IBM Global Technology Services

レジリエンシー
サービス

情報漏えいに対する最善の防御の策定

事業継続性とサイバー・セキュリティーの連携で費用を節約して企業評価を保護できます

IBM

情報漏えいの影響からビジネスを保護する

情報漏えいはもはや*もし起きたら*ではなく、*いつ起きるか*という問題です。

世界中のほとんどのセキュリティー・リーダーは、この自明の真理を受け入れています。これらの専門家たちは、犯罪者ハッカーがますます巧妙になり、IT 防御が絶えず進化している中で、現在のサイバー・セキュリティー環境がこれまでになく複雑になっていることを理解しています。

絶対確実なデータ保護というのは、実現不可能でないとしても、困難な目標です。しかしサイバー犯罪と戦い、データを保護するための支援が、すぐに利用できるよう準備されています。IT セキュリティー・リーダーが情報漏えいへの対応計画立案と対応自体に事業継続マネジメント (BCM) を関与させた場合に、企業は不法侵入の可能性を低減させるとともに、万一情報漏えいが起きた場合のビジネスへの影響を緩和できるという証拠が今ここにあります。

これらは IBM が依頼して米調査会社 Ponemon Institute (ポネモン・インスティテュート) が単独で実行した、*2016 年情報漏えいのコストに関する調査: 事業継続マネジメントの効果*での調査結果です (図 1 を参照)。この調査のために、ポネモンの調査員は世界中の 383 の企業で働く 1,596 人にインタビューしました (図 2 を参照)。企業規模は、社員 500 人未満から 75,000 人以上までにわたります。全企業が情報漏えいを経験しており、影響を受けたレコードは 3,000 件から 101,000 件の間です。[1]

このレポートは、BCM をサイバー・セキュリティーの対応と連携させることが、情報漏えいによって起きる損害を緩和するのに役立つ理由を検証し、この調査からの情報を使用して BCM チームとサイバー・セキュリティー・チームの協力を形成するためのビジネス・ケースを構築しています。

