ISSUE 143

BOARD PERSPECTIVES:

取締役会のリスク監視：Risk Oversight

ランサムウェア：リスクの分析と重要な資産の保護

ランサムウェアは、現在、多くの人々が理解と対応に苦心している脅威です。ランサムウェアが毎日のように話題になるこの不確実な世の中で、経営陣はどのように戦略的に対応すればよいのでしょうか。

2017年のWannaCryとNotPetyaの攻撃は、ランサムウェアが持つ潜在的な破壊力を世間に知らしめました。それ以来、ランサムウェアの攻撃は次々と多くの組織に対して衰えることなく続いています。2021年にはコロニアルパイプライン社やKaseya社のインシデントが発生し、このような犯罪が後を絶たないことを示しています。

レピュテーションの棄損や多額の身代金支払い、および事業継続への影響はすべてランサムウェアに関わる懸念事項です。一方、話題の中心によく上るのは、知的財産や顧客情報の漏洩や、国家の支援を受けた攻撃者集団である可能性のある者と不快な取引を行わなければならないことに対する不安です。

これらの攻撃の被害を受けた企業のほとんどがその経験を積極的に共有しようとしないため、ランサムウェア攻撃の数と被害の深刻度や範囲などは未知のものとなっています。ただし、米国におけるランサムウェアの総コストは、2021年[1]には、およそ200億ドルにも上り、攻撃による平均要求額は3倍に上昇しています。[2] また、サイバー保険契約を行う上でのセキュリティ管理の要求水準が高まって、組織がそうした保険に加入する資格をもつことが今まで以上に難しくなる可能性があります。

明確に言えることは、ランサムウェア攻撃について包括的な対策ができている企業はほとんどなく、また懸念していない企業はないということです。また、規模や場所に関係なく、すべての企業がランサムウェアに対してなんらかの弱点を持っているということです。

最近のランサムウェアの攻撃者の目的は破壊です。これまでのような、企業のITシステムに侵入および待機して、数か月かけてデータや金銭を窃取するような方法は今日ではとられなくなってきています。ものの数分で、迅速に侵入し、データを窃取・暗号化し、身代金を要求します。

ランサムウェアは、かつてはデータを無作為に暗号化する自動化されたマルウェアでしたが、今は、非常に進化したもの

1 “The 2021 Ransomware Statistics, Data, & Trends You Need to Know,” by Raffi Jamgotchian, Triada Networks, May 30, 2021: https://triadanet.com/ransomware-statistics/.

2 “Ransomware Payment Demands Triple in 1H 2021, Coalition Reports,” by D. Howard Kass, MSSP Alert, July 30, 2021: www.msspalert.com/cybersecurity-research/ransomware-demands-triple-coalition-reports/.

protiviti®

Face the Future with Confidence

になっています。最近のランサムウェア攻撃では、検出を回避するために高度に難読化された特殊なツールと組み合わせて企業のシステム環境に忍び寄る手法を使用しています。攻撃者は最大のインパクトを与えるために、平均4～6週間の滞留期間を設け、データを抽出します。身代金の支払いを拒否した企業は、盗み出されたデータを公開されてしまいます。最も重大な問題は、悪意を持った攻撃者が最終的に企業を支配することです。

ランサムウェア市場も進化しています。有料のマルウェアを提供するRansomware as a service（RaaS）を利用することで、システムを暗号化し、攻撃者が身代金を受け取る攻撃のサイクルを短縮しています。また、攻撃者は、オープンマーケットプレイスを通じてネットワークへのアクセス権を購入することもできます。

一方、クライアントに代わって身代金支払いの交渉を行うブティッククサービスもあります。米国の州立法府のうち、ランサムウェアによる身代金の支払いを禁止することを検討している州がありますが、FBIは米国議会にそのような禁止令を出さないように薦めています。[3] この動向を知るためには、ビジネスについての深い専門知識が必要になることがよくあります。

攻撃手法がますます巧妙になり、問題がより深刻化しており、企業も新しい対策法を取り入れ、対応しなければなりません。この進化する脅威の状況に自信を持って対応するには、オペレーショナル・レジリエンス、サイバー脅威に対する知識、そしてサイバーセキュリティ対策を組み合わせる必要があります。

