protiviti®
Face the Future with Confidence

取締役会のリスク監視：Risk Oversight

サイバーリスクの監視における課題

今日、どの取締役会も、常に変化しつつあるサイバー脅威の環境の中で、自社の保護に向けられる限られたリソースの投資を監視するという課題に直面しています。プロティビティが複数の現職取締役と行った最近の議論の中で、取締役会の監視に密接に関連するサイバーセキュリティに関する興味深いトピックが複数特定されています。

ISSUE 101

企業が顧客体験を変革し、グローバルな成長戦略を実行するためにデジタル・テクノロジーへの依拠を拡大し続ける中、サイバーセキュリティは最重要リスクとして舞台の中央に留まると考えられます。プロティビティとノースカロライナ州立大学のERMイニシアティブが実施した最近のグローバル調査[1]では、700名を超える取締役と上級経営者が、サイバーリスクを全体の中で3番目に重要なリスクに位置付けており、金融サービス、テクノロジー、メディア・コミュニケーション、ヘルス・ライフサイエンス、およびエネルギー・公益事業において、事業にとって「大きな影響のある」リスクとしています。取締役とCEOのどちらも、サイバーを2番目に重要なリスクと評価しています。

今日の企業は2つのグループに分類されます－セキュリティ侵害が発生し、そのことを認識している企業と、セキュリティ侵害が発生しているが、そのことを認識していない企業です。サイバーセキュリティ・リスクの管理における現実は、それらのリスクを排除することは不可能であること、また、それらのリスクを管理するためのリソースは有限であり、リスク・プロファイルは常に変化しており、なかなか安全性の確保に近づけないということです。さらに、組織はイノベーションを行い、競争力を維持するために、ITリソースを必要としています。サイバーリスク対応への要請は重要ではありますが、取締役としては、それがIT予算の多くを占め、イノベーションを抑圧することがないようにすべきです。

2017年12月、全米取締役協会(NACD)のイベントにおいて、プロティビティは18名の現職取締役との夕食を兼ねたラウンドテーブルを開催し、取締役会のサイバーセキュリティ監視について議論を行いました。多くの議論が行われてきたトピック、例えば、限られた保護措置を組織の最も重要な資産とシステムの可用性に向ける、常に変化し続ける脅威の状況と関連するリスク許容度を理解する、および不可避的に発生するインシデントに備えるといったトピックを再び取り上げるのではなく、議論に参加した取締役は、取締役会レベルにおけるサイバーリスク監視に関するその他の興味深い洞察を明らかにしています。以下では、議論となったトピックを紹介します。

戦闘に勝利しても戦争に勝利するとは限らない

ラウンドテーブルにおける議論では、政府機関、産業施設、インフラストラクチャ、および多くの事業組織を標的とした、国家の支援を受けた攻撃が、より強力かつ高度なものとなってきていることに焦点が当てられました。高度持続的脅威(APT)への実効性のある対抗は、より早期の発見とより高度な対応戦術を必要とします。しかし、ほとんどの米国企業は、サイバーに関しては1990年代の作成計画を運用しているように思われる一方、中国などの攻撃側の国家は2050年の作戦計画を用いているように見られます。

ATPを特に危険なものとしているのは、企業の予防的対抗措置に適応できるということです。ATPは、コンピューターあるいはネットワーク・サーバーに侵入しマルウェアを送り

1 Executive Perspectives on Top Risks for 2018, Protiviti and North Carolina State University's ERM Initiative, December 2017, available at www.protiviti.com/toprisks.

込むための経路を変えることができ、マルウェアの中身も徐々に変えられているかもしれません。ATPは、目的を達成した後は痕跡を隠そうとするか、あるいは不確定期間休止状態にあり、定められた時点ないしは指定された状況になった際に活動を開始するため、気付かれないことが目標となります。

これらの脅威のペースについていく(あるいは、ほとんどの場合には、追いつく)ための軍拡競争において、企業は政府が提供する利用可能な情報を利用し、準備度合いを高めるためにそれを用いることにコミットする必要があります。取締役は経営陣に対して、エマージングリスクについての情報を得ることができるよう、政府部門の適切な窓口との関係構築・維持を提案すべきです。例えば、攻撃者が持つリソースが増加し、攻撃者が用いる手法がより高度になる中、米国の規制当局とさまざまな政府機関は、複数の業種を対象とした情報共有分析センター(ISAC)を立ち上げました。ISACは非営利組織であり、重要なインフラストラクチャに対するサイバー脅威に関する情報の収集と共有を行うための一元的なリソースを提供しています。多くの情報が提供されているため、企業は情報のモニタリングを継続的に行うために十分なリソースを配分し、新たな脅威や顕在化しつつある脅威に対応するために取るべき行動を決定すべきです。

