Legal Wire

pillsbury

Japan Practice

Vol. 69 / February 2020

国際的な圧力がサイバーセキュリティへの脅威を高める

–サイバーセキュリティへの脅威に取り組むための実務的手段—中東における高まる緊張感その他サイバーセキュリティ事故の脅威が増加する事態において何をすべきか。

タマラ D. ブルーノ、ブライアン E.フィンチ、キャシー・レンチェナー

- ニュース又は企業方針が、サイバーセキュリティの脅威を高める場合、その脅威に対処することが重要です。本稿では、そのような対策案について紹介します。
- サイバーセキュリティ対策で、2020 年 3 月 21 日に施行される、ニューヨーク州民のデータを有する全ての事業に対して幅広いサイバーセキュリティ要件を課す、ニューヨーク州 SHIELD 法が遵守されていることも確認しましょう。

イランとの間の緊張感の高まりが報道される中、米国の事業に対するサイバー攻撃の可能性についての懸念が高まっています。米国国土安全保障省（The Department of Homeland Security）は、サイバーセキュリティ・インフラストラクチャー・セキュリティ庁（Cybersecurity and Infrastructure Security Agency）（以下、CISA といいます。）を通じて、これに対して意識と警戒を高めることを推奨する警告及び指針を公表しました。各業界特有の警告に関しては、規制対象企業に対して、各行政当局により別途発せられ、これには、例えば、連邦準備銀行（こちら）及びニューヨーク州金融サービス局（こちら）による、金融システム及び銀行に対する脅威に関する発表等が含まれます。

企業はこれらの警告を深刻に受け止め、警告が示す多様な推奨事項を実行することを十分検討すべきです。とりわけ、国家によるサイバー攻撃は、深刻な事業の混乱を引き起こすものであり、その結果として、多岐にわたる事業回復費用、顧客への補償、法的及び規制対応費用、賠償費用といった巨額の支出が発生するためです。例えば北朝鮮が 2014 年にソニーピクチャーズに対してサイバー攻撃をした際、ソニーピクチャーズは、ソニーの社内メールが公表されるという辱めだけでなく、IT 費用、映画「ザ・インタビュー」の興行収入への打撃、及び法的費用の損害を被ったといわれています。また、ロシアが送り出したといわれている NotPetya という破壊的ランサムウェアは、100 億ドルを超える損失をもたらしたといわれています。NotPetya により、製薬会社、法律事務所、運送会社を含むほぼ全ての産業界の企業が影響を受けました。

各種の新法が、サイバーセキュリティに対する一層の注意及び資源投入の拡充を企業に要求するにつれ、サイバーセキュリティに対する法的又は規制上の要請は一層高まっているといえます。そして、各企業は、このような現状を踏まえ、起こりうるイランによるサイバー攻撃に対する警告を真摯に受け止めるべきでしょう。更に、恐らく最も重要なのは、圧倒的多数のイラン関連の警告が発

せられていたという事実それ自体が、サイバー攻撃の被害者が近時のサイバー脅威の波を“認知”していたという事実の十分な証拠として働きうるということです。それゆえ、企業は、将来的なサイバー攻撃による被害を見据えた合理的な対策を執らなければならないのです。

これらの多様な警告の対象から完全に除外される経済セクターはありません。CISA がその発表（こちら）において示したとおり、イランは、過去 10 年間にわたり、無数の高度なサイバー攻撃を実行し、相当高性能なサイバー能力を持つと知られています。イランのサイバー攻撃は、金融サービス、エネルギー、政府設備、化学、ヘルスケア、重要な製造業、通信及び防衛産業基地を含む種々の産業部門を対象としてきました。CISA の発表による警告は、イスラム革命防衛隊のための複数年にわたる大規模なサイバーアタックによる知的財産や個人情報の窃盗キャンペーンを含む、イランによる多数の高度かつ重大な攻撃を列挙しています。

これらの警告を踏まえて、企業は次のような対策を検討すべきです。

1. 組織のサイバーシステムへの脅威に対処するために、適切な対策がとられているか、IT 部門に再確認すること。IT 部門が上述の CISA からの警告を認識しており、この警告にある技術的な推奨事項を優先事項として実行していることを確認しなければなりません。経営陣は、IT 部門に対して、方向性を示し、サイバーセキュリティーが優先事項であると理解させることが重要です。さもなければ、企業のサイバーセキュリティー状態に影響を与えうる、又はサイバー防衛としては優先事項だが IT 事業にとっては重要度の低いプロジェクトを遅延させる場合があるかもしれません。サイバーセキュリティへのリスクが高まったために追加措置が必要となった企業は、かかる対策を即座に実施すべきです。

2. 文書又は研修を通じて従業員との間でコミュニケーションを取ること。従業員全てが、不審な E メールやその他コンピューターの異常に注意を払う必要があります。全ての従業員が研修を受け、意識を高めておくことが重要です。

