ExtraHop

ExtraHop

サイバーセキュリティの信頼度指数：アジア太平洋地域 2022 年版

この 5 年間、アジア太平洋地域のサイバーセキュリティにとって多忙な時期でした。ここに示すのは、IT セキュリティ・リーダーが考える次の一手です。

この 5 年間、IT セキュリティ担当者とチームは間違いなく脚光を浴びてきました。IT セキュリティは、企業において IT 予算に占める割合が高く、しかも伸び続けている領域です。にもかかわらず、セキュリティ・チームが課題に対処するのに必要な予算と人材は、大幅に不足し続けています。

リソースの拡充は、サイバーセキュリティが現代の組織において果たす役割に対する、取締役会、経営幹部、および意思決定者の一般的な理解度を示しています。

そうした理解は、ほとんどの場合、実際に攻撃を受けた経験によって生まれます。

当社の調査によると、アジア太平洋地域の組織の 83% がこの 5 年間に一度はランサムウェアによる侵害を経験しています。組織が攻撃を受けたことは話題にしづらいことを考えると、その割合はさらに高くなりそうです。事実、20% の組織が仮に侵害を受けても公表しないとしています。

取締役会や経営幹部がサイバーセキュリティに投資することで、安全性と継続性を確保した事業活動を期待していることを考えると、侵害件数の報告は問題となります。

- 脅威環境がこれまでになく目まぐるしく変化する中、IT セキュリティ意思決定者がセキュリティ・チームに大きな影響をもたらすにはどうすればよいでしょうか。
- アジア太平洋地域の IT セキュリティ意思決定者は、どうすれば自社の脅威の検知・防御に対する信頼を深め、その信頼を取締役会、およびスタッフに伝えることができるでしょうか。

このレポートでは、まず IT セキュリティ意思決定者が示している信頼について分析します。その上で、そうした信頼を揺るがす可能性があるいくつかの要因を取り上げます。そして最後に、現実を反映し、継続的な投資を正当化する、より確実なサイバーセキュリティ・チームの構築に向けて柔軟に対処する方法について説明します。

自社サイバーセキュリティ・チームに対する信頼について

サイバーセキュリティ・チームに対する信頼を公表すると余計な注目の的になり、思わぬ面倒を招きかねません。また、攻撃者と防御側の間に長期に渡り存在するアンバランスによって表現が抑えられることもあります。防御者がどんなにリスクの排除を試み、盲点を特定しようとも、一般的なプロトコルの欠陥、新たなエクスプロイト、脆弱性チェーンなど、予見することができない新たな脅威が常に出現し、セキュリティと信頼を揺るがします。

にもかかわらず、過去に実施した同様の調査では、一部の IT セキュリティ・リーダーには自社の備えと脅威検知・防御能力に対する過信が見受けられました。セキュリティに対する信頼度と、安全ではないプロトコルが驚くほど普及し、攻撃の成功頻度が高いという事実との間には、明らかなギャップがあります。

私たちは、このことを念頭に置いて、アジア太平洋地域における答えの調査に取りかかりました。このレポートで紹介するのは、オーストラリア、シンガポール、および日本の調査結果です。いずれも重要な地域市場ですが、企業文化的特徴が大きく異なっており、それが今回の調査結果にも反映されています。アジア太平洋地域全体の視点に加え、アプローチの違いを浮き彫りにするために国別の詳細も示します。

自社対応能力を高く評価しているのは 39% に過ぎない

地域全体で見た場合、IT セキュリティ・リーダーは直面する脅威について現実主義的で、自社が脅威に適切に対応できると自信を示しています。しかしながら、自社がサイバーセキュリティ脅威を阻止または軽減する能力を大いに信頼していると答えた回答者は 39% にすぎず、あまり信頼していないと答えた回答者も同じ割合でした。