検知能力の向上

ラウンドテーブルに出席した取締役は、ほとんどの企業における対抗措置の成熟度と、リスクのより実効的な低減を促進する上で取締役会レベルが行い得ることについての懸念を挙げました。経営者と取締役会が、自社が象徴するもの、自社が行っていること、および自社が保有する知的財産に基づいて、自社がATPの標的になっていると考えるのであれば、組織のサイバーセキュリティ能力は、高度な攻撃者や企業の内部関係者を牽制するために伝統的に用いられてきたコントロール、ツール、および対応の仕組みを超えたものに進化させる必要があります。プロティビティの経験では、ほとんどの業種にわたって、発見的コントロールやモニタリング・コントロールは変化し続ける脅威の状況に比して成熟度が低い状態に留まっており、適時にセキュリティ侵害を検知できないままとなっています。

想定される攻撃活動のシミュレーションを定期的に実施し、防衛の仕組みによってセキュリティ侵害が検知され、セキュリティ・チームが迅速に対応できることを確実とすべきです。しかし、そのようなシミュレーションに関するプロティビティの経験では、あまりにも多くの場合において、テストの実施を許可したお客様の企業は、プロティビティのテスト活動を検知できませんでした。多くの経営者が考えているのとは反対に、セキュリティ・サービス・プロバイダへの管理業務の委託によって問題が解決するものではありません。これは、多くの場合、プロセスや企業とサービス・プロバイダ間の調整が破綻し、その結果として攻撃活動が検知されないためです。高度な攻撃者が、セキュリティ侵害活動の適時の検知に繰り返し失敗してきたシステム環境に侵入することになれば、ゲームオーバーです。

期待を経営者に明確に伝える

ラウンドテーブルに出席したある取締役は、最高情報責任者(CIO)あるいは最高情報セキュリティ責任者(CISO)が、「心配する必要はありません、その件については対応しています」と主張したり、同じように押し返したりしてきたときには、対話が行き詰まり、取締役は対話をどこに進めたらよいかがわからなくなり、サイバーリスクの低減について不十分にしか理解していないままとなる傾向があると述べています。これに続くラウンドテーブルでの議論では、以下の複数のテーマが示されています。

- **適切な問いを投げかける** — 取締役会が、状況認識、戦略と業務、内部関係者による脅威、インシデント対応、およびその他の関連するトピックについて、適切な問いを投げかけることが重要です。(全米取締役協会が2017年に公表したサイバーリスク監視に関する資料の付録に、関連性のある問いが提示されています。)[2]

- **取締役会の構成の見直しを検討する** — 取締役会がITとセキュリティに関するより多くの専門知識から得るところがあるのであれば、テクノロジーの専門家−取締役、あるいは取締役会に助言を提供する第三者−が必要であるかもしれません。取締役会は「ビジネスパーソン」を取締役に迎え入れる傾向があるため、求められるテクノロジーに関する経歴を持つ者(および/あるいは助言者)を迎え入れるべきか検討する意義があるかもしれません。

- **サイバーセキュリティあるいはテクノロジーを担当する取締役会委員会を別個に設置する** — 脅威の状況の重大性、および企業の事業戦略の実行におけるテクノロジーの役割にもよりますが、このことは常に選択肢の一つです。

取締役が詳細な点に立ち入るための時間は限られていますが、取締役は、企業のレピュテーション、ブランドイメージ、および顧客からの評価・信用に影響を与え得るサイバーインシデントに関する期待を、全ての階層の経営者に対して明確とすべきです。サイバーセキュリティ戦略とリスク許容

2 See Appendix A, NACD Director's Handbook Series on Cyber-Risk Oversight, NACD, 2017, available for purchase at www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687.

