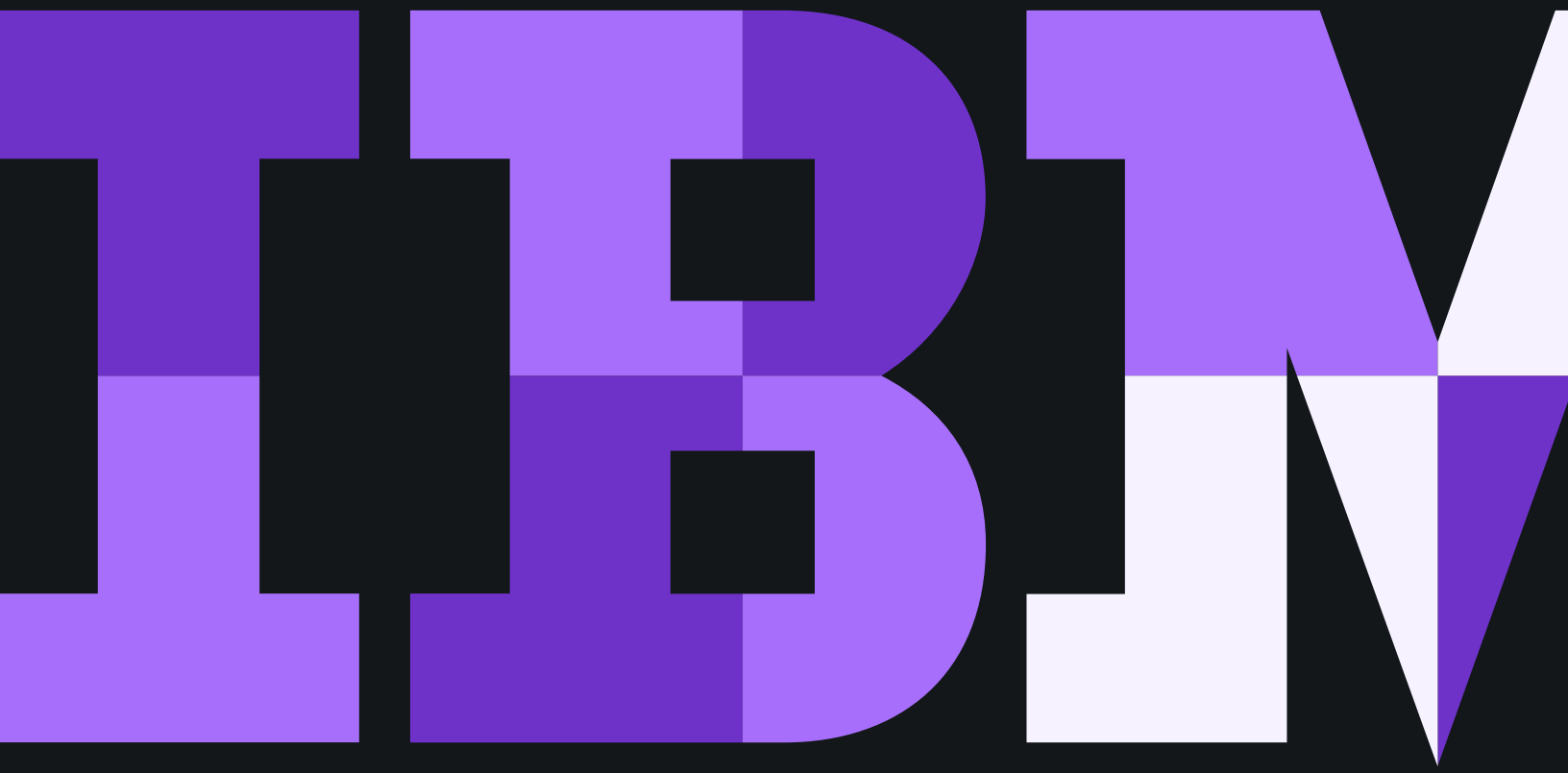
IBM Security

2020 年 1 月

サイバーセキュリティー・リスクを管理するための戦略

セキュリティーおよびコンプライアンス対策の評価と向上



IBM

目次

現在のサイバーセキュリティー状況

データ漏えい、ランサムウェア攻撃、個人情報の流出などのサイバーセキュリティー問題に神経をとがらせていても、効果的な対策が取れている企業は多くありません。多くの企業で、明確で連携のとれたセキュリティー戦略が策定されておらず、サイバーセキュリティー成熟度に対する知見が限られており、サイバーセキュリティー・インシデントに対応する計画が策定されていたとしても、それを十分に実行できません。リスク管理に対する大部分の組織のアプローチは、非常にリスクが高いと言えるでしょう。

組織は、組織の統合合併、買収、売却や、クラウドなどの発展途上のテクノロジー、IoT や耐量子セキュリティー、規制コンプライアンスの変更など、IT リスクを増大させる力に直面しています。同時に、セキュリティーやコンプライアンスに対応しながらイノベーションを進め、発展しなければなりません。企業の成長の足かせになる問題には、以下が挙げられます。

