protiviti®
Risk & Business Consulting.
Internal Audit.

Risk Oversight vol.66
取締役会のリスク監視

サイバー攻撃リスクを自信を持って管理する

サイバーセキュリティ攻撃は引き続きメディアの高い関心を集め、取締役会において今日的な意味を持つテーマであり続けています。情報セキュリティは、戦略、リスク管理、変更管理およびアクセスコントロールの全てにおける情報システムの機密性、完全性および利用可能性（可用性）に関係しています。以下では、この重要な課題について考察します。

リスク管理においては、リスクを除去することは不可能であり、リソースは限られており、リスクプロファイルは変わり続けているというのが現実です。サイバー攻撃についても同じことが言えます。このため、変わり続けるサイバー攻撃の状況とリスク許容度を理解し不可避的に発生するインシデントに備えることにより、組織の最も重要な情報資産とシステムの保護に焦点を当てることが重要です。

主要な考慮事項

企業全体にわたって最も重要な情報資産を定義したり、サイバーセキュリティリスクに対する許容度の徹底的な評価に重点的な注意を払ったりしている企業はほとんどありません。現実には、ほとんどの企業は自らのリスク許容度は低いと考えていますが、あたかもそれが比較的高いかのように行動しています。知らず知らずのうちに、全てのシステムと情報資産に同一水準の高いリスク許容度を適用してしまうのです。実際、本当に重要な情報資産とシステムに焦点を当てている企業はほとんどありません。

実際、セキュリティを確保するということは容易ではありません。全てのサイバーセキュリティを効果的に管理できる組織はどれだけあるでしょうか。防衛境界線の内側で業務を行うために雇われたIT業務受託者によるうまく仕組まれた攻撃を防止できる組織はどれだけあるでしょうか。そのような組織は多くありません。しかし、対象を絞った投資とセキュリティリスク許容度の引き下げにより、組織は最も重要な情報資産のセキュリティ確保により近づくことができます。

誰もが自宅におけるセキュリティリスクを認識しています。ほとんどの自家保有者は、自宅が犯罪者の標的となるリスクを低減するために、全ての入り口を施錠する、外出時には照明をつけたままにする、あるいは手頃な価格のセキュリティシステムを据え付けるといった基本的な対策を講じていますし、ゲートのあるコミュニテイに住むことを選択する人もいます。しかし、これらの対策のいずれか、あるいはそれらの組み合わせによって、特定の住居に標的に定めた者による侵入を確実に防止できると本当に信じている人はいるでしょうか。おそらくはいないでしょう。

ほとんどの家の持ち主はこのようなリスクを受容しています。彼らは住居への侵入を困難にすることに加えて、家財や貴重品に保険を掛けることにより残余リスクをカバーしています。多くの人は、貴重な資産や重要な文書・記録といった本当に重要な少数の物品に焦点を当てることを合理的と考え、追加的な

予防措置を講じています。ほとんどの人は、自宅に強盗が押し入ることなど考えたくもないわけですが、自らの財産を保護するために手間を掛けたり金銭を支出したりすることを厭いません。

企業ではこのような合理的な思考プロセスをうまく適用できておらず、全社的なセキュリティの確保について誤った認識を持っています。セキュリティはハッキングや技術的侵害に関するものだけではありません。ほとんどのサイバー攻撃は巧妙に行われますが、必ずしも技術的なものだけではありません。サイバー攻撃はハッキング技術を利用する場合もありますが、攻撃者は業務受託者として防衛境界線の内側に入れば事足りるため、多くの場合にはこのスキルは必要ではありません。さらに言えば、ほとんどの組織においてはセキュリティを突破することは困難ではないことから、業務受託者になることすら必要ではないかもしれません。

ここでは、水際対策ではなく、ITセキュリティに関して適切な焦点を当てる上での3つの重要な点について考察を行います。

最も重要な情報資産を保護する上での最重要事項に焦点を当てる ― 多くの組織のITセキュリティにおける焦点は特定されているというよりも包括的となる傾向にあるため、全てのシステムについて同じ方法による保護措置が取られる、最も重要性の高い資産に十分な注意が払われない、不必要なコストが生じるといった結果となります。価値の高いデータ、情報および情報システムの識別を行うためには、IT組織が事業部門のリーダーと協力し、様々な資産に係るリスク許容度について合意する必要があります。これはITセキュリティ管理の焦点を最も重要性の高い領域に当てる上での助けとなります。取締役会の監視の下、IT組織と事業部のリーダーは、以下のような事項を検討すべきです。

