KPMG
cutting through complexity

あずさ監査法人

April 2014

サイバー犯罪：矢面に立つ保険会社

Stephen Bonner（KPMG UK）
Jon Dowie（KPMG UK）
Kevvie Fowler（KPMG Canada）

銀行がより精巧かつ効果的に攻撃から自らを防御するようになるにつれ、多くのサイバー犯罪の焦点が変化し、保険会社が標的となるケースがますます増加しています。このリスクは極めて現実的で深刻なものです。保険会社は喫緊の課題として対策を強化する必要があります。

焦点の変化

アメリカの悪名高い犯罪者であるウィリー・サットンは、銀行強盗に入った理由を聞かれた際、無理もありませんが、「そこには金があるからさ」と答えたと言われています。近年では、インターネット、オンラインの接続性、リモート・アクセスの著しい発展により、銀行は再びサイバー犯罪の標的になっています。銀行には現金があるというだけではありません。銀行は全顧客の重要情報も保有しているため、そのような情報が犯罪者の手に渡れば同様に価値のあるものなのです。ただし、現在では、多くのサイバー犯罪の焦点は、銀行から保険会社へと急速に移行しています。

これには多くの理由があります。おそらく最も重要かつ直接的な理由は、単にこの10年ほどの間に、銀行の防御がより精巧で効果的になったことです。銀行業界はサイバー攻撃の脅威を評価し、対抗策を講じてきました。主な措置としては、何重もの技術的な保護を実装し、さらには情報交換を行い、強力な対抗策をともに開発するために、銀行業界全体が（最終的にはすべての銀行が直面する課題への）協力しました。あらゆる攻撃を防ぐことが不可能なのは明らかあり、当然のことながら、各銀行は、損失をもたらすそのような企てを公表することには消極的です。しかし、一般的には、銀行はサイバー犯罪を効果的に撃退するようになりました。

もう1つの主な要因は、サイバー犯が、儲けの標的になりうるのは銀行だけではないと気づいたことです。確かに現金があるのは銀行です。しかし、保険会社から現金を盗むことも可能です。さらに、入手できる高価なものは現金だけではありません。保険会社は、保険料率算定

表、保険金請求、事故・損害情報を守る必要があります。ほぼ同等の価値があるのは、顧客の詳細情報（個人情報、氏名、住所、口座明細、パスワード、健康・ライフスタイルに関する情報、カード情報等）で、当該情報は現金を得るために悪用されるか、同様の犯罪を目論む他の犯罪者に売られる可能性があります。

加えて、保険会社は銀行に比べて、顧客との親密なやり取り、および頻度も極めて少ないのが一般的です。近年では銀行と顧客の関係が希薄になっているとはいえ、一般的に銀行と顧客が、週または月に何度も取引をしていることは依然として事実です。対照的に、保険会社は保険金請求がある場合、または生命保険会社については顧客が退職または死亡した場合のみ、顧客とのやり取りが生じます。この顧客との疎遠な関係は、潜在的な不正または犯罪的な攻撃の特定に、保険会社が極めて不利な立場にあることを意味します。さらに、保険会社を狙う犯罪の企ては、銀行を狙う場合に比べまだ一般的ではないかもしれませんが、成功した場合のリターンがはるかに莫大になる可能性があるのです。銀行のカードやクレジットカードの情報を漏洩することで数百万ドルを得られる可能性があるのに対して、不正な保険金請求に成功すると桁違いの金が手に入るかもしれません。単純な金銭的メリットが唯一の動機というわけではありません。以下で見るように、保険会社は、多数の金融サービス会社とともに、複数の課題に直面しています。

保険会社は、新たなオンライン・チャンネル、ソーシャルメディア、テレマティックスおよびウェブベースの支払請求管理システムを通じて、大量の顧客データを蓄積するようになったため、サイバー犯にとって保険会社はますます魅力的な対象となっています。2012年、米国の保険会社は、重大なセキュリティ侵害により、110万人の保険契約者と潜在顧客に被害を及ぼしました。ハッカーは、氏名、社会保障番号、免許証番号、出生日情報を盗み出しました。保険会社は迅速に対応し、被害者に対して信用状況の監視（credit monitoring）と、なりすまし犯罪からの保護（identity theft protection）のサービスを提供しました。これには、なりすまし犯罪に対する保険補償（控除免責条項なし）の無償提供に要した100万米ドルが含まれます。別のケースでは、グローバルに展開する保険会社に対して、顧客の個人情報の紛失を防止するための十分なシステムと統制を整備していないとして、220万英ポンドの罰金が科されました。

脅威の理解

この脅威を理解し（かつ当該脅威から保護）するためには、サイバー犯罪の種類を理解することが重要です。

- **組織犯罪**：サイバー犯罪の脅威は比較的限定されており、少額の利益を得たいという出来心から生まれると考えたくなるかもしれません。しかし、近年の事例は、極めて高度な組織犯罪のグループが、金融サービス会社、そして最近では特に保険会社へのサイバー攻撃に本腰を入れるようになったことを決定的に示しています。これらのグループは緻密で冷酷な犯罪グループです。彼らは、会社のネットワークに自動でインストールされる破壊工作ソフトやボットネットを用いて、セキュリティ情報を漏洩したり、重要情報を社外に送信したり、社内のネットワークを外部のサイバー犯の支配下に置き「奴隷化」してしまいます。

