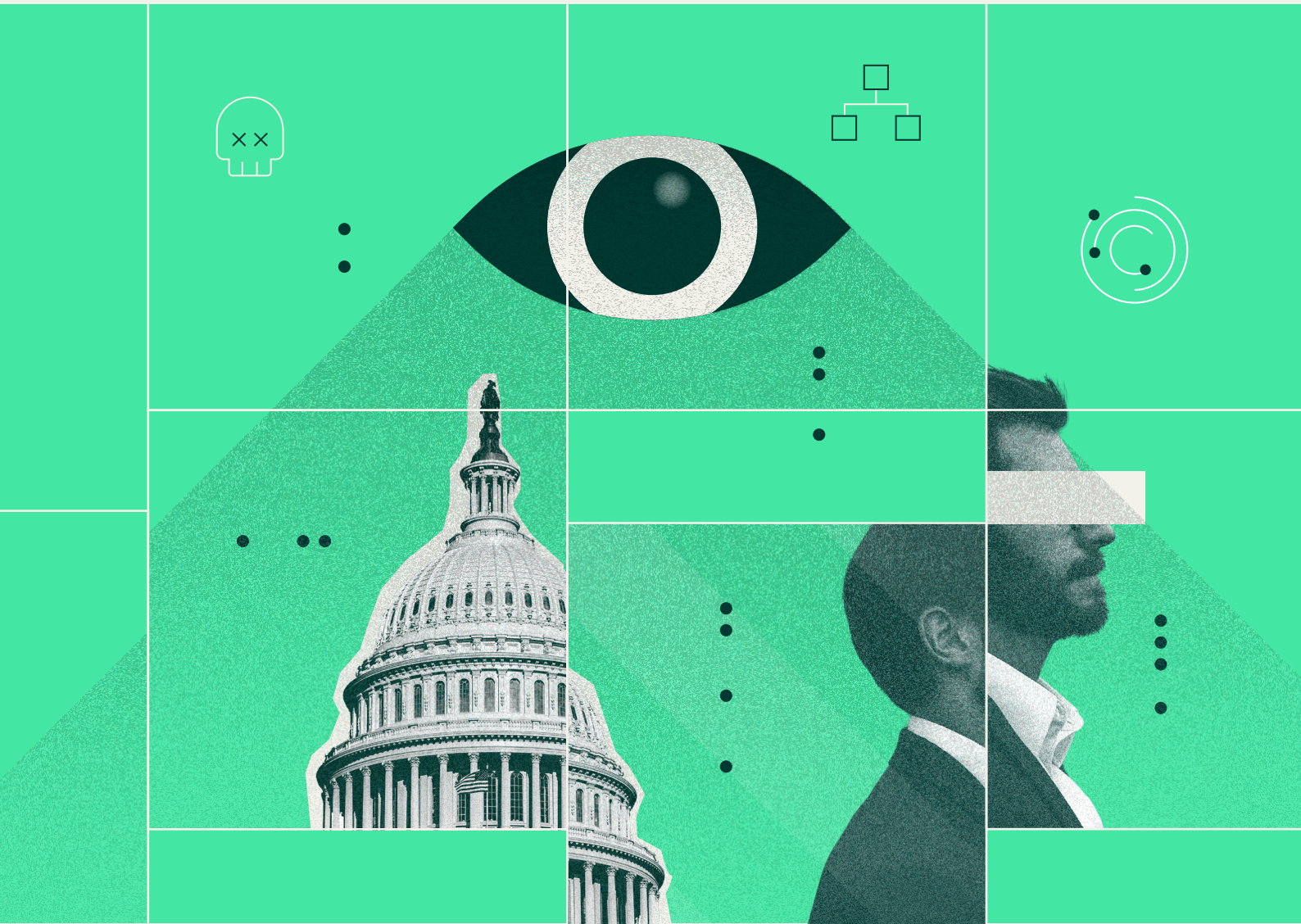
Rubrik Zero Labs

ホワイトペーパー

データセキュリティの現状

サイバー犯罪の人的影響



目次

はじめに p3

回答者の構成 p5

1.0 セキュリティをとりまく状況 p6

1.1 サイバー攻撃は件数、影響度合いともに急増し続けている
1.2 組織は自社の攻撃耐性に自信を失っている
1.3 既知の脅威は依然として最大の課題

2.0 現状 p10

2.1 ITやセキュリティチームのリーダーはデータ保護に不可欠なリソースが依然として必要
2.2 大きな打撃を与えるサイバー犯罪の影響
2.3 セキュリティ戦略の遂行に奮闘するリーダーたち

3.0 解決 p14

3.1 ITやセキュリティチームのリーダーが次に目指すもの
3.2 ベストプラクティス

まとめ p19

本書では、データについて、およびデータが脅威にさらされたときに私たちがどのような影響を受けるか、について説明します。また、データにかかわる人々、つまり仕事でデータを必要とする人、データを脅威にさらす犯罪者、データを保護する人についてもお話します。