図 1: Get the *2016 年情報漏えいのコストに関する調査: 事業継続マネジメントの効果*を入手する。

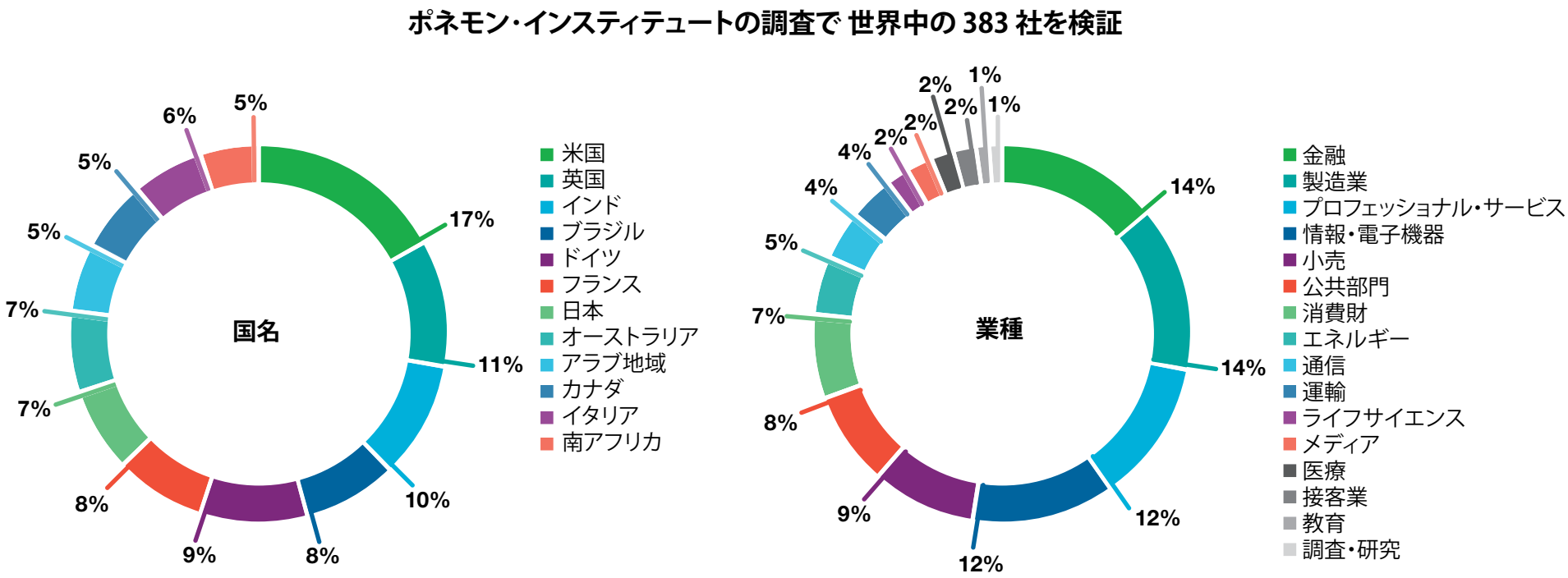

図 2: 2016 年 情報漏えい時に発生するコストに関する調査で 12 カ国の 16 業種の企業を検証しました。

BCM とセキュリティーを連携させるためのビジネス・ケース

BCM が関与しないことは、大きな損害を出す間違いとなる可能性があります。調査した企業の中では、漏えいした各レコードを修復するコストは、インシデントに対する計画立案および対応に BCM が関与した場合は 149 ドル、BCM が関与しない場合は 167 ドルで、漏えいしたレコード当たりのコストが 11% 低くなっています。これらの漏えいは何千ものレコードに影響する可能性があることから、BCM が関与した企業の情報漏えいのコストの合計は平均 371 万ドルで、BCM が関与しない企業が費やした 429 万ドルよりも 15% 低くなっています。

この調査によると、情報漏えいインシデント対応の計画と実施に BCM が関与すると、次のような効果もありました。

- 漏えいを 26% 速く検出
- 漏えいの阻止時間を 40% 短縮
- ビジネス・プロセスの中断の発生が 26% 少ない
- 重大な情報漏えいが起こる可能性が 29% 低い

しかし、情報漏えいに対する計画立案と対応に BCM を関与させるには、やらなければならないことがまだたくさんあります。調査では、参加した企業の 48 パーセントもが、これらの活動に BCM が関与していないか、非公式に関与しているだけだと言っています。この調査に含まれる明確な証拠から、企業は BCM とサイバー・セキュリティーが対応で協力するビジネス・ケースを構築する必要があるという根拠を得たことになるでしょう。

漏えいのコスト増大

情報漏えいの全体のコストが増大し続けています。なぜでしょうか。ポネモンによると、ほとんどの情報漏えいは犯罪および悪意ある攻撃によって起きています。これらの漏えいは検出や阻止に非常に時間や労力もかかるため、レコード当たりのコストが最も高くなっています。

BCM がどのように漏えいの影響を緩和するか

ポネモンの調査では、サイバー・セキュリティーの対応に BCM が関与すると、データ侵害の制限と漏えいの影響の緩和の両方ができることがわかりました。その方法は? 単一の答えはありませんが、組織構造が役割を果たしているようです。BCM と IT セキュリティーの両方が例えば企業の大きなリスク管理部門の一部である場合、2 つの間の相互作用が起きる可能性があります。IBM は、事業継続性において 50 年を超える実績があり、以下のことも信じています。

サイバー・セキュリティー運用部門は、BCM の経験とビジネス知識から学ぶことができます。

ビジネスが登場して以来、ビジネスを中断する災害が起きる可能性は存在してきました。長年の経験を経て BCM の技量は習熟してきており、イベントの検出、評価、対応において、考え抜かれて予行演習をした方法が確立されてきました。BCM のリーダーは、サイバー・イベント発生時の IT 依存関係の識別に重要な、強力なビジネス運用の知識を構築している傾向があります。情報漏えいに対する計画立案と対応に BCM が関与する組織では、この経験とビジネス知識がセキュリティーの IT 専門知識と組み合わさって、情報漏えいを防止し、漏えいが起きた場合に対応するためのより包括的な計画を作成することができます。

BCM は伝統ある厳しいテスト、準備、対応を策定して、サイバー・セキュリティーの対応を強化できます。

BCM はより長く続いている組織として、数多くのタイプのリスクを評価、モニター、緩和するための厳しい手法を開発してきた可能性もあります。これはリスク管理、機密保護、事業継続マネジメントなどのさまざまな業界標準を遵守する組織では特にそうです。広く採用されている業界標準に適合している、または認定されている企業は、リスクを識別して緩和する強力なプロセスを開発するのに必要な作業を行っています。強力なリスク管理 (ISO 31000)、事業継続への対応計画とテスト (ISO 22301)、情報漏えいに対して IT 環境を保護する能力 (ISO 27000) をとおして、組織は情報漏えいイベントに効率的に対応して迅速に終結できる可能性があります。

BCM は危機発生時にアップストリームとダウンストリームの伝達の中核として機能します。

BCM は複数分野にまたがる機能であり、通常会社の IT、運用、通信および法務部門などにまたがっています。BCM はこれらの部門の人員と強力なビジネス関係を築いて維持していることが多く、危機または中断の発生時に誰に連絡するべきかなどを大抵知っています。この伝達計画は、情報漏えいへの対応を準備し、侵害に対処し、企業評価への損害を阻止しようとする上で、セキュリティー部門にとって非常に貴重であることは明らかです。

