株式会社テリロジー

<SecurityGate blog　抄訳版>

January 5, 2021

リスクアセスメントを成功させる 10 ステップとは

はじめに

リスクアセスメント戦略を成功させる秘訣は、最初のプラン段階で全体にわたる明確なコミュニケーションが必要です。技術部門と間接部門がアセスメント戦略について自社の目的に沿っているかどうかを確認するため、アセスメントを実施する事前準備として、以下の 10 ステップについて解説します。

1.社内環境のリスクマネジメントを精査する

公的に大きな影響を及ぼす重要な機密情報のリスクマネジメントは社内取締役会での稟議事項の一つです。IT、OT、または企業インフラ全体のサイバーリスクによってビジネスオペレーションに影響を及ぼす場合、これは企業業績に関わる重要なリスク課題です。

2.ビジネスへの影響分析(BIA)を精査する

ビジネスへの影響分析(**B**usiness **I**mpact **A**nalysis)では、リスクアセスメントの重要なアプローチの１つとしてこの分析手法が加えられます。企業がこの分析監査を含めたリスク改善として、利害関係者はアセスメントの重要性について同意する必要があります。

3.リスクアセスメント担当者を選任します

企業のリスクアセスメント担当チームをリードし、最初から最後まで責任を負うには、経験豊富な人材が必要です。通常、IT または OT のマネージャー、シニアアナリスト、またはこれら同等レベルの能力者が選任されるべきです。この重要なポジションを担うには、リスクアセスメントに関わる質問内容を理解出来る能力が必要です。殆どの質問内容を自分で回答できなくても、最終的に他部門関係者と協力してリスクアセスメントのタスクを完璧に遂行できるリーダシップが求められます。

4.リスクアセスメントの利害関係者を選出します

特にリスクアセスメントのカバー領域に複数の社内事業部門が含まれる場合は、通常、複数の利害関係者が存在します。CISO、IT/OT 部門管理責任者、または同等レベルの事業部門責任者は、社内全体の利害関係者をうまくまとめ、リスクアセスメントを実施するための予算を割り当てる責任があります。彼らは、リスクアセスメントの調整役を務める上でおそらく最も重要な人材であり、リスクアセスメント戦略に対して企業全体に確実に浸透されるようにする役割を果たします。

5.利害関係者の連携を推進する

上記ステップ 1 とステップ 2 が完了した場合、経営メンバーはこのリスクアセスメントに対して何を期待し、それがビジネスにどのように影響を及ぼすかの明確な戦略を持つ必要があります。ただし、リスクアセスメントにとって必要な情報は部門ごとに異なるため、部門ごとにニーズを検討することが重要です。そして、利害関係者はサイバーセキュリティ戦略に従い、リスクアセスメントのメリットを認識する必要があります。

6.予算を決める

OT/ICS 環境でのリスクアセスメントは、PDCA サイクルによる継続的に行われるべきです。そして、リスクアセスメントは IT、OT、および運用設備部門で予算をシェアして、サイバーセキュリティ対策に見合った予算を決めることが必要です。全体のリスクマネジメントの中で、このプロセスの予算がカバーする範囲を利害関係者に通知する必要があります。予算にはリスクアセスメントの作業費用とアセスメント監査レポート費用が含まれますが、その他追加としてこのリスクを回避するための修復作業費用も事前に考慮するとか いずれにしても予算がどこまでの範囲をカバーするかを明確にすることが重要です。

7.リスクアセスメントの目標を設定する

リスクアセスメントを開始する前に、すべての利害関係者は、実行可能なステップについて合意する必要があります。リスクアセスメントで目標が設定された場合、その目標を達成するという確固たるステートメントを共有します。これによって効率の良いリスクアセスメントが促進されます

8.リスクアセスメントコントロール手段を決める

リスクアセスメントを効果的にコントロールするには、すべての担当者が自分の担当領域、使用プログラム、それとターゲットの OT/ICS 設備に関する明確な認識が必要です。リスクアセスメントを開始する前にこの重要なタスクを事前に確認することで、リスクアセスメントの質問内容に迅速に回答することができます。そして、リスクアセスメントコントロール範囲を利害関係者に回覧し、合意します。

9.ガイドラインまたはワークスコープを設定する

すべての利害関係者と共有するすべてのタイムラインについてのスコープを設定します。このステップでは、すべての事業部門から承認を得て、部門内で優先的なワークとして認識し、共有できるようにすることが重要です。

10.イベントカレンダーを作成する

イベントカレンダーを作成することで、関係するすべての担当者の説明責任が明示されます。リスクアセスメントは、キックオフの直前にワークスコープを共有します。すべての利害関係者がタイムラインを確実に維持できるように、結果の共有もキックオフの前にカレンダーに含める必要があります。

おわりに

効率的なサイバーリスクアセスメントを行うには、OT/ICS オペレーションの稼働時間、チーム要員の安全性、およびコーポレートガバナンスの目標をサポートするリスクマネジメント戦略が不可欠です。筆者の経験では、サイバーリスクアセスメントは、会社全体で殆ど調整されていない状態でカレンダーイベントを設定してしまうことがよくあります。このため、カレンダーがこの計画外のイベントやビジネスの変更でいっぱいになると、リスクアセスメントが優先順位の低いものになってしまう可能性があります。

サイバーセキュリティ対策の中でリスクアセスメントに割り当てられる予算は、多くの成果を生み出し、戦略的に最も重要な領域に焦点を当てます。企業は、従来の手動プロセスをデジタルツールと自動化に置き換えることで、サイバーリスクアセスメントの費用を確実に節約し、同時により効率的な進め方を実現できます。海外の SecurityGate ユーザでは、同社のプラットフォームを前提にこうした 10 ステップによるベストプラクティスが行われています。弊社は、国内の OT/ICS でもこのベストプラクティスを参考にして顧客に提案していきます（筆者）。

出典

10 Steps for a Successful Assessment Strategy

https://securitygate.io/blog/10-steps-for-a-successful-assessment-strategy/

関連リンク

SecurityGate.io

https://securitygate.io/

お問い合わせ窓口

株式会社テリロジー

グループ事業推進統括部 OT/IoTセキュリティ事業推進部

SecurityGate 担当 宛

製品に関するお問い合わせは当社のお問い合わせフォームからお寄せください

この資料は、SecurityGate.io. の CEO である Ted Gutierrez 氏 の寄稿したブログの記事をもとにテリロジーが翻訳したものです。