Rubrik Zero Labsの初回レポート（Rubrikが委託し、調査はWakefield Research社が実施）では、データ保護を定型業務としている人の視点を通して、データ保護における人々への影響についても解説します。

Rubrik Zero Labsは、データのセキュリティリスクを軽減するための、ベンダーにとらわれない実用的な情報提供に取り組んでいます。また、実際のサイバー脅威の評価とサイバーレジリエンスのベストプラクティスに基づいて、ゼロトラストデータセキュリティの成果を促進します。Rubrik Zero Labsでは、次の3つをメインに焦点をあてています。

1

不正検知の運用を可能にする
データに基づいた監視と傾向分析から、積極的かつ実行可能な意思決定ポイントを導出します。

2

リスクを軽減する
調査、パブリックアドボカシー（公的な提唱活動）、パートナーシップに対する取り組み、データセキュリティのコアテクノロジーや組織としての経験を踏まえた新技術採用を通じて、サイバー攻撃の減少に取り組むようにします。

3

コミュニティを改善する
セキュリティのトピックやモデル、外部の出版物について詳しく調査し、データセキュリティの分野において信頼できるアドバイザーの役割を果たします。

「まず相手の話に耳を傾けなさい。自分は最後に話しなさい」。

マネジメントの父と呼ばれたピーター・ドラッカーは、こう述べました。「まず相手の話に耳を傾けなさい。自分は最後に話しなさい」。Rubrik Zero Labsはこの精神に基づいて、サイバー犯罪に日々取り組んでいる人々の声に耳を傾けることから始めたいと考えました。

偏りのない見解を得るために、当社のクライアント以外の人々から話を聞くようにしました。そのために、10ヵ国の1,600人を超えるITやセキュリティチームのリーダー（その半数がCIOとCISO）に対して、データセキュリティの現状についてインタビューしました。次に、最も優れたサイバーセキュリティのエキスパート数人に、今回の調査によって明らかになったこと、および組織がデータのセキュリティ確保のためにできることについて伺いました。以下のデータと展望をご覧ください。

1,600人以上
IT/セキュリティのリーダー

819人
CIOとCISO

10ヵ国
世界の国々

回答者の構成

この世界規模の調査は、Rubrikが委託したWakefield Research社により、従業員500人以上の企業のIT/セキュリティ意思決定者1,625人（ディレクター、VP、CIO、CISO）を対象に実施されました。この調査は、2022年7月18日～7月27日、米国、英国、フランス、ドイツ、イタリア、オランダ、日本、オーストラリア、シンガポール、インドで実施されました。

役職（人）	241 VP	565 ディレクター	408 CISO	411 CIO
地域（人）	500 北米地域	625 ヨーロッパ地域	500 アジア太平洋地域	
会社の規模	366 2,500人以上	505 1,000～2,499人	754 500～999人	

1.0
セキュリティをとりまく状況

1.1
サイバー攻撃は件数、影響度合いともに
急増し続けている

1.2
組織は自社の攻撃耐性に
自信を失っている

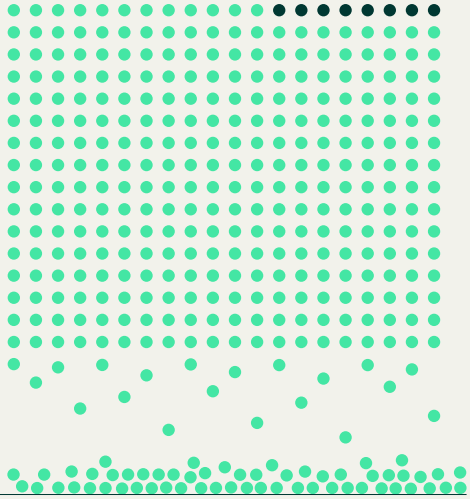
1.3
既知の脅威は
依然として最大の課題

1.1 サイバー攻撃は件数、影響度合いともに急増し続けている

サイバーセキュリティに対しては長年、重点的に取り組みや投資を行ってきましたが、私たちの耳に届くのは「サイバー脅威は依然として衰えていない」というニュースです。実際には状況は悪化しています。