各国の間には大きな差があります。シンガポールの IT セキュリティ・リーダーの 52% が自社の態勢に強い自信を持っているのに対し、オーストラリアは 43%、日本は 23% にとどまっています。以下、その信頼の根拠について探ってみましょう。

前述のように、サイバーセキュリティに対する自信は危うい考えです。純粋に歴史的観点やリスクの観点から見て、自信を持ちすぎない、または控えめにすることは理にかなっています。

また、この 5 年間のサイバーセキュリティ運用の状況と、サイバーセキュリティの社内的な注目度と重要性の高まりにも留意する必要があります。企業は、投資拡大によってサイバーセキュリティを支えてきました。取締役会や経営幹部は投資利益を期待していますが、これはたいてい「信頼」という言葉で表現されます。

2022 年のサイバーセキュリティ予算の増額を見込んでいる企業は、全体の 3 分の 2（61%）弱でした。シンガポール（70%）とオーストラリア（66%）に比べて日本は低く、予算の増額を見込んでいると答えた回答者は 48%にとどまり、49%が前年並みと答えています。全体的に見て、サイバーセキュリティ予算の減額を予想した回答者はほとんどいません。

セキュリティに関する社外向けメッセージは、標的になったり攻撃を受けたりすることは避けられないと表現されがちです。しかし、取締役会や経営幹部は、そうしたリスクに対する説明責任が高まっており、十分な信頼が必要です。そこで頼りにされるのが、IT セキュリティ・リーダーとそのチームに対する信頼です。しかし、説明責任のため、サイバーセキュリティに関する自社の信頼が正当なのか、過剰なのか、自社で個別に、独自の調査やデュー・ディリジェンスを実施する動きが、取締役会や執行委員会の間に広がる可能性があります。

セキュリティ分野の技術的な性質を考えると、過信の程度を判断することは難しいかもしれませんが、このレポートでは「自社の信頼スコアにおける矛盾」を見極めるいくつかの指針として、たとえリーダーが信頼を示していても、行動パターンや手法によって信頼を損ねている事例を紹介します。

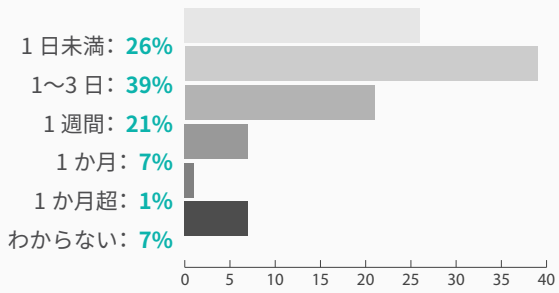
こうした矛盾点を見極める知識や意識があれば、さらに尋ねるべき事柄を理解し、取締役会や経営幹部に対して表された信頼の強さを本当に検証するのに役立ちます。

尋ねるべき事柄

本調査の大部分では、IT セキュリティに対するベスト・プラクティス・アプローチの不足が明らかになっていますが、自社の信頼スコアに適切に反映されていないか、信頼スコアを損なっている可能性があります。

まず、セキュリティ・チームがすでにうまく機能している、つまり追加の精査を行う正当な根拠がないかもしれない領域があります。

深刻な脆弱性にパッチの適用または対策の実施にどのくらいの時間を要していますか？



2022 年の調査で、ほとんどの国で認められた好ましい傾向として、アクセス制御やサプライチェーン攻撃の可能性が十分に理解されているようです。半数強（51%）の企業が第三者に自社のネットワークへのアクセスを許可しており、同時にこのグループのほとんど（86%）がセキュリティ面を考慮しています。ただし、シンガポール（96%）とオーストラリア（87%）に比べて日本（74%）は低く、4 社中 1 社はセキュリティに及ぼす影響を考慮していません。

