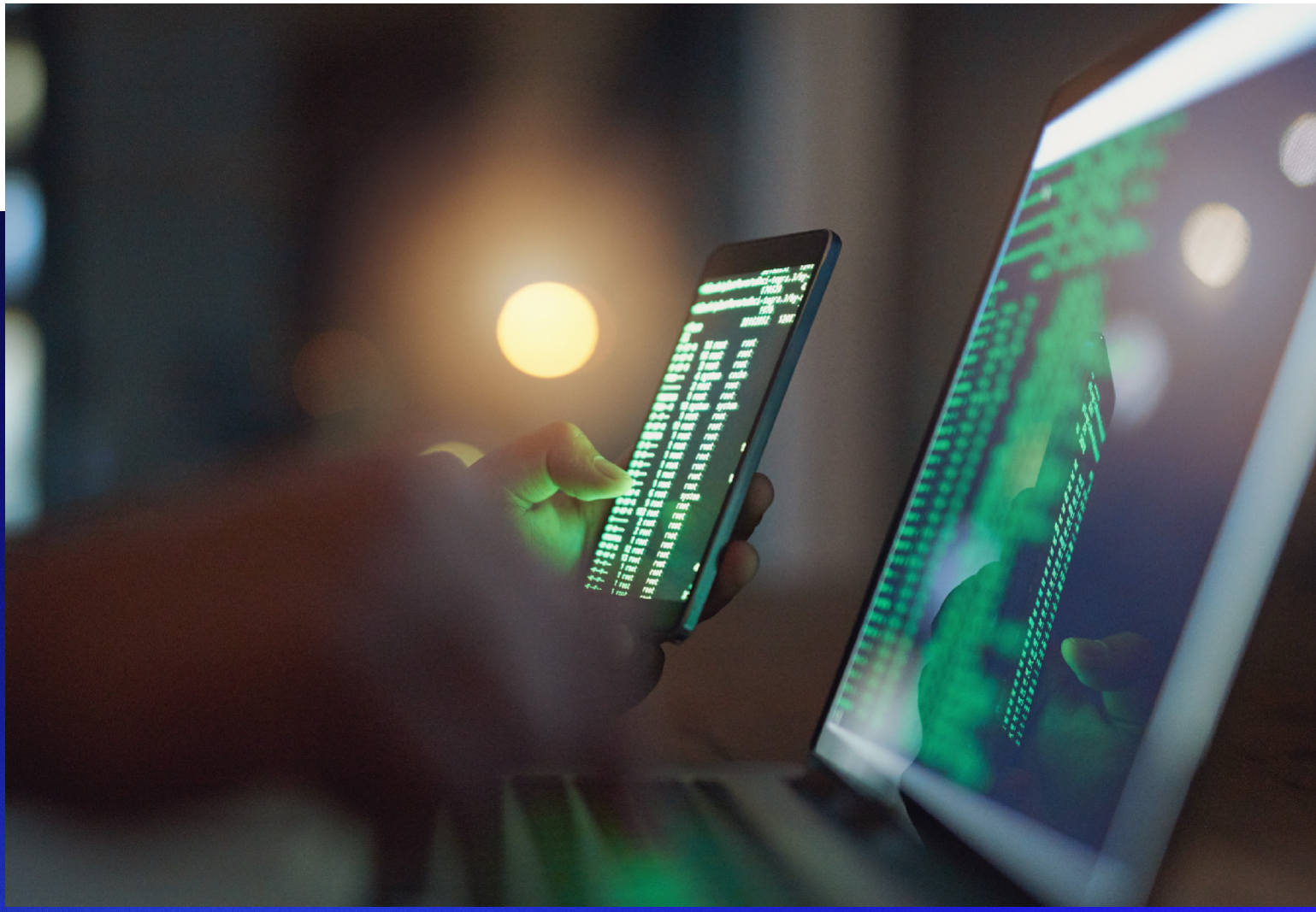
Secureworks®

WHITEPAPER

一面報道のコスト：拡大し公表されるセキュリティ侵害の脅威について知るべきこと



メディアで大々的に報道されるようなサイバー攻撃の被害者になった場合のコストは、近年ますます増大しています。ロンドンを拠点とする外貨両替サービス企業の Travelex は、2019 年 12 月下旬に発生したセキュリティ侵害で、ランサムウェアのオペレーターに 230 万米ドルを支払ったとされています[1]。2020 年 4 月には、米国の法律事務所が身代金 2100 万ドルの要求を受け、その後、額が 4100 万ドルに引き上げられました[2]。わずか 3 ～ 4 年前の一般的な身代金の要求額は 1 万ドルほどでした。