98%

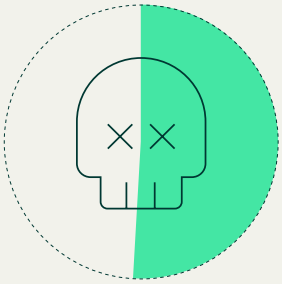
ITやセキュリティチームのリーダー1600人以上のうち、昨年中に少なくとも1回のサイバー攻撃を認識したと回答した割合。



平均すると、ITやセキュリティチームのリーダーは昨年に47回の攻撃を受けたことを認識している

52%

データが侵害された回答者の割合。



51%

同期間にランサムウェア攻撃に対処した割合

> 攻撃による組織内への侵入は、小規模の社内チームで対処できる範囲を超えています。今や、組織の意思決定者、多くの組織や公的機関では、この脅威を認識し、影響を受けています。

1.2 組織は自社の攻撃耐性に自信を失っている

攻撃の対象領域が拡大、サイバー犯罪の巧妙化など、ニュースでは多くのハッキング攻撃を報道しています。結果、IT/セキュリティのリーダーと、組織の重役は、自社は脅威に対抗できるのかという疑問を抱くようになりました。

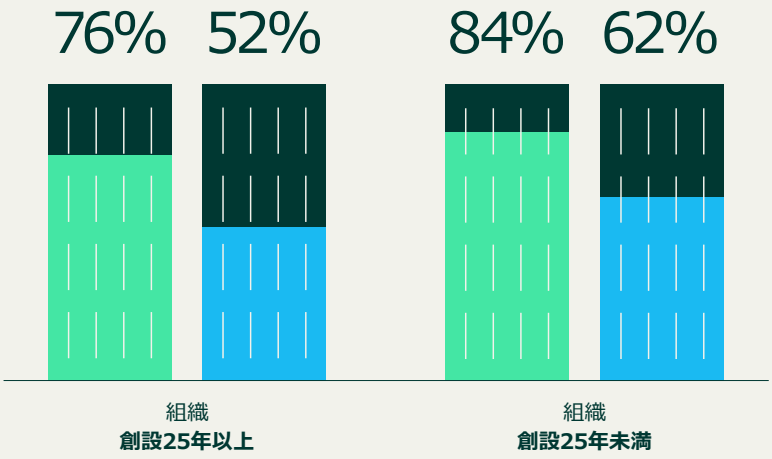
33%

のITやセキュリティチームのリーダーが「取締役会/経営幹部のリーダーは、サイバー攻撃を受けたときのデータ保護とアプリケーション復元について、ほとんど、あるいはまったく自信がない」と考えています。

92%

ITやセキュリティチームのリーダーが、来年サイバー攻撃を受けたら、ビジネスを継続できなくなると懸念しています。

ランサムウェア攻撃に直面したときの支払いについて



組織の取締役会/経営幹部は、サイバー攻撃を受けたときのデータおよびアプリケーションの復元能力にどれくらい自信を持っていますか。

27%

絶対的な自信がある

40%

ほぼ自信があるが少々心配になる

33%

ほとんど（またはまったく）自信がない

1.3 既知の脅威は依然として最大の課題

ゼロデイ攻撃はサイバーセキュリティ業界で大いに注目を集めているものの、昨年この攻撃を受けたと回答したのは回答者のうち約1/3にとどまり、来年の最大の脅威とみなしている回答者はわずかでした。

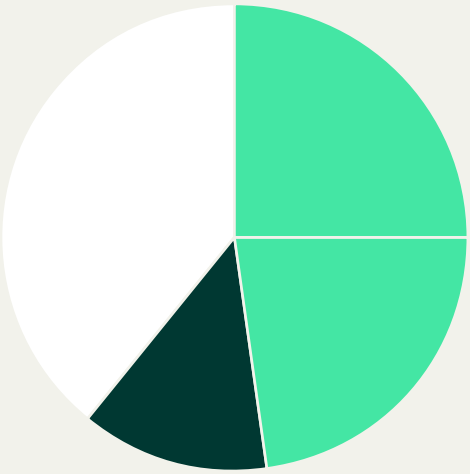
39%

昨年、ITやセキュリティチームのリーダーの認識レベルでゼロデイ攻撃と関係したサイバー攻撃は、39%だけでした。つまり、攻撃の約2/3がよく知られた脆弱性と手法を利用したものでした。