また、ほとんどのセキュリティ・チームは脆弱性の発見に素早く対応しており、64%のチームが 3 日以内に軽減策を実施するか、（もしあれば）パッチを適用できるとしています。その一方で、28%のチームは軽減策の実施またはパッチの適用に 1 週間以上を要しています。内訳をさらに細かく見ると、対応に要する期間が 1 日未満というチームが 26%、1〜3 日が 39%、1 週間が 21%、1 か月以上が 8%となっています。自社の対応時間のベンチマークを実施することが重要です。その一方で、脆弱性への対処にはある程度の

時間を要することを理解することも重要です。パッチや軽減策が問題を修正する以上に、システム間の依存関係や相互依存関係を壊さないことを確認するために、かなりの検証を行う必要があります。本番システムへの予期しない影響を回避するには、セキュリティ・チームに作業のための十分な時間を与えることが不可欠です。

サイバーセキュリティ・チームのその他の側面では、信頼スコアを検証するにはかなり適切な質問が必要かもしれません。

まず、リソースの配置について、必ずしも意見の一致は見られません。回答者の 24% はほとんどのリソースを境界での脅威の検知に重点配置し、32% はネットワーク上での侵害後の活動の検知に重点配置し、42% は両方に同等の比重を置いてリソースを配置しています。一度、自社の状況と理由を確認してみるとよいでしょう。なお、境界セキュリティへの重点配置が少ないのは、ほとんどの企業（81%）がすでに十分に配置しているという自信があるからかもしれません。

次に、リソースや投資のレベルにもかかわらず、サイバーセキュリティ・インシデントの半数は旧態依然のセキュリティ・チームに原因があります。セキュリティ機能を支えているリソースを考えると、この数字は表面上、高く見えます。しかし、現在の「態勢」に対する負担がかなり高いことを考えると、人員、プロセス、およびテクノロジベースの活動や成果の間で、セキュリティへの投資全体を一から見直す必要があるかもしれません。

セキュリティ・インシデントの半数は旧態依然としたセキュリティ・チームに原因あり

「人員」面では、79% の回答者が専任の社内セキュリティ担当者を置いています。また、このグループの 71% はそれらの担当者を支援するために外部のマネージド・サービス・パートナーを使用しています。どちらかと言えば、企業は十分な人員を確保しています。雇用市場は相変わらず厳しい状態が続いていますが、完全なリモート・ワーク・モデルによって利用可能な人材市場が拡大しており、66% の回答者は在宅勤務の傾向が進んでいると答えています。40% の回答者は、2022 年に専任の社内セキュリティ担当者を増員または雇用する予定で、外部リソースを使用する意向の回答者も同数に上っています。

それに対し、6% の企業は専任の社内チームも社外チームも置いていません。これは少ない数字に見えるかもしれませんが、全企業に適用した場合、基本的なサイバーセキュリティ保護が欠如した企業が非常に多く存在することになります。このグループに含まれる企業は心配の種になるかもしれません。

ほとんどの企業は、サイバーセキュリティのプロセス成熟度も達成しています。これは、社内外の人材による混成チームの場合に重要です。本調査では、82% の回答者がサイバー攻撃またはサイバー緊急事態に対応するに当たって、自らの役割を理解していると答えています。プロセス成熟度が旧態依然のセキュリティ・チームの一因である可能性は低いでしょう。

主な心配の種はテクノロジであり、これは本調査でも裏付けられています。パッチ未適用のデバイスや時代遅れのプロトコルの使用は、防御者の信頼を弱めています。半数以上（54%）の回答者は、サイバーセキュリティ・インフラストラクチャの最後の更新が 2020 年以前で、5 分の 1 の企業は更新されずに 3 年以上が経過したテクノロジを使用しています。さらに、76% の回答者がレガシー・システムが攻撃されることを懸念していると答えています。

意外なことではありませんが、2022 年の体制改善のための重点投資領域は、テクノロジ関連が上位 3 項目を占めており、脅威の検知と対応のためのツールへの投資が 51%、ハイブリッド / リモート・ワークフォースのセキュリティ改善が 48%、ハイブリッドおよび / またはマルチクラウド・セキュリティの改善が 39% となっています。

