ISSUE 125

BOARD PERSPECTIVES:

取締役会のリスク監視：Risk Oversight

運用回復力と取締役会の役割

運用システムに悪影響を及ぼす変更に直面した組織なら、中心となる重要なビジネスを継続する準備をしなければなりません。取締役会はこの準備を監視する上で重要な役割を果たします。

運用回復力の監視について取締役会の新しい視点を探る目的で、Protivitiは2019年12月の全国企業取締役協会（NACD）で、現役取締役グループと会って経験を話し合いました。以下はいくつかのポイントです。

どの企業もテクノロジー企業である。 ほとんどの企業はデジタル技術に大きく依存しています。従って、運用回復力（業務環境に悪影響を及ぼす破壊的な変化に耐え、中心となる重要なビジネスと機能を提供し続ける能力）は非常に重要なスキルです。運用回復力は、大規模なサイバー攻撃、停電、疫病大流行などによる壊滅的な運用障害や技術的障害から、ビジネスが識別、防止、対応、回復し、学習するのに役立つプロセスを通じて達成されます。

企業が、(1)ビジネスの失敗、市場破綻、経済的影響を引き起こす可能性のある幅広い脅威に対処し、規制当局、政策立案者、その他の外部利害関係者を巻き込み、(2)ビジネス、ネット空間、第三者そして技術等の回復力を向上させることで、運用回復力の概念は進化し続けます。

例えば、金融サービス業が提供する製品やサービスの中断は消費者や市場参加者に損害を与え、組織自身の存続可能性を脅かし、金融市場の不安定さを生み出す可能性があります。その結果、運用回復力の話題が拡大して規制への注意を換気できる可能性があります。

NotPetyaサイバー攻撃はその大きな影響力から、運用回復力事例が拡大した好例です。[1] そして人間が会話することはサイバー攻撃よりも広い影響があります。たとえば、人為的ミス、テロ行為、ユーティリティシステムの障害、気候関連の壊滅的な事象など、あらゆる場所で大規模な停電が発生する可能性がありすべてのビジネスに影響を及ぼす可能性があります。

運用回復力はどこから始まるのか。 取締役達は、業務の回復力は自社にとってのコアビジネス（サービス）と機能の「フロントツーバック」評価から始まることに合意しました。「影響」を考える際は、顧客、第三者、規制当局、投資家などの外部利害関係者や環境も頭にいれながら、組織の4つの壁を超えることが重要です。重要度を判断する基準の例としては、そのビジネスの全体的な収益の割合、顧客に対する1日の予想影響額、サービスを提供または消費する市場参加者の数、サービスなしでビジネスが活動できる期間、および大規模な回復活動がサービスに影響を与える場合の法規制範囲などがあります。

1 "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Andy Greenberg（2018年8月22日）をご参照ください。www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

protiviti®
Face the Future with Confidence

最も重要なサービスと機能が決定されると、組織は、悪影響を及ぼす破壊的な事象の影響度とそれらを防止および検出する方法を評価し、対策を講じて回復につなげることができます。その後、組織は、壊滅的な運用・技術的障害から学ぶ能力の強化プログラムによって運用回復力を構築することができます。

円卓会議の間、取締役は「フロントツーバックビュー」が会社の内部業務の4つの壁を越えて広がることに合意しました。今日のほとんどの組織は相互に関連しているため、特定のビジネスに対する悪影響が外部の利害関係者に影響を与えるかどうか理解することが重要です。

それが起こった場合、私たちは何をするのか。 経営陣は、重要なサービスと機能ごとに影響許容範囲を評価する必要があります。たとえば、回復と解決の計画を作る前に、運用回復力が必要な事態に対してどこまで許容できるのでしょうか。発生事象を受け入れて会社との取引を継続する顧客の許容度というのは何でしょうか。他の外部利害関係者の期待や重大事態への対応はどのようなものでしょうか。

組織の回復性を評価するときに経営陣が考慮することは次の通りです。事象やその影響度のスピード、影響の持続性、事象が発生した場合の会社の対応計画の充分性、事象の結果として会社が直面する補償されないリスク（例えば、重大な環境・健康および安全上の損失度）等。発生可能性を考えるよりさらに重要なことは、企業が対応するための準備の方です。「それは起こるだろうか」ではなく「それが起こったらどうするのか」が問題なのです。

取締役会はどのように関与すべきか。 このシナリオにおける取締役会の適切な役割に関する質問がNACD円卓会議で何度も浮上しました。全体としてグループは、投資家、規制当局、またはその両方への開示を必要とする可能性が高い事象について取締役会に速やかに通知されるべきである点で合意しました。なお、取締役会は事象に対する会社の対応を知る必要がありますが、対応策を指示すべきではありません。取締役会はまた、(1)経営陣が最も重要であると特定したサービスの内容の理解と支援、(2)影響度を測るための許容範囲の選択、(3)経営陣の運用回復力戦略実行のガバナンスと監視の提供、(4)深刻な問題に対処するためにCEOと協力すること等に関与すべきです。