ランサムウェアによる要求額が増大していることは周知の事実ですが、被害を受けた組織のコストを急増させる原因は、このような攻撃だけではありません。

2018 年 9 月に発覚した British Airways (BA) のセキュリティ侵害による総被害額は、10 億米ドルに達するとも推定されています。この攻撃では、データが暗号化されたり身代金要求があったりしたわけではありません。サイバー犯罪者は BA のウェブサイトのサードパーティコードを使って消費者を詐欺サイトに誘導し、そこで 50 万人もの顧客の個人を特定できる情報と約 38 万件のクレジットカード番号を取得したのです。

このような身代金以外のコストは、複数のカテゴリーに分類され、その影響も短期的なものと長期的なものがあります。例えば、事業上の損害や評判・信用の失墜など、他と比較すると理論的推定になるコストもありますが、侵害への対応計画にはリスク計算の要素も含むため、最悪のシナリオを考えておくに越したことはありません。

公表されたデータ侵害に関連するコストが身代金だけではないことは明白です。実のところ、他のコスト要素が非常に大きく、身代金は多くの場合発生する総コストのほんの一部に過ぎません。

事業コストと技術コスト

情報が漏洩した直後は、組織の事業システム自体が部分的または完全に侵害された状態になる可能性があります。事業に部分的な影響が出たり、場合によっては完全に停止したりする場合もあり、それに伴って収益に影響が生まれます。最初に優先すべき事項は、インシデントの範囲とそれによる被害を確認し、脅威アクターを排除して、組織が業務に復帰できるように可能な限り修復することです。

事業コストと技術コストは、侵害の種類や、システムの侵害が部分的か全体に及ぶのか、そしてどの程度の技術的リカバリーが必要なのかによって異なります。少なくとも、システムのリカバリーは組織内の既存の技術リソースを使い、通常業務に支障をきたすことになります。外部の専門家によるインシデント対応サービスに依頼し、費用を支払う必要がある場合もあります。

特にバックアップや復号化キーがない状況でのランサムウェアでは、他のタイプの侵害よりも、修復に大きな技術リソースが必要になる可能性があります。

顧客がサービスにアクセスできないと知ると、コールセンターのコストも上昇するでしょう。プロセスを手動で実行する必要があれば、一時的に人数を増やさなければなりません。Travelex が侵害を受けた時には、30 ヶ国にわたる自社のシステムを停止し、システムの復元開始までの 2 週間、ペンと紙での作業に立ち返らざるを得なかったうえ、攻撃から 1 ヶ月たっても依然として一部のウェブサイトはつながらない状態でした。

1 BankInfoSecurity, Travelex Paid $2.3 Million to Ransomware Gang: Report
2 Computer Weekly, Law firm hackers threaten to release dirt on Trump

それどころか、システムへのアクセスを取り戻すのにかかるのをはるかに上回るコスト面での影響が、法務、マーケティング、カスタマーサービス、広報など、事業全体に及ぶおそれがあります。多くの場合、危機管理やコンピュータフォレンジックなど、費用負担の大きなサポートを、高度な専門知識を有する外部アドバイザーに求めることになります。

$7,500

CCPA の違反 1 件 (インシデント 1 件、被害者 1 名) あたりの罰金額。

規制によるコスト

個人を特定できるデータが公開された場合、規制による罰金が課せられる可能性があります。現在多くの国や地域で、組織はセキュリティ侵害の事実を非常に限られた期間内に公表する義務があります。

GDPR (EU一般データ保護規則) が施行されて以降、規制当局による罰金の規模が劇的に増加し、コスト負担を押し上げています。英国の情報コミッショナー局 (ICO) は、BA に対して1億 8300 万ポンド (2 億 3400 万米ドル) という過去最高額の罰金を科すとしています[3]。これに対して、GDPR 施行以前の最高罰金額は、940 万人の顧客の個人情報が漏洩した Cathay Pacific のセキュリティ侵害について科せられた 50 万ポンドでした。