度に関する期待は、企業のリスクアペタイト・ステートメントに組み入れるべきです。

サイバーセキュリティに関する取締役会への報告と指標の改善

エクィファクス社や他社におけるセキュリティ侵害の重大性は、取締役会として自らが認識していないことが何であるのかを明確にするために十分な深度で調査を行っていたのかという問いを投げかけています。この観点から、ラウンドテーブルに出席した取締役は、あまりにも多くの場合において、取締役会への報告ではハイレベルの情報のみが提供されていると述べています。従って、問うべきであるのは、サイバーセキュリティに関するどのような報告と指標を取締役会は要求すべきであるか、ということです。ラウンドテーブルでの議論では、検討すべき複数の重要領域が示されています。

- **システムの脆弱性の数** — 経営者は、リスクの高いシステムの脆弱性を特定し、その推移を報告すべきです。取締役会は、経営者による脆弱性の特定、定量化、および優先順位付けが十分なものであると考えているでしょうか。

- **パッチ適用に要する時間** — 認識済みのリスクの高いシステムの脆弱性に対するパッチ適用に要する時間は、通常は60日から90日です。一般的には30日が望ましい基準と考えられていますが、それすら長すぎる場合もあります。[3]

- **セキュリティ侵害の発見に要する時間** — 攻撃が開始され、それが最終的に発見されるまでに経過する時間は、プロティビティの経験では、平均的には6か月です。これは、リスクを考えると、かなり長い期間であると言えます。

- **セキュリティ侵害への対応に要する時間** — 取締役会は、セキュリティ侵害の発見から、脅威の拡散と影響を低減するための対応計画の開始までに経過する時間が、十分なものであると考えているでしょうか。

- **監査での指摘事項の是正に要する時間** — サイバーセキュリティの改善に関する外部監査または内部監査の推奨事項に関しては、取締役会は、リスクの高い監査での指摘事項について、是正プロセスの完了に要する時間を含めて、モニタリングを行うべきです。

- **外部を通じて行われたセキュリティ侵害の割合** — プロティビティの経験では、セキュリティ侵害の50パーセントが、組織自体ではなく、組織が利用しているベンダーにおいて発生しています。これは注意を払うに値する、驚くべき数値です。

- **セキュリティ・プロトコルの違反数** — 経営者は、組織全体にわたってセキュリティ方針や手続きの違反数を測定し、違反数の推移を報告することにより、サイバーセキュリティの改善に向けた進捗が見られるのかを示すべきです。

これらの指標は網羅的ではありませんが、これらの指標について報告を行うことにより、取締役会はサイバーリスクの監視における有用な情報を得ることができます。興味深いことに、ある取締役は、取締役会が経営者に対して何かに関する報告をより多く求めると、それに関する不正事象が減少する傾向にあると述べています。サイバーも例外ではありません。取締役会は、経営者としての姿勢を定める上で、焦点を絞ったダッシュボードによって結果を閲覧できるようにすべきです。この点に関して、全米取締役協会が2017年に公表したサイバーリスク監視に関する資料には、サイバーリスク報告についての指標とダッシュボードの例が含まれています。[4]

しかし、取締役は、ダッシュボード報告の利用にあたって注意すべきです。経営者は多くのデータを提供する傾向がありますが、取締役会は、自らが認識していないことが何であるのかを明確にするためにより深堀する必要があります。例えば、組織が管理・保護しているデータ量に関する指標があるとすれば、データが暗号化されているかについて、より深堀した問いを投げ掛けるべきです。ある健康保険を提供している企業では、移行時にはデータを暗号化していましたが、保存時にはデータを暗号化されていなかったために、暗号化されていなかったデータの流出が発生したことをお考え下さい。この企業において8千万に近い記録への不正アクセスが発生したのは、この微妙な理由によるものです。

基本に注意を払う

ラウンドテーブルにおける議論の中で、取締役は、以下を含むサイバーセキュリティに関する複数の基本的な課題を挙げています。

- **リスクの高いパッチを優先する** — 脆弱性に対するパッチの適用は取締役会の視野に完全に入っているため、取締役は、パッチ適用プロセスは縦割り組織の問題と捉えられることがあると述べています。これらの事項に対する組織の迅速かつ積極的な対応を確実とするために、経営者

3 “How Long Does It Take to Implement a Patch?” Board Perspectives: Risk Oversight, Issue 97, Protiviti, November 2017: www.protiviti.com/US-en/insights/bpro97.

4 See Appendices E and F, NACD Director’s Handbook Series on Cyber-Risk Oversight, NACD, 2017, available for purchase at www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687.

