時間の短縮とリソースへの影響を最小限に抑えることができます。インスタントマスリストアのスピードと規模により、組織は迅速に通常業務に復帰することができます。サイバー保険の申請では、バックアップからのリストアが成功した場合の予測復旧時間を要求するものもあります。
- **復旧プロセスのテスト:** 復旧プロセスを定期的にテストすることで、データ損失の際にバックアップを正常にリストアできることを確認し、人為的なミスによるデータ損失のリスクを低減することができます。保険会社の中には、過去6ヶ月以内にサーバーやデータのリストアに成功したことを保証するよう求めることもあります。

このようなバックアップと復旧の機能を企業のソリューションに持つことで、保険会社に対して、企業がサイバー攻撃の際にデータ損失を防ぎ、ダウンタイムを最小限に抑えるための積極的な措置を講じていることを証明することができます。 これにより、復旧に成功する可能性を高め、サイバー保険とその条件を購入する能力も高めることができます。

4. データ保護戦略において、サイバー保険はどのような役割を果たしますか?

サイバー保険は、サイバー脅威からビジネスを保護するための包括的なアプローチのひとつです。ここでは、サイバーセキュリティ体制を強化するための追加の対策をいくつか紹介します:

- 強力なパスワードと二要素認証を導入します。バックアップシステムのパスワードは、他の管理者資格に使用するパスワードとは異なるものを使用します。
- 定期的にソフトウェアをアップデートし、セキュリティパッチを適用します。
- 重要なデータは定期的にバックアップし、オフサイトのサイバー保管庫 (通常、クラウド) に保管します。
- フィッシング詐欺を見分け、セキュリティのベストプラクティスに従うよう従業員を教育します。
- 脆弱性スキャンや侵入テストなど、定期的なセキュリティ評価を実施します。
- すべてのインシデント対応計画を策定し、定期的に更新します。
- 最新のサイバー脅威と傾向に関する情報を入手し、ビジネスや業界に適用される規制を理解します。

[1] Minimize Risk by Better Knowing and Managing Your Data, Michael Hoeck, Gartner, December 2022

5. サイバー保険は、私のビジネスに必要ですか?

あなたのビジネスにサイバー保険が必要かどうかは、ビジネスの規模、収集/保存するデータの種類、データ侵害やサイバー攻撃の潜在的な影響など、いくつかの要因によって決まります。

あなたのビジネスが機密性の高い顧客情報を保存している場合や、金融取引を行っている場合、または日常業務がテクノロジーに依存している場合は、特にサイバー脅威の影響を受けやすいといえます。このような場合、サイバー保険は、データ侵害の際の金銭的損失、風評被害、法的責任に対する重要な保護を提供してくれます。

大企業はもちろん、中小企業であっても、サイバー保険の恩恵を受けることができます。なぜなら、データ侵害のコストは、その規模に関係なく、ビジネスにとって多額になり、そしておそらく壊滅的なものになる可能性があるからです。サイバー保険に加入することで、サイバー攻撃に関連する金銭的リスクを保険会社に転嫁することができます。

まとめ

Cybersecurity Venturesによると、2023年のサイバー攻撃コストは世界で8兆米ドルに達すると予想されています。ランサムウェアやサイバー攻撃への対策には、多層的なセキュリティアプローチが不可欠です。サイバー保険、最新のデータ管理とデータセキュリティプラットフォーム、内部セキュリティ対策、人材育成はすべて、組織のデータを保護し、攻撃後にデータを復旧する役割を果たす可能性があります。

ここで説明した対策を講じ、包括的なサイバーセキュリティ戦略を導入することで、サイバー攻撃からビジネスを守り、データ侵害への備えを万全にすることができます。

サイバー保険は、サイバー攻撃やデータ侵害による経済的なダメージから企業を守るために、あらゆる規模の企業にとって賢明な投資となり得ます。

詳しくはこちらをご覧ください: www.cohesity.com/jp

COHESITY

Cohesity.com/jp | Cohesity Japan 株式会社 | 東京都千代田区大手町1-6-1 大手町ビル4F

9100069-001-JP 3-2023