しかし、これは簡単ではありません。堅牢で一貫性が有り、スピーディーに攻撃に対応するサイバー防御システムを構築する必要があります。例えば、次のような項目です。

侵害ポイント	対応方法	
ユーザーによるWebサイト上のパスワードの使い回し	• セキュリティ意識向上トレーニング	• ポリシー遵守の組織文化醸成
ユーザーのパスワードやアクセス権がダークウェブなどで流通	• サイバー脅威インテリジェンス • パスワードポリシーの管理	• 脆弱性管理
攻撃者による脆弱なシステムへのアクセス	• 多要素認証（MFA） • ネットワーク分離	• 高度な脅威保護
攻撃者による特権IDの窃取	• 特権ID /アクセス管理 • 強力なアクセス管理	• 高度脅威対策ソリューション
攻撃者が外部送出の準備のためデータを収集	• データ損失防止 • 侵入検知システム	• エンドポイント脅威検知対応ソリューション（EDR）
攻撃者がランサムウェアを実行	• エンドポイント脅威検知対応ソリューション（EDR） • サイバー保険	• システムとデータのバックアップ
攻撃者からの恐喝要求	• インシデント対応 • 危機管理	• 法的措置

ランサムウェアに攻撃された場合の対応の複雑さを踏まえ、組織が直面するリスクの分析と重要な資産の保護という課題への対応のために、経営陣は何ができるでしょうか。以下に4つの提案を示します。

3 “Amazon’s New CEO Andy Jassy Says This 4-Word Lesson Is the Most Important He’s

最高情報セキュリティ責任者（CISO）の準備

CISOの中には、取締役会への状況報告に自信のない方や、自身が自己主張できる立場ではないと思い込んでしまう方もいます。さらに、取締役会の心に響き、適切なレベルで対話をすることの重要性を認識しつつ、そのために重要な戦略的コミュニケーションスキルが不足している可能性があります。

CISOの役割は、企業の重要な資産のセキュリティを確保するために非常に重要であり、取締役会とCISO双方で対話をすることが重要です。そのために、取締役会は次のことを行う必要があります。

- CISOに対して期待を明確にすると共に、議論のために十分な時間を確保し、追加のリソースと予算が要求された場合に耳を傾け、CISOに自信を持たせる。
- CISOに懸念事項を伝えることにより、取締役会への説明に先立ち、課題の優先順位を決められるようにCISOを支援する。
- 取締役会は、共有した期待に対してCISOの説明を聴き、サイバーセキュリティに関するディスカッションの時間が限られている場合は、オフラインで詳しい説明を聴く。
- CISOを取締役会における戦略的パートナーとして位置付け、関心のある取締役との会議でCISOを支援する。
- CISOを取締役会が問題の重大さについて理解を深める教育責任者として位置づける。
- CISOの採用、およびその後継者育成に関する経営陣の基準を理解し、承認する。
- CISOが戦略的な見解を持ち、現場部門の運用の対応に囚われないよう支援し、価値のある戦略を描くことをサポートする。

効果的なサイバーセキュリティの監視のための取締役会の役割

ランサムウェア攻撃が発生すると、多くの場合、問題が解決されシステムの構造的完全性が修復されるまで、取締役会全体が責任を持って取り組みます。

CISOは、サイバーセキュリティ対応の基礎となるさまざまな業務運用に関する責任を持ち、現場の管理者はその有効性に責任を負っています。取締役は、今後の対応計画およびその実施を支援するため、CISOの説明から自信を得る必要があります。

関係者全員が、過去の攻撃から学んだ教訓を活かし、脅威に対して継続的な評価を行う必要があります。

CISOを、取締役会のメンバーとして、または取締役会の客観的なアドバイザーとして、追加の専門知識の展開が必要かどうかを定期的に確認する必要があります。

取締役による適切な質問（サードパーティー含む）

多くの取締役会は、ランサムウェアの攻撃が他の企業などではどのように発生したか、自分の組織もサイバー犯罪者によって同じ手法で攻撃にさらされる可能性があるかどうかを理解しようとします。

取締役は、状況認識、戦略と運用、内部脅威、インシデント対応、および関連トピックについて、経営陣を代表して適切な質問を発しなければなりません。サイバーリスクの監視に関する全米取締役会（NACD）の出版物の付録は、関連する質問を示唆しています。[4]ランサムウェア攻撃に備え、取締役は、企業全体の視野から攻撃の被害の評価とインシデントへの対応と準備に焦点を当てる必要があります。

- ミッションクリティカルなシステムや機密データを管理する、業務委託先がランサムウェア事案の被害にあうと、自社への直接攻撃と同じように、多大なインパクトを与える可能性があります。
- 会社のシステムやデータへのアクセス権限をサードパーティが持っており、それらが攻撃者に漏洩した場合、会社自体が攻撃にさらされる可能性があります。