11%

のITやセキュリティチームのリーダーが、前に受けた攻撃以降、脆弱性を十分に修正できていないと回答しました。

48% のITやセキュリティチームのリーダーが来年の最大の脅威を次のように予想しています。



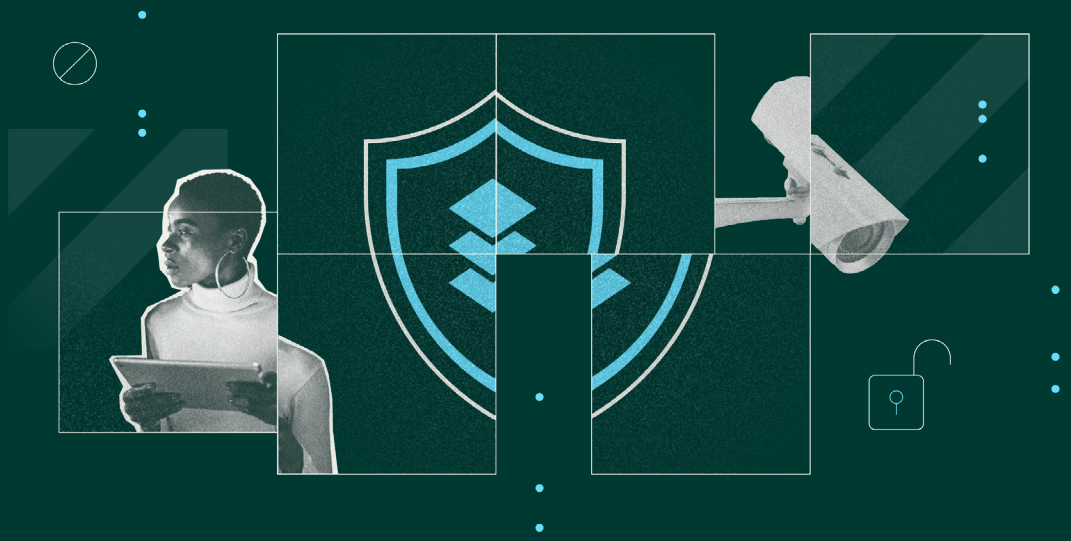
25%
データ侵害

23%
ランサムウェアイベント

比較すると、わずか
13%
ゼロデイ攻撃

> 件数が急増して注目度が高まるサイバー攻撃、新たに出現する脅威、既知の問題を解決するための課題といった要素が重なり、IT/セキュリティ担当者に対して多くのことが要求されています。

2.0
現状



2.1
ITやセキュリティチームのリーダーは データ保護に不可欠なリソースが依然として必要

2.2
大きな打撃を与えるサイバー犯罪の影響

2.3
セキュリティ戦略の遂行に 奮闘するリーダーたち

2.1 ITやセキュリティチームのリーダーはデータ保護に不可欠なリソースが依然として必要

サイバーセキュリティ業界は、何年にもわたり、優れた人材の不足に直面しています。Cybersecurity Ventures社によると、サイバーセキュリティの求人は、2013年の100万人から2021年には350万人へと350%増加しています。Rubrik Zero Labsの調査回答者は、当然ながら、組織を保護するうえでの最大の課題として「人材」を挙げており、それにツール、予算、経営幹部レベルや取締役会のサポートが続きました。

サイバー攻撃から組織を保護するうえでの上位5つの課題を挙げてください

1. ITチームまたはSecOpsチームの人材が不足している
2. サイバーセキュリティのツールとソリューションが整っていない
3. データセキュリティの予算が不足している
4. 経営幹部/取締役会によるデータセキュリティの優先順位付けが行われていない
5. サイバー攻撃に対する保護対策についてチーム間で意見が統一されていない

従来、

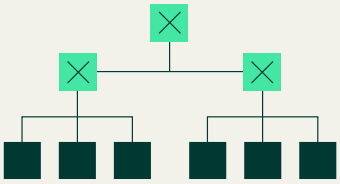
リソース不足は小規模な組織でよく見られる現象です。小規模な企業では、サイバー攻撃と戦う負担は大きいですが、人材も少なく予算も限られています。

