DNSのROI：
リスク低減と賢明な投資のためのガイド

DNSセキュリティのビジネスケース：コスト、リスク軽減、およびROI

大企業にとって、ドメインネームシステム（DNS）インフラのセキュリティ確保は、ビジネス上の必須要件です。DNSの障害は、長時間のダウンタイム、法的リスク、および評判の低下を招く可能性があります。しかし、広範なサイバーセキュリティ戦略において、ドメインセキュリティは見過ごされがちです。

本洞察レポートでは、障害によるコストや、リスクおよびROIを効果的に伝える実践的な方法を概説することで、意思決定者がDNSセキュリティに関する説得力のあるビジネスケースを構築できるよう支援します。

DNSセキュリティの失敗がもたらす真のコスト

DNSセキュリティの障害は、当初のダウンタイムをはるかに超える連鎖的な影響を引き起こす可能性があります。ダウンタイム中の減収が最も顕在的なコストである一方、コンプライアンス上の懸念、法的費用、ブランド価値の低下といった間接的な影響は、定量化が困難なものの、長期的にはより大きな代償となる可能性があります。

サイバーセキュリティのリーダーたちは、ドメインを標的とした脅威を、孤立した技術的問題ではなく、重大なビジネスリスクとして捉えるようになってきています。「CISO Outlook 2025」によると、回答者の70%がセキュリティ脅威の増加を予想しており、98%が今後3年間で増加すると予測しています。[1] 脅威の状況が深刻化する中、組織は稼働時間の確保、顧客の信頼、および事業継続を支える基盤となる対策に優先的に取り組む必要があります。

> *DNS障害からの復旧のために、チームが昼夜を問わず対応していたにもかかわらず、後になって「なぜもっと強固な対策を講じていなかったのか」と問われる場面を私は目にしてきました。だからこそ、DNSセキュリティを事後の対応ではなく、計画的な投資として捉えることが重要なのです。*
>
> **マーク・フレッグ（Mark Flegg）**
> *CSCセキュリティ製品およびサービス担当シニアディレクター*

直接コストと間接コスト：拡大する波及効果

直接コストとは、重要なサービスが停止した際に発生する即座に把握可能な費用であり、具体的には次のようなものがあります。

ダウンタイムによる損失：業務の混乱、取引の失敗、顧客の離脱

緊急のITサポートおよびインシデント対応：社内のITチームや外部の専門家によるサービスの診断と復旧への取り組み

返金およびサービスレベル契約（SLA）違反による違約金：SLA違反により顧客やパートナーに支払うべき補償金

拡大し続ける隠れたコストの波

しかし、Splunkのレポートが明らかにしているように、直接コストは経済的影響の「第一波」に過ぎません。[2] その波及効果が広がっていくにつれ、水面下に潜む間接コストが蓄積され始め、最終的には当初の費用を上回る可能性さえあります。

規制当局による罰金および法的和解：規制産業で事業を展開する企業は、サービスの中断やデータ漏洩により、コンプライアンス違反や訴訟に直面する可能性があります。

評判およびブランドイメージの毀損：顧客の信頼を失うことは、市場での地位、顧客維持、および収益の成長に長期的な影響を及ぼす可能性があります。また、組織はステークホルダーを安心させ、投資家からの懸念に対応し、インシデント対応の取り組みについて透明性を確保する必要がある場合もあります。

ランサムウェアや脅迫の要求：攻撃者がDNS設定を操作してトラフィックをリダイレクトしたり、アクセスをブロックしたりすると、企業は金銭的な脅迫の試みに直面する可能性があります。

サイバー保険料の値上げとセキュリティ投資の増加：DNSの障害、特にセキュリティ侵害を伴うものは、保険会社がリスク・エクスポージャーを評価するため、保険料の値上げにつながる可能性があります。

