先進的なサイバーリスクマネジメントチームを構築するための5つのステップ 2020年

サイロ構造を脱却して効率的なコラボレーションを

SecurityScorecard

目次

はじめに

サイバー犯罪はこの10年の間、ニッチな犯罪から現代企業にとって最も重大なリスクの1つになりました。新しい脅威が絶えず顕在化する中、サイバー攻撃の被害者数は年々増加しています。

Deloitte社の調査レポート『The future of cyber survey 2019』によると、回答者の95%が幅広い意味でのサイバー攻撃の被害に遭っており、その内の57%がサイバー攻撃を2年以内に体験しているとのことです。[1]同時に、サイバーセキュリティにかかる費用は世界的に増加しており、2021年には年間6兆ドルを超える見込です。この数字は2015年の3兆ドルの2倍に上ります。[2]

5100万ドル

2019年にNorsk Hydro社がサイバー攻撃によって被ったとされる損失額。この攻撃により同社の生産はストップ。[3]

[1] The Future of Cyber Survey 2019年, Deloitte社; https://www2.deloitte.com/za/en/pages/risk/articles/2019-future-of-cyber-survey.html

[2] The 2020 Official Annual Cybercrime Report; Herjavec Group; https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

[3] Prepare for the Expected Safeguard Value in the Era of Cyber Risk, 2019年, Aon; https://www.aon.com/getmedia/33c32425-fa93-4b7f-bf47-d0597f0133ab/aon-c-suite-cyber-report.aspx

リスク軽減を目的に毎年多くの費用をかけているのに、それに見合う効果が得られない場合があります。それはなぜでしょうか？

貴社はいまだに、リスクマネジメントとはコラボレーションによる取り組みではなく、独力で行うべき一度限りの仕事であるという考えの下で運営されているかもしれません。しかし、十分に明らかになっていることは、企業はそのすべての部署を脅かすリスクに直面しているということです。サイバーセキュリティを「IT担当者の問題」として捉えるのは、時代遅れの考え方です。サイロ化されたアプローチに依存し続けていては、問題を組織全体で明確化するための取り組みが損なわれ、侵害を受けた後の是正作業が遅れ、企業の脆弱性が高まります。

いまだに古い方法を利用している企業は少なくありません。Deloitte社の調査によると、セキュリティに関する連絡係を各事業部門に置いている企業は、全体の30%未満です。

2020

2020年、**従業員がリモートワークに移行する中、サイバーセキュリティにおけるコラボレーションがかつてないほどに重要になっている。**デジタルトランスフォーメーションが加速し、効率性へのニーズが高まっている。企業の多くが時代遅れのサイロ化されたアプローチに依存しているが、これは企業全体の課題であり、すべての従業員がもっと連携する必要がある。

私たちSecurityScorecardは、現在進化しているリスクに立ち向かうには、企業全体のサイバーセキュリティ戦略を統合することが絶対に不可欠であると考えています。つまり、サイロ構造を解体し、セキュリティエキスパートが各事業部門を横断して関与できるようにすることが必要です。最適な戦略をとることにより、未知の脅威を明らかにし、優れた意思決定を伝達するための企業全体としての理解が深まるため、セキュリティチームとテクノロジーの効率性が高まります。私たちはこれを先進的なサイバーリスクマネジメントと呼んでいます。

では、ここからどこに進めばいいのでしょうか？　当社は、140万社以上を継続的にモニタリングし、セキュリティレーティングを提供してきました。[4]また、中小企業から大企業まで世界中の企業にオートメーションツールを提供してきました。この経験から、企業のセキュリティ対策をモダナイズするのに役立つ5つのステップが明らかになりました。

本書では、この5つのステップを実行する方法を示す包括的な概要を説明します。対象となる読者は、セキュリティオペレーション、インシデントレスポンス、脆弱性マネジメント、リスク分析、脅威分析、不正行為防止、ベンダーリスクマネジメント、セキュリティリーダーシップに従事している人です。読者は次の事項を学ぶことができます。

