SNAPSHOT INSIGHT

サイバーセキュリティにおける最初と最後の防御線を築く

The Registerの読者を対象にした調査で見えた現状

situation publishing. | INFINIDAT

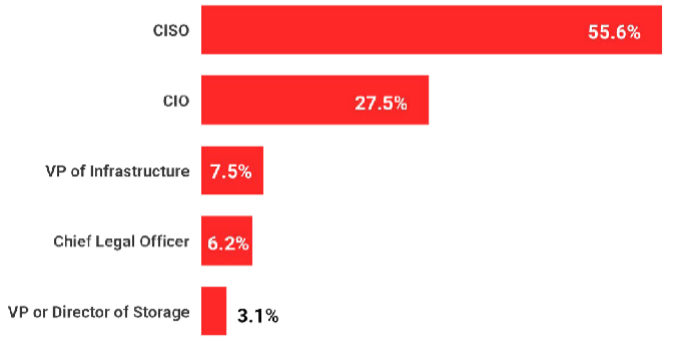
不正アクセス、窃盗、破損からデータやアプリケーションを守るために、多くの組織が最善を尽くしています。

しかし、防御が100%完璧なITインフラストラクチャは存在しません。不運にもサイバーセキュリティインシデントが発生し、企業のシステムが停止してミッションクリティカルなデータが盗まれてしまった場合、多くのケースでは、一刻も早くデータを復元し、システムを復旧することが最後の防御線となります。

私たちは2025年2月、The Registerの読者を対象に調査を実施し、1万人以上の従業員を抱える大規模な組織における防御のプロビジョニング、優先順位付け、実装の現状や、防御の構築にエンタープライズストレージシステムが果たす役割について探りました。調査結果は以下のとおりです。

サイバーセキュリティとその予算確保を積極的に進めている組織には、明確な主導役が存在します。調査対象者の組織の大半（55.6%）では、CISO（最高情報セキュリティ責任者）がその責務を担っています。それがCIO（最高情報責任者）である組織は1/4強（27.5%）、インフラストラクチャ担当VP（バイスプレジデント）とCLO（最高法務責任者）となるとさらに少なくなります（それぞれ7.5%、6.2%）。興味深いことに、ストレージ担当VPやディレクターという声はほとんど聞かれず、調査対象者の組織のわずか3.1%にすぎませんでした。多くの組織では、この特殊なポジションに熱意のある人材が就いていないと考えられます。

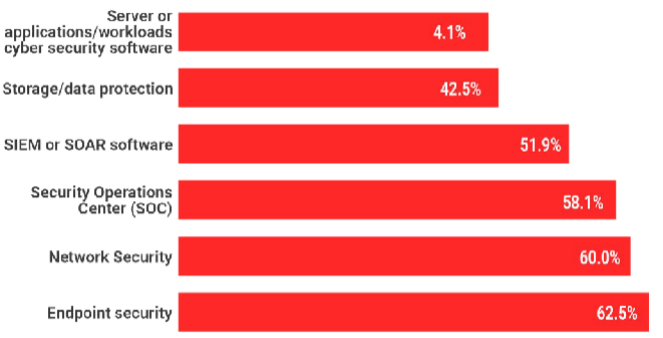
あなたの組織内でサイバーセキュリティとその予算確保を推進しているのは誰ですか？



大企業ではサイバーセキュリティ防御の規模も大きく、ITインフラストラクチャ内の各所で複数のツールやテクノロジーが運用される傾向にあります。今回の調査にもこの傾向が見て取れます。投資対象の主なテクノロジー分野をたずねる設問では、回答は多岐にわたりました。たとえば、デスクトップ、ラップトップ、スマートフォン、タブレットなどのエンドユーザーデバイスをロックダウンするエンドポイントセキュリティは、回答者の62.5%が優先事項としてあげています。ネットワークセキュリティ（60%）やセキュリティオペレーションセンタープラットフォーム（SOC、58.1%）も同様に重要とみなされています。