「ファイブナイン」の稼働率を目指し、よりスマートな質問を投入

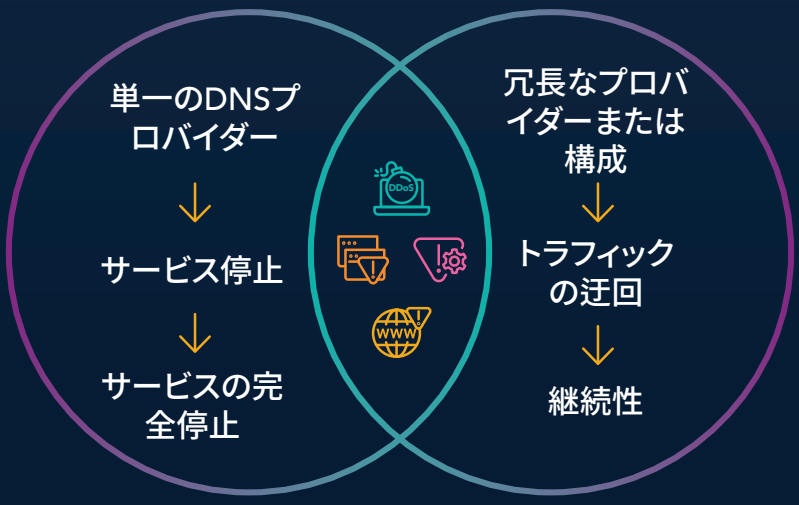
企業の稼働率に対する期待値は高まっています。「ファイブナイン」の原則、すなわち99.999%の稼働率は、年間5分未満のダウンタイムに相当します。多くの組織がこれを信頼性のベンチマークとして扱っていますが、DNSサービスの保証内容はプロバイダーやサービス階層によって異なります。実際には、プロバイダーの実稼働実績、特に負荷がかかったり攻撃を受けたりした際の対応力こそが、理論上の稼働率目標よりも確かな指標となります。

現在、多くの企業が、顧客向けサービス、社内アプリケーション、および業務上不可欠なワークフローを支えるために、クラウドベースのインフラストラクチャやサードパーティのプラットフォームに依存しています。こうしたプロバイダーは拡張性とパフォーマンスを向上させることができる一方で、特に可用性が単一のプロバイダー、地域、または構成に依存している場合には、運用にリスクをもたらす可能性もあります。DNSの耐障害性計画には、障害、設定ミス、または上位ネットワークの品質低下が発生した場合でも、可用性を維持できるような冗長化戦略を組み込むべきです。

> *企業は、複数の地域、バックアップ、フェイルオーバーシステムなど、あらゆる場面で障害に備えています。しかし、DNSに関しては、単一のプロバイダーや構成で「これで十分」とみなされることが依然として多すぎます。あらゆるデジタルサービスが依存しているものについて、そのように決めつけてしまうのは危険です。*
>
> **マーク・フレッグ（Mark Flegg）**
> *CSCセキュリティ製品およびサービス担当シニアディレクター*

単一障害点となるDNSのリスクと耐障害性の高いDNSアーキテクチャ

これらのリスクを総合すると、DNSセキュリティが単なるIT上の付随的な課題ではなく、企業のリスク低減における中核的な要素として扱われるべき理由が明らかになります。さらに、「CISO Outlook 2025」の調査によると、最高情報セキュリティ責任者（CISO）は、今後3年間で予想される脅威の上位に、ドメインおよびDNSハイジャックを挙げています。[3]



DNSは、ウェブサイト、電子メール、社内アプリケーションの利用を可能にする上で極めて重要な役割を果たしていますが、その保護対策が不十分なケースが少なくありません。そのリスクは甚大であり、以下のようなものが挙げられます。

分散型サービス拒否（DDoS）攻撃：攻撃者は、DNSインフラを標的とした大規模な攻撃を行い、サーバーを機能不全に陥らせ、サービス停止を引き起こします。

プロバイダーのサービス停止：単一のDNSプロバイダーに依存している企業は、そのプロバイダーでダウンタイムが発生した場合、システム全体が機能しなくなるリスクを負っています。

構成エラー：DNSレコードの不適切な変更といった単純な構成ミスが、サービス全体に支障をきたす可能性があります。

ドメイン乗っ取り：レジストラレベルでの不正な変更によりトラフィックがリダイレクトされ、評判やセキュリティ上のリスクにつながる可能性があります。

DNS障害によるコストの定量化

DNSセキュリティリスクの財務的影響を評価し、伝達しようとする企業にとって、年換算予想損失額（ALE）の計算式は、潜在的な損失を定量化する体系的なアプローチを提供します。この手法は、サイバーセキュリティの責任者が技術的なリスクをビジネス視点の財務用語に変換するのに役立ち、DNSセキュリティへの予防的な投資を正当化することを容易にします。

