Deloitte.
デロイト トーマツ

サイバーリスクの評価
取締役会・経営陣への重要な質問

リスクを転じて
パフォーマンスを上げる

リスクを転じてパフォーマンスを上げる

これまでリスクは最小化または回避するものであると考えられてきており、価値の保護が重視されてきました。しかし私たちは、リスクも価値を生み、正しい方法でアプローチすれば、ビジネスパフォーマンスを向上する上で特別な役割を果たすことができると考えています。

サイバーリスクの問題を考えてみましょう。利用するテクノロジーの増加とグローバル化の進展はサイバーリスクの重要な要素です。一方、これらは企業競争力を推進するエネルギー源でもあります。こうした要素を排除する組織は、価値を保護できたとしても、おそらくビジネスで後れを取るでしょう。逆にサイバーリスクをうまく管理する手段を見つけた組織は、利用するテクノロジーの増加やグローバル化の波に乗って優れたパフォーマンスを上げていくことになるでしょう。

このような組織になるための道のりの第一歩は、自らの組織のサイバーケイパビリティの現状を把握することです。本書と自己評価ツールの目的は、リーダーの皆様に、サイバーリスクの認識を新たにするための重要な質問に回答していただくことです。例えば次のような質問です。

- 社内に適切なリーダーや人材がいますか？
- 正しい対象に重点を置き、投資していますか？
- 自社のサイバーリスクプログラムの効果をどのように評価していますか？

今日のトップ企業がリスク管理を通じて企業価値を保護する術を学んできたのだとすれば、次世代のリーダーは、リスクも価値を生む機会だと認識している方々と言えましょう。デロイトの世界中のリスクアドバイザーが専門家として皆様を正しく導き、リスクを転じてパフォーマンスを上げていくような組織に生まれ変わるお手伝いをさせていただきます。

オーウェン・ライアン
グローバル・リスク・アドバイザリー・リーダー

リスクについての責任の所在

企業に属する者にとってサイバーリスクは避けられないものですが、その最終的な監督責任の所在は経営トップにあります。

しかしながら、取締役会・経営陣の多くは、進化し続けるサイバーリスクの監視、検知、対応といった日々の課題とは切り離されているのが現状です。自社のサイバーリスクに関わる現状について見識を深める経営者こそ、ビジネスをよりよく管理するために不可欠な認識を得ることができるのです。

効果的なサイバーリスク管理は、取締役会・経営陣レベルの意識改革から始まります。リスクを理解する、パフォーマンスを管理する、組織のサイバー成熟度を上げる、こうした力を養う第一歩は、重要な質問に答えることから始まることが多いのです。これらの質問に答える結果、ビジネスをよりリスクに対して「予防」が効いた状態に、「発見」ができる状態に、「回復」ができる状態に導くことができるのです。
今日、これら3つの全てが非常に重視されています。しかし、従来のサイバーリスク管理で注目されたのは「予防」であり、「発見」（幅広い脅威のランドスケープを包括的に監視すること）や「回復」（攻撃に対応し、回復すること）はさほど注目されませんでした。経営陣の皆様、次の「重要な10の質問」にお答えください。「予防」、「発見」、「回復」の観点から現状をより理解していただく一助となると思います。

1. **サイバーリスクを評価し、当事者意識をもって、効果的な管理を実践していますか？**
2. **適切なリーダーや適切な社内人材がいますか？**
3. **リスク選好やエスカレーション基準を含む、サイバーリスクの適切な報告体制が確立されていますか？**
4. **正しい対象に重点を置き、投資していますか？そうである場合、その決定をどのように評価し、測定していますか？**
5. **社内のサイバーリスクプログラムやケイパビリティをどのように業界基準や同業者のそれと平仄をあわせていますか？**
6. **サイバーセキュリティを強く意識するマインドやサイバーセキュリティの意識の高い文化が組織全体にいきわたっていますか？**
7. **サードパーティーのサイバーリスクから組織を守るために何をしてきましたか？**
8. **サイバー関連の事故が発生した場合、素早くダメージを封じ込め、対応に必要なリソースを迅速に動員することができますか？**
9. **自社のサイバーリスクプログラムの効果をどのようにして評価していますか？**
10. **自社は展開している事業において、高度に接続されたエコシステムの中の堅牢でセキュアな結合点となっていますか？**