- 複雑な規制要件
- セキュリティー戦略との連携、サイバーセキュリティーおよびコンプライアンス成熟度の欠如
- 頻繁な組織的変更
- セキュリティー・スキル不足
- セキュリティーの「ベスト・プラクティス」に関する不確実性

279 日

データ漏えいを検知し阻止するために必要な時間の世界平均

25,575 レコード

データ漏えいの世界平均規模

ビジネス損失

データ漏えいコストの最大要因[1]

リスクに対抗するアクション

最新のサイバーセキュリティー脅威と規制コンプライアンスに対応するのは容易ではありません。多くの企業が、自社のサイバーセキュリティーおよびコンプライアンス対策に対する理解を深め、ベスト・プラクティスを学習し、サイバー空間での不確実性の中でビジネス目標を達成するために、信頼のおけるアドバイザーの助けを借りています。信頼のおけるアドバイザーがいれば、混乱を予測し、変化するセキュリティー・ランドスケープに適応し、セキュリティーを視野に入れながら、新しいイノベーションを進めて競争上の優位性を獲得できます。

大規模組織では、リスク、コンプライアンス、ガバナンスをより効率的に管理するための計画を策定する際に、正確なベンチマークが必要です。これらの評価には、リスクの定量化、外部組織によるセキュリティー・リスクの特定、自分のシステムの弱点を見つけるための侵入テスト、従業員やテクノロジーを検証するサイバー攻撃シミュレーション、要件の特定、サイバー攻撃に対応するための組織文化の構築が含まれます。

サイバー攻撃対応訓練は、大手組織のリスク管理戦略の一部として組み込まれつつあります。訓練では、セキュリティー・チームと経営幹部が、セキュリティー攻撃シミュレーションを同じ環境で体験し共有できます。サイバー攻撃対応訓練を体験することにより、組織のインシデント対応計画の抜け穴を評価し、セキュリティーおよびコンプライアンス・チームがインシデント対応を組織全体にどのように統合すべきかを批判的に評価できます。

Finastra 社のサイバー攻撃措置を IBM が検証

ロンドンに拠点を置く Finastra 社は、世界最大規模の金融テクノロジー企業で、サイバー攻撃対応訓練を受けて、大陸を超えたデータ漏えいに対処する自社の能力を IBM Security を活用して検証しました。

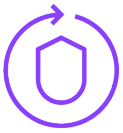
動画を見る

セキュリティー・リスク管理の柱: 評価、軽減、管理

セキュリティー・リスクを最小限に抑えるためには、組織の弱点とその対応策を特定する必要があります。

サイバーセキュリティーおよびコンプライアンスに対する現在の取り組みを評価

リスク軽減方法を特定



今後のリスクを管理

この種のセキュリティー内省をする場合、適切な質問をし、効果が実証されているアプローチを使用して結果を出す、組織外からの視点を持った、経験豊富で信頼のおけるアドバイザーがいると大いに役立ちます。**データ漏えい、規制違反など、組織の評判や利益に損害を与えるリスクを持つ隠れたセキュリティー脆弱性を発見する必要があります。**

セキュリティー・アドバイザーは多数の事例と業界のベスト・プラクティスを基に、効果が実証されているメソドロジーを使って、アイデンティティー・リスクとソリューションの両方を特定しリスクを軽減できます。

セキュリティーは継続的に対応する必要がある問題です。アドバイザーは、セキュリティー・モニタリング、管理、トレーニングを継続的に提供し、お客様のセキュリティーおよびコンプライアンス・プログラムを長期的に調整するため、お客様は、強力なセキュリティーおよびコンプライアンス対策を維持し、セキュリティーに対する企業文化を育成し、新しい脅威に対応することができます。

成功するセキュリティー戦略は、上層部から始まります。信頼のおけるアドバイザーは、最も重要なセキュリティーおよびコンプライアンス・イニシアチブのためのリソースの優先順位付け、意思決定の連携、経営幹部からの支持を獲得するための推奨事項をセキュリティー・チームに提供できます。セキュリティーはデジタル戦略および転換イニシアチブの中心部分であるため、これには、クラウド、IoT、モバイルなどのイニシアチブが含まれます。

信頼できるアドバイザーが、リソースの優先順位付け、意思決定の連携、経営幹部からの支持を獲得するための推奨事項をセキュリティー・チームに提供する

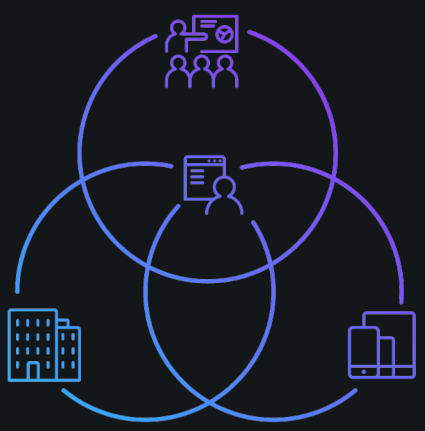
予想外の事態に対応

リスクはあらゆる所に潜んでいます。それは、会社の外から、隠れたランサムウェアや総当たり攻撃の形で現れ、そこに注意を奪われている間にデータを盗み出します。あるいは、会社の内側から、信頼されたアイデンティティーの陰に潜んでいたり、あるいは単純な人為ミスを通して現れます。また、自動化された工場にはじまり、AI を使用した顧客対応センターにいたるまで、商機の陰に潜んでいます。