ALEの計算式は次のように定義されます。

SLE × ARO = ALE

単一損失期待値（SLE）：単一のDNS障害による財務的影響。これには直接的なコスト（および、可能であれば間接的なコスト）が含まれます。

年間発生率（ARO）：1年間にそのようなインシデントが発生すると予想される回数の推定値。

年間予想損失額（ALE）：DNSセキュリティの不備による年間予想損失額。

組織のリスク状況を基にSLE（損失額の上限）とARO（許容リスク額）を算出することで、企業はALE（年間予想損失額）を算出できます。これは、潜在的な財務的リスクを具体的に測定し、DNSセキュリティへの予防的投資を正当化するための有効な手段となります。

> *多くの組織が、DNS関連の脅威によるコストを定量化することに苦慮しており、その結果、セキュリティへの投資を正当化することが難しくなっています。ALEの計算式は、財務リスクを評価するための実用的なモデルを提供し、意思決定者が予防的なDNSセキュリティによってビジネスに及ぼされる影響を把握するのに役立ちます。*
>
> **マーク・エグルストン（Mark Eggleston）**
> *CISO、CSC*

DNSセキュリティのビジネス価値の伝達

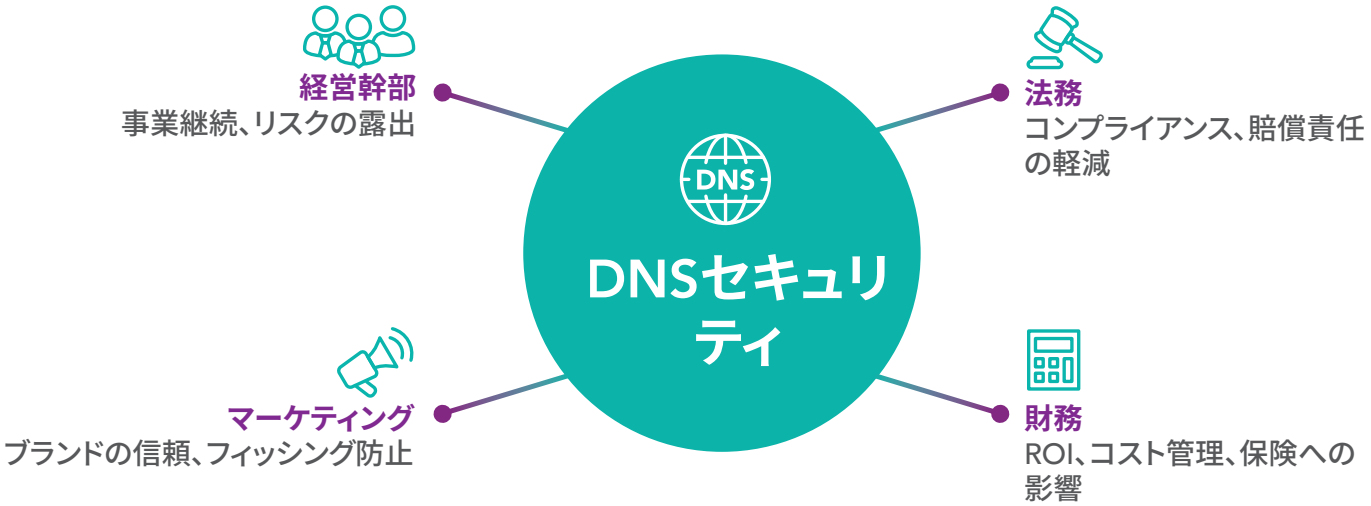
ドメインを悪用した脅威に対する認識が高まっているにもかかわらず、多くの組織は依然として対策が不十分だと感じています。「CISO Outlook 2025」によると、「ドメインベースの脅威に対抗するための適切なツールを導入している。」と回答した回答者はわずか22%でした。[4] リスクと対応態勢の間に生じているこのギャップこそが、ROIを重視したDNS対策の有効性を最も強く示しています。

資金調達を確保するためには、サイバーセキュリティの責任者は、ドメインのセキュリティを稼働時間、顧客の信頼、コンプライアンス上のリスク、および運用の回復力と結びつけることで、DNSのリスクをビジネスへの影響として具体化しなければなりません。

> *DNSは今日の脅威環境を想定して設計されたものではありませんが、顧客、従業員、パートナーを適切に誘導するために、依然として私たちが依存しているシステムです。だからこそ、DNSセキュリティは他の主要な管理対策と同等の注意を払う価値があるのです。*
>
> **マーク・フレッグ（Mark Flegg）**
> *CSCセキュリティ製品およびサービス担当シニアディレクター*

