RSA® ARCHER® IT & SECURITY RISK MANAGEMENT

ソリューション概要

はじめに

組織は、ファイアウォール、ウイルス対策、侵入防止システム、侵入検知システム、脆弱性スキャナー、セキュリティ ポリシー、ID管理、物理的なアクセス制御などの防御策を何層にも重ねて講じることで、増大するセキュリティ課題と格闘しています。こうした防御レイヤーは、基本的な防御策を提供し、今日の脅威から保護するために不可欠である一方、それぞれがセキュリティ インフラストラクチャをより複雑なものにしています。このように複雑さが増大することで、セキュリティ リスクの発生場所や脅威が現実化するスピードを明確に一致させることが難しくなっています。

セキュリティ部門はこうした防御レイヤーによって作成されるセキュリティ関連データの増加という課題も抱えています。既に膨大な量のビジネス データを保護する必要があるにもかかわらず、さらにデータが追加されています。ビジネスにとって最も重要なデータは何かということを的確に理解していない場合、ITチームおよびセキュリティ チームは、最も関連性の高いセキュリティ イベントを判断するのに苦慮することになります。

セキュリティは、今日のテクノロジー シフト（特に、クラウド プロバイダーや外部プロバイダーへのビジネス要素の移行）の影響を受ける傾向が強くなっています。企業がより多くのビジネス クリティカルなプロセスやITサービスを社外に移行するにつれてセキュリティ制御の（全てではないにしても）大部分を外部の関係者に依存することになります。こうした第3のプラットフォームへの移行によって、セキュリティ要件およびコンプライアンス要件の両方の課題が増大します。

今日の脅威やインシデントは絶えず変化しており、経営陣は、増大するサイバー リスクに対して組織がどのように対処するかということに強い関心を持っています。経営陣はセキュリティ リスク、つまり風評被害、財務的な影響と規制違反、侵害その他のセキュリティ イベントの調査と解決にかかる純コストについて、これまで以上に懸念しています。

ITおよびセキュリティに見識をもたらす

ITリスク部門およびセキュリティ部門がテクノロジー関連リスクの全体像をまとめ上げて描写するには、複数の運用グループが協力し、作業を調整する必要があります。セキュリティ ポリシーは、規制やビジネス要件に沿って調整する必要があります。脅威および脆弱性の管理プロセスは、増大する脅威に後れを取らないように俊敏性が必要です。セキュリティ オペレーションは、組織に対する能動攻撃を迅速に特定し、リスクにさらされる資産を保護できるよう、アクティブで入念なものでなければなりません。セキュリティ戦略は即時的で戦術的であるだけでなく、革新的でコスト パフォーマンスに優れたソリューションをもたらす必要があります。最後に、セキュリティ コンプライアンスは、適切な制御が設計され、効果的に運用されるようにする必要があります。

RSA Archer IT & Security Risk Management のメリット

RSA® Archer® IT & Security Risk Managementを利用すると、セキュリティ部門は強化された可視性、解析、アクション、メトリックのメリットを享受できます。

GRC のコンテキストでのサイバーセキュリティ リスクの結び付け

ビジネス プロセスが相互につながっている今日での組織は、急速に変化するサイバーセキュリティ リスクの複雑性や連鎖する影響に効果的に対応できる必要があります。RSA Archerなら、セキュリティ プロセスとデータを企業全体のリスク/コンプライアンス業務に結び付けることができます。そして、IT部門およびセキュリティ リスク部門は、ビジネス上の重要性の観点からビジネス リスクとITリスクとの間の関係性を考慮して、管理責任と説明責任を確立したり、ITおよびセキュリティ リスクをより広範なガバナンス/リスク/コンプライアンス プログラムに結び付けることができます。

IT およびセキュリティ リスク管理に多様な側面から対応

ITおよびセキュリティリスクを効果的に管理するには、ITセキュリティリスクを全面的に管理できるような方法でセキュリティプログラムを構成する必要があります。ITおよびセキュリティリスクプログラムは、ポリシー、基準、コンプライアンスから脅威、脆弱性、攻撃に至るまで、多様な側面からリスク管理に対応する必要があります。RSA Archerを利用すると、ITチームおよびセキュリティ チームは、プロセスを一元管理し、サイバー脅威を優先順位付けし、最新の脅威を的確に把握することができます。

ビジネス コンテキストとプロセス イネーブルメントとの橋渡しを行う

今日のITおよびセキュリティ リスクの管理には、単なるデータ速度やデータ フィードよりはるかに多くのものが伴います。テクノロジーの問題によって組織全体が深刻なリスクにさらされる可能性があるため、ITリスクはビジネスの観点から把握する必要があります。ビジネスとITを確実に調整することで、ITおよびセキュリティ リスク管理プログラムは、安全なビジネスを維持するために対応する必要があることを円滑に実行できます。RSA Archer IT & Security Risk Managementは、リスクを効果的かつ効率的に特定およびエスカレーションするプロセスを確立することで、人とテクノロジーの間のギャップを解消します。