取締役会・経営陣が、常に進化し続けるサイバー攻撃の脅威に組織が対応しやすくするための重要な役割を担います。

ネットワーク化とデジタル化が進むビジネスの世界において、サイバー脅威やサイバー攻撃はますます増え、複雑化してきています。こうした新たな環境の中で、サイバー攻撃のリスクは今まで以上に高まり、サイバー攻撃に対抗するための管理は、業務上、戦略上欠かせないものになっています。今日のサイバー犯罪は、もはやこれまでの詐欺や盗難といった枠に収まらず、巨大な犯罪ネットワーク、第三国が支援するハッカー、サイバーテロリスト等の活動領域として、サービスの中断、データの破損・破壊、被害者から金銭、アクセス権限、企業秘密を奪うことを目的とした「ランサムウェア」といったリスクの領域にまで広がっています。

今日、サイバーリスクと企業の業績は密接に絡み合っており、サイバー犯罪に絡む目に見えるコストは、資金の盗難やシステムの破壊を始め、規制による罰金、損害賠償、被害当事者に対する金銭的な補償にまで及びます。一方、目に見えづらいコストとしては、知的財産の盗用、顧客やビジネスパートナーからの信頼の失墜、組織の評判やブランド力の低下等による競争上の優位性の損失等が含まれます。リアルなサイバー攻撃の影響範囲は、個々の組織の損失を超え、大規模なインフラ停止や国全体の財政システム、ひいては経済の健全性に対する信頼を揺らがす可能性まで秘めているのです。

最上位の課題

こうした危機に見舞われる中、取締役会・経営陣は、サイバーリスクを最上位のビジネスリスクとして対処すべきであり、そのためには企業文化に深く浸透した意識レベルが求められるとの認識を深めてきています。ビジネスのあらゆる局面にデジタル機器が関わる現代社会において、サイバーリスクに対する懸念は、ITや企業といった枠を越え、あらゆるパートナー、あらゆる顧客、あらゆる従業員、そしてあらゆるビジネスプロセスに及んでいます。

セキュリティはいずれ侵害されるだろう—ということに気がついたのであれば、最も深刻な脅威は何か、その脅威が資産をどのようにミッションクリティカルな危険に曝しうるかをリーダーは把握することに努めるべきです。組織の保護という観点で、取締役会・経営陣の皆様は今まで以上に積極的に役割を果たすことが必要であり、効果的な取り組みを担保するためにまさに苦心される方も多いはずです。経営人としての責任は何か、どのような能力を培うべきか。問うべき質問は何なのか——こうした問いや進化し続ける脅威の広がりの前に、すべての脅威の可能性に備えることは困難です。単なる「可能性」ではなく「高い可能性」について備えることが、リーダーにとって賢明な道筋となるのです。

こうした課題に対する包括的な解決策はありません。リーダーである経営陣の皆様においては、まず、皆様の組織にあったサイバーセキュリティプログラムの策定を、もし既にそれがあるのであればその改定から始めてみてください。次ページ以降に記載した「重要な10の質問」は、進化を続ける課題への効果的な取り組み方、サイバーリスクの軽減策、機会の予測方法といった、マネジメントの中で現在進行しているサイバー戦略に関して、取締役会のディスカッションを促進してくれることでしょう。

あなたの組織の成熟度を評価する

サイバーリスクに関する重要な質問とその回答から成る本リストは、サイバーに対する組織の態勢を評価する効果的なガイドとしてご活用いただけます。また、情報セキュリティチームに対する適切な問いかけや重要情報の提供を促す材料として、さらには、サイバーリスクに対する強靭性の継続的な監視・改善にご活用いただけます。

各質問は、具体的な強みや弱点を特定し、改善の道筋を示すことを目的としています。質問に対する組織の回答によってサイバーセキュリティ成熟度が高・中・低のどのレベルに該当するかを判定できます。

サイバーセキュリティ成熟度の基準

高レベル

組織内に強固なサイバーリスク体制が整っている。

中レベル

サイバーリスク対策は整備されているが、改善の余地がある。

低レベル

サイバーリスク管理は後れていて、対策は限定的で改善の余地が多い。

予防、発見、回復とは

予防

業界のサイバー規格・規則等に準拠しながらも、新規・既知の脅威から身を守るリスク重視のコントロールを強化することにより、基本的なセキュリティ・ケイパビリティを確立し、継続的に維持すること。