対象者層の把握：メッセージの最適化

DNSセキュリティへの投資を確保するためには、サイバーセキュリティの責任者は、さまざまなステークホルダーの優先事項に合わせてメッセージを調整する必要があります。セキュリティチームが技術的なリスクに注力する一方で、他の部門はそれぞれのビジネス目標、財務上の懸念、あるいは運用上の課題が存在します。各チームの利益と関連付けてDNSセキュリティの重要性を提示することで、チームの支持を得られる可能性が高まります。



経営幹部：DNSセキュリティのビジネスへの影響

経営幹部層は、財務実績、リスク管理、および競争上の優位性に重点を置いています。DNSはシステムの稼働維持に不可欠であるため、経営幹部の最優先課題である事業継続と災害復旧においても中核的な役割を果たします。DNSを単なるIT経費ではなく戦略的投資として位置づけることで、組織全体のレジリエンス（回復力）との関連性を明確にすることができます。

> *取締役はDNSそのものには関心がなく、ブランド保護やサイバーセキュリティ上のリスクを重視しています。技術的な詳細を避け、あくまでビジネスの視点から議論を構成しましょう。参考まで、『ウォール・ストリート・ジャーナル』などのメディアでサイバーセキュリティがどのように取り上げられているか、ぜひお読みください。*
>
> **マーク・エグルストン（Mark Eggleston）**
> *CISO、CSC*

法務部門：規制遵守と法的リスクの低減

企業の法務部門は、業界規制の遵守と法的リスクの低減を最優先事項としています。EU一般データ保護規則（GDPR）、カリフォルニア州消費者プライバシー法（CCPA）、NIS2指令など、多くのデータプライバシーおよびセキュリティの枠組みにおいて、機密情報を保護するための強力なセキュリティ対策が求められています。適切なDNSセキュリティ対策が講じられていない場合、企業はデータ漏洩、フィッシング攻撃、不正なドメイン移転などのリスクにさらされ、これらはすべて法的措置や罰則につながる可能性があります。

マーケティングおよびブランド担当チーム：評判の保護とフィッシング対策

マーケティングチームは、ブランドの評判、顧客の信頼、デジタルエンゲージメントを担っていますが、これらはすべてDNS関連の脅威によって損なわれる可能性があります。DNSセキュリティを単なるIT上の問題ではなく、ブランド保護戦略として位置づけることで、経営陣にとってより切実な、自分事としての課題へと変わります。

> *ドメインセキュリティは、従来のサイバーセキュリティ上の常識を超え、不正なサイトの脅威からデジタルエコシステム全体を保護することを意味します。CISO（最高情報セキュリティ責任者）はこれを二次的なリスクと見なすかもしれませんが、マーケティングやブランディングにとっては最優先事項です。*
>
> **マーク・エグルストン（Mark Eggleston）**
> *CISO、CSC*

財務および調達部門：費用対効果、ROI、および保険上のメリット

財務の意思決定者や調達チームは、コスト、効率性、そして測定可能なROIに基づいて投資を評価します。ドメインセキュリティリスクが財務に与える影響を実証する効果的な方法の一つは、大きく取り上げられたニュースから実例を引き出すことです。時には、最近起きたインシデント事例を共有するというシンプルな行動だけでも、投資不足が招く、目に見える代償を財務チームに認識させることが可能になります。適切に保護されたDNSは、事業中断の発生率を低減し、財務の安定性を支える役割も果たします。

DNSセキュリティを単なる技術的な防護策ではなく、ビジネスを推進する要素として位置づけることで、組織全体からの幅広い支持を得て、DNS保護策が戦略的な優先事項として扱われるようにします。

ROIの証明：予防的なDNSセキュリティのビジネスケースの構築

DNSセキュリティへの投資を確保するには、単にリスクを強調するだけでは不十分であり、測定可能な財務的および業務上のメリットを実証する必要があります。CISOやサイバーセキュリティの責任者は、セキュリティ上の懸念を明確なビジネス価値へと転換し、DNSセキュリティへの投資がどのようにコスト削減、業務の効率化、および財務リスクの最小化につながるかを示さなければなりません。

