ベンダーリスクマネジメントを紐解く

Dipti Patelは、CISA、CISM、ISO 27001 LA、ITIL V3の資格を持つ、情報セキュリティ及びサイバーレジリエンスにおいて世界的な実績のある大手ITサービス会社、タタコンサルタンシーサービシズ社のセキュリティコンサルタントです。Patelは、ガバナンス、リスク、コンプライアンス（GRC）についての優れた理解者であり、トレンドなGRCの考え方と技術を取り入れています。彼女の連絡先の電子メールアドレスは、diptiapatel@gmail.comです。

今日のビジネスにおいて、外部委託はしばしば標準的な戦略となっています。外部委託は、企業にとって潜在的に非常に大きな利益をもたらしますが、一方で、解決が困難で規模が大きく破滅的なセキュリティの脅威も引き起こします。過去2年間、巧妙なサイバー攻撃者により、ベンダーのネットワークや接続を経由した強力な攻撃が仕掛けられ、金銭や非常に多くのクレジットカードの記録、顧客の重要な個人情報が盗み取られています。

セキュリティインシデントについて、現在のサービスプロバイダや請負業者（23パーセント）および過去のパートナー（45パーセント）に起因すると考える組織に大きな変化が起きています。[1] 標的及び企業外脅威の変化により、現在および近い将来のリスクランドスケープが形作られています。予想されるこれらの変化を戦略的な視点でとらえることで、セキュリティとリスクのリーダー層は、新たに出現するリスクを管理しながら、新たなビジネスチャンスを発掘することができます。つまり、包括的なサイバーリスクマネジメント方針の一部として、企業はベンダーセキュリティリスクに対する十分な監視が必要であることは明らかです。

問題の核心

大部分の人は、ベンダーとの相互接続が小売業者へのサイバー攻撃につながることを予想すらしておらず、何か月も気付かない場合も多くあります。インパクトが大きく予測が困難なこのようなリスクに対応したリスクマネジメントプログラムはほとんどありませんでした。このようなイベントはまれで、多くの場合、通常の予測範囲を超えるものだったからです。

セキュリティ侵害のニュースは大きく取り上げられ、攻撃者や組織的なサイバー犯罪者および一部の国家がニュースのヘッドラインで報じられました。プライスウォーターハウスクーパース社のアンケートによれば、約3分の1（32パーセント）の回答者は、内部関係者による犯罪は外部の者によるインシデントと比較して大きなコストを伴い被害が大きい、と答えました。[2] 大部分の人は、内部の脅威の原因は従業員だけではなく、退職者、サービスプロバイダ、コンサルタント、請負業者、サプライヤー、およびビジネスパートナーもその対象であることを認識しています。

ベライゾン社は2013年度を「小売業者のデータ漏洩の年」と名づけました。小売業者のデータ漏洩が世界中で467件ありました。2014年も大規模なデータ漏洩事件の発生が続いており、やはり、クレジットカードデータ、個人情報、重要な健康記録、および財務情報がターゲットになっています。[3]韓国では消費者情報の大規模な漏洩事件が発生し、セキュリティ違反により、1億500万件の支払用のカードアカウントが漏洩しました。[4]ドイツのフェルデン市では、1800万件の電子メールのアドレス、パスワードを含む情報が盗まれたと市の職員が発表しました。[5]

世界各地の監督当局は、ベンダーセキュリティを強化するという流れに乗っています。組織はベンダー関係の件数増加と複雑化の拡大が続いており、監督当局はベンダーセキュリティに関するガイドラインを改定し、組織に対してベンダーリスクへの取り組みを強化するよう指示しようとしています。たとえば、米国通貨監査局（OCC）と米国連邦準備制度理事会は、サードパーティとの関係に対するリスクマネジメントのガイドラインの改定版を発表しました。このガイドラインでは、金融機関がサードパーティとの関係に関するアセスメントがいかに必要であるかについて根本的な転換を求めています。特に、組織が重大なリスクにさらされる可能性のある重要な活動に携わっているサードパーティに対して、サードパーティとの関係についての強力なリスクアセスメントとプロセスのモニタリングの導入を呼びかけています。[6]

