小規模組織向けサイバーセキュリティ

CISO 向けチェックリスト：第三者との繋がりを守る

サイバーセキュリティを念頭に置いたベンダーの選定

潜在的なベンダーを評価する際は毎回、次の質問事項を確認すること:

- ☐ 貴組織に似たクライアントにサービスを提供するにあたってどのような経験があるだろうか?
- ☐ 既知のサイバーセキュリティ規格へのコンプライアンスを文書化しているだろうか（NIST フレームワークもしくは ISO 27001、または SOC2 レポートを提供可能だろうか)?
- ☐ サービスを履行するために貴組織のどのデータおよび／またはアセットにアクセスする必要があるだろうか？また、不要と思われるアクセスを要求しているだろうか?
- ☐ 保持した貴組織のアセットおよびデータをどのように保護するつもりだろうか?
- ☐ 自社の第三者サイバーリスクをどのように管理しているだろうか？また、そのサプライチェーンセキュリティに関する情報を提供できるだろうか?
- ☐ 貴組織に影響を及ぼすインシデントが発生した場合、どのようなディザスタリカバリおよび事業継続性プランを抱えているだろうか?
- ☐ 貴組織内の動向、脅威、および変化を連絡するにあたって、どのような手段を講じるだろうか?

第三者を通じたリスクの特定

以下のステップを含めた、第三者サイバーリスクアセスメントを実行すること:

- ☐ 全てのベンダー関係ならびに各関係で晒されるアセットおよびデータを網羅したリストを作成して、継続的に更新する。
- ☐ 各ベンダーまたは第三者がアクセス可能なデータを審査して、各アクセスレベルが「最小権限の原則」に従っていることを確認する。
- ☐ ベンダーのシステムにデータ漏洩が発生した場合の貴組織への影響に基づき、ベンダーと第三者の関係性を順位付けする（低、中、高)。
- ☐ リスクが最も高いベンダーから始めて、各プロバイダーのサイバーセキュリティ性能および関連規格への遵守について評価する。
- ☐ 定期的なセキュリティ評価計画を策定する。最もリスクが高い、および／または顧客データへのアクセス権が最も多いベンダーに関しては、時々オンサイトアセスメントを実施することが望ましい点に留意する。

第三者のセキュリティ管理

- ☐ 徹底したデューディリジェンスを実施する。ベンダーとの提案、契約、事業継続性、インシデントレスポンス、そしてサービスレベル契約に関するあらゆる要求に関して、サイバーセキュリティの期待を設定する。サイバーインシデントが発生した場合の責任および義務について合意する。
- ☐ 貴組織がデータの取引または共有を行う金融機関およびその他のエンティティのサイバーセキュリティ慣行について問い合わせる。なお、貴組織のベンダーおよび第三者もまた、貴組織が遵守するべきサイバーセキュリティ要件に従う必要がある点に留意する。
- ☐ サイバーセキュリティ規格に対するベンダーのコンプライアンスを監視するため、確立および合意済みの措置を取る。
- ☐ 機密データを取扱うベンダーに問い合わせて、貴組織が同ベンダーで抱えているアカウントにおいて二要素認証、暗号化、またはその他のセキュリティ対策を提供しているか確認する。
- ☐ 必ず、インストールする全ての第三者ソフトウェアおよびハードウェアにセキュリティ用のハンドシェイクが設定されていることを確認する。こうすることで、ブートプロセスが認証コードによってセキュア化され、コードが認められない限り実行されない。
- ☐ 偽物または仕様に一致しないベンダーの製品に遭遇した場合、解決策に向けて交渉するか、出口戦略を見つける。
- ☐ 毎年、ベンダーとの契約を見直し、必ず貴組織の戦略的方向性およびデータセキュリティの規制要件を引き続き満たしていることを確認する。契約終了時には、アセットまたはデータの返却、ベンダー側で完全に消去されていることの確認、貴組織のシステムまたはサーバーへの一切のアクセスの無効化に関する規定を含める。

情報の共有

- ☐ 貴組織のベンダーおよび取引先にセキュリティの問題について連絡できる、明確な伝達経路と連絡先が存在することを確認する。
- ☐ 信頼できる、実践的なサイバーセキュリティ情報を内部および外部ステークホルダー（金融セクター内外のエンティティおよび公的機関を含む）と適宜共有できる手順が配備されていることを確認する。
- ☐ FS-ISAC などの情報共有組織に加わり、その他の脅威情報ソースを求めることで、他組織が第三者との間で経験している脅威、脆弱性、インシデント、およびレスポンスに関する最新情報を追跡する。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org