3. サイバーセキュリティ及びプライバシーデータの侵害があった場合の事業継続計画が最新のものであり、システムが適切なバックアップを取っていることを確認すること。この事業継続計画は、常に最新のものである必要があり、行政当局等を含む関係者に関わる情報が最新のものでなければなりません。また、かかる計画が有効に実施されるためには、模擬演習も必要です。机上での実践演習やその他の方法で、組織におけるサイバー攻撃への対策が十分であるか否かを検証することが適当です。社内の全ての人間が、緊急事態に自身が行うべき役割を認識するためには、計画の模擬演習が肝要です。

4. 国家支援のサイバー攻撃が保険対象に含まれるか否かを確認するために、保険を見直すこと。サイバー事故に特化された保険は、典型的に、サイバーテロを保険対象範囲に含めており、財産保険は、物理的損害を含むサイバー攻撃による企業への損害を保険対象範囲に含めている場合もあります。しかし、ほぼ全ての保険約款は、“戦争”を除外しており、これをもとに国家支援のサイバー攻撃は保険範囲に含まれないと主張する保険会社もあります。保険約款における文言はそれぞれ異なるので、保険代理店や顧問弁護士に問い合わせることが適当です。

5. 自社のサイバーセキュリティプログラムが最新のものであり、業界のベストプラクティス並びに法律及び規制上の要件を遵守しているか確認すること。最近強化傾向にある規制を遵守していることが大切です。サイバーセキュリティを組織における法的ニーズとして取り扱うべきという傾向は強くなってきており、他の法的リスクと同等に扱うことが求められるよ

うになってきています。適切に保護されていないシステムを維持することは、深刻な事業上の問題や法的リスクをもたらし、かつ合理的なサイバーセキュリティ予防措置及び制御の欠如もまたリスクの惹起につながります。Graham Leach Bliley 法やニューヨーク州金融サービス局によるサイバーセキュリティー規則（23 NYCRR Part 500）のように、企業に対して、合理的なサイバーセキュリティ予防措置を設けることを要請する既存の法律や規制は、長きにわたって、多数存在します。今回施行される SHIELD 法を含む法的・規制上の要請は増加しており、2020 年 3 月 31 日に施行される SHIELD 法は、産業ごとの垣根を越えて、企業に対して、包括的なサイバーセキュリティプログラムを設けることを義務付けています。

ニューヨーク州居住者の私的情報を有する全ての企業は、2020 年 3 月 21 日までに、データの秘匿性を守るために、合理的なデータセキュリティ予防措置を講じなければなりません。その他のサイバーセキュリティに関する特定の法的要請（上記 Graham Leach Bliley 法や 23 NYCRR 500）に従っていることを示すことができれば、それらの企業は、かかる予防措置義務の対象から除外されます。SHIELD 法は、ニューヨーク州居住者に関する情報について、包括的なサイバーセキュリティプログラムを設けることを求めるもので、ニューヨーク州の規制を強化するものです。その予防措置は、組織の規模や複雑性に応じてテーラーメイドすることができますが、最低限、以下の全ての事項を含まなければなりません。

- サイバーセキュリティコンプライアンスプログラムを実施するための従業員の任命及び研修
- 契約で定められた予防措置を伴う、適切なサイバーセキュリティを維持できる第三者の利用
- ネットワーク及びソフトウェアの設計並びに情報処理、伝達及び保存を含むサイバーセキュリティプログラムのリスク評価
- サイバー攻撃やシステム障害を検知し、予防し、それに対応するための手続的かつ物理的予防措置
- サイバーセキュリティプログラムの有効性の監視及び点検
- 事業のために不要になったデータを、合理的な期間内に、安全に、確実にかつ永久的に廃棄する手続き
- サイバーセキュリティプログラムの変更が求められる事業又は環境の変化に取り組むための定期的なプログラムのアップデート

これらに未対応の企業は、自社のサイバーセキュリティプログラムが、SHIELD 法を遵守したものかを検証し、ニューヨーク州の規律に従っていない場合には、速やかにプログラムをアップデートすることを検討しなければなりません。弊所は、貴社の現在のサイバーセキュリティプログラムの評価、貴社のサイバーセキュリティチームのポリシー、手続き、研修及び点検を策定し、適切な実践演習の開発のお手伝いをいたします。

本稿の原文（英文）につきましては、International Pressure Raises Cybersecurity Threats をご参照ください。

本稿の内容に関する連絡先

奈良房永（日本語版監修）
31 West 52nd Street
New York, NY 10019
+1.212.858.1187
fusae.nara@pillsburylaw.com

荒井菜々子（日本語版作成協力）

Tamara D. Bruno
2 Houston Center, 909 Fannin, Suite 2000
Houston, TX 77010-1028
+1.713.276.7608
tamara.bruno@pillsburylaw.com

Brian E. Finch
1200 Seventeenth Street, NW
Washington, DC 20036
+1.202.663.8062
brian.finch@pillsburylaw.com

Cassie Lentchner
31 West 52nd Street
New York, NY 10019
+1.212.858.1211
cassie.lentchner@pillsburylaw.com

Legal Wire 配信に関するお問い合わせ

田中里美
satomi.tanaka@pillsburylaw.com

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.
© 2020 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.