KPMG あずさ監査法人

サイバーに本気で取り組む
重要資産を守るには

May 2019

Matthew Martindale
KPMG in the UK

James Arnold
KPMG in the US

保険会社が直面するサイバーリスクは常に変化しています。次の攻撃に対する備えは万全でしょうか。

好むと好まざるとに関わらず、保険会社はハッカーの標的になりつつあります。ハッカーは、保険会社の意思決定者と規制当局者が長年理解してきたこと、すなわち保険会社が世界で最も価値のあるデータの一部を所有しているという事実を知っているのです。

事業部門にもよりますが、保険会社は単に個人が特定できる情報を所有するだけでなく、健康記録、財務状況、運転歴、家族歴、信用情報などのきわめて個人的な情報にアクセスすることが可能です。サイバー泥棒はそのすべてを狙っています。

取る価値のないリスク

それと同時に、保険会社にはサイバー攻撃に関連するリスクもまた出現しています。サイバー調査の実施から法的防御までのすべてにかかるコストだけでなく、サイバー攻撃が起きた場合には、システムがシャットダウンし、調査が行われ、プロセスがアップデートされる間に混乱が発生する可能性があります。

サイバー攻撃による評判への影響も甚大になる恐れがあります。顧客は保険会社に対し、自らの保険資産だけでなく自分のデータもまた保護されることを期待しています。この信頼が損なわれれば、顧客はすぐにでも保険会社の変更へと動きかねません。一旦離れた顧客を呼び戻す機会は少ないでしょう。

世界の規制当局はリスクの高まりとその影響について認識しています。その結果、多くの規制当局がサイバーセキュリティおよびプライバシーに関する厳しい法律の公布へと動いています。その内容は、保険会社に対し、従来よりもはるかに高い水準のサイバー対応の整備を求めるものです。EUの一般データ保護規則（GDPR）、カリフォルニア州のプライバシー法、ニューヨークのサイバーセキュリティ法、あるいは英国の新しい法律など、規制当局は保険会社に対し、サイバー攻撃への強固な理解と備えを求める姿勢を強めています。

変化するターゲット

サイバーリスクが一定不変のものであれば、大半の保険会社がハッカーを締め出し、コンプライアンスを確保するのに何の問題も生じないでしょう。しかし現実には、サイバーリスクは常に変化し、進化し続けています。新たな脆弱性を取り除こうとしても、ハッカーは常に一歩先にいます。ハッカーの中には単に刺激を求めるだけの退屈したティーンエージャーもいますが、多くの場合、ハッカーは非常に高度な知識を持ち、専門的に従事し、（しばしば）潤沢な資金を持つ犯罪者です。サイバー空間の脅威を上回ることは困難です。

直面するリスクも急速に変化しています。以前には攻撃の大半は、秘密情報にアクセスしてそれを盗むため、あるいは何らかの事業上の混乱を引き起こすために、脆弱性を悪用することに主眼を置く傾向がありました。しかし、これからは企業の信頼感を損ね、顧客に予期せぬ難題を突き付けるような形でのデータの改ざんやルールの変更など、保険会社の事業の信頼性に対する攻撃が始まる可能性があります。

変化し続けているのはリスクだけではありません。期待もまた変化しています。実際、大規模なサイバー攻撃が起こるたびに、サイバーセキュリティに対する顧客の期待は高度化しています。昨年には十分であるとみなされていた対応が、現在では不十分であると酷評される傾向にあります。企業は、その会社または業界が巻き込まれたか否かに関わらず、最新の攻撃から学ぶことを期待されています。

大規模なサイバー攻撃が起こるたびに、サイバーセキュリティに対する顧客の期待は高度化しています。昨年には十分であるとみなされていた対応が、現在では不十分であると酷評される傾向にあります

現実をよく見る

当社の経験およびデータによると、一部の保険会社の意思決定者は、自社が直面するリスクについて十分に理解していないように思われます。KPMGインターナショナルが昨年実施した保険会社のCEOに対する最新の調査によると、自社がサイバー攻撃に対し脆弱である可能性があると考えているのは回答者の49%のみでした。これは危険な思考です。すべての組織はその規模や分野に関わらず、サイバー攻撃に対して脆弱です。

より憂慮すべきであると思われるのは、将来のサイバー攻撃に対して自社に十分な備えがあると考えている保険会社のCEOが54%にすぎないことです。CEOが直面するリスクについて十分認識していると仮定しても（当社の調査からはそうでないことがうかがえます）、このデータからは、多くの保険会社がサイバー計画および対策に関して非常に遅れていることに気付いていることを示しています。