ICO が「セキュリティ措置が貧弱」と評したこの事案に対して、BA に科される罰金はさらに高くなる可能性もありました。科せられる予定の罰金額は、当時の BA の年間収益の約 1.5 %に相当しますが、GDPR 下で認められている罰金の上限は、年間収益の 4 %です。

カリフォルニア州消費者プライバシー法 (CCPA) に基づくと、罰金額は違反1件につき最高で 7500 米ドルに達します。インシデント 1 件、被害者 1 名につき 7500 ドルということなので、BA のような侵害規模の場合、GDPR の罰金を大きく上回ることになります。

進取的なランサムウェアのオペレーターはこれを見通し、規制当局による罰金のリスクを脅しに使って、被害組織に早急に身代金を支払うよう要求します。支払いを怠った場合、盗まれた顧客の名前が脅威アクターのリークサイトに公表されることになります。

顧客コスト

罰金に加え、データが公開された可能性があることを顧客に通知するという義務が、さらなる財務上の影響となる可能性があります。通知をすれば、顧客はパスワードを変更することで自分自身を保護する対策を取ることができますが、顧客が補償請求や集団訴訟を起こす原因にもなります。

- Equifax は、2017 年 9 月の侵害公表後、被害を受けた顧客との世界規模の和解に合意し、顧客への保障として最大 4 億 2500 万米ドルを支払うことになりました[4]。
- Walmart はデータ侵害を公表しなかった結果、ダークウェブへの個人情報リークを招いたとして集団訴訟を起こされています[5]。

3 Information Commissioner's Office, Intention to fine British Airways £183.39m under GDPR for data breach
4 Federal Trade Commission, Equifax Data Breach Settlement
5 Top Class Actions, Walmart Class Action Lawsuit Says Customers Subjected to Data Breach

- BA に対しては集団訴訟が進められ、顧客の登録が 2021 年 1 月に締め切られました。最終的な請求額は GDPR の罰金を超える可能性があります[6]。

和解費用に加えて、弁護士費用や訴訟関連費用が発生するうえ、顧客への通知に必要なプロセスがさらにコストとしてのしかかります。

事業上の損害

セキュリティ侵害によって組織が顧客をどのくらい失うかは、侵害の性質と組織自体の性質に依存します。E コマースのウェブサイトでダウンタイムが生じると、特定のものを早く購入したい消費者はすぐに他のサイトへ行ってしまうため、大きな売上損失につながります。Amazon で 2018 年 7 月のプライムデーに発生したダウンタイムの原因は明らかになっていませんが、売上損失額は 1 億米ドルに達したと推定されています[7]。そして、一度去ってしまった顧客は戻らないかもしれません。英国の銀行の TSB で 2018 年に起こった IT トラブルは、セキュリティ侵害によるものではありませんでしたが、同行は 8 万人の顧客を失ったと見られています[8]。

大企業であれば、顧客はサプライヤーを急に変更することはできないでしょうが、契約の更新を躊躇することになりません。Travelex の場合では、侵害から 3 週間経過後も、ホワイトラベルの外国為替サービスを利用していた銀行やスーパーマーケットで、業務に支障が続いていました。ここでもまた、収益は失われます。

規制によるもう 1 つの影響は、侵害を非公表にできなくなったということです。つまり、システムの機能停止によってサービスを提供できなくなるからというのはもちろん、顧客がデータや金銭に関してその会社を信用しなくなるからということで、短期的に顧客が失われてしまいます。

これは当面の取引に限ったことではありません。契約の開始や新たな段階への移行を決まった日に実施できなければ、契約が締結されなかったり、破棄条項が実施されたりして、取引と収益が競合他社に渡るおそれがあります。

長期的に見ると、その影響は市場での組織の地位を左右する可能性さえあるのです。

評判と信用の失墜

セキュリティ侵害による組織の業績への長期的影響を個別に評価することは困難です。例えば、British Airways と Travelex はともに新型コロナウイルスの流行からも深刻な影響を受けています。しかし、特にサービスを提供できない期間が長く続くと、市場での地位を以前のレベルにまで回復させるのは難しく、費用もかかります。ブランドやその他の無形資産の価値が損なわれ、企業業績に影響を与える可能性もあります。

---

6 Lawyer Monthly, BA Back Down on Data Breach Claim Window
7 Business Insider, Amazon's one hour of downtime on Prime Day may have cost it up to $100 million in lost sales
8 Independent, TSB IT meltdown cost bank £330m and 80,000 customers