世界各国での情報漏えいのコスト

ポネモンの調査によると、情報漏えいのレコード当たりのコストは国によって著しく異なります。調査したすべての企業 (BCM が関与している企業としていない企業) を考慮した場合、情報漏えいは米国で最も高くついており、調査した企業は漏えいを緩和するために平均でレコード当たり 201 ドルを費やしています。米国に続くのはドイツで、レコード当たり 194 ドル費やしており、その次がカナダの 189 ドルです。逆に、調査した企業の中で、インドの企業が情報漏えいの緩和に費やしているのが最も少なく、レコード当たり 51 ドルです。次がブラジルの70 ドル、そして南アフリカの 101 ドルです。

情報漏えいに対する計画立案と対応に BCM が関与すると

40% 情報漏えいの阻止にかかる平均時間が短縮

セキュリティーと BCM の共同プログラムを構築する方法

では企業はどうやって情報漏えいに対して BCM とセキュリティー運用の対応を調整するのでしょうか? IBM は次のような方法を提案します。

1. **レジリエンシー・プログラム全体の効果を判断します。** BCM とサイバー・セキュリティーは両方とも、包括的なビジネス・レジリエンシー・プログラムの独立かつ関連した構成要素として機能する必要があります。効率的なビジネス・レジリエンシー・プログラムは、情報漏えいを防止し、漏えいが起きた場合に損害を緩和するために多くのことができます。企業が現在のレジリエンシー・プログラムの効果に不安がある場合、レジリエンシー運用を、広く採用されているモデル (サイドバーの「IBM ビジネス・レジリエンシー・フレームワーク」を参照) と比較することを検討する必要があります。

2. **事業継続性とサイバー・セキュリティーの両チームに相互代表を設けます。** 指名された事業継続性とサイバー・セキュリティーの専門家はそれぞれ互いのチームのメンバーとして働く必要があります。例えば事業継続性チームの人員は、サイバー・セキュリティーの計画立案セッションに参加し、関連する事業継続性の情報、プロセス、手順を共有し、該当する場合にはサイバー・セキュリティーの諮問委員会に出席する必要があります。事業継続性の専門家は、情報漏えい対応チームの一員として、セキュリティー、BCM、ビジネス・リーダーの間を橋渡しする必要もあります。

3. **更新した事業継続性計画で共同の情報漏えいシミュレーション・テストを実行します。** 共同の情報漏えいシミュレーションと事前訓練は、情報漏えいが起きたときに、どの事業継続性プロセスと情報をインシデント対応チームがアクセスできるか、その必要があるかをサイバー・セキュリティーが判断するために特に有用なことが実証されています。そして BCM の継続性計画は、重要なアプリケーションまたは人員が長期間使えない状態で運用を継続することを考慮に入れる必要があります。さらに、BCM とセキュリティーは協力して、情報漏えいの最中とその後に行うべき行動を識別し、それらのプロセスと手順を可能な限り綿密に調整する必要があります。

BCM の関与率は国によってさまざま

世界のどの地域で、企業は情報漏えいに対する計画立案と対応に BCM が関与している傾向が最も高いでしょうか? ドイツの企業の 67 パーセントがポネモンの調査で BCM の関与ありと回答し、それから日本の企業の 62 パーセント、米国で調査した企業の 44 パーセントが関与ありと回答しています。ブラジルの企業はわずか 25 パーセントの関与率で、情報漏えいへの準備と対応に BCM の関与ありという回答が最も低く、アラブ諸国の 29 パーセント、インドの 34 パーセントが続きます。

4

危機管理担当者を任命して漏えい後の事業継続性とサイバー・セキュリティーの作業を調整します。 情報漏えいが起きたときの連絡のために、事業継続性チームのメンバー 1 人とサイバー・セキュリティー・チームのメンバー 1 人を指名します。これらの単一の連絡先の 2 人が情報を共有し、適切な修復ステップが行われていて調整されていることを確認します。焦点となるのは、分野間で、また該当する場合には企業全体で、情報の共有もできることです。

5

ニーズを識別して予算の範囲内で優先順位を管理します。 継続性およびセキュリティーの部門は、情報漏えいの際の手順を調整するために何が必要かを識別する必要があります。データ・バックアップ・プロトコルとオフサイト・ストレージを評価する必要があります。必要に応じて、ネットワーク・トラフィックのセグメント化または再ルーティングのために新しい手順を導入する必要があります。企業は、受け入れられるリスクと予算の限度のバランスを取る必要があります。「情報漏えいのコストに関する調査」を使用して、追加の資金を得るために説得力のあるビジネス・ケースの構築を始めることもできます。

IBM 社内の事業継続性とセキュリティーのプログラム

IBM はデータ保護、データ回復、およびビジネス回復力全体の分野において、市場のリーダーかつイノベーターです。これらの実践への取り組みは、まず社内から始まります。