将来のサイバー攻撃に対して自社に十分な備えがあると考えている保険会社のCEOは54%にすぎません

最大の穴を塞ぐ

明るい面としては、保険会社がサイバーリスクを大幅に削減し全般的な備えを強化するために取りうる対策が数多くあることです。

対策の1つは、会社全体のアクセスコントロールを改善することです。実際、過去10年間に起こった膨大な数のサイバー攻撃は、従業員のアクセス認証情報を盗み（フィッシング）、それを使ってさまざまなシステムに侵入すること（最終目標はデータを奪い、意のままになるアクセス権を入手し、オペレーターや「スーパーユーザー」のレベルにまで到達すること）に重点が置かれていました。社内および関連するサードパーティーの双方にわたってアクセスコントロールを強化することで、予想される攻撃のベクトルのかなりの部分をそらすことが可能になると考えられます。

別の明白な対策は、貧弱なシステムおよびソフトウェア管理の問題に集中する傾向があります。実際、より悪質な攻撃の多くは「周知の脆弱性」――最新のセキュリティおよびソフトウェアパッチをダウンロードするだけで（大部分は）全滅できるソフトウェア・セキュリティの隙間――を利用しています。2017年のランサムウェア「WannaCry」による攻撃は、自社のセキュリティをアップデートしなかった組織に被害をもたらしました。

また保険会社は自社のサイバーリスク報告の改善に取り組むことも重要です。現実には、大半のリスクマネジャーや意思決定者は、特定の日や月について自社が直面している実際のリスクのほんの一部分しか目にしていません。報告が各部門で細分化され、リスクの現状のほんの一部しか伝わらない、あるいはサイバー攻撃が引き起こす可能性のある相互依存的なリスクの可能性が無視されることがあまりにも多いのです。第1線防御と第2線防御において、サイバーリスクとその制御について現実的な視点を確実に持つことが、リスク管理にとって不可欠です。

サイバーリスクを組み込む

これらの対策は現在保険会社が直面しているサイバーリスクの大部分を除去するために有益ですが、組織が今後の攻撃に十分な備えを確保するためにはより一層の対策が必要です。

たとえば、保険会社は自社のカルチャーや危機管理カルチャーの中に、一定水準のサイバー意識を組み込むことに取り組む必要があります。すべての従業員がリスクを理解し、警戒強化の必要性を受け入れなくてはなりません。これはある程度、従業員の意識に対する「ペナルティ」アプローチから、従業員がコンプライアンスおよびイニシアティブを示すことに対し見返りが得られるようにする「奨励」アプローチへの転換に関わることです。

またリスクマネジャー、経営幹部、取締役会は、組織がサイバーリスク全体、可能な対策、現時点での「リーディングプラクティス」について、より一層強固な意識を確実に備えるよう取り組む必要があります。業界内、あるいは業界横断的なフォーラムやタスクフォースへの参加は有益な第一歩となります。社内のガバナンスプロセスの向上およびサイバー教育の強化もまた重要です。

リスクマネジャー、経営幹部、取締役会はまた、組織がサイバーリスク全体、可能な対策、現時点での「リーディングプラクティス」について、より一層強固な意識を確実に備えるよう取り組む必要があります

サイバーについて本気で取り組む

保険会社のCEOおよび意思決定者は、絶え間なく発生するサイバーリスクに疲労困憊しているかもしれません。それは理解できますが、言い訳にはなりません。過去数年間の規制の傾向を見ると、顧客データが盗まれた場合、あるいはサイバー攻撃によってシステムが操作不可能な状態になった場合には、組織の幹部が責任を問われることになるであろうことが明白になってきています。十分な対策を確実に講じることは取締役会および経営幹部の責任です。

したがって、もし御社がサイバー攻撃に対する備えが十分でない場合――そしてこの原稿の読者の46%は備えが不十分であると知っています――今がサイバーセキュリティについて真剣に取り組む時です。

寄稿者

Matthew Martindale

KPMG in the UK

E: matthew.martindale@kpmg.co.uk

英国の保険会社および投資マネジメント市場においてKPMGのサイバーセキュリティサービスを主導。2000年にKPMGに入社後、金融、石油・ガス、電気通信、政府機関、製造業、消費財業界の顧客に対するサイバーセキュリティのアドバイスおよび保証業務に主に従事。

James Arnold

KPMG in the US

E: jrarnold@kpmg.com

KPMG米国サイバーサービスグループのプリンシパル。KPMGのサイバー対応業務の主導を支援。国内の保険セクターリーダーでもあります。法律およびビジネスのスキルにより、法的調査、サイバーセキュリティ調査、サイバー保険、データプライバシー、データマッピング、データ識別および修正、サイバー規制、証拠となり得るデジタルデータの復旧などに関する分野で成果を挙げています。

編集・発行

有限責任 あずさ監査法人

KPMGファイナンシャルサービス・ジャパン

financialservices@jp.kpmg.com

この文書はKPMGインターナショナルが2019年3月に発行した「Frontiers in Finance, Issue #60」の「Get serious about cyber」をベースに作成したものです。

翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。