RSA Archer IT & Security Risk Management

新しい技術を利用したIT セキュリティに対する脅威は、現在の複雑なビジネスにおいて広がりを見せています。RSA Archer IT & Security Risk Managementを利用すると、ビジネスで重要な資産の判別、セキュリティ ポリシーと標準の確立と伝達、攻撃の検知と対処、セキュリティの不具合の特定と修正、ITリスク管理に関する明確なベスト プラクティスの確定ができます。

RSA Archer IT & Security Risk Managementは、リスク管理の成熟化に関するお客様固有のビジネス ニーズを満たす多様なユース ケースを提供します。

Issues Management

RSA Archer Issues Managementは、セキュリティ/リスク/コンプライアンス関連のあらゆるユース ケースに適用され、セキュリティ インシデント、内部統制の不足や欠如、注意またはエスカレーションが必要な例外から生じた問題を捕捉して統合します。問題管理を利用すると、組織は、内部監査および外部監査による発見事項、規制による検証で明らかになった問題、自ら特定した管理上の問題についてカタログ化したり、問題解決のための説明責任を確立したり、コミットメントや期日に照らして修正計画を追跡したりすることができます。優れたレポート作成によって、すべてのレベルの経営陣および取締役会は、未解決の問題、優先順位、修正スケジュールの全容を簡単に把握できます。

IT & Security Policy Program Management

RSA Archer IT & Security Policy Program Managementを利用すると、外部の規制義務をドキュメント化できます。また、その規制義務への変更を追跡するための体系的なレビュー/承認プロセスを確立して、ビジネスへの影響を把握し、対応の優先順位を設定することができます。

IT Controls Assurance

RSA Archer IT Controls Assuranceにより、すべてのIT資産にわたる統制のパフォーマンスについての評価およびレポート作成や、統制評価や監視の自動化が実現されます。一元化されたシステムが導入されるので、コンプライアンス レポートを作成するためにIT資産をカタログ化し、IT統制をドキュメント化するためのレコード体系を確立できます。IT統制をテストする効率化されたプロセスやワークフローを利用することで、手動統制に関する標準化された評価プロセスを導入したり、自動化されたシステムからのテスト結果を統合したりできます。コンプライアンス評価中に特定された問題が一元管理されるため、コンプライアンス ギャップの追跡やレポート作成ができます。ギャップの修正作業をドキュメント化および監視できるため、コンプライアンスの不一致にタイムリーな方法で対処できるようになります。

IT Security Vulnerabilities Program

RSA Archer IT Security Vulnerabilities Programは、セキュリティ チームが高リスクな脅威を特定し優先順位を付けられるようにするビッグデータ アプローチを採用しています。資産のビジネス コンテキスト、アクショナブルな脅威 インテリジェンス、脆弱性評価の結果、包括的なワークフローを組み合わせることにより、ITセキュリティ リスクをプロアクティブに管理することができます。IT資産は完全なビジネス コンテキスト オーバーレイを使用してカタログ化できるため、スキャンや評価のアクティビティをより適正に優先順位づけできます。こうした統合型の脆弱性調査プラットフォームによって、ITセキュリティ アナリストは、アラートを導入し、脆弱

性スキャン結果を深堀りし、問題が発生と同時に解析することができます。パワフルで柔軟なルール エンジンが新しい脅威、期限切れの問題、変化するビジネスのニーズをハイライト表示します。既知の脆弱性リスクと適用されたビジネス コンテキストとを関連づけるこの機能は、対応や修正作業を優先順位付けするのに役立つものであり、重大なギャップを埋めるスピードを高め、コストを削減できます。

IT Risk Management

RSA Archer IT Risk Managementを使用すると、ITリスク管理の目的で組織構成要素とIT資産をカタログ化できます。このユース ケースには、ITリスクをカタログ化するためのリスク登録、ITの事前構成済みリスク評価、事前構成済み脅威評価の方法論、IT統制をドキュメント化するためのカタログが含まれます。RSA Archer Issues Managementもまた、リスク評価で挙がったギャップや発見事項を管理するために使用されます。

ITリスクを明確に可視化できれば、評価プロセスの効率化、ITリスクの特定の迅速化、タイムリーなレポート作成の確実化が可能になります。リスクと内部統制とを結び付けることで、IT統制要件の伝達と関連づけが容易になり、コンプライアンス ギャップの削減や、リスク軽減戦略の改善ができます。こうした俊敏なリスク管理フレームワークを利用することで、企業内の要件の変化に遅れずに対応したり、最も影響の大きいITリスクにリソースを集中させることができます。

PCI Management

RSA Archer PCI Management を利用すると、PCI（クレジット カード業界）コンプライアンス プロセスの効率化、評価の自動化、規制の準拠に必要な作業の軽減を実現できます。組織化されたプロジェクト管理アプローチによって、PCI コンプライアンス プログラムを即座に開始できます。また、継続的な評価の効率的な実施、構造化されたレポートの作成、リスクの管理と軽減に必要な可視化の実現もできます。PCI Management は他の RSA Archer GRC ソリューションと完全に統合されているため、お客様は、効率的で持続可能な PCI コンプライアンス プログラムを導入でき、また結果を収集してより広範なエンタープライズ リスクとコンプライアンスのパフォーマンス メトリックに関する情報を提供することが容易にできます。