2.2 大きな打撃を与える サイバー犯罪の影響

サイバー犯罪の高まりとリソース不足が重なって、ITやセキュリティチームのリーダーやそのチームだけでなく、組織全体が大きな打撃を受けています。

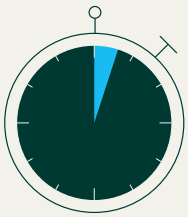
96%

のITやセキュリティチームのリーダーが、自身の雇用への不安や、組織や同僚間の信頼の喪失など、感情的、心理的に多大な影響を受けていると述べています。



36%

の調査対象の組織が、昨年、サイバー攻撃とその後の対応により、リーダーを交代しました。



わずか5%

の組織だけが、サイバー攻撃の検知後1時間以内にビジネスを継続できたか、通常業務に戻れました。

回答した組織の96%が、サイバー攻撃の結果、マイナスの影響を受けています。サイバー攻撃の結果、組織はどのような影響を受けましたか。

42%	41%	40%	36%	5%
否定的な報道やイメージの悪化	顧客の流出	収益の損失	リーダーの交代が余儀なくされた	株式への悪影響

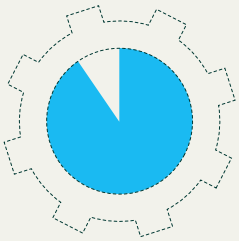
> 従業員の極度の疲労、複雑さの増大、極めて不安定な脅威の状況により、業務や、需要が高く数の少ない人材確保に多大な負担がかかっています。攻撃の侵入が公になるにつれて、1回の侵害による悪影響が組織全体に及んでいきます。

2.3 セキュリティ戦略の遂行に奮闘するリーダーたち

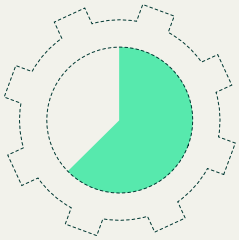
ITやセキュリティチームのリーダーは、攻撃に効果的に対処し、積極的な改善を行うためには、ITチームとSecOpsチームの連携強化が重要と強調しています。また、グローバルなサイバーセキュリティ問題を解決するために、官民の協業の必要性も訴えています。しかし、Rubrik Zero Labsの調査結果からわかるのは、これらの提案を推し進めるのは実際には難しいということです。

31% の調査対象のリーダーが、組織の保護に関して、ITチームとSecOpsチームはある程度連携している、またはまったく連携していないと述べています。

回答者は、官民の協業について次のように回答しています。

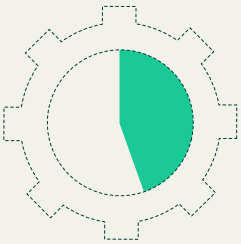


89%
有益であると考える



64%
極めて有益であると考える

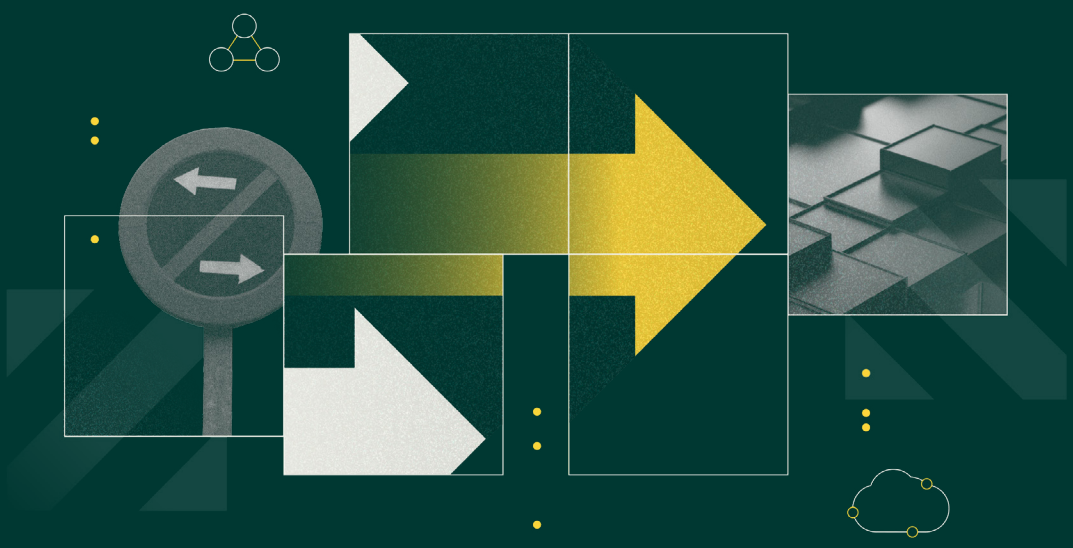
しかし、サイバーセキュリティに取り組むために官民の協業に関与していると答えた回答者は、半数に届きませんでした。