- 組織における最も重要性の高いデータ、情報資産および情報システムは何か。それらが最も価値の高い資産であるのはなぜか。失われてはならないものは何か。
- 最も重要性の高い資産はどこにあるのか。それらはその場所以外には本当に存在しないのか。
- 最も重要性の高い資産へのアクセスはどのように、いくつのシステムを介して、行われているか。
- 最も重要性の高い資産へのアクセス権限を有しているのは誰か。ITサポートを行う業務受託者を介してアクセスすることは可能か。誰が、何に基づいて、業務受託者への権限付与を行っているのか。

これらおよびその他の事項の検討は、組織の予防的および発見的セキュリティ対策とインシデント発生時の対応計画において焦点を定める上で助けとなります。

変わり続けるサイバー攻撃の状況を理解する ― 最近行われたグローバルな調査では、サイバー攻撃とそれが企業の中核的事業を混乱させる可能性がリスクの上位に位置付けられており、ほとんど全ての業種において上位5のリスクの一つとされています。さらに、プライバシーや個人情報および情報セキュリティに関する課題も、上位10のリスクに含まれています。[1]

取締役は、これらのリスクや、自らの企業が直面するその他の重要なリスクを的確に理解しているでしょうか。おそらくそうではないでしょう。複数の業種にわたって前例のない規模のサイバー攻撃が行われ、知的財産と事業機密が遺失しレピュテーションが損なわれたとの報道が、取締役会に対する警鐘となったのはこのためです。取締役は、サイバーセキュリティは全社的セキュリティの課題であり、単にITセキュリティの課題に留まるものではないことに気が付き始めています。

重要なセキュリティリスクには、機密情報の漏洩、従業員のコンピューターへの意図しないウィルスのアップロード、従業員が機密情報入手を目的とするソーシャル・エンジニアリングの一層の標的となることが含まれます。多くの組織は、複数のシステムに侵入し、長期間にわたって大量のデータを収集し、そのようなデータを敵対者または攻撃者のネットワークに送信するといった高度で持続的な攻撃を含む今日の洗練されたサイバー攻撃と効果的に闘うためのプロセス、テクノロジおよびガバナンスを欠いています。

企業が持つ最も重要な情報資産、業種と事業活動の特性、および潜在的な攻撃目標としての知名度に基づいて、経営者は

※1 プロティビティとノースカロライナ大学ERMイニシアティブが行った調査の結果「Executive Perspectives on Top Risks for 2015: Key Issues Being Discussed in the Boardroom and C-Suite, Protiviti and North Carolina State University's ERM Initiative」は、以下のウェブサイトから入手可能です: protiviti.com/toprisks

組織のサイバーセキュリティリスクを評価し、以下の事項を検討すべきです。

- 誰が攻撃を行ってくる可能性があるか。
- どのように攻撃を行ってくる可能性があるか。
- 自社の最大の脆弱性はどこにあるか。
- 業務委託先と社内関係者に対するエクスポージャーは何か。
- これらの課題の管理における現在の内部統制はどの程度有効で、何が我々にとっての負担になっているか。
- 侵入テストを行っているか。そうであれば、どのようなテスト結果であったか。
- 内部監査人および外部監査人はどのような課題を指摘しているか。
- 過去のサイバー攻撃の特質と深刻度はどのようなものであったか。再度攻撃が行われた場合に、どのようにそれを知ることができるか。
- 何かが生じた場合の事業への影響を明確に理解しているか。

これらおよびその他の事項への回答は、変わり続けるサイバー攻撃の状況を明確にし、セキュリティ対策の実施において方向性を示す上で助けとなりうるものです。

インシデントや危機に備える — 組織が取る予防的措置にも関わらず、様々な規模のサイバーインシデントは不可避的に発生します。企業が効果的なインシデント対応計画の策定に率先して取り組む必要があるのはこのためです。対応計画は、機密データや個人特定情報を保持する組織にとっては特に、単なるベストプラクティスというだけではなく、然るべき注意を払う義務があり、かつそれを実践しなければならないものでもあります。

過去においては、多くの組織は事業継続性テストを1年または半年ごとに行っていました。これらのテストは、発生可能性が比較的低いインシデントへの企業の対応について完全なシミュレーションを行うというものでした。現在、組織は発生可能性が比較的高い事業継続に関するインシデントが生じる恐れに直面していますが、そのようなインシデントに対する適切な準備を行っている組織はほとんどなく、事業継続性テストを行っている組織はさらに少ないというは皮肉なことです。事業継続プログラムのテストと同じロジックを、効果的なインシデント対応プログラムにも適用することが必須です。率先した対応を行うことにより、組織が予期せぬ事態に対処し、最悪の事態に備えた計画を立てることが可能になります。