発見

組織が属しているエコシステムのすべての領域において、優れた状況把握を発揮することにより違反や異常を検知すること。

回復

不可避のサイバー攻撃を受けた後、素早く通常オペレーションに復帰し、ダメージを補修する能力を確立すること。

1 サイバーリスクを評価し、当事者意識をもって、効果的な管理を実践していますか？

経営の上位レベルでのアカウンタビリティの適切性を判定することは不可欠です。例えば、監視の実態が、サイバーイベントに関する5分程度のアップデートを時々行うという状況であれば、リスクを効果的に管理しているとは言えません。

高レベル

- ☐ 取締役会・経営陣は、執行役員レベルにサイバーリスク管理の責任を課し、サイバーリスクプログラムの策定・監督ならびにその実行確認の責任を負っている
- ☐ 取締役会・経営陣は、サイバー攻撃の脅威やそれに伴う組織への潜在的な影響について定期的に報告を受けている
- ☐ 取締役会は、ITやサイバーリスクの知識を有する1名以上のメンバーで構成されている、もしくは戦略的アドバイザーを適切に活用している
- ☐ サイバーリスク対応専用に設置されたシニアマネジメントレベルの委員会、もしくはマネジメント・取締役で構成される混合委員会、あるいはそれに代わる、臨時的なシニアマネジメントレベルの委員会が、サイバープログラム全般に十分な時間を割いている
- ☐ 通常のアップデート、予算分析、マネジメントに対する厳しい質問により、評価される

中レベル

- ☐ 上層部や取締役会の監視は、サイバー問題に目を向けているものの、多くは利害関係者とのコミュニケーションや特定の構造への監視がいまだ十分な具体性がない状態である
- ☐ 取締役会は、ITやサイバーリスクに関する実用的な知識を有している
- ☐ サイバー問題に関してマネジメントに異議を唱えるだけのサイバー評価能力が欠けている
- ☐ 取締役会は、サイバー方針や戦略的要件を断続的に評価する

低レベル

- ☐ トップの姿勢には、サイバー重視、戦略的課題としての認識が欠けている
- ☐ ITセキュリティ上の特定の課題に対するリーダーの関与が限定的である
- ☐ 取締役会のITやサイバーリスクに関する経験が不十分で、課題解決はIT担当者に一任されている
- ☐ サイバーリスクの監視や関連する予算要件の評価が、非常に概括的な状態のままである

2

適切なリーダーや適切な社内人材がいますか？

組織の誰もがサイバーリスクに何らかの責任を負っています。誰もが責任を負いながら多くのリーダーが時代遅れの業務に忙殺されていると、組織は、サイバーリスクの最終的な説明責任を負うべき適切な、「正しい」リーダーを任命できません。

高レベル

- ☐ サイバーリーダーは、組織の運営方法を理解し、ビジネスと連動し、活動の優先度を適切に判断するための技術面とビジネス面の見識を兼ね備えている
- ☐ 情熱的でやる気に満ちたメンバーが所属するチームに、最新のサイバー動向や脅威、ビジネスへの影響に関する情報が提供されている
- ☐ 取締役会・経営陣は、サイバーリスクに関するディスカッションをしている
- ☐ 適切な領域に特化した業界特有の経験を有する熟練スタッフが十分に確保されている
- ☐ 業界や組織のリスク特性や、重要度に沿った補償や報酬に関する各種プログラムが整備されている

中レベル

- ☐ サイバーリーダーは任命されているが、サイバーセキュリティに関連する技術面のリスクが主たる対象である
- ☐ サイバーリーダーは、実用的な業界知識はあるが、組織の運営に関する知識が不十分である
- ☐ サイバーリスクは重視されているが、比較的概括的な状態になっている
- ☐ サイバーリスクの問題がIT部門やマネジメントレベルで停滞することが多い
- ☐ IT部門や一部のビジネス部門に熟練スタッフは存在するものの、業界特有の脅威に関する知識は限定的である

低レベル

- ☐ 上層部はサイバーリスクをほとんど重視していない
- ☐ サイバーに関する知識や人材がIT機能に区分されている
- ☐ 特定の新しいテクノロジーに関しては、その都度、訓練プログラムが構築されている
- ☐ 人材戦略への投資不足により、スタッフの離職率が高い