44%
官民の協業に関与している

> 重要な取り組みおよび投資にもかかわらず、組織はその実施に苦労しています。アーキテクチャとプロセスの抜本的な変更が長期的な利益となりますが、その実現には困難を伴います。

3.0
解決



3.1
ITやセキュリティチームのリーダーが次に目指すもの

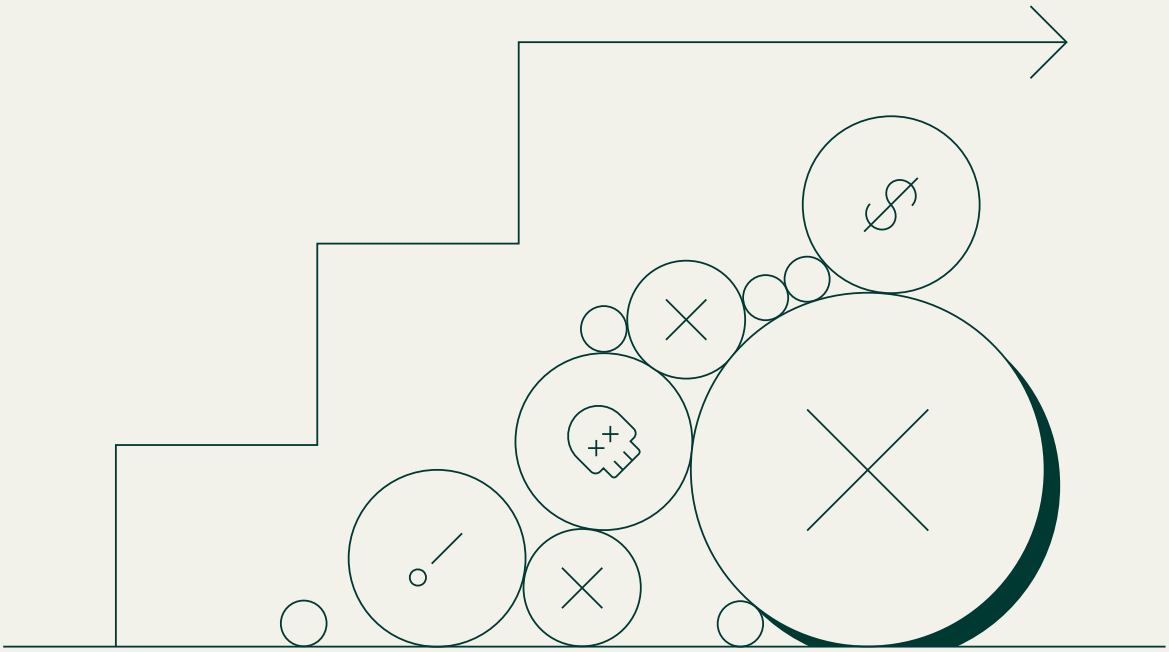
3.2
ベストプラクティス

3.1 ITやセキュリティチームのリーダーが次に目指すもの

Rubrik Zero Labsの調査結果によると、ITやセキュリティチームのリーダーは、サイバー攻撃から自社データを保護するうえで増え続ける課題に絶えず直面しています。

これらの課題を克服するために、リーダーには何ができるでしょうか。

サイバーセキュリティの専門家は、この厳しい現実に取り組むための推奨事項を示しています。彼らは状況の深刻さを認め、企業が自社とデータを守るためにできる3つのベストプラクティスを提案しています。



3.2 ベストプラクティス

1 データ侵害の対策は、毎週の侵害に対抗できなければならない

ITやセキュリティチームのリーダーは、昨年、組織に対するサイバー攻撃を平均47件認識したと回答しました。これはほぼ1週間に1回攻撃を受けていることになります。攻撃が増加する可能性は高いため、ITやセキュリティチームのリーダーは、攻撃に毎週対処する能力が求められます。組織は、インシデントのたびにサイバー対策と危機管理計画の両方を繰り返し迅速に実行して、時間の経過に従いサイバーレジリエンスを向上させなければなりません。サイバーレジリエンスが向上すると、各チームはより迅速かつ確実に業務を復旧し、その後の侵害の影響を少なくすることができます。

攻撃対策の取り組みを周知し、継続的に改善していくプロセスには、ITやセキュリティチーム以外の部門からの参加が必要です。たとえば、法務、HR、コミュニケーションといったチームも、時間と労力を集結する必要があります。