適切な指標によるダッシュボードでコミュニケーションをサポート

CISOからのレポートや指標は、取締役会に情報を提供し、全体的なエンタープライズリスク管理（ERM）ダッシュボードに統合する必要があります。

主な指標として次のようなものが挙げられます。

- システムの脆弱性の件数
- パッチを実装するために必要な時間
- 違反の件数
- 攻撃者の滞留時間（侵害を検出するために必要な時間）
- 違反が検出されてから対応にかかる時間
- 監査で検出された項目の改善にかかる時間
- 第三者経由での違反の件数
- セキュリティプロトコルの違反の件数

ランサムウェア攻撃にさらされた場合、攻撃者の滞留時間は特に重要です。攻撃者がネットワーク内で検出されない時間が長いほど、身代金要求のために利用できるシステムやリソースを見つける可能性が高くなります。

最近のランサムウェア攻撃者は、多くの場合、資金が豊富で、ビジネスに精通しており、高度なハッキングのスキルを持っています。取締役会は日常業務の詳細について責任を負いませんが、データの機密性と会社の知的財産、評判、ブランドイメージ等の株主にとっての価値を考えると、サイバーセキュリティに対する責任を果たすことは重要です。

4 See Tool A: Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards, NACD, 2020, available for purchase at www.nacdonline.org/insights/publications.cfm?ItemNumber=67298.

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検討すべき事項です。

- ランサムウェアの影響を防止または抑制できる効果的な各種セキュリティ対策が施されていますか。
  - これらの対策には、特権アカウントを保護するための対策は含まれていますか。
  - これらの対策はどのくらいの頻度で点検されますか。攻撃者のスキルが進化する中、攻撃を想定したテストを定期的に実行することにより、防御体制が攻撃を検出し、タイムリーに対応できることを確認していますか。
  - ランサムウェアによる被害を軽減するためのバックアップ戦略は何ですか。たとえば、継続的なバックアップサイクルがあり、バックアップのオフサイト保存が行われていますか。
  - ランサムウェア攻撃が発生した場合のインシデント対応計画は何ですか。計画は組織内でどの程度広く共有されていますか。ランサムウェア攻撃の標的になった場合に備えた体制（サードパーティーを含む）がありますか。
- 重要なシステムとデータがどこにあるか、失ったり、奪われたりすることが許されない重要な資産が何か、また、計画外のシャットダウンが許容できないシステムがどれかを知っていますか。事業継続のためのプロセスは整っていますか。ランサムウェアインシデントの発生に対応すべく、24時間体制での防御・監視を行っていますか。
- 会社は、調査費用、交渉費用、身代金の支払い、その他の付随的損失を含む補償を備えたサイバー保険で保護されていますか。
- 取締役会は、サイバーセキュリティに関するCISOへの期待を定義し、パフォーマンスに対する明確な説明責任を確立していますか。
  - 組織にリスクアペタイトステートメントがある場合、サイバーセキュリティおよびランサムウェア攻撃に対する取締役会の期待は組み込まれていますか。
  - 経営陣が使用し、取締役会に報告した指標は、最優先のサイバーリスクがどのように管理されているかが明確になるようサポートしていますか。それらは、取締役会の監視や、CISOの取締役会とのコミュニケーションに役立っていますか。
  - ランサムウェアインシデントが起こった場合の影響を効果的に定量化できますか。
- パンデミックにより加速した、リモートワークや、バーチャルな顧客対応への移行は、標的型のランサムウェア攻撃や高度標的型攻撃のリスクを高めていますか。犯罪者がリモートワーカーを悪用するリスクに対処していますか。サードパーティリスク管理プログラムは、ランサムウェア攻撃へのエクスポージャー（リスクにさらされている度合い）を考慮していますか。

プロティビティの支援

プロティビティは、サイバーセキュリティとプライバシーの分野において、新たに展開した専門的なランサムウェアアドバイザリーおよびリカバリサービスを提供することで、ミッションクリティカルな運用を攻撃し妨害する悪意のある攻撃者の脅威に、企業が対応するよう支援します。プロティビティのサービスは、ランサムウェア攻撃による被害を受けた組織に対し、速やかな危機対応や事業再生、および長期的なレジリエンスに向けて体制を築くことができるように設計されています。

プロティビティのクロスソリューションチームは、「予測する」「対応する」そして「回復する」という3つの主要なフェーズを通じて、お客様のランサムウェアに対するレジリエンス、およびビジネス全体のサイバーセキュリティ体制の強化を支援します。オペレーショナル・レジリエンスは取締役会と経営層にとって最優先事項であり、強力な危機管理計画と最新のデータ保護対策は、業務の維持や効率と回復時間の改善、そして、より安全な組織になるために重要な要素です。