セキュリティ予算がサイバーリスクと同じペースで増加するとは限りません。「CISO Outlook 2025」によると、2024年から2025年にかけて予算が大幅に増加したと回答したのは回答者のわずか7%であったのに対し、80%が「適度な増加」と回答しています。[5]

このような状況下では、DNSへの投資は、リスクの測定可能な低減と運用におけるレジリエンスを実証する必要があります。

リスク軽減と効率化によるコスト削減

強固なDNSセキュリティ体制は、サイバーリスクの低減を広く支えるものであり、これにより組織はサイバー保険会社との良好な関係を維持し、広く受け入れられているセキュリティフレームワークに準拠することが可能になります。サイバー保険契約では通常、DNSに特化した割引は提供されませんが、ドメイン保護を強化することは、適切なサイバーセキュリティ対策を実践していることを示し、脅威を軽減することにつながります。

また、組織は、特に迅速な対応が求められる場面において、再現性および拡張性のある手法を優先しています。「CISO Outlook 2025」の調査では、回答者の半数がインシデント対応計画の策定と定期的なテストを実施しており、同数がAIベースの監視・強制ソリューションを利用していると報告しています。[6] DNSセキュリティは、可視性を向上させ、緩和措置を迅速化し、障害発生時の事業継続性の強化を通じて、運用の成熟化へと向かう潮流に合致するものです。

自動化は、DNSの構成の管理から新たな脅威の監視、インシデントへの対応に至るまで、ドメインセキュリティ運用の手作業による負担を軽減する上で重要な役割を果たしています。また、デジタル証明書の管理においても、自動化の重要性はますます高まっています。2029年までのCA/Browser Forumの変更に伴い証明書のライフサイクルが短縮されるため、組織はSSL（Secure Sockets Layer）およびTLS（Transport Layer Security）証明書の更新頻度を大幅に増やす必要が生じる可能性があります（将来的には年間平均8回の更新）。そのため、有効期限切れやサービス中断を防ぐためには、自動化された更新ワークフローが不可欠となります。

財務モデルを用いたDNSリスクの定量化

経営陣や財務チームは、データに基づく意思決定を行うことで、最大の成果を上げることができます。DNS関連の攻撃、ダウンタイム、またはDNSハイジャックによる潜在的な金銭的損失を推定するために、年間予想損失額（ALE）方程式や情報リスクの要因分析（FAIR™）フレームワークといったサイバーリスク定量化（CRQ）モデルが活用されます。これらのモデルを適用することで、サイバーセキュリティの責任者は、予防的な投資によってはるかに大きな財務的損失を防ぐことができるという具体的な数値を提示できるようになります。

シナリオベースのリスク評価を実施することも、DNS障害によって引き起こされる潜在的な事業中断や財務的影響を明らかにするもう一つの方法です。現実の攻撃シナリオをモデル化することで、組織はDNSセキュリティ対策の不備がもたらす「隠れたコスト」を可視化することができます。

脅威インテリジェンスとリスクの優先順位付けの強化

進化し続ける脅威に先手を打つには、潜在的なリスクを継続的に把握しておく必要があります。全米ISAC協議会（National Council of Information Sharing and Analysis Centers）などの業界別情報共有グループに参加している組織は、新たなDNS関連の攻撃に関する早期警告や洞察を得ることができます。

さらに、継続的な脅威エクスポージャー管理を導入することで、セキュリティチームは最も緊急性の高いDNSの脆弱性に優先的に対処できるようになり、高リスクなシナリオが深刻化する前に、リソースを効率的に割り当てて、リスクの最小化を図ることが可能になります。

当社のDNSコスト計算ツールによるコスト削減効果の測定

DNSセキュリティの経済的メリットを理解するには、明確なコストモデルが必要です。以下のDNS内部コスト計算ツールは、取引の損失、修復コスト、業務の混乱などの変数を考慮に入れ、企業がDNSのダウンタイムによる真のコストを見積もるのに役立つ計算式を提供します。

"DNSセキュリティの価値を見積もるのに、複雑なモデルは必要ありません。DNSのダウンタイムを、生産性の低下、取引の損失、復旧時間といった実際のビジネスへの影響と関連づければ、ROIの正当化ははるかに容易になります。

