ISSUE 113

BOARD PERSPECTIVES:

取締役会のリスク監視：Risk Oversight

サイバーセキュリティに一層の焦点を当てる

サイバーセキュリティに関しては、多くのことが言われており、重要な洞察が提供されています。脅威のレベルはますます高まる一方で、取締役会においても依然として重要なトピックとなっています。ただ、新しい話しは何かあるのでしょうか。

取締役会の監視において重要分野であるサイバーセキュリティに関して新たな視点を確認すべく、プロティビティは、2018年12月の全米取締役協会主催のディナーラウンドテーブルで20人の現役取締役と会い、彼らの経験について協議しました。以下は、その協議からの重要なポイントです。

防御と検知には過剰投資とならないように、対応と復旧には過小投資にならないようにしましょう。 効果的なサイバーセキュリティは、防御から始まり、検知、特定、対応および復旧と進んでいきます。プロティビティは、NISTフレームワーク[1]で定義されているこれら5つのサイバーセキュリティのステップを活用して、経営陣がこれらのステップ全体でそれぞれの会社における進捗状況を評価するグローバル調査を後援、支援しました[2]。調査結果によると、防御と検知で最も評価が高く、特定、対応および復旧が最も低いことがわかりました。サイバーセキュリティへの投資が、ほとんど防御ステップに対処するためのものであったことから、参加した経営陣は、避けることのできないサイバー攻撃に対して、検知と対応において、バランスの取れたプログラムが組織には必要であることで意見が一致しました。

ただ、ほとんどの取締役は、全体的なサイバーセキュリティ予算しか見ていないと報告されており、NISTの5つのドメインにわたる会社の投資は十分に認知されていません。

ある取締役は、NISTフレームワークを使用した成熟度評価と、5つのドメイン全体の進捗状況を監視して、それらを望ましい成熟度レベルまで改善することについて語っていました。全体として、サイバーセキュリティに関しては、組織は防御のステップを超えて次に進むことが重要となります。取締役会は、経営陣と協力して、サイバー侵害を特定、検知、対応、復旧する組織能力を定期的に評価および監視し、適切な投資が各ステップを支えていることを確認する必要があります。推奨される有益な一つの手順は、発生する可能性のあるサイバー攻撃のシナリオを実行し、結果を確認することです。サイバーセキュリティへの対応と復旧機能を評価することによって、大変役に立つ成果を得ることが可能となります。

サイバー対応の「リーダー」と「初心者」の間の侵害検知におけるパラドックスを理解しましょう。 プロティビティの調査では、デジタルリーダーは初心者よりも多くのサイバー攻撃を

1 NISTサイバーセキュリティフレームワークは、米国の民間組織にコンピューターセキュリティガイダンスを提供します。www.nist.gov/cyberframeworkで入手できます。

2 「サイバーセキュリティの必須事項：急速なデジタル化の世界におけるサイバーリスクの管理」は、ESI ThoughtLab、WSJ Pro Cybersecurity、プロティビティ、およびその他の組織の共同努力により、複数の業界を対象に、ベンチマーク分析およびパフォーマンス評価のツールを利用して、1,300人の世界の経営者を対象とした厳密なグローバル調査と分析を実施したものです。この調査は、http://go.dowjones.com/cybersecurity-imperativeで入手できます。

protiviti®

Face the Future with Confidence

報告していることがわかりました。ラウンドテーブルでは、デジタルリーダーがセキュリティ活動の監視に優れ、より強力な検知手段を持っている可能性など、いくつかの理由が明らかになりました。また、採用する新しいテクノロジーとデジタル化により、攻撃対象領域が拡大する可能性が高くなります。組織は、デジタルの成熟度を高めるために、常に集中し、サイバーセキュリティを最優先事項に位置づける必要があります。リスクを最小限に抑えるために、企業はデジタル変革プロセスの各ステップにサイバーセキュリティを組み込む必要があります。