リスクを明るみにさらし、解明するには信頼のおけるアドバイザーが必要です。**ガバナンス、リスク、コンプライアンスの管理を改善するためには、組織のリスクの全容を正確に把握する必要があります。** 誰でも、サイバー攻撃の被害に遭うまでは、自分が被害者になるとは思っていません。セキュリティー・アドバイザーは、リスクを特定、定量化、優先順位付けし、それを管理します。

信頼のおけるリスク管理は、１人の個人、または１つのチームの責任ではありません。これには、すべての人、機械、組織の要素を横断し、事業部門、リーダー、プロセスにわたって連携された、系統的なアプローチが必要です。

信頼のおけるリスク管理には、すべての人、機械、組織の要素を横断し、事業部門、リーダー、プロセスにわたって連携された、系統的なアプローチが必要です。



IBM Security の信頼性

IBM Security があれば、リスクに一人で立ち向かう必要はなくなります。IBM のサービスにより、プロセス、人、テクノロジーにわたってリスクを効果的に管理する、適切なセキュリティーおよびコンプライアンス能力を手にできます。セキュリティー環境は新しい脅威の方向、新しいコンプライアンス規制、または予想もしない事態によって変化していますが、IBM のセキュリティーに関する専門知識を活用すればリスクを常に確認できます。

IBM Security の提供する専門知識を利用することにより、効果的なセキュリティー戦略を構築し、組織全体のセキュリティーおよびコンプライアンス対策を批判的に評価し、能力 （データ漏えいにどれだけ迅速に対応できるかなど）を正確に測定し、管理体制の中にある弱点を特定できます。IBM Security には、以下をはじめとする、お客様のリスクを評価、軽減、管理するために必要な人、メソドロジー、経験があります。

IBM Security Strategy Risk and Compliance Services (SSRC): お客様の現在のセキュリティー・ガバナンスを企業目的に照らし合わせて評価し、リスク管理戦略およびプログラムの策定をお手伝いし、セキュリティー成熟度の向上を支援します。IBM は、以下を通してお客様のリスク、コンプライアンス、ガバナンスの管理改善をお手伝いいたします。

- 経営幹部および経営役員に対するセキュリティー・アドバイス・サービス
- リスクの定量化
- 合併/買収のセキュリティー・リスク査定
- クラウド・セキュリティーとコンプライアンス対応
- データ・プライバシー戦略
- 規制遵守およびガバナンス
- 外部組織によるセキュリティー・リスク査定および管理
- 自動化された IT リスク管理
- 重要インフラのセキュリティー
- SAP セキュリティー戦略評価およびリスク軽減
- 従業員のセキュリティー意識管理

SSRC による、セキュリティー・リスクの評価、軽減、および管理。規制遵守、データ・プライバシー・レディネス評価、リーダーシップのためのリスク定量化など、IBM Security Strategy Risk and Compliance サービスが専門家のガイダンスを提供します。

IBM Security Command Centers: IBM Security Command Centers は、セキュリティーに対する企業文化と準備状況を改善し、攻撃に備えます。サイバー攻撃対応訓練を通して、複数の部署にわたって構成されたチームが、セキュリティー攻撃のシミュレーションを体験することで、現実のサイバー攻撃シナリオに対処するためのスキルと自信を獲得できます。Executive Briefing Center では、お客様のセキュリティー対策を大幅に改善しリスクを最小限に抑える、経験豊富なインシデント対応者、侵入テスト担当者、セキュリティー戦略家、リーダーなど、IBM のセキュリティー専門家からのサービスを受けられます。

関連トピック

コンプライアンス: お客様の組織が移動中および保管中のデータをどのように処理しているかを追跡し、コンプライアンスをいつでも証明できる状態にあるかを判定する必要があります。より簡単に管理、実装できるコンプライアンスにより、規制の変更に対応します。他の優先事項にリソースを割り当てられるよう、組織がコンプライアンスに対応するためのソリューションを使用します。IBM Security の人材とテクノロジーを使ってコンプライアンス対応を簡素化します。

リーダーシップと企業文化: 技術革新、市場の変動、スキル要件の変化などの要素により、セキュリティーおよびコンプライアンス・ポジションに影響を及ぼす流動性が発生する可能性があります。組織を守る魔法の盾はありませんが、セキュリティー傾向に関する最新の調査結果と知見、革新的なソリューションにアクセスできれば、お客様のセキュリティーおよびコンプライアンス・ポジションを改善する、効果的な対策を取ることができます。

出典

1. Ponemon Institute and IBM Security, “2019年度版 情報漏えい時に発生するコストに関する調査”

IBM Security

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in Japan
January 2020

GDPYL8KD