企業は、ベンダーに関するセキュリティ手法を強化し、進化し続ける脅威とセキュリティニーズに対応し続けていかなければなりません。

ベンダーセキュリティガバナンスへの対応

サプライヤーやビジネスパートナー間とのデータ量およびデータ共有が指数関数的に急増している今日の相互接続されたビジネス環境において、サードパーティに関するリスク監視やデューディリジェンスの欠如は不安材料になります。セキュリティの視点からベンダーリスクの監視を行うには、ベンダーとの契約内容の明確化と合わせてベンダーセキュリティリスクの管理と軽減のためのポリシーとガイドラインを策定するという、企業全体をカバーするプログラムが必要です。

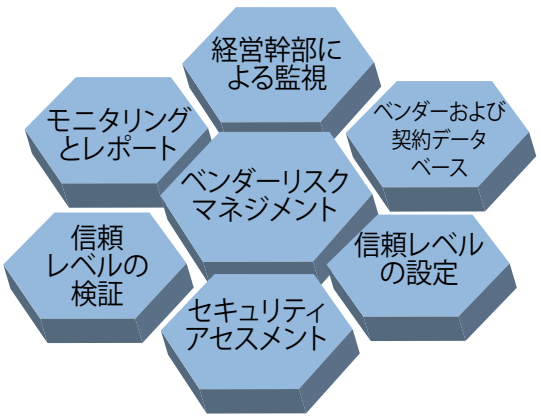
Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

このような監視を行うことにより、組織はサイバーセキュリティプログラムの改善だけでなく、潜在的に将来における法規制上、法律上の立ち位置の向上にも役立ちます。以下の6つのステップは、組織はベンダーセキュリティガバナンスポリシーを開始することを可能とすることに役立ちます。(**図1**)。

図1 - ベンダーリスクマネジメントプログラムとコンポーネント



出典:Dipti Patel。転載許諾済

1. **経営幹部による監視**- 経営幹部の連携およびビジネスの前後関係は、組織全体に適切に導入するためには非常に重要です。適切な連携は指令センターのようなものであり、プログラムに必要な方針、プロセスやガイドラインを提供します。外部委託の判断は戦略的なものであり、単なる購買判断ではありません。つまり、ベンダーリスクマネジメントプログラムについて、役員会が方向性を示すことが最も重要です。このプログラムに関して、次の職務から、経営の指示を受けるべきです。
   - コンプライアンス機能。組織が順守すべきベンダーリスクマネジメントについて、具体的なルールが記載された法規制や他のコンプライアンスの要求事項を提示するために。
   - ITリスクとコントロール機能。ベンダーと共有するアクセス方法やデータの重要性に応じて、リスクとリスクレベルを決定するため。ベンダーリスクマネジメントプログラムでは、この機能が提供する重要なリスク指標を利用すべきであり、これによってアセスメント時のリスク対応を行います。

Enjoying this article?

- *Vender Management: Using COBIT 5*を読みましょう。
  www.isaca.org/vendor-management
- *Knowledge Center*にある*Risk Management*のサイトで、より多く学び、議論し、そして協働しましょう。
  www.isaca.org/topic-risk-management

   - 契約ガバナンス機能。ベンダー契約に、セキュリティアセスメントの必要性とこれらのアセスメントを実施するためのベンダーの責任が、適切に記述されることを保証するため。
2. **ベンダーおよび契約のデータベース**- 今日の多くの組織では、多数のサードパーティやサービスプロバイダと取引しています。リスクマネージャーがアセスメントを開始するにあたり一般的に関心を持つ部分は、契約情報、責任分担表もしくは更新された契約の紛失です。これは、特に複数のチームが購買の目的に関わっている場合、非常に困難な作業になります。ベンダーおよび契約のデータベース(VCD)により、他のサードパーティとの関係(合同事業、公益事業組織、ビジネスパートナー、再委託先など)を含むベンダーの正確かつ完全な棚卸しを確実に行うことができます。
3. **信頼レベルの設定**- ベンダーリスクマネジメントプログラムを効果的に行うためには、同じタイプのリスクアセスメントをすべてのベンダーに対して行ってはいけません。むしろ必要なのは、リスクが最も高いと考えられるベンダーサービスを識別し、それに従って優先順位をつけることです。最初のステップは、現行のリスクマネジメントの観点から、どのベンダーとサービスが対象範囲であるかを理解します。対象のベンダーを識別し、優先順位をつけた後、社内のコントロールレベルとベンダーが保有するコントロールレベルを比較し、その結果に従って、ベンダーに対するデューデリジェンスアセスメントを実施します。このアセスメントの結果によって、信頼レベル評価基準(TLR)を適切に設定し、再アセスメントとモニタリングの点から今後の要求事項を設定することができます。このアプローチは、最も重要なベンダーの関係にリソースを集中し、リスクの低い関係に対する不要な作業を制限します。たとえば、TLRが高いベンダーは、TLRが低いベンダーより優先する必要があります。