3 リスク選好やエスカレーション基準を含む、サイバーリスクの適切な報告体制が確立されていますか？

有意義なサイバーメッセージを組織全体に策定することは、サイバー関連の事故や懸念が生じた場合の情報の流れをよくします。しかし、経営陣に情報を上げる実際のプロセスはもとより、報告すべき情報の基準を明確に定義できるか否かで、「機能的」と「効果的」の差が生まれます。

高レベル

- ☐ リスク選好とサイバーリスクが明確化され、既存のリスク管理・ガバナンスプロセスに組み込まれている
- ☐ 企業全体で確立されたサイバーリスクポリシーが、必要に応じて取締役会で承認・審議されている
- ☐ サイバーリスクプログラム全体にわたって役割と責任が明確に定義・運用されている
- ☐ KRI（主要リスク指標）やKPI（主要パフォーマンス指標）が存在し、重大あるいは致命的なサイバー関連の事故が発生した場合、限界や閾値を超えるものを上級経営者に報告するためのプロセスが整備されている
- ☐ 事故管理方針には、サイバーリスクプログラムと連動した報告基準が含まれている
- ☐ サイバー保険の価値の評価・監視体制が整備されている

中レベル

- ☐ 既存のサイバーリスクポリシーの運用が、IT分野以外では不十分だ
- ☐ サイバーリスクは、通常のリスク管理、ガバナンスのプロセスにおいて一般的なリスクとして対応されているだけである
- ☐ リスク選好がサイバーリスク方針に反映されていない
- ☐ サイバーリスクの対応は、主体的というより受け身である
- ☐ 臨時の上級経営委員会が、サイバーフレームワークの導入に関するディスカッションに十分な時間を割いている

低レベル

- ☐ 正式なサイバー方針は整備されていない
- ☐ リスクの報告は、事故発生時にその都度、実施するだけである

4

正しい対象に重点を置き、投資していますか？そうである場合、その決定をどのように評価し、測定していますか？

リスクとパフォーマンスが密接に関係する中、リーダは何に資源を投入しているのか把握すべきです。また、リーダーはサイバー問題のために適切な資源を配置しているか把握すべきです。人的戦略の策定不備、サービスに対する過剰な支払い、運用コストに関わるその他の障害は、すべて現実的なリスクにほかなりません。

高レベル

- ☐ 戦略的な計画から日常業務に至るすべての組織活動において、サイバーリスクが考慮されている
- ☐ 大半の脅威に対処するための基本的なセキュリティ対策に投資を集中させ、戦略的に決められた資金が組織の最重要プロセスや情報に対するリスク管理に投入されている
- ☐ いわゆる「ブラック・スワン」のリスク特定に組織は尽力し、可能性は低くても発生時の衝撃が巨大な脅威を予測・回避するプログラムが整備されている
- ☐ 組織の投資や予算がリスクと連動（投資の明確なビジネスケースが存在する）され、サイバー戦略に反映されている
- ☐ 上級経営者は、組織のサイバー方針の実行をサポートするための適切な資金や十分な資源を提供している
- ☐ 想定される課題に対応するための仕組みが存在する

中レベル

- ☐ サイバー方針は内部に重点を置いたもので、業界基準のプロセスは加味されていない
- ☐ サイバー戦略と投資は、互いに連動もサポートもしていない
- ☐ 基本的なセキュリティ対策に対する投資と非常に高度な攻撃に対する対策への投資のバランスが悪い
- ☐ 脅威に対する高い認識は、企業全体のインフラやアプリケーションの保護に集中している
- ☐ 個人識別情報の保護を実施している
- ☐ IT資産脆弱性の自動監視機能が整備されている
- ☐ 想定される「ブラック・スワン」のリスクに対する有意義な仕組みがない

低レベル

- ☐ サイバーに関する戦略、対策、投資計画が整備されていない
- ☐ 基本的なネットワーク保護や旧来型の識別方法によるセキュリティ対策はあるものの、新しいテクノロジーやメソッドに対する関心はほとんどない
- ☐ IT資産の脆弱性評価を時々実施する
- ☐ サイバー投資のビジネスケースをほとんど策定していない