イノベーション資金の「サイバー萎縮」を管理しましょう。取締役会は、イノベーションを抑制することなく、サイバーリスクにどのように効果的に対処するのでしょうか。この重要な問題は両刃の剣と言えます。それは、ほとんどのイノベーションは、常に新しいデジタルテクノロジーの採用を伴うため、サイバーリスクが増大するからです。ラウンドテーブルでは、イノベーションそのものは、そもそもビジネス戦略に関するものであり、ITや「イノベーション」そのものの予算項目の一つであってはならないと強調されていました。それは、むしろ、企業の成長戦略の全体的な予算の一部であるべきということです。また、イノベーションを安全に推進するため、イノベーションチームが使用する設計や開発アプローチにおいては、例えば、アジャイルやDevOps含めて、リスクとサイバーセキュリティを組み込む必要があります。

内部の敵に気をつけてください。プロティビティの調査によると、ほぼすべての企業(87%)が、外部の攻撃者への抜け穴を提供する可能性のある、訓練を受けていない一般スタッフをビジネスに対する最大のサイバーリスクと見ています。何人かの取締役が指摘したように、内部の脅威と戦う上で役立つ解決策はありますが、通常、取締役会はそれらがどれほど効果的かを認識していません。国家や洗練された外部の攻撃者による攻撃にさらされているのは、これらのグループが訓練されていないインサイダーを悪用することが多いためです。取締役は、第三者へのエクスポージャーを含むインサイダーリスクについて何が行われているかについて、取締役会がサイバー管理に関する問い合わせの量を増やす必要があることに意見が一致していました。低コストのサイバーセキュリティ対策はもちろんのこと、いろいろと試行錯誤した人もいますが、少なくともインサイダー対策のために、従業員のトレーニングとコミュニケーションを続ける必要があります。

サイバーリスクを定量化して「クラウンジュエル(最重要分野)」に価値を置くにはいくらかかるかを理解しましょう。定量化は、組織が維持するさまざまな種類のデータおよび情報システム資産と、最も防御する必要があるものを理解する上で、経営者と取締役会を大いに支援し、資産保護の優先順位付け方法を監視することを可能にします。FAIR方法論は、リスクシナリオをシミュレートするモンテカルロ法などの手法を使用して、リスクを分析するためにリスク定量化ソフトウェアを採用しているため、この分析を支援できます。定量的リスク分析を実施すると、ITチームとセキュリティチームはリスク選好の閾値を設定し、取締役会とのサイバーセキュリティ・コミュニケーションの強化につながります。リスクが財務的に定量化されると、リスクベースの意思決定を含め、サイバーリスク管理が強化されます。

サイバーセキュリティの監視に対する取締役会の信頼を高めましょう。サイバー脅威は理にかなった懸念事項です。100年にわたって確立され、育まれた企業の評判は、たった1つのサイバー攻撃により深刻で永く続く損害を被ることがあるのです。その結果、組織内および第三者を含む環境下において、サイバーセキュリティリスクの監視方法について、取締役会が完全な自信を持つことは困難です。ラウンドテーブルの参加者は、取締役はこの情報は経営陣に頼らなければならないが、取締役会は、適切な質問を行い、独立した立場の者から保証の提供を受け、焦点を合わせたダッシュボードを監視し、評判とブランドイメージを維持し続けることが如何に必要かについて、明確な期待を設定し、取締役会の監督機能を常に最新のものとしていくことが重要であるとの認識で一致しました。

変化する景観をしっかりと把握しましょう。ラウンドテーブル議では、変化するサイバー脅威の状況と、進化する情報を常に把握することの重要性について多くのコメントが寄せられました。(例:ランサムウェア、クレジットカードや、未承認のモバイルデバイス、第三者の脅威、国家が支援するサイバー攻撃を超えて拡大するデータ価値など)。進化する脅威は複雑化することにより、機密情報やその他の機密情報の開示に対する懸念から、とらえどころのない目標となることから、民間部門と公共部門の間の協力と情報共有の強化が必要になっています。今や、ゲームのルールが変更されたのです。顧客の個人データやクレジットカード情報を保有していない場合でも、実質的にどの組織もサイバー攻撃の影響を受けやすくなっているのです。

重要な洞察を含むNACDラウンドテーブルのさらなる詳細については、イベントに関して、プロティビティが取りまとめた概要をご覧ください。(www.protiviti.com/US-en/insights/active-directors-cybersecurity)