地域別の統計

オーストラリア

43% が自社のサイバー脅威対応能力を非常にまたは完全に信頼しています
19% が常にランサムウェアを特定し、阻止できると答えています
77% が社内ネットワークへの攻撃者の侵入を防止できると確信しています
69% がレガシー・システムが攻撃されることを懸念しています
66% が 2022 年は IT セキュリティ予算の増額を見込んでいます
76% が専任の社内セキュリティ・チームまたはスタッフを置いています
63% がサイバーセキュリティ・チームの人材確保が難しいと答えています
71% がリモート・ワークによってサイバーセキュリティ・スタッフの雇用が容易になったと答えています
56% が社員はソーシャル・エンジニアリング攻撃を認識できると確信しています
64% が法的措置や罰金の脅威により、セキュリティの意思決定において経営陣に行動が促されていると答えています
49% が NDR（Network Detection and Response）ソリューションを使用しています

シンガポール

52% が自社のサイバー脅威対応能力を非常にまたは完全に信頼しています
31% が常にランサムウェアを特定し、阻止できると答えています
88% が社内ネットワークへの攻撃者の侵入を防止できると確信しています
87% がレガシー・システムが攻撃されることを懸念しています
70% が 2022 年は IT セキュリティ予算の増額を見込んでいます
87% が専任の社内セキュリティ・チームまたはスタッフを置いています
66% がサイバーセキュリティ・チームの人材確保が難しいと答えています
77% がリモート・ワークによってサイバーセキュリティ・スタッフの雇用が容易になったと答えています
63% が社員はソーシャル・エンジニアリング攻撃を認識できると確信しています
86% が法的措置や罰金の脅威により、セキュリティの意思決定において経営陣に行動が促されていると答えています
74% が NDR（Network Detection and Response）ソリューションを使用しています

日本

23% が自社のサイバー脅威対応能力を非常にまたは完全に信頼しています
17% が常にランサムウェアを特定し、阻止できると答えています
76% が社内ネットワークへの攻撃者の侵入を防止できると確信しています
73% がレガシー・システムが攻撃されることを懸念しています
48% が 2022 年は IT セキュリティ予算の増額を見込んでいます
75% が専任の社内セキュリティ・チームまたはスタッフを置いています
24% がサイバーセキュリティ・チームの人材確保が難しいと答えています
56% がリモート・ワークによってサイバーセキュリティ・スタッフの雇用が容易になったと答えています
35% が社員はソーシャル・エンジニアリング攻撃を認識できると確信しています
68% が法的措置や罰金の脅威により、セキュリティの意思決定において経営陣に行動が促されていると答えています
55% が NDR（Network Detection and Response）ソリューションを使用しています

ランサムウェアの状況に関する特記事項

本調査では、アジア太平洋地域におけるセキュリティ対応能力とそれに対する信頼のほか、ランサムウェア・インシデントの予期しない影響についても検証しました。

ランサムウェア攻撃は頻度、重大度共に 2021 年にピークを迎え、オペレータ間で大きな変動はあるものの、世界全体では

1 日数千件のペースで攻撃が発生し続けています。

本調査の回答者のうち、この 5 年間にランサムウェア・インシデントを一度も経験していない企業は 17% にすぎません。

- 48% は 1〜5 回の攻撃を受けています
- 35% は 6 回以上の攻撃を受けています

しかし、20% の回答者は、たとえ侵害されたとしてもその情報開示を極力控えると答えています。すでに触れたように、感染を経験した企業の自己申告数は控えめであり、実際の数ははるかに上回っている可能性があります。とりわけ、この 5 年間に 58% の企業が 1〜5 回、42% が 6 回以上のランサムウェア・インシデントを経験していることを考えると、その可能性が高いと言えます。平均すると、すべての企業がランサムウェア攻撃を年に 1 回受けている計算になります。