組織は顧客だけでなく、サプライチェーン内での地位をも失うおそれがあります。パートナーデータの取り扱いに関する配慮が欠けていたり、攻撃の影響が続く中でも業務を継続するレジリエンスが不足したりするのが露呈した組織とは、サプライヤーは取引をしたがりません。

侵害により IP が盗まれれば、競合他社が自社の製品やサービスを向上させることで市場で肩を並べ、それにより収益がさらに減少するということも考えられます。米国企業における IP 盗難によるコストは、年間 6000 億米ドルにのぼると見積もられています[9]。

小規模企業が侵害の被害を受けると、倒産も起こり得ます。

潜在的なコストは他にもあります。保険料は翌年上がる可能性が高く、また、減収の補填のために資本の調達が必要になる場合があります。

一度攻撃に成功した後も攻撃者はシステム内部に潜んでいるかもしれず、それを完全に排除しなければ、すべてが再発するおそれがあります。そうなると、またしても数週間から数ヶ月の短期的なコストが発生することになります。オーストラリアのビール会社 Lion は、2020 年に、ランサムウェア攻撃を立て続けに 2 回受けています。

リスクへの理解と備え

今やセキュリティ侵害には公の監視の下で対処しなければならないという事実から、組織はもはや逃れることはできません。これまで述べた様々な潜在的コストは、確実なものもそうでないものもありますが、十分な備えをしておくこと、そしてセキュリティポリシーで監視と検出の重要性を強調しておくことの大切さを明確に表しています。

攻撃者の中には確かに高いスキルを持っている者もいますが、多くの侵害は基本的なセキュリティ上の見落としが原因で発生します。インシデント対応の予測や計画の欠如や、利害関係者へのクライシスコミュニケーションによって、事態がますます悪化することもあります。

重要なのは、侵害によって起こり得る短期・長期両方の影響をビジネスリーダーが理解しておくことです。そして、備えこそが一番の対策です。適切な備えと、正しい情報に基づく入念な対応を行うことで、財務上のコストと信用コストの両方を削減することができます。上手くいけば、高い透明性や準備した対応への手際よい移行によって、世間の信用をかえって高めることさえ可能です。

つまり、セキュリティチームだけでなく、組織の上層部も、公表されるセキュリティ侵害に伴うリスクを理解しなければいけないということです。

また、組織のセキュリティスタンスが持つ実利的な側面が十分に理解されている必要があります。その認識が不足していると思われる組織での周知は特に大切です。

最後に、日和見的なサイバー攻撃者の関心から逃れられる組織はほぼ無いに等しいことを、上層部は理解しておく必要があります。この理由だけをとっても、セキュリティ侵害に備えることは賢明なのです。すべての組織にとって、入念で適切なインシデント対応計画とメッセージング戦略が不可欠です。

---

9 CSO, Intellectual property protection: 10 tips to keep IP safe

結論

組織のサイバーセキュリティに関する意思決定は、企業のビジネスリスクプロファイルの文脈の中でのみ行うことができます。情報漏洩への対応、またランサムウェアの場合には、身代金を支払うかどうかの決定は、取引上のリスクに関連する意思決定になります。しかし、潜在的コストには様々な要素があり、長期的な損害が出る可能性もあるため、適切な準備の重要性を認識することが不可欠です。

Secureworks®

セキュアワークス (NASDAQ: SCWX) は、デジタルで接続された世界で組織を保護するサイバーセキュリティのリーダーです。

当社は、何千もの顧客からの可用性を統合し、あらゆる場所のあらゆるソースからデータを収集して分析し、セキュリティ侵害の防止、リアルタイムでの悪意ある活動の検出、迅速な対応、そして新たな攻撃の予測を行います。当社は、お客様に「知識を集めて、もっとずっと安全な (Collectively Smarter. Exponentially Safer.™) 」サイバー防御を提供します。

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place, 1
Creechurch Ln London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3
5DA United
Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs Forest,
Sydney NSW Australia 2086 1800 737 817

日本
〒212-8589
川崎市幸区堀川町 580
ソリッドスクエア東館 20 階
03-6893-2317
www.secureworks.jp

※ 本文書は www.secureworks.com で公開されている The Cost of Making the Front Page: What You Need to Know About the Growing Threat of Public Breaches の抄訳となります。原文 (英語) と和訳の内容に差異があった場合には、原文の記載が優先されます。