protiviti®
Risk & Business Consulting.
Internal Audit.

Risk Oversight vol.44
取締役会のリスク監視

サイバーセキュリティリスクを管理する

24時間絶え間ないコミュニケーションチャネルへのアクセス、情報共有と連携が必要とされるナレッジベースのエコノミーにおいては、ビジネスにおいてウェブベースアプリケーションの活用が普及しています。これは反面、セキュリティの観点から大きなリスクとなります。

最近のサーベイでは、サイバー攻撃によって企業の中核事業が中断されることは重要リスクのひとつにランクされ、特に金融業、IT企業、メディア産業においてはトップ5リスクの一つとされています。過去2年間、様々な産業おいて高度なサイバー攻撃による知的財産・企業機密の毀損が大々的に報道されています。*1

また、最近のレポートでは、100社以上の米国企業からの知的財産が背後に中国軍がいるとされるハッカーにより窃取されているとされ、人間の弱み・信頼につけこんだフィッシングメール等の手法が用いられていると分析されています。*2

さらにはこのような状況下、米国SECが米国におけるサイバー攻撃の開示要請をしているにもかかわらず*3、公表されているサイバー攻撃の事例は、全体の氷山の一角にすぎないと多くの人は思っています。大多数の企業は投資家が逃げ出すことを恐れ、サイバー攻撃を受けた事実の公表に消極的であるというのが理由の一つです。

最近の研究によると、投資家400人以上のうち78.1パーセントは過去にサイバー攻撃の標的とされたことのある企業に投資することを躊躇すると回答し、68.7パーセントは過去に情報漏洩があった企業に投資することに消極的である旨回答しています。*4

このような環境とリスクを鑑みて、いまや、あらゆる企業はサイバー攻撃から自社を守るように、より注意しなければなりません。

主要な考慮事項

投資家もいずれはサイバー攻撃の本質、つまり世の中に蔓延したものでありかつ時には不可避なものであるということに気付くでしょう。また、サイバー攻撃は企業のみならず政府にとっても悩みとなっています。著名な組織体においては、毎日数千件ものネットワーク侵入の試みを受けているところもあります。このような状況に対して必要なのは、事故を早期に発見・対応し、ダメージを抑える仕組みです。

とくに、動機が何であれ、サイバー犯罪者が高度な手法を用いてオンライン情報をコントロールする方法を入手して主要なインフラを脅かすことを想定しなければなりません。主要なセキュリティリスクには、機密情報の漏洩、従

*1 Executive Perspectives on Top Risks for 2013: Key Issues Being Discussed in the Boardroom and C-Suite「経営者による2013年トップリスク」:
プロティビティ及びノースカロライナ州立大学ERM Initiative http://www.protiviti.com/toprisks
*2 "Human Frailty Lets Cyber Thieves Attack, Expert Says" Brian Browdie, American Banker, March 19, 2013/08/13
*3 プロティビティSEC Flash Report SEC Staff Provides Guidance on Public Companies' Disclosure Obligations Relating to Cybersecurity Risks and Cyber Incidents,
2011年10月 http://www.protiviti.com/en-US/Documents/Regulatory-Reports/SEC/SEC-Flash-Report-Cybersecurity-Incident-Guidance-101711-Protiviti.pdf
*4 "Cyberattacks, Data Breaches Scare Off Investors, Study Says" John P. Mello, Jr., Network World 2013/2/27
http://www.networkworld.com/news/2013/022613-cyberattacks-data-breaches-scare-off-267157.html

業員のコンピュータにウイルスの意図しないアップロードがあり、従業員を対象としたいわゆるソーシャルエンジニアリング攻撃による情報入手もますます増えています。しかし、複数のシステムに侵入して大量のデータを収集し、攻撃者の元に送信する持続的標的型（ATP）攻撃を含むサイバーセキュリティの脅威が増加しているのに対し、多くの企業では対応するためのプロセス、テクノロジー、ガバナンスが不足しています。

その結果、効果的な対応プランがなかったために、持続的標的型（ATP）攻撃等を受け、情報漏洩に至ってしまい、結果に苦慮している企業の数は激増しています。対応プロセスの向上を求めている組織体は増加しており、そのためには、以下の4つの事項を考慮しなければなりません。

危機対応をトップマネジメントの優先事項とする

危機に対する準備・識別・封じ込め・駆除はそれぞれ重要ですが、危機対応について特に重要なのは経営者のサポートを得ることです。過去に非常事態に直面したことがある場合は別として、そうでない企業の経営者は強固な危機対応プログラム構築に予算を与えることに消極的です。法律や業界規制によって危機対応プログラムが必要な場合でさえ、以下のような落とし穴に陥ることがあります。

- 企業の事業またはIT分野外の責任者を満足させる程度の中途半端な計画
- 具体的な報告エスカレーションプランや、計画実行のための役割・責任体制、プロトコルなどの欠如
- 要請への準拠のみ監査し、計画の実施を監査しない
- 継続的標的型（ATP）攻撃等の新しい脅威に対応するなど、対応計画のアップデートをしない