IBM はサーバー・セキュリティーと事業継続性に対するリスクを識別して対応するための高度な社内アプローチを導入しています。この多面的なアプローチの一部として、IBM はセキュリティーと事業継続性、さらにはインフラストラクチャーとデータ管理のための方針と手順を確立しました。これらの中には、事業継続性とサイバー・セキュリティーのリスクと戦うための、技術および手順のコントロールの導入と継続的評価が含まれます。

コントロールが重なり合うことにより、セキュリティーと事業継続性の両部門が協力して、ネットワーク、ユーザー・デバイス、サーバー、アプリケーションおよびクラウド・ソリューション、そしてそれらに保管されるデータに対する脅威や攻撃に対して防御することができます。IBM はセキュリティーと継続性を企業全体にわたる関心事と考え、定期的なテスト、社内コミュニティー、その他のイニシアチブを組み合わせて使用して、社員の間でセキュリティーと継続性への認識と責任のカルチャーを育成しています。IBM はまた、グローバルなインシデント対応チームを設けて、サイバー・セキュリティーと継続性への脅威やインシデントに対応しています。

情報漏えいに対する計画立案と対応に BCM が関与すると

26% 情報漏えいの検出にかかる平均時間が短縮

IBM をお勧めする理由

世界中での何千ものレジリエンシーとセキュリティーへの取り組みをとおして、IBM はビジネスを継続させてデータを安全に保つための実績のある方法と最先端のテクノロジーを構築してきました。現在 IBM には 10,500 社以上のお客様を担当する 4,000 名の IBM レジリエンシー・サービス専門家がいます。世界中の 54 カ国で 300 を超えるクラウド・レジリエンシー・センターを運用しています。BCM とセキュリティーをより綿密に統合するのに役立つ具体的なサービスには、以下のようなものがあります。

- *IBM レジリエンシー・コンサルティング・サービス*
- *IBM 事業継続マネジメント*
- *IBM サービスとしてのレジリエンシー・コミュニケーション*

IBM ビジネス・レジリエンシー・フレームワーク

IBM ビジネス・レジリエンシー・フレームワークは、企業が相互依存型 IT およびビジネス運営に関する 7 つの階層全体でのレジリエンシー運用について検証するのに役立ちます。7 つの階層とは、ビジネス戦略とビジョン、組織と人材、プロセス、アプリケーション、データ、IT インフラストラクチャー、および施設・設備です。その検証において、フレームワークは企業がレジリエンシー運用の弱点を明らかにして、既存のレジリエンシーの状態から望ましい状態へと変わるための行程を立てるのに役立ちます。

情報漏えいに対する計画立案と対応に BCM が関与すると

$6,591 漏えいの検出から阻止までの 1 日当たりのコストを節約

レジリエンシー・コンサルティング・サービスは、企業が情報漏えいに対する脆弱性などを含む自らのリスク態勢を評価し、レジリエンシー全体の計画の一部としてデータ保護と漏えいへの対応を改善する方法を判断するのを支援します。

IBM にレジリエンシーとセキュリティーのプログラムの管理を任せたいと考える企業には、IBM は**事業継続マネジメント**・サービスを提供します。これらのサービスでは、IBM はお客様の BCM 部門の延長として機能し、IBM レジリエンシー・センターまたはお客様によって決められた場所のいずれかにおいて、レジリエンシーおよびデータ保護のソリューションのすべてまたは一部 (お客様の要望により) を管理します。

危機または中断が起きたときのインシデント管理を改善するために、IBM は**サービスとしてのレジリエンシー・コミュニケーション** を提供しています。この高可用性でクラウド対応のインシデント管理サービスは、対話型ワークフロー管理ツールを使用して計画外の重大なイベント発生時の対応時間を改善して、企業が適切なイベントに適切な時点で適切な人材を携わらせることができるようにします。

ポネモンの調査が示すように、BCM が情報漏えいに対する計画立案および対応に関与することにより、企業はビジネス運営と評価への影響を抑えながら、侵害のコストと継続時間を減らすことができます。IBM は企業が継続性とセキュリティーの作業を調整して、情報漏えいの可能性を最小に抑え、万一起きた場合にもより迅速かつ効果的に回復できるよう支援します。

情報漏えいに対する計画立案と対応に BCM が関与すると

9% 企業評価への損害を低減

詳細情報

IBM レジリエンシー・サービスが企業の情報漏えいを保護する支援を提供する方法については、以下の Web サイトを参照してください。

ibm.com/services/resiliency

[1] すべての統計は、「2016 Cost of Data Breach Study: Impact of Business Continuity Management, Ponemon Institute LLC, 2016」からのものです。

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町19-21

IBM のホームページは以下をご覧ください
ibm.com

BUW03060-JPJA-00