4.セキュリティアセスメント- ベンダーリスクを適切にコントロールし管理するには、継続的なアセスメントが必要です。ベンダーに対して実施するアセスメントのタイプは、TLRと頻度に応じて決定することが重要です。**図2**は、プログラムに含まれ得るアセスメントのタイプの例を示しています。

図2 - TLRに基づくアセスメントタイプ

信頼レベル評価基準（TLR）	アセスメントタイプ
低	ベンダーの自己アセスメント
中	机上レビュー、インフラストラクチャのアセスメント
高	オンサイトレビュー、インフラストラクチャとアプリケーションのアセスメント

出典:Dipti Patel。転載許諾済

良い参考事例として、アセスメントの範囲を、セキュリティ標準と実践（例えば、ISO27001、COBIT®、OWASPなど）および、特定のコンプライアンス要求事項（例えば、ペイメントカードインダストリーデータセキュリティスタンダード（PCI DSS）を組み合わせて設定することができるでしょう。

5.信頼レベルの検証- 外部委託との関係は通常、繰り返しが重ねられ、関係が成熟するにつれ発展したものとなります。顧客の組織が戦略的に外部委託を増やす場合、共有する情報とリソースの増加を想定して、信頼レベルの検証も行うべきです。テクノロジーの進歩に伴い、ビジネス環境は絶えず変化し、法規制上の要件が増大しているため、信頼レベルの検証は継続的に実施します。最も合理的かつ効果的な発見を得るには、実施中のアセスメントの結果を使用することが最適だからです。

6.モニタリングとレポート- 反復的なプロセスでは、実施した信頼レベルに基づいて、ベンダーを継続的にモニタリングし、定期的にアセスメントすることが必要です。プログラムでは、ベンダーセキュリティの状況とリスクレベルについて、組織を目標の姿に発展を支援する権限を有する経営責任者と情報を共有すべきです。ビジネスの視点からリスクを説明する場合、特に、社内の利害関係者、社内監査部門、ビジネスライン、および必要に応じて取締役会に報告するための資料を作成する場合は、追加的な機能となります。

結論

ベンダーリスクマネジメント管理は、技術的なコントロールプロセスから効果的な管理プロセスに情報セキュリティを向上させるための次のステップになります。ベンダーに対する定期的なセキュリティアセスメントによって、組織は、ビジネス部門が関係するセキュリティリスクを認識し、リスクの移転、低減、保有によって効果的にリスクを管理していることを確認することができます。包括的なベンダーセキュリティアセスメントを実施することで、企業は、システムやデータがセキュリティ基本方針に整合して使用されているかを認識することができます。

ベンダーリスクマネジメントは単なるプロジェクトではなく、継続的なプログラムであり、持続を維持するためには、継続的な信頼が必要です。基礎部分のフレームワークが構築されると、組織は、ガイドラインや手順書の改善およびアセスメント調査票の合理化や自動化などの活動を通して成熟度の向上を確認することができます。認識とコミュニケーションは、プログラムが有効に運用され、意図する結果（企業がビジネスパートナーやベンダーと共にセキュリティを確保）を確実に達成するためのキーポイントになります。

後注

[1] PricewaterhouseCoopers, “Managing Cyber Risks in an Interconnected World. Key Findings From The Global State of Information Security Survey,” 2015, *www.pwc.com/gx/en/consulting-services/information-security-survey/*

[2] *Ibid*.

[3] Verizon, 2014 Verizon Data Breach Investigations Report, *www.verizonenterprise.com/DBIR/2014/*

[4] *Op cit*, PricewaterhouseCoopers 2015

[5] Brewster, Thomas; “Germany Investigating Data Breach Affecting 18 Million,” *TechWeek Europe*, 7 April 2014, *www.techweekeurope.co.uk/workspace/germany-id-theft-18m-143269*

[6] Office of the Comptroller of the Currency, “OCC Bulletin 2013-29. Description: Risk Management Guidance,” USA, *http://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html*