経営層のサポートがあれば、これらの失敗を避ける確率が格段に上がります。

予防的な人的・IT セキュリティ体制を構築する

基準の策定や予備練習が完了したら、その次には従業員に対する教育を実施しなければなりません。この段階で、セキュリティの重点は、ITのインフラ基盤から、日々の業務・活動を通じて企業を支える人的資源へと移行します。強固な周知徹底プログラムの構築及び全体的なリスク意識を高めることにより、従業員はリスクの高い行動を認識し、攻撃にも対応し、「人的セキュリティ体制」を構築することが可能となります。

アンチウイルス、アンチスパイウェア、ウェブフィルタリングテクノロジー等の強固なITセキュリティコントロールに加え、従業員教育及び意識向上により、適切な人員はテクノロジーを活用して必要な結果を出し、またリスクが事業を揺るがす可能性を低くすることができるのです。

報告プロトコルを活用し、トップの可視性を確保する

いまだにセキュリティ漏洩をIT部門のみに任せ、取締役会や経営者がその他の「IT問題のうちのひとつ」としてしか考えていない企業が多くあります。しかし、実際は、企業は法律上・ビジネス上の目的に応じた危機対応プログラムの基準を設定する必要があります。そのためには、資金・売上・システム、B2BあるいはB2Cへの影響などの指標を用いて、事故の危機のレベルを明確に定義しなければなりません。さらには、事故を取締役会に報告する際の要件も定義しなければなりません。

危機対応のためのオペレーションフレームワークを構築する

企業は経営者の可視性・サポートのある危機対応プログラムを構築する必要があります。そのためには、①企業の法律上・契約上の義務、②プライバシーに関する要件、③サイバーセキュリティ事故の報告ポリシー、④国際事業の複雑性、の理解に基づき、危機対応チームのためのオペレーションフレームワークを危機対応プランに含める必要があります。オペレーションフレームワークとして、例えば、以下の項目が必要です。

- 既存の情報セキュリティプログラムを統合・補完し、テクノロジーが更新され、企業の内部・外部の接続ネットワークが文書化されていることを確認する
- コンプライアンス、IT, セキュリティ、広報、法務、事業部など、適切な利害関係者からの情報を含める
- 組織内の役割・責任を明確化する

- 報告プロトコル、連絡手続きにより、適切な利害関係者が事故対応・開示に関する重要な意思決定に関わるようにする
- 事故対応・漏洩の開示に関する法規制上の義務に応える
- 事故の規模・性質上、企業内部のリソース能力を超えた場合に、信用できる適格な外部リソースを確保しておく
- 企業の決定した方針を実行できるよう、当局・メディアにコンタクト先を確保する・
- 危機対応プログラムを定期的に監査する

すべての必要事項を網羅したわけではありませんが、以上は企業の危機対応プランの有効性を増強するのに役立つポイントです。企業はまた適切な外部リソース（国際的ビジネスを営むのであればグローバルに）を確保することや、当局との関係を慎重に考慮する必要があります。セキュリティ事故が発生した場合に備え、対応プランは関連情報・証拠を保全し、必要な法的措置をとり、eディスカバリに関連する費用・時間・負担をも考慮しなくてはいけません。

取締役会の考慮事項

以下は企業の営む事業に内在するリスクの性質に応じて、取締役会が考慮すべき事項です。

・情報漏洩の発生・増加・影響を低減できるような事故対応プロセスが導入されているか。企業の規模、文化、法律上の要請、事業目的に沿った対応プランの策定に主要な利害関係者のサポートがなされているか。

・企業の事故対応プランは、事故の性質に応じてアクションを特定した手続きにより補完されているか。また、この手続きは定期的に評価されているか。

・取締役会が事後報告を受けるべき事故と、対応自体に関与すべき事故が明確化されているか。

プロティビティの支援

プロティビティはセキュリティ事故・攻撃について世界クラスの事故対応・法務調査プラクティスを確立し、対応計画の実行、法務調査分析、対応計画の高度化について専門性を有しています。プロティビティは世界中でIT環境及び企業全体に対するサイバー攻撃を予防し、危機対応・法務調査サービスを提供し、攻撃の影響を低減するとともに回復・改善措置の支援を実施しています。さらには、企業のコーポレートガバナンス、従業員教育、報告プロセスへの取り組みも支援しています。プロティビティは米国PCIカウンシル及び主要クレジットカードブランドによって事故対応・調査サービスを提供する会社として認められた8社のうちの1社であり、また、CSO Magazine誌の「21世紀の15最悪セキュリティ漏洩」のうち2件について事故対応サービスを提供した実績があります。

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。現在、世界の70を超える拠点で約2,900名のコンサルタントが活躍しています。

protiviti®
Risk & Business Consulting.
Internal Audit.