Security Incident Management

RSA Archer Security Incident Managementを利用すると、膨大な量のセキュリティ アラートに対応したり、セキュリティ インシデントをエスカレーション、調査、解決するプロセスの管理を導入することができます。一元化されたシステムを活用してIT資産のカタログと完全なビジネス コンテキスト オーバーレイとを組み合わせることで、優先順位付けされたセキュリティ アクティビティを促進することができます。目的に合わせたワークフロー、アラート、レポート作成はセキュリティ インシデントへの対応プロセスを効率化するのに役立ち、チームは確信を持って行動することができます。

定義済みの手順を使用してインシデント調査を追跡および管理し、適切な処理と修正ができるようになります。ワークフローが明確に定義されているため、セキュリティ アナリストはより効果的に時間を活用し、セキュリティ インシデントのクローズをより迅速化できます。こうした統合プロセスは、SIEM/ログ/パケット収集インフラストラクチャに関する投資収益率の拡大にも役立ちます。また、セキュリティ チームは最も影響の大きいインシデントに重点的に取り組み、組織全体のセキュリティ暴露リスクを効果的に管理および軽減できます。

Security Operations & Breach Management

RSA Archer Security Operations & Breach Managementを利用すると、システムを一元化し、インシデントの優先順位設定のためにIT資産をカタログ化できます。このカタログ内の完全なビジネス コンテキスト オーバーレイによって、セキュリティ イベントの優先順位を設定することができます。セキュリティ インシデントに関するワークフロー主導型のレポート作成を利用することで、セキュリティ マネージャーは最も差し迫った問題を的確に把握することができます。インシデントの処理手順に関するベスト プラクティス コンテンツは、セキュリティ アナリストがアラートに効果的かつ効率的に対応するのに役立ちます。さらに、侵害が発生した場合は、目的に合わせたワークフローが追跡調査や修正アクティビティを管理するのに役立ちます。セキュリティ オペレーション マネージャーは、主要パフォーマンス指標の監視、制御の有効性の測定、SOC（セキュリティ オペレーション センター）チーム全体の管理を効果的に行うことができます。

セキュリティ イベントやインシデントに対処するインシデント対応プロセスは、セキュリティ オペレーションを管理するより広範で成熟したアプローチに統合されています。明確に定義されたワークフローを利用することで、SOCマネージャーはアナリストの時間とリソースをより適正に割り当て、セキュリティ インシデントのクローズを迅速化できます。こうした統合プロセスは、SIEM/ログ/パケット収集インフラストラクチャに関する投資収益率の拡大にも役立ち、またセキュリティ チームは、侵害などのインシデントに迅速に対応して、セキュリティ リスク全体を効果的に管理および軽減することができます。

IT Regulatory Management

RSA Archer IT Regulatory Managementは、ITおよび機密データ環境に影響を与える外部の規制義務をドキュメント化するのに必要なツールと機能を提供します。これにより俊敏なポリシー フレームワークの基盤が形成され、組織はビジネスおよびITのコンプライアンス リスクの変化に遅れずに対応することができます。規制義務の変更を追跡するための体系的なレビュー/承認プロセスを確立し、ビジネスへの影響を把握し、対応の優先順位を設定することができます。そして、企業が遵守する必要がある規制その他のコンプライアンス

RSA

要件について、正確な指針を経営幹部やIT組織に迅速に提供することができます。ITのコンプライアンス要件と内部統制とのつながりを改善することで、ギャップが低減され、経営幹部は、ビジネスに影響を与えるIT関連の問題に対するより正確なインサイトが得られます。

Information Security Management System

RSA Archer Information Security Management Systemを利用すると、情報セキュリティ管理システムを迅速に徹底調査し、レポート作成や認定のための適合性明細書をドキュメント化できます。また、情報資産、アプリケーション、ビジネス プロセス、デバイス、設備といったISMS（情報セキュリティ管理システム）に関連する個々のリソースをカタログ化したり、関連するポリシー、基準、リスクをドキュメント化して保持することもできます。このように情報セキュリティ管理システムを一元的に表示できるため、資産の関係性の把握やインフラストラクチャの変更管理をより簡単に行うことができます。また、評価中に特定された問題を一元的に追跡できるため、ギャップの修正作業について一貫性のある方法でドキュメント化、監視、効果的に対応できるようになります。

まとめ

RSA Archer IT & Security Risk Managementはセキュリティに対してビジネス リスク ベースのアプローチを提供することで、最新のセキュリティ脅威、対応不備のあるセキュリティ プラクティス、セキュリティ コンプライアンスに関する運用上の失態といったリスクを軽減できます。また、セキュリティに関するビジネス コンテキストの確立、セキュリティ ポリシーと基準のドキュメント化と管理、攻撃の検知と対処、セキュリティ脆弱性の特定と修正を行うこともできます。