- 先進的サイバーリスクマネジメントチームを構築して最適化するための5つのステップ
- 企業内サイバーセキュリティに関する効率的なコラボレーションと、世界中のサードパーティとの効率的なコラボレーションを実現するための手法とテクノロジー
- 企業全体のコミュニケーション戦略を実施する方法（計画を成功に導くカギ）

[4] SecurityScorecard Trust Portal, https://trust.securityscorecard.com/

本書の内容はステップごとに分かれていますが、リスクマネジメントプログラムの一部の項目がすでに完了していたり、特定の要素が他よりも優先されたりする場合もあると思われます。したがって、本ガイドを最大限活用するために、貴社にとって最も重要なステップから読み進めていっても構いません。各セクションのキーポイントは強調表示させてあります。

Step 1:

ビジネス目標を特定し、それにサイバーセキュリティを合致させる

デジタルトランスフォーメーションにより、取引をするベンダーの数が増え、使用中のエンドポイントデバイスの数がコンスタントに増加するに従って、企業のリスクプロファイルはいっそう複雑になってきています。管理すべきことがたくさんあります！ **このステップでは、企業を成功に導くために、より戦略的に思考し、サイバーセキュリティが必要な場所を特定するための方法を学んでいきます。**まず社内チームがその達成のために関与している収益目標およびビジネス目標と、これらに戦略を合致させる必要がある主要ベンダーを特定することから始めます。次に、サイバーセキュリティが既存のリスクフレームワークにどのように適合しているのかを調査します。これは次のステップで行う導入をスムーズに行うためです。

Step 2:

非技術スタッフに サイバーセキュリティを説明する

セキュリティ問題について、すべての従業員がセキュリティ責任者と同レベルの知識を持っているわけではありません。彼らにとってセキュリティ問題は、日々留意すべきことではないので、喫緊の問題には見えません。セキュリティが重要である理由を彼らに理解してもらう必要があります。**このステップでは、サイバーセキュリティを簡単に理解できるようにする方法を学んでいきます。この方法を通じ、企業全体の安全性を高めるベストプラクティスを従業員が採用できるよう、支援を行います。**さらに、プロセスをサポートできるセキュリティツールについて学びます。これらのツールを活用してセキュリティをコラボレーションによる取り組みとし、すべての事業部門が、オンボーディングを行うサードパーティ、ベンダー、サプライヤーのセキュリティのオーナーシップをとれるよう、支援を行います。

Step 3:

サードパーティのパートナーおよび ベンダーと協力する

Opus社とPonemon Institute社による調査によると[5]、59%の企業がサードパーティによるデータ漏洩を経験しています。違反のリスクを軽減し、コストのかかる事業中断を回避するには、サプライチェーンに完全かつ継続的な可視化を組み入れることが不可欠です。ベンダーリスクマネジメント計画を推進するには、サードパーティとの強固な関係を築くことが極めて重要であり、テクノロジーが重要なサポートとなります。**このステップでは、ベンダーとシームレスに連携することによって、サイバーセキュリティ調査票のプロセスをスピードアップし、是正作業を迅速化し、リスクを軽減する方法を学びます。**

[5] 2018 Data Risk in the Third-Party Ecosystem: Third Annual Study, Ponemon https://opus.com/ponemon

Step 4:

経営幹部や取締役会が理解できる実用的なインサイトを提供する

経営幹部、取締役会、外部ステークホルダーに対し、サイバーセキュリティ対策についてのレポートを作成する必要性が高まっています。しかし、経営幹部には、サイバーセキュリティイニシアチブに関するすべての技術情報に注意を払う時間はありません。彼らが知る必要があるのは、サイバーリスクが業務機能に与えている影響や、サイバーリスクを軽減するための、マーケット動向に合致した投資方法です。一部のセキュリティリーダーにとってこのことは、経営幹部のために何時間もかけて手作業でレポートを準備することを意味します。**ここでは、リスクレーティングプラットフォームを使って、経営幹部が知る必要があるメトリクスを含む自動作成されたレポートを、簡単に取り出す方法を説明します。**