マーク・フレッグ（Mark Flegg）
CSCセキュリティ製品およびサービス担当シニアディレクター

DNSコスト削減計算ツール	指標
DNSを管理するスタッフ数	2
スタッフ1人あたりの年間給与	$75,000
利益コスト：人件費の約30%	$45,000
年間ハードウェア、ソフトウェア、および帯域幅コスト	$40,000
内部DNSを実行するための総コスト	**$160,000**
外部DNSサービスの想定コスト	$50,000
外部DNSサービスの利用による総節約額	**$110,000**

注：数値は一例です。

サイバーセキュリティの責任者は、定量化可能なコストの削減、業務効率の向上、および財務リスクの低減を実証することで、経営幹部、財務部門、リスク管理担当者の優先事項に直結するDNSセキュリティへの投資を正当化する説得力あるビジネスケースを構築することができます。

ビジネスにおけるDNSセキュリティの優先化

DNSセキュリティは、組織のサイバーセキュリティ戦略において極めて重要でありながら、最も見落とされやすい要素の一つです。本レポートが示すように、DNSセキュリティの不備が招く代償は、ダウンタイムにとどまらず、財務的損失、規制当局からの罰金、そして企業評価の失墜という多岐にわたります。

技術的な対策の実施に加え、CISOやセキュリティ責任者は、DNSセキュリティの重要性を「経営の言語」で伝える必要があります。メッセージを経営陣の優先事項と整合させ、リスクを定量化し、ROIを実証することで、組織はデジタル資産を保護するために必要な投資を確保することができます。

今、DNSセキュリティを強化するための積極的な措置を講じることで、将来的に発生し得る高額なインシデントを未然に防ぐことができます。**貴組織を守るための最適な個別ソリューションについて、今すぐCSCにご相談ください。**

cscdbs.com

経営陣からサイバーセキュリティへの賛同を得るための3つのステップ：

1. 関係構築：経営陣の優先事項を理解し、着実かつ戦略的なアプローチを取る。
2. 経営陣の視点に立つ：サイバーセキュリティをガバナンス上の課題として位置付ける。全米取締役協会（NACD）のガイドラインなどを活用する。
3. 進捗を示す：ダッシュボードやその他の分かりやすい視覚資料を活用し、セキュリティ投資の効果を提示する。

マーク・エグルストン（Mark Eggleston）
CISO、CSC

お気軽にお問合せください　1 800 927 9800 | cscdbs.com

CSCについて

CSC　は、セキュリティ脅威の分野で信頼されているインテリジェンスプロバイダーです。ドメインのセキュリティと管理、デジタルブランド保護、フラウド対策を重点領域とし、Forbes 誌の「グローバル 2000」や Interbrand® (インターブランド) が発表する「世界で最も価値の高いブランド100社」に名を連ねる企業に選ばれています。グローバル企業がセキュリティ体制に多額の投資をする中、当社のDomainSec℠プラットフォームはサイバーセキュリティの見落としを把握し、オンラインのデジタル資産やブランドを守るのに役立っています。CSCが独自に開発したテクノロジーにより、企業はセキュリティ体制を強化して、オンライン資産やブランドの評判を狙うサイバー脅威ベクトルを防ぎ、収益の壊滅的な損失を回避することができます。CSCはまた、オンラインブランドのモニタリングとエンフォースメントアクティビティを組み合わせたオンラインブランドプロテクションを提供し、特定のドメインを標的とするファイアウォール外のさまざまな脅威を多角的に把握します。さらに、攻撃の初期段階でフィッシングに対処する不正防止サービスも提供しています。CSCは、1899年以来、米国デラウェア州ウィルミントンに本社を置き、米国、カナダ、ヨーロッパ、およびアジア太平洋地域にオフィスを構えています。CSCは、クライアントのロケーションに関わらずビジネス展開ができるグローバル企業であり、当社がサービスを提供する各ビジネスで専門家を採用することにより、これを実現しています。cscdbs.comをご覧ください。

[1]*CSC, The CISO Outlook 2025, 2025, https://www.cscdbs.com/en/resources/2025-ciso-cybersecurity-outlook-report/.*

[2]*Splunk, The Hidden Costs of Downtime, 2024, https://www.splunk.com/en_us/form/the-hidden-costs-of-downtime.html.*

[3]*CSC, The CISO Outlook 2025.*

[4]*CSC, The CISO Outlook 2025.*

[5]*CSC, The CISO Outlook 2025.*

[6]*CSC, The CISO Outlook 2025.*

DBS03112026