インシデント情報を包み隠さず開示している企業は、全体の 3 分の 1 にすぎません。これはセキュリティ・チームの期待に反している場合が多く、実際にセキュリティ・チームの 3 分の 2 が透明性を支持しています。これは、潜在的な風評被害や財務的損失の方が、倫理的配慮やソーシャル・ライセンス（社会的営業免許）の考慮に勝ることを示しています。

また、本調査では次のことも明らかになっています。

- 身代金を支払うと攻撃回数が増加すると大多数が考えているにもかかわらず、45% の企業は身代金の支払いに応じています。
- 44% の企業はランサムウェア専門または総合の保険に加入しています。

2022 年のアクション・アイテム

NDR（Network Detection and Reponse）：

34% の企業が NDR（Network Detection and Response）システムをすでに導入済みであることに加え、42% の回答者が今年投資する予定です。

ソーシャル・エンジニアリング戦略：

21% の回答者がソーシャル・エンジニアリング戦略をすでに実施していることに加え、47% が 2022 年に実施する予定です。また、58% がソーシャル・エンジニアリングの手掛かりを識別できるように社員をトレーニングするとしています。

サイバー脅威に対するトレーニングと識別能力の強化：

46% の企業が社員にサイバー脅威に対するトレーニングを実施する予定であり、同じく 46% が識別までの時間を改善する予定です。

リソースの拡充：

40% の企業が専任の社内セキュリティ・スタッフの増員または雇用を計画しています。また、同じ割合の企業が 2022 年に外部のマネージド・セキュリティ・サービスを使用する予定です。

まとめ:サイバーセキュリティ・チームに対する投資と信頼

アジア太平洋地域の IT セキュリティ・リーダーは、脅威の増大と高度化に対する自身または自社の防御能力を過信していません。その反面、自社の防御能力にあまり信頼を示していないリーダーが多すぎます。取締役会や CEO が IT セキュリティ・リーダーの信頼評価の低さを疑問視し、サイバーセキュリティへの既存の投資レベルを維持する必要がある「正当な理由」を示すよう迫るのも時間の問題です。

その質問に対する答えは、適切な支援を欠いたチームの経験に目を向けることかもしれません。最後のシステム更新から 3 年以上が経過している 20% の IT セキュリティ・リーダーにとって、今すぐ投資し、行動を起こすことが必要です。その他のリーダーの間に見られる、レガシー環境がセキュリティに及ぼす影響や 1 年に何度も侵害を受ける脅威に対する懸念の高さは、サイバーセキュリティ・チームがあっという間に時代遅れになり、脆弱になることを物語っています。

つまり、どの企業にも自社のセキュリティ・チームに対する信頼を高めるためにできることがあるということです。さまざまな対策が考えられますが、ほとんどの IT セキュリティ・リーダーにとって最も重要なのは、脅威の検知と対応ツールへの新たな投資です。一連の新たな投資と更新により、サイバー防御のあらゆる部分に対する信頼を、より安心なレベルにまで引き上げることが十分可能と思われます。

本調査について

本調査は、ExtraHop の依頼により、StollzNow Research 社が 2022 年 1 月に実施したものです。調査対象者として、従業員数 50 人以上の幅広い業種の企業の IT 意思決定者を、オーストラリア、シンガポール、および日本からそれぞれ 100 人ずつ選びました。

ExtraHop Networks について

ExtraHop は、脆弱性をつかれたり、巧妙に裏をかかれたり、侵害されたりすることから企業を守り、高度な脅威を阻止するという使命を担っています。ExtraHop のダイナミックなサイバー防御プラットフォームは、クラウド・スケールの AI を使用して、お客様のビジネスが危険にさらされる前に、高度な脅威に対する検知、対応を実現します。ビジネスを保護しながら前進させることを可能にすることが妥協のないセキュリティです。

ExtraHop

info@extrahop.com
www.extrahop.com