はこの課題の取り扱いを改善する必要という点で、ラウンドテーブルに出席した取締役は意見の一致を見ています。

- **多要素認証について検討する** — ある取締役は、どの組織もこのコンピューター・アクセス・コントロールを整備すべきであると述べています。従って、取締役会は、このセキュリティ措置について経営者と議論を行うべきです。

- **フィッシングについての認識を高める** — 鍵は、組織に送り付けられるフィッシング・メールの数ではなく(ダッシュボードに示される指標であるかもしれませんが)、この手法によって騙されるユーザーが企業にどれだけ多くいるのか、そして組織がどのように対応するかです。例えば、適切な対応は、フィッシング・メールを開いてしまった全ての人々に対してセキュリティ研修を行うことであるかもしれません。

- **セキュリティ対策としてデータ分割を行う** — 悪意を持ってネットワークとシステムに侵入する者が全てのデータにアクセスすることができないよう、規制当局は組織に対してデータ分割を行うことを期待しています。データ分割は、アクセスコントロールが損なわれた場合において、重要なデータと最も重要な資産を保護する上で大きな重要性を持ちます。

- **インシデント対応とリカバリー計画の継続的な見直しを行う** — セキュリティ侵害が発生した後の事業継続計画は、ほとんどの場合において不十分であることがラウンドテーブルにおいて指摘されています。これは、多くの場合において、計画が旧態依然としたものであるためです。従って、取締役会は、組織のインシデント対応および事業継続計画の十分性について経営者と議論を行い、その後の状況についてモニタリングを行う必要があります。

独立的なサイバーセキュリティ評価を行う

革新的な変革の取り組みによって、組織のデジタルフットプリントは拡大し続けています。また、それらの拡大は、企業が整備しているセキュリティ保護を上回っているという厳しい現実があります。現時点においてサイバーリスクを受容可能な水準にまで低減可能なセキュリティとプライバシーに係る内部統制の仕組みは、おそらく経営者が認識しているよりも早い段階で不十分なものとなることが避けられないのです。

より厳しい現実は、1年前に経営者が取締役会に対して「有効」であると提示した解決策は、今日は不十分であるかもしれないということです。そのため、組織は、確立したフレームワーク[5]を用いた組織全体のサイバーセキュリティの現状評価の実施を検討すべきです。そうすることにより、望ましい状態を達成しようとする上での改善機会を特定し、優先順位付けを行うことができます。そのようなレビューによってギャップあるいは即時の是正を必要とする脆弱領域が特定された場合には、取締役会は、経営者がそれらの領域について適時の対応を行っていることを確認すべきです。

情報テクノロジー(IT)およびセキュリティ組織における課題を認識する

ラウンドテーブルでの議論の中で、多くの組織は現在のサイバー脅威に対応するよう構成されていないとの指摘が行われました。従って、組織は、テクノロジーおよびセキュリティの観点から自らの再構築を行うことを真剣に検討する必要があります。つまり、組織は、物事のやり方を変える必要があるのです。取締役会が経営者に問うべきであるのは、ある課題をどれだけ迅速に解決できるのか、ということです。その課題の解決策によって現行業務や従前のシステムに混乱が生じるため、その実施には時間を要すると経営者が主張するのであれば、それは危険信号です。

ラウンドテーブルでの議論は、ITおよびセキュリティに関するリソースの不十分さという課題にも及びました。現実においてリソースは限られているため、組織は重要なデータと情報システムにリソースを適切に振り向けなければなりません。しかし、多くの場合、経営者はこの点において十分に積極的ではなく、組織において重要なセキュリティ侵害やセキュリティ上の課題が生じていない場合には特にそうです。多くの企業は単純に、自らが何を知らないのかを知らないのです。そのため、経営者がITリソースをサイバーセキュリティに優先的に振り向けることが難しくなります。イノベーションが必要であることによっても事態は複雑となっています。プロティビティのリサーチでは、成熟した企業は今日、IT予算の約13パーセントのみをイノベーションに振り向けていることが示されており、この割合は過去10年の間に低下してきています。

サイバーセキュリティ保険の価値を検討する

ラウンドテーブルに出席したある取締役は、データ侵害、事業の中断、およびネットワークの損傷を含む、様々なサイバーセキュリティ・インシデントに伴う財務リスクの一部を移転する手段として、サイバーセキュリティ保険の重要性に言及しています。これはとりわけ、企業の取締役や執行役を対象とした損害賠償責任保険はこれらの課題をカバーしていない可能性があるためです。

企業がサイバーセキュリティ保険に加入する場合には、保険会社は企業に対して、一定のガイドラインに準拠し、上述の

5　そのようなフレームワークの例としては、米国国立標準技術研究所(NIST)のサイバーセキュリティ・フレームワークが挙げられます：www.nist.gov/cyberframework