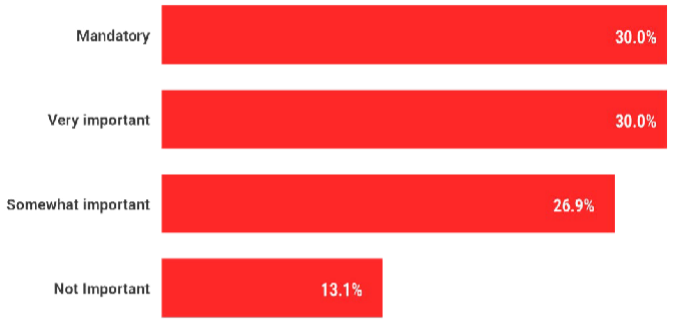
セキュリティ情報およびイベント管理（SIEM）、セキュリティオーケストレーション、自動化、対応（SOAR）サイバーセキュリティソフトウェアは、半数強（51.9%）が主要な投資分野としてあげています。これは、組織がサイバーセキュリティのプロビジョニング、保護、管理の負担を軽減するうえで自動化の重要性が増していることを反映しています。それよりは少し下がるものの、それでも相当数の調査対象者（42.5%）が、ストレージとデータ保護を優先度の高い支出にあげています。サーバやアプリケーション／ワークロードのサイバーセキュリティソフトウェアも同程度の投資先となっています（41.2%）。

あなたの組織のサイバー戦略では、主にどのようなテクノロジー分野に投資していますか？



セキュリティの自動化の価値は、組織における検出とリカバリプロセスの自動化の重要性を測る別の設問の回答と相関関係にあります。約1/3（30%）が必須、同数が非常に重要と回答しています。1/4が自動検出とリカバリプロセスをある程度重要とし、まったく重要でないとみなしているのはわずか13.1%でした。

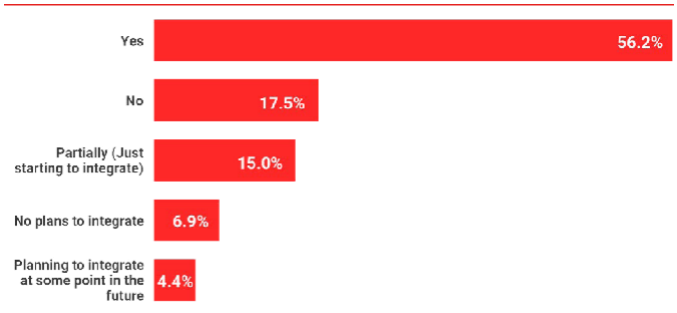
あなたの組織にとって、検出とリカバリプロセスの自動化はどの程度重要ですか？



ストレージアーキテクチャがほかの形式のサイバーセキュリティ防御と統合されている場合、保存されたデータの保護は簡単です。特に、SIEM、SOAR、SOCアプリケーションでは管理と構成を自動化できます。多くの調査対象者（56.2%）が、自分の組織ではストレージソリューションが全体的なサイバーセキュリティ環境に統合されていると回答し、15%が統合に向けた取り組みに着手したところ、4.4%が今後の統合計画を立案中としています。統合していない（17.5%）、または今後統合する計画もない（6.9%）と回答したのはわずか1/4弱でした。

統合により、一般的なログや通知にとどまらず、全体的なサイバーセキュリティ環境や付随するストレージ導入環境にわたりイベントの自動化や調整を行うことができます。予防ツールで生成されるアラートを統合し、エンタープライズストレージデータ保護を強化します。イベントが自動化されることで、データの破損が拡散する可能性が低減されます。最低限でもこのような仕組みを統合し、企業の最も重要なデータアセットを自動的に保護すべきです。

あなたの組織のストレージソリューションは、SOC、SOAR、SIEMアプリケーションなどの全体的なサイバーセキュリティ環境に統合されていますか？

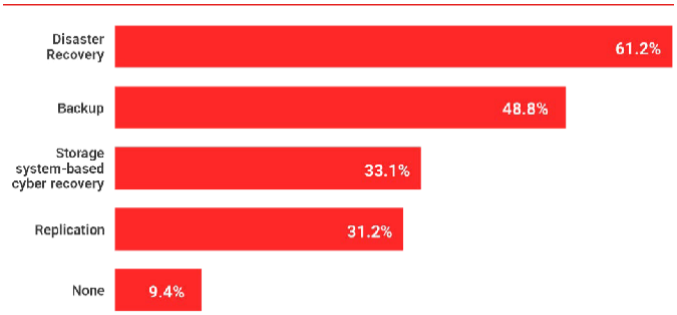


組織のサイバーセキュリティ戦略における最後の防御線は、インシデント後にデータ、アプリケーション、システムの運用を復旧することです。どのような戦略を取るかは、重要なITサービスやアセットを復旧できるタイミングによります。