5

社内のサイバーリスクプログラムやケイパビリティをどのように業界基準や同業者のそれと平仄をあわせていますか？

自社は遅れをとっていないか、サイバーリスクに効果的に対処している企業とどこが違うのか。これらを知ることは大切です。では、遅れをとっているという事実に気づいた後、どう行動しますか。その問題の責任を積極的に取るべきは取締役会や経営陣です。他にはいません。

高レベル

- ☐ 包括的サイバープログラムは、業界基準やベストプラクティスを活用し、既知の脅威の予防と発見ができるように、また、新規の脅威情報を継続的に取得できるように、そして、タイムリーな対応と回復を実現できるようになっている
- ☐ サイバープログラムの策定、運用、保守、改善・改良ができるように業界のフレームワークを確立している
- ☐ 自社のサイバープログラムについて、外部のベンチマーク評価を受けている
- ☐ 各種ポリシー、業界基準、法令等に対する社内コンプライアンスを定期的に検証している
- ☐ 認証を受けることができる重要な事業領域では、正式な認証を受けている（例：ISO/IEC 27001:2013）

中レベル

- ☐ サイバープログラムは、基本的なオンライン・ブランド・モニタリング、マルウェア自動解析、手動電子証拠開示、犯罪者・ハッカー調査、従業員・顧客の行動プロファイリング、内部ユーザーを対象とした特定プラットフォーム間のモニタリング等、多数の業界ベストプラクティス・ケイパビリティを実施している
- ☐ コンプライアンスプログラム等の内部プログラムを時々見直している

低レベル

- ☐ サイバー対策の実施はその場しのぎで、業界基準やベストプラクティスを参考にすることはほとんどない
- ☐ コンプライアンスや規制上の要求に応じて、非定期的にかつおおまかな見直しを実施する場合がある

6

サイバーセキュリティを強く意識するマインドやサイバーセキュリティの意識の高い文化が組織全体にいきわたっていますか?

「予防」、「発見」、「回復」がより実行できる企業となるべく、態勢を強化しようと、多くの企業が教育や啓発活動を重視していますが、そうなることは容易なことではありません。どのように行動を変えるべきか。その答えを導くのは、取締役会や経営陣の皆様です。

高レベル

- ☐ トップの力強い姿勢により、取締役会・経営陣は強固なリスクカルチャーや持続可能なリスク・リターン思考を推進している
- ☐ 個人の利益・価値・倫理等が、組織のサイバーリスクの戦略・選好・許容度・アプローチと連動している
- ☐ 役員たちが共通言語を用いてオープンかつ率直にサイバーリスクについて気楽に語ることが、共通理解の促進につながっている
- ☐ サイバーリスクに関する全社的(全従業員、サードパーティー、契約社員等)な教育・啓蒙活動が確立している
- ☐ 個々の職務内容に即した啓発活動や訓練が、サイバーの責任に対する従業員の理解を深めている
- ☐ 社員はリスク管理について個人的責任を負い、必要に応じて、他者に参加するよう積極的に働きかけている

中レベル

- ☐ 一般的な情報セキュリティの訓練や啓発活動が確立されている
- ☐ 資産リスクや脅威タイプに重点を置いた、サイバー啓発活動が確立されている

低レベル

- ☐ 利用規定が整備されている
- ☐ IT以外で、サイバーリスクはあまり重視されていない
- ☐ 啓発活動や訓練はあくまで受け身で、しかも、セキュリティ侵害やコンプライアンス違反等が実際に発覚しなければ実施されず、また訓練の対象人数も限定的である

7

サードパーティーのサイバーリスクから組織を守るために何をしてきましたか?

セキュリティ侵害の原因の多くは、契約社員やベンダーといったビジネスパートナーに由来します。サイバー上の懸念事項は自社のオフィスの外にまで及んでいるため、パートナーと連携し、その業務を把握し、その関係から生じるリスク要因を受け入れる必要があります。

高レベル

- ☐ 重要なアウトソーシングや下請け業務等について、サイバーリスクは評価プロセスの一部と見なされている
- ☐ すべてのサードパーティーは一貫したプロセスを通じて関与し、各種ポリシーやコントロール(監査権等)が組織の期待やリスク許容度に沿って整備されている
- ☐ サイバー問題について、サードパーティーは関連するニーズやリスクにあわせてカスタマイズされた特別な訓練を受講している
- ☐ リスク管理プログラムには、重要なサードパーティーとの関係や情報の流れのプロファイリグ、評価が含まれている
- ☐ サードパーティーからサイバー関連の事故がタイムリーに通知されるようなプロセスが整備されている
- ☐ サードパーティーのプロファイリングやリスク評価に基づいて、アウトソーシング業務の潜在的サイバーリスクの軽減措置が講じられている