「組織がサイバー攻撃を受けるのは、可能性があるかどうかではなく、いつ攻撃を受けるか、という問題となっています。「対策」が最大の武器となります。リーダーは対応するための戦略を策定・実践することで、攻撃発生時にビジネスを迅速に復旧する適切なチーム、ソリューション、プロセスを整える必要があります」。

ジョン・W・トンプソン氏
元マイクロソフト取締役会会長、
元シマンテックCEO

「サイバー攻撃に対処するには、ITやセキュリティチームだけでなく、あらゆる部門のビジネスリーダー間のコラボレーションが必要です。

しかし、サイバー攻撃への対策には、コラボレーションだけではなく、継続的なトレーニングと実践が必要です。考え抜かれたデータのセキュリティおよび復旧計画が整備されていることは、ビジネスのレジリエンスと業務の効果的な継続性を実現するための基本的なステップです」。

マイケル・メストロビッチ
Rubrik CISO、米国中央情報局（CIA）の元CISO

3.2 ベストプラクティス

2 リーダーは自社のデータについてもっと多くの質問をする必要がある

サイバー攻撃において、データはしばしば被害者として扱われます。しかし、データオブザーバビリティのテクノロジーを利用すれば、組織はデータアセット自体を使ってサイバーリスクを軽減し、インシデントの対応時間を短縮できます。

IT/セキュリティのリーダーが自問すべき重要な質問には、次のようなものがあります。

- 自社で作成・管理しているデータの量はどれくらいか
- 機密データ、または個人情報はどれか
- そのデータはどこに保管されているか
- それにアクセスできるのは誰か
- ビジネスに最大の影響を与えるデータはどれか
- 自社には、データの量、重要性、機密性、アクセスに基づいたポリシーを実施するための適切なテクノロジーやプロセスが整っているか
- こういったデータへのアクセスを維持するのに不可欠なのはどのサポートシステムか、また、それらはどのような手続きで運用されるのか
- データに関する疑問に、どのくらい早く答えを出せるか

従業員が出社とリモートワークのハイブリッド環境へ移行しつつある現在、これらの疑問に答えを出すのは難しいことかもしれません。とはいえ、リモートワークの従業員も、組織が攻撃に対処し、災害対応、内部犯行、データ漏洩事故など、さまざまな状況に対するレジリエンスを向上させる助けになります。

最新のサイバー脅威に備えるには、ITやセキュリティチームのリーダーは、機密情報が含まれている自社のデータについて、誰がアクセス権を持ち、どこに格納されているかなど、詳細を把握している必要があります。攻撃者は盲点を突くのが得意ですから、ITやセキュリティチームのリーダーはユーザーが常に攻撃を未然に防ぐことができるようにする責任があります。

Asheem Chandna氏
Greylock Partnersのパートナー

組織とそのデータを守るには、結局は基本的なレジリエンスが重要となります。そしてレジリエンスはデータを保護することによってもたらされます。サイバー攻撃が従来の防御対策をすり抜けたとしても、データが安全なら、事業を迅速に復旧して難局を乗り切れる余地があります。

Shay Reddy氏
CISO、Hanna Andersson

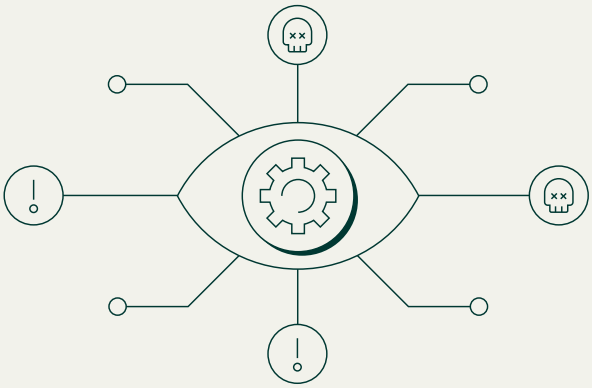
3.2 ベストプラクティス

3 サイバーリスクと脅威に関するインサイトをチーム間で共有する

Rubrik Zero Labsの調査結果が示すように、回答者の大多数は、不安定な経済、予算の引き締め、競合する優先事項、グローバルな紛争リスクなど、幅広い要因によって、将来的には割り当てられるリソースが減っていくだろうと考えています。

困難な要因が増加している状況では、チームが部門を越えて共同作業し、データを共有ビューの下で業務を行うことが重要になっています。ビューを共有してコラボレーションを促進することは、迅速な対応と復旧が必要となるサイバーインシデントが発生した際に、特に重要となりますが、日常業務の遂行にも役立ちます。