Step 5:

セキュリティ施策を運用可能にし、可視性と透明性を維持する

このステップでは、セキュリティイニシアチブを企業内のさまざまなチーム間で運用可能にする方法と、自動化されたソリューションを活用し、各部門の計画の可視性を維持する方法を学びます。これにより、脅威検出を最適化し、各レスポンス機能の優先順位付けができるようになります。最新のリスクマネジメントには、既存プロセスにおける効率的なコラボレーションとシームレスな統合が必要です。社内チームやサードパーティと協力して業務を行えば、企業は既存ツールの投資収益率（ROI）を高め、リスクを軽減し、コンプライアンス体制を強化することができます。

効果的なコラボレーションが行われているか？

さまざまな地域と業界の企業と協働してきた中で当社が気付いたことは、是正期間を大きく左右するのは、しばしばなおざりにされる要素、すなわちチーム間でのコラボレーションの度合いであるということです。ステップ1に進む前に、自社の現在の立ち位置を把握することが重要です。貴社がサイバーリスクに関して協力するために、実行できるすべてのことを行っていると確信している場合は、ギャップが一切存在していないことを確認してください。

以下の質問表に答えれば、サイバーセキュリティについてのコラボレーションとコミュニケーションに関する、自社の基本的な準備レベルを測定できます。「はい」か「いいえ」をチェックして、自社の現在の立ち位置を把握し、改善の余地がある分野を確認します。*

99%

セキュリティチームやITチームが少なくとも1年前から認識している脆弱性が、それが解決される前に悪用される比率（Gartner社調べ）。この憂慮すべき統計を見ると、問題は必ずしも脅威の特定ではなく、実際のところコミュニケーションの不足であると言える。[6]

確認項目	はい	いいえ
企業内のすべての従業員がセキュリティを理解し、またそれが従業員にどのように直接的な影響を及ぼすのかを理解している。		
企業内のすべての従業員がセキュリティに注意を払っている。		
IT部門は、利用しているすべてのサードパーティサプライヤーをマッピングしており、すべてのベンダーが適切なガバナンスプロトコルに従っていることを確認している。		
社内のセキュリティエキスパートがサイバーセキュリティ問題を事前に防止できるよう、各事業部門が社内のセキュリティエキスパートと協力している。		
各事業部門は、新しいベンダーとの取引を開始する前にセキュリティチームを参加させている。		
セキュリティチームは、セキュリティツールを最大限活用しているとともに、自身の機能を最大化するため、必要に応じてアウトソーシングを行っている。		
セキュリティチームは、最大限の効率性で業務を行っている。		
セキュリティ目標は、収益目標と整合している。		
エグゼクティブチームと経営幹部は、サイバーセキュリティイニシアチブの重要性と影響力を理解している。		

** いずれかの確認項目で「いいえ」があった場合は、効率的なコラボレーションと業務を行うための専門知識、各プロセス、ツールを最大限に活用していない可能性があります。*

[6] How to Respond to the Threat Landscape, 2019年, Gartner;
https://www.gartner.com/en/conferences/emea/security-risk-management-germany/featured-topics/threat-landscape

- SecurityScorecard の充実した **Professional Services Offerings** では、SecurityScorecard RatingsとAtlasを先進的なサイバーリスクマネジメント計画に組み入れる方法について、登録した専門家からアドバイスを受けることができるため、当社の業界をリードするカスタマーサービス以上のサービスを利用できる。

このプラットフォームでは、クリティカルな脆弱性や問題が発見されるたびに、さまざまな形態のコラボレーションとコミュニケーションを利用できます。既存のプロセスにシームレスに適合する多様なツールを利用できるので、企業は問題を是正し、更なるインシデントの発生を防止するために、他の事業部門やサードパーティに迅速に連絡することができます。

詳細については、以下へお問合わせください

SecurityScorecard

株式会社 電通国際情報サービス
金融ソリューション事業部 営業企画部
https://www.isid-security.com/ssc/
g-security@group.isid.co.jp
Tel: 03-6713-7030