中レベル

- ☐ アウトソーシング業務の潜在的サイバーリスクの軽減措置が講じられている
- ☐ アウトソーシングや下請け業務に関わる評価は奨励されているが、その適用は一貫性に欠けている
- ☐ サイバー関連の事故に関するサードパーティーからの報告基準が、契約に組み込まれていない
- ☐ 内外の脅威情報に一定の相関関係がある

低レベル

- ☐ 基本的なネットワーク保護のみ整備されている
- ☐ サードパーティーの評価およびサイバーリスクの保護策は存在しない

8

サイバー関連の事故が発生した場合、素早くダメージを封じ込め、対応に必要なリソースを迅速に動員することができますか?

非常にセキュアと言われる企業でも、セキュリティ侵害を発見するまでに数日から数週間かかることは珍しくありません。大切なのは、実際の脅威を検知した時の対応力、つまり自社のプロセスに対する自信があるかどうかです。上層部の観点から言うと、事故対応の重要なケイパビリティに含まれるのは、明確なその場の指揮系統、万全のコミュニケーション計画(緊急連絡先を含む)、法的な問題・広報の必要性・ブランドへの影響・業務上の影響等の幅広い視点です。

高レベル

- ☐ セキュリティ障害や事故に対応する対策やコミュニケーションについて、明確な報告および決定プロセスが存在する
- ☐ サイバー関連の事故の対応方針や手順が、既存の事業継続計画や障害回復計画に組み込まれている
- ☐ 危機管理やサイバー関連の事故の対応計画・手順が文書化され、演習・シミュレーション・対話等によるリハーサルが実施されている
- ☐ サイバー関連の事故に対応するため、主要なステークホルダー向けの内外のコミュニケーション計画が策定されている
- ☐ 組織は、業界のシミュレーションや訓練の演習に積極的に関与している

中レベル

- ☐ 基本的なサイバー関連の事故対応方針・手順は整備されているが、既存の事業継続計画や障害回復計画に効果的に組み込まれていない
- ☐ サイバー攻撃シミュレーションが定期的に実施されている
- ☐ 企業全体のサイバー攻撃の演習が断続的に実施されている

低レベル

- ☐ IT事業継続や障害回復に関わる何らかの演習がある
- ☐ サイバー関連の事故に関わる方針、対応計画、コミュニケーションは最低限しか存在しないか、もしくは存在しない

9 自社のサイバーリスクプログラムの効果をどのようにして評価していますか?

この質問に対する回答はシンプルに「最初から最後まで評価する」ということです。ただし、言うは易しです。もう一つの課題は、「システムの向こう側を見通す」ことです。これは、批判的な視点を持って、企業全体への影響を把握し、ITプロセスのみならず、業務プロセスも検討することであり、その実現には、取締役会や経営陣のリーダーシップと関与が求められます。

高レベル

- ☐ 取締役会・経営陣はサイバーセキュリティ・プログラムの効果が検証され、ギャップが特定された場合はリスク選好を踏まえて適切に管理されるよう努めている
- ☐ 既存の軽減策の妥当性を含め、組織のサイバーセキュリティ方針や実行計画の定期的な見直しや検討に、取締役会またはその管轄委員会が関与している
- ☐ 業界に適したサイバーセキュリティ・コントロールとのギャップを特定するため、定期的な脆弱性に関する内外評価(ヘルス・チェック、侵入テスト等)が実施されている
- ☐ モニタリング活動には、サイバーセキュリティ予算の定期的な評価、サービスのアウトソーシング、事故報告、評価結果、方針の見直し・承認等が含まれている
- ☐ 四半期レビューの一環として、内部監査でサイバーリスク管理の有効性を評価している
- ☐ 今まで以上に組織を強くするため、重要な教訓を吸収し、プログラムの強い部分であっても「予防」と「発見」をさらに強化することに組織は時間を割いている

中レベル

- ☐ 業界特有ではなく、ごく基本的なサイバーリスク評価が、定期的なスケジュールで実施されている
- ☐ 内部監査でサイバーリスク管理の効果を評価しているが、その頻度は年一回以下である
- ☐ サイバーリスク管理を改善するため、学んだ教訓を時々、一貫性なく、適用している