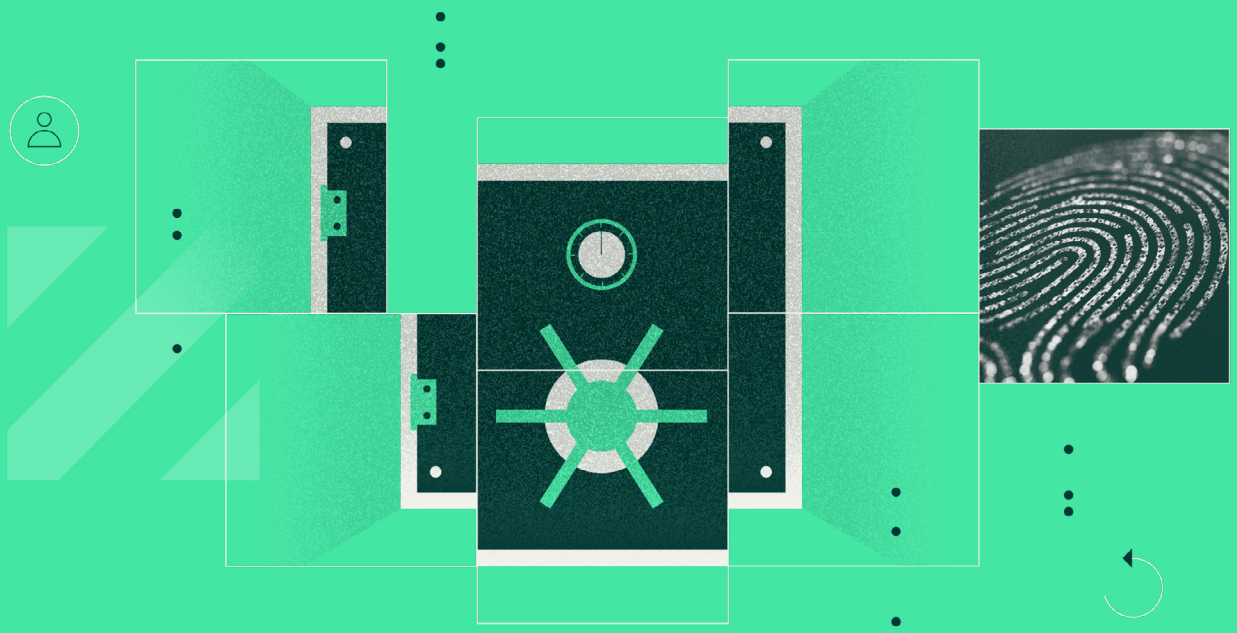
組織全体で同じツールやプロセス、ビューを使用するチームが増えれば増えるほど、優れた決定が下され、大規模に適用されるようになります。



私たちはサイバー攻撃を受けたときの心理的側面や、インシデントを検知した後に発生することの多い大混乱を見落としがちです。ところが、攻撃者は間違いなくそれを理解しており、犯罪者も国家アクターも、攻撃を行った時に感情的な反応を生み出そうと試みています。これは犯罪的な恐喝や、ハッキングや漏洩などの攻撃が増加していることからも明らかです。結局、多くの場合、ITやセキュリティチームのリーダーがこうしたサイバー攻撃の責任を負うことになります。これらの攻撃に対して、最も効果的な方法のひとつは、ある時点で、大変な困難が生じることを受け入れ、将来に「さらなる困難が生じる」ことを回避することです。よって、幅広い分野をカバーする防衛策が必要です。ベストプラクティスや攻撃から学んだこと、シミュレーション、フレームワークを共有して協力しあえば、共同で防衛対策を強化し、攻撃による心理的影響を最小限に抑えることができます。

Chris Krebs氏
CISA元ディレクター、Krebs Stamos Group共同設立者

まとめ



サイバー犯罪との戦いにおける
データ保護

多くの組織は自社のデータやアプリケーション、インフラを保護するために
多大な時間とリソースを費やしていますが、サイバー犯罪は依然として脅威となっています。
ITやセキュリティチームのリーダーには、経営幹部からの注目や擁護、予算、人材という形での
サポートが必要です。

しかし、これらのリソースだけでは十分ではありません。
組織は、サイバー犯罪者との戦いにおいて自社のデータアセットを活用する必要があります。
そうすれば、組織はデータを実用的なものにして、
データの安全性を維持し、より簡単で安全かつ迅速に復元できます。