今回の調査によると、多くの組織（61.2%）が最後の防御線としてディザスタリカバリを活用し、48.8%がバックアップを重視しています。また、現状で1/3がストレージシステムベースのサイバーリカバリソリューション、ほぼ同数（31.2%）がレプリケーションを利用しています。

気がかりなのは、調査対象者の9.4%が自分の組織に最後の防御線はないと回答していることです。複数のオプションを併用することでも関連リスクの軽減は可能なので、今後取り組んでほしいところです。

あなたの組織のサイバー戦略において、最後の防御ラインは何ですか？

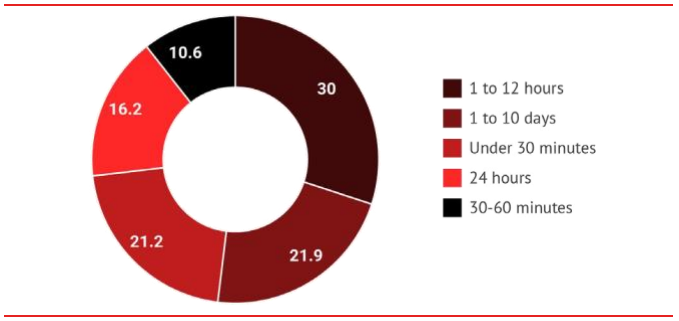


前述したように、これらの要素は、組織がサイバーインシデントからリカバリするまでの時間に直接的な影響を与える可能性があります。サービスレベル契約（SLA）の要件から、状況が深刻になる前にビジネスに生じるダウンタイムの程度を想定できます。

調査対象者の1/3弱（30%）が1～12時間で復旧する必要があると回答し、16.2%が24時間未満でリカバリを完了する必要があるとしています。データを復元する前に、マルウェアやランサムウェアによる破損が生じていないか確認する必要があります。この確認作業を、企業は目標復旧時間（RTO）に間に合うように実施します。

さらに要求度の高いビジネスもあります。21.2%はリカバリのSLAが30分未満、10.6%は1時間未満となっています。

あなたの組織のビジネスでは、リカバリについてどのようなSLAが必要ですか？



あなたの組織では、サイバーリカバリイベントのデータをどのように検証していますか？

サイバーインシデント後に組織が重要なデータ、アプリケーション、システムを迅速に復旧できるかどうかには、復元したデータを検証し、損失や破損がないことを確認する速度も影響します。多くの企業がさまざまなツールやプロセスを使用し、復元したデータの完全性や正確性を検証しています。今回の調査でも、いくつかの方法があげられています。

たとえば、この重要な作業について半数強（50.6%）がアプリケーションの所有者を信頼し、半数弱（47.5%）がストレージやバックアップのベンダーが提供するツールを活用しています。ちょうど40%がセキュリティのスペシャリストやフォレンジックコンサルタントを採用し、37.5%がセキュリティベンダーが提供するツールを使用しています。

重要なデータとアプリケーションを脅威から守ることは、あらゆる組織にとって終わりのない戦いであり、インシデントからの迅速なリカバリを調整、検証することも同様に、有効なサイバーセキュリティ防御における重要な要素です。

幸いにも、このような課題への対処に役立つベンダーソリューションが数多く存在します。Infinidatのエンタープライズサイバーストレージレジリエンスとサイバーストレージリカバリソリューションの詳細については、こちらをクリックしてください。

協賛：Infinidat

INFINIDAT

Infinidatについて

Infinidatは、InfiniVerseに基づく包括的なデータサービスを実現するプラットフォームネイティブのプライマリおよびセカンダリストレージアーキテクチャを企業とサービスプロバイダーに提供します。Infinidatのユニークなプラットフォームは、卓越したIT運用のメリットを提供し、オンプレミス環境やハイブリッドマルチクラウド環境にわたって最新のワークロードをサポートします。Infinidatのサイバーレジリエントバイデザインインフラストラクチャ、従量課金制のパフォーマンス、100%の可用性、サイバーセキュリティを保証するSLAは、企業のITおよびビジネスにおける優先事項に合致しています。受賞歴のあるプラットフォームネイティブのデータサービスや、高い評価を得ているホワイトグローブサービスはお客様から継続的に推奨されています。

詳細は、www.infinidat.com/ja