低レベル

- ☐ サイバー評価や内部監査評価は散発的、もしくは一切ない
- ☐ サイバー対策は比較的固定されており、改善する場合も基本的な経験に欠けている

10

自社は展開している事業において、高度に接続されたエコシステムの中の堅牢でセキュアな結合点となっていますか？

パートナーのサイバー体制が万全であれば、それはサイバーに対する皆様の姿勢に影響します。しかし、パートナーからすれば、サイバーリスクは双方向の問題です。皆様は弱い関係となっていませんか。サイバーリスクのリーダーになっていますか。サイバーや幅広いビジネス領域にポジティブな影響を与えていますか。脅威情報を共有するために同業者やパートナーと協力することは、ビジネスリーダーがサイバーリスクに対して、より現実に直結した総合的なアプローチを構築するためのほんの一例にすぎません。

高レベル

☐ 内部のステークホルダー、外部のパートナー、法的機関、規制当局等との強い連携が維持されている
☐ 情報セキュリティやプライバシーを侵害しない、革新的な共有イニシアティブを支持している
☐ 産業界、独立系分析機関、政府機関・諜報機関、学術機関、研究機関等との知識・情報の共有をしている
☐ パートナー、顧客、エンドユーザーを含めた、共有の取組みや関係の拡大を図っている
☐ 業界基準やサイバー推進を支持するベンダーを選択している
☐ 弱い関係とならないための成熟したプログラムを自社で維持している

中レベル

☐ 脅威情報に関しては、同業者とアドホックな共有、もしくは政府・民間部門と積極的に協力している

低レベル

☐ 外部との関係構築は最低限で、同業者・政府・外部団体等と情報・知識を共有していない

より高い目標や戦略的目標を設定する

組織のリスクリーダーは、構築であれ、改良であれ、目指すべきサイバー成熟度の状態を設定することが重要です。その目標を効果的に定義するためには、サイバーのリーダーとそれ以外の組織の意思決定者によるディスカッションを通じ、ビジネス環境とそれに伴う優先順位を理解することが必要です。すべての組織があらゆる領域で最高レベルのサイバー成熟度を維持する必要はありません。コストと時間のバランスを取りつつ戦略的目標を達成するため、組織をサポートするのが、この目指すべき状態です。多くの場合、目指すべき状態を設定することで、サイバーリスクのプラクティスが重要とされる領域について、組織の成熟度は高まる傾向にあります。成熟した高度なサイバーリスクプログラムを策定することは、単にお金の使い方を変えることではありません。根本的に異なるアプローチを取ること、つまり、個々のニーズに特化したプログラムを策定するために、「予防」、「発見」、「回復」について組織固有のバランスをもって各種ケイパビリティに投資することこそがその本質なのです。

現状を把握しましたか

以上の評価結果から判断される現在の成熟度は、皆様の戦略やミッションをサポートするものでしたか。それとも妨げるものだったでしょうか。もし、成熟度の指標と目指すべき成熟度の状態が連動していない、もしくは適切なサイバー目標をまだ設定していないのであれば、今こそサイバーリスクの態勢強化に着手する時です。

当然のことながら、100%安全な組織になることなど不可能です。しかし、盗難、規制上の罰金、損害賠償、風評被害等、様々なサイバー脅威の影響を管理し、大幅に軽減することは十分に可能です。共に取り組むことで、国家レベル、さらには世界レベルの大規模なインフラ停止やビジネスの中断といった増大する危険性を最小化することができるのです。

国内ネットワーク

有限責任監査法人 トーマツ

東　京　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1112
大　阪　〒541-0042　大阪府大阪市中央区今橋4-1-1 淀屋橋三井ビルディング　Tel:06-4560-6021
名古屋　〒450-8530　愛知県名古屋市中村区名駅1-1-1 JPタワー名古屋　Tel:052-565-5511
福　岡　〒810-0001　福岡県福岡市中央区天神1-4-2 エルガーラ　Tel:092-751-1517

デロイト トーマツ リスクサービス株式会社

本　社　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1300
名古屋　〒450-6337　愛知県名古屋市中村区名駅1-1-1 JPタワー名古屋　Tel:052-565-5950