また、取締役会の関与がどれほどきめ細かいものでなければならないかについても多くの議論がありました。会社の評判を損ないブランドイメージを傷つける可能性のある事項がタイムリーな監視を必要としていることを、多くの取締役が認識しました。

個々の取締役は運用回復力に関する技術専門家である必要はありません。しかし、取締役は、上級管理職に建設的にアプローチし、重大な運用回復力に影響を及ぼす意思決定を評価するために十分な知識、スキル、経験をまとめて持つべきです。円卓会議の取締役は経営陣に対して明確な説明責任と執行責任を確立すべきであり、この点に関して戦略の声明が役立つことに合意しました。そのためには、自社の運用回復力テスト プログラムがどのように組織されているか、さまざまな回復策の準備と対応をどの程度の業務リーダーが従事しているかを理解しておくことが役に立ちます。取締役はまた、経営陣が適切な情報を取締役会に提供し、運用回復力プログラムに関する定期的な報告を行うことを期待する必要があります。

全体像に焦点を当てて、それをシンプルに保つ。 このポイントは、運用上のリスクを定義する際には組織を破壊するような事象に焦点を当てるべきだというラウンドテーブルの中で作られました。これは、取締役会の関与を保証する大局的焦点です。この点で、評判とブランド低下リスクは重要な考慮事項です。

関連ポイント：事象、システム、その他多くの特定事象に関する詳細に巻き込まれないでください。経営陣は、大規模中断があったときに具体的にどのサービスがビジネスを停止するかを明確に理解しておく必要があります。取締役はCEOと協力して、組織のリスク認識と倫理的行動の望ましい文化を明確にする必要があり、どちらも運用回復力に対する会社のコミットメントに影響を与えます。取締役会の監視の下でその文化を確立し維持する責任は経営陣にかかっています。

このラウンドテーブルの詳細はwww.protiviti.com/US-en/insights/operational-resiliencyへアクセスの上、プロティビティの完全要約版をお読みください。

取締役会での質問

以下は、取締役会が会社業務に内在するリスクに基づいて考慮してほしいいくつかの有益な質問です。

- 運用回復力に対する組織の準備はどの程度ですか。経営陣は、組織としての準備を確実にするためにこの話題に十分な注意を払いましたか。取締役会はいかにしてそれを知りますか。
- 組織は運用回復力向上にどのように取り組み、取締役会と上級幹部は、全体的な運用回復に関する目標と戦略を確立しその戦略の実行を監視する上でどのように関与していますか。このトピックは役員室で議論されていますか。もしそうならどのように行いますか。
- 組織は、重要なビジネス サービスとそれらのサービスの影響の許容範囲を定義していますか。確立された許容範囲を超えて影響を及ぼす可能性のある極端だが想定しうる事態を考慮しましたか。このプロセスは取締役会に対して開示されていますか。
- 経営陣は、組織がサードパーティ ベンダーに依存することや、重要なビジネスに対して示されたリスクレベルを明確に理解しているということを示しましたか。

プロティビティの支援

組織と提携して、全体的な運用回復力を見る内部監査計画を策定し、これを既存の監査に組み込み、運用回復力プログラムに対する保証を提供します。この点で、当社は、次のような問題に対処するために、指示に従って、エグゼクティブリーダーおよび/または取締役会または監査委員会に協力し報告します。

- 重要なビジネスサービスを正式に定義しましたか。
- 影響範囲は確立されテストされていますか。
- 運用の回復性を適切に管理するためのしくみはありますか。
- 適切な「度を超えているが想定しうる」シナリオは定期的にテストされていますか。

これらの活動を通じて、企業の継続性管理、IT 災害復旧、サイバーセキュリティインシデント対応に関する既存の活動を基盤に作り上げた堅牢なテストプログラムを通じて、組織が運用回復力を実証し改善することをプロティビティは支援します。

監査委員会の自己評価のための考慮事項

このようなダイナミックな時代には、取締役会とその常任委員会、および個々の取締役が定期的に業績を自己評価し、そのプロセスの結果に基づいて取締役会のパフォーマンスを向上させるための実践的な計画を策定することがベストプラクティスとなります。監査委員会のために弊社が作成、公開した例示的な質問は以下で入手可能です。
www.protiviti.com/US-en/insights/bulletin-assessment-questions-audit-committees.
これらの包括的な質問は、委員会の構成、チャーター、議題、焦点を考慮し、組織が直面している現在の課題に照らして委員会の評価目標に合わせてカスタマイズすることができます。

取締役会がリスク監視プロセスを評価すべきタイミング

TBI Protiviti ボードリスク監視メーター™ は、取締役会にリスク監視プロセスを更新し、真に重要な機会とリスクに焦点を当てる機会を提供します。取締役会は、多くの取締役が自己評価を行う方法を反映した、リスク監視を評価するための柔軟で費用対効果の高いツールを提供しています。この評価ツールの詳細に関しては以下の TBI ウェブサイトをご覧ください。
http://theboardinstitute.com/board-risk-meter/.

protiviti®