サイバーセキュリティ評価を通じた証跡の提出を求めるかもしれません。企業が適切なフレームワークを基準とした評価を行っていないのであれば、取締役はなぜ行っていないのかを問うべきです。それはサイバーセキュリティ保険のコストを軽減する上で重要であるかもしれません。

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に関連して取締役会が考慮すべき事項です。

- 企業は、自社が象徴するもの、自社が行っていること、および自社が保有する知的財産のために、国家的な標的となる可能性があるか。その可能性がある場合には、
  - 企業は、自らが必要とする先進的な検知および対応能力を有しているか。
  - 想定される攻撃者がより高度な手法を用いることを前提とした、想定される攻撃活動のシミュレーションを定期的に実施し、防衛の仕組みによってセキュリティ侵害の検知と対応が適時に行われることを確実としているか。
  - 経営者は、自社における脅威の状況を踏まえ、適切なフレームワークを基準としてサイバーセキュリティの成熟度を評価し、改善が必要な領域についてフォローアップを行っているか。
- 取締役会は、サイバーセキュリティに関する経営者への期待を明確化し、結果に対する明確な説明責任を持たせているか。組織がリスクアペタイト・ステートメントを有する場合には、取締役会のサイバーセキュリティに関する期待はそれに組み入れられているか。
- 取締役会は、サイバー事項に関して経営者が行う報告と経営者が用いている指標が十分なものであることを確認しているか。それらの指標は、上述の指標例や基本に注意を払うという課題を含めて、最重要のサイバーリスクの管理、および取締役会の監視に関する領域について、主なパフォーマンスとリスクを示しているか。
- 取締役会は、実効性のある対応・リカバリー計画が整備されていることを確認しているか。その計画について、机上訓練を通じた評価、定期的なテスト、および脅威の状況や人員、システム、業務プロセスの変化に対応した調整が行われているか。
- イノベーションを支えるために十分なIT予算が確保されているか。そうではない場合、業務リスクに関する予算は、釣り合いの取れたものであり、重要事項（企業の最重要資産）の保護に焦点が当てられているか、最も可能性の高い種類の攻撃を特定するよう、サイバー脅威の状況に見合ったものとなっているか、また、事業への影響を最小限に抑えつつシステムを復旧させられるよう、インシデント対応について積極的なものとなっているか。

プロティビティの支援

プロティビティは企業と共に、以下の様な根本的な情報セキュリティの課題に焦点を当てています。

- 何を保護する必要があるのかを認識しているか（例えば、最も重要なデータと情報システム資産）、それらはどこに存在するか。それらの資産について以下の事項を考慮しているか。
  - それらの資産を十分に保護しているか。何によってそのことを確認できるか。
  - 誰からそれらの資産を保護しているのか、誰に対してそれらの資産へのアクセスを許可すべきか、アクセスを許可すべき者とそうではない者をどのように区別できるか。
  - 保護の仕組みは有効であるか。設計されたとおりに機能しているか。
  - 計画どおりに物事が行われていない場合に、どのようにしてそのことを把握するのか。
- 自社の環境に対する新たな脅威の認識と想定される攻撃手法の検知を適時に行い、脅威に合致するよう保護の仕組みを見直しているか。
- よからぬことが起こった際に対応する準備ができているか。そのようなインシデントを管理する能力を有しているか。インシデントが発生した際に、その再発を防ぐことができるか。

プロティビティは、幅広い種類のセキュリティとプライバシー評価、アーキテクチャ、トランスフォーメーションと管理に関するサービスを提供し、セキュリティとプライバシーに関するエクスポージャー（例えば、顧客データの喪失、収益の喪失、あるいは レピュテーションの低下）を未然に特定し対応する上での企業の支援を行っています。プロティビティは、全ての業種の企業と共に、情報セキュリティ・プログラムの成熟度や統制の有効性を評価し、必要である場合には改善策の策定と実施を支援しています。

セキュリティ・インシデントへの対応、主体的なセキュリティ・プログラムの確立、個人情報とアクセス管理対応、および業

種に特有のデータセキュリティとプライバシーの課題への対応における企業の支援に関して、プロティビティは、確たる実績を有しています。世界クラスのインシデント対応における経験と専念により、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おける深い専門知識を有しています。

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。20ヶ国、70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®