取締役会の考慮事項

以下は、企業の業務に内在する固有のリスクに基づいて、取締役会が検討した方がいいと思われる推奨される質問です。

- 会社は、それが代表するもの、或いは事業推進上の、またはそのIPの価値に基づいて、国家レベルのターゲットになり得るでしょうか。もしそうなら、会社は必要とされる高度な検知および対応能力を備えていますか。脅威の根源の高度化が進んでいることを考えると、攻撃活動のシミュレーションは定期的に実行され、防御活動により違反を検知してタイムリーに対応できるようになっていますか。

- 取締役会は、経営者に対するサイバーセキュリティへの期待を定義し、結果に対する明確な説明責任を確立していますか。組織にリスク選好の声明がある場合、サイバーセキュリティに対する取締役会の期待は組み込まれているでしょうか。

- 取締役会は、サイバー問題に関して経営陣が使用する報告と指標に満足していますか。指標は、最優先のサイバーリスクの管理方法に関する主要なパフォーマンスとリスクの指標をサポートし、取締役会の監督に情報を提供する領域に対応していますか。脅威の変化に応じて追加の洞察を提供するために、メトリックは時間とともに改善されていますか。

検討すべき取締役会に関するその他の質問については、www.protiviti.com/US-en/insights/active-directors-cybersecurity での完全な要約をご覧ください。

プロティビティの支援

プロティビティは組織と協力して、基本的な情報セキュリティの質問に焦点を当てます。

- 最も重要なデータおよび情報システム資産（「クラウンジュエル」）とそれらの場所を知っていますか。これらの資産に関して、我々はそれらを適切に世話しているか、誰から保護しているか、防御は意図したとおりに機能しているか。誰にアクセスを許可すべきか、どのように理解しているのか。

- 新しいサイバー脅威を認識し、可能性のある攻撃手法をタイムリーに検出できますか？ もし検出できるなら、保護対策を脅威に対応できるように調整できますか。

- インシデントが発生した場合、再び発生しないようにすることは可能ですか。

プロティビティは、さまざまなセキュリティおよびプライバシー評価、アーキテクチャ、変換、および管理サービスを提供し、組織が問題を把握する前に、セキュリティおよびプライバシーの危険性を特定して対処できるようにします。すべての業界の企業と協力して、プロティビティは、情報セキュリティプログラムの成熟度とコントロールの有効性を評価し、必要に応じて改善点の設計と構築を支援します。プロティビティには、ワールドクラスのインシデント対応で、企業がセキュリティインシデントに対処し、プロアクティブなセキュリティプログラムを確立し、IDとアクセス管理を行い、業界固有のデータセキュリティとプライバシーの問題を処理することに関して、実証済みの支援実績があります。

Board Instituteが取締役会のリスク監視の新たな評価ツールを公開

TBI Protiviti Board Risk Oversight Meterは、取締役会が自らのリスク監視プロセスを見直し、真に重要性のある機会とリスクに焦点を絞ることを確実にする機会を提供するものです。プロティビティは、企業が自信を持って未来に立ち向かうための継続的なプロセス改善を促進することにコミットしており、柔軟で費用対効果に優れたツールを提供するためにBoard Instituteと協力しています。このツールは、取締役会が自らのリスク監視について行う定期的な自己評価を支援するものであり、多くの取締役が好ましいと考える自己評価のあり方を反映したものです。

詳しくはこちら：www.protiviti.com/boardriskoversightmeter

プロティビティについて

プロティビティは、企業のリーダーが自信をもって未来に立ち向かうために、高い専門性と客観性のある洞察力や、お客様ごとに的確なアプローチを提供し、ゆるぎない最善の連携を約束するグローバルコンサルティングファームです。27ヶ国、75を超える拠点で、プロティビティとそのメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジー、オペレーション、データ分析におけるコンサルティングサービスを提供しています。プロティビティは、Fortune 1000の60%以上、Fortune Global 500の35%の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。プロティビティは、1948年に設立され現在S&P500の一社であるRobert Half International（RHI）の100%子会社です。

protiviti®