効果的なインシデント対応プロセスは、サイバー攻撃の影響を低減する準備をするために非常に重要です。包括的なインシデント対応プログラムに関する予算措置を確実にするためには上級経営者のサポートが必要です。伝統的に、最高情報責任者以外の上級経営者は、インシデント対応計画の実施にほとんど関与してきませんでした。しかし、米国国立標準技術研究所が作成したサイバーセキュリティの枠組み、侵害事案の開示に係る要件、および個人特定情報に関する業界規制と基準が出されたことや、重大な侵害事案に関する最近の報道を受けて、上級経営者は現在、このような取り組みをよりサポートするようになってきています。これらのプログラムは、現行のITセキュリティの統合と補完を行い、様々なステークホルダー（例えば、コンプライアンス、IT、企業セキュリティ、広報、法務）の視点と関与を組み込んだインシデント発生時において従わなければならない明確な方向性と中核的プロセスを提供します。

このプログラムは、組織内のグループと個人に対して役割、責任および説明義務を割り当て、対応と開示に関する重要な意思決定への適切なステークホルダーの関与を確実とする報告ルートと情報伝達手続を定め、具体的なインシデントの種類に応じて取るべき行動に関する指導要領を示すべきです。例えば、分散型サービス妨害（DDoS）攻撃への対応方法は、マルウェア・インシデントの管理方法とは大きく異なります。

インシデント対応計画は、少なくとも1年ごとに評価を行い、インシデント対応や侵害事案の開示に関する規制上の義務に対応しなければなりません。また、インシデント対応計画は組織の決定を素早く行動に移すために、適切な関係者が法執行当局およびメディとのコンタクトを維持することを確実なものにしなければなりません。また、インシデントの範囲や内容が社内の人的リソースだけでは量あるいは能力を超える場合には、信頼性と適格性を備えた第三者の支援を得られるようにすべきです。

取締役会の考慮事項

以下は、事業体の活動に内在するリスクの特質に関連して取締役会が考慮すべき事項です。

- 遺失を許容できない自社にとっての最も重要な資産および／あるいは何としてでも予定外の機能停止を生じさせてはならないシステムを識別しているか。それらの資産は保護されているか、またどのように保護されているかを把握しているか。自社のセキュリティ戦略において、最も重要性の高い資産と一般的なサイバーセキュリティを区別しているか。
- サイバー攻撃の状況と最も重要性の高い資産に関するリスク許容度について、定期的な評価を行っているか。自社の最も重要な資産とシステムは本当に安全と信じているか、および／あるいは識別されたリスク事象は発生しえないと考えられるか。
- セキュリティ・インシデントを許容水準に低減するための自社の戦略は、バランスが取れており、的を絞っているか。率先してインシデント対応計画の定期的なテストを行い、その有効性を評価しているか。
- 許容しえないセキュリティ・インシデントが何かを把握しているか。セキュリティ侵害の発生、急増あるいはそれによる重大な影響というリスクを低減するための有効なインシデント対応プロセスが整備されているか。主要なステークホルダーは、組織の規模、文化、規制上の義務、および事業目的に適した計画の策定をサポートしているか。
- 自社のインシデント対応計画は、具体的なインシデントの種類に応じて取るべき行動に関する指示を示す手続きによって補完されているか。対応計画は定期的に評価されているか。対応の監督において取締役会が主たる役割を担うべき事象が何であるかが明確になっているか。

プロティビティの支援

プロティビティは、セキュリティとプライバシーの評価、構築、変革および管理に関する多様なサービスを提供し、組織がセキュリティおよびプライバシー・エクスポージャー（例えば、顧客データの遺失、収益の逸失、あるいは顧客に対するレピュテーションの低下）を識別し、それらが問題となる前に対応を行うのを支援しています。プロティビティには、企業のセキュリティ・インシデント対応、率先的なセキュリティ・プログラムの構築、個人特定情報やアクセス管理への取り組み、および業種特有のデータ・セキュリティやプライバシー事項の取り扱いに関する支援について明確な実績があります。世界クラスのインシデント対応およびフォレンジック調査実務の構築および強化における経験と専念によって、プロティビティはセキュリティ戦略、対応実施、フォレンジック分析、および対応計画策定について深い専門知識を有しています。

プロティビティについて

プロティビティ（Protiviti）は、リスクコンサルティングサービスと内部監査サービスを提供するグローバルコンサルティングファームです。北米、日本を含むアジア太平洋、ヨーロッパ、中南米、中近東、アフリカにおいて、ガバナンス・リスク・コントロール・モニタリング、オペレーション、テクノロジ、経理・財務におけるクライアントの皆様の課題解決を支援します。プロティビティのプロフェッショナルは、経験に裏付けられた高いコンピテンシーを有し、企業が抱えるさまざまな経営課題に対して、独自のアプローチとソリューションを提供します。

protiviti®
Risk & Business Consulting.
Internal Audit.