  組織犯罪のネットワークはまた、実際には何も盗む必要がないことに気づき始めています。標的とする組織から実質的には身代金ともいえる金銭を引き出すには、単に、損失（または経営上のダメージや混乱）が生じるかもしれないという脅威を与えるだけで十分なのです。繰り返しますが、多くの会社は攻撃を受けたことを公表するのに消極的です。むしろ、要求された金銭を密かに支払ってきた場合が多いのです。

サイバー犯罪組織がまき散らす破壊工作ソフトの逆行分析から、犯罪ネットワークが焦点を当てている標的の種類を解明することは可能です。昨年あたりからは、次第に保険会社が標的になりつつあるという証拠が出てきています。

オンライン上での保険契約の購入が急速に拡大したことにより、組織犯罪の大きなチャンスとなりました。低価格に惹かれる顧客が合法的な保険会社と不正な保険会社を見分けることは困難です。インターネット上に開設された「実態のないブローカー」が、偽の保険商品を売り、保険料を徴収するものの、保険補償なしに「保険契約者」を置き去りにする事態が多発しています。

- **軽犯罪者**：用語が示すように、軽犯罪者は、セキュリティを侵害し、報酬を引き出そうとする、ありとあらゆる機会を標的とします。軽犯罪者は、標的及び手口の両方において比較的無差別であり、容易に攻撃可能な、修正プログラムのないシステムや、誤った設定のシステムといった、多くの場合、単に分かりやすい脆弱性を狙っています。現在、保険業界は近代化しつつあり、多くの保険会社が、顧客が自分で保険契約を管理できるポータルを立ち上げています。軽犯罪者はこの事実を知っているため、攻撃するために、脆弱な部分を探知する特別なソフトを用いて、そのようなポータルをスキャンすることが可能です。犯罪者を次の標的へと移行させる簡単な方法は、システムに分かりやすい脆弱性が存在しないよう徹底することです。組織犯罪に巻き込まれる場合に比べて、さらされるリスクは少ないのかもしれませんが、軽犯罪者による脅威（そして、失敗に終わったとしても、それにより引き起こされるおそれのある混乱）は重大である可能性があります。

- **国が支援するサイバー犯罪**：特定の国においては、脆弱な西洋の企業から現金またはデータを引き出すために、または、より広範な組織的攻撃の一環で当該企業を脅迫・要求できる能力を保持するために、高度な技術的機能を開発・保持していることは疑いの余地がありません。

  従来の電子スパイ活動、商業スパイ活動、商業的・戦略的メリットを得るためのデータの窃盗の線引きは曖昧です。国境を越えた合併・買収（M&A）取引において、複数の国が商業スパイ活動に関与していたことを示す証拠があります。保険会社は（西洋の多くの他の産業セクターとともに）、これらのすべての危険に対して脆弱です。

- **「ハクティビスト」とテロリスト**：現金とデータを違法に引き出すことだけが、サイバー犯の動機となるのではありません。いわゆる「ハクティビスト」、テロリスト、およびその他の犯罪者を犯罪に駆り立てる動機は、会社の経営能力を混乱させたい、損害を与えたい、または破壊したいという欲望も含めて、多岐にわたるのかもしれません。この場合、予測はほぼ不可能なため、この脅威を未然に防ぐことはなおさら困難です。ただし、このような活動に関与するような多くの犯罪グループは、間接的な犯罪に対して、特に興味を持つことが示されています。例えば、製薬会社、動物実験を行う研究所、防衛関連企業等と取引のある保険会社は、この方面からサイバー攻撃犯罪の標的となる可能性もあるのです。

どう対処するか

まず、明らかに優先すべきは、最新の脅威の性質を認識することです。保険会社は歴史的に、人員を動員して、広範に病気・事件の発生パターンを分析し、特に懸念がある場合は個々の事例を調査することにより、不正な支払請求に対して自らを守ろうと模索してきました。しかし、今日の脅威は財務上の損失のリスクだけではなく、財務上と評判の両方にダメージを与えるおそれのある、システムとプロセスの崩壊というリスクがあります。カナダ金融機関監督局（OSFI）は近年、金融機関が、サイバー攻撃に対する準備と保護のレベルを自己評価

する方法についてガイダンスを公表しました。[1] また、保険会社は脅威と成功事例について情報を共有する体制およびプロセスを構築することにより、銀行セクターの成功からも学ぶことができます。

次に、保険会社のバックオフィスの技術とシステムは、銀行で日常的に使用されているものの一世代以上前のものであることは明白です。異なるシステム間の接続性と調整が欠如しているため、侵害や流出の企てを特定し、対抗する能力が劣っています。自動化されている部分が少ないこと、手作業が多いこと、また情報処理プロセスにおいて未処理(break)となる件数が多いことは、潜在的な脆弱性を増加させます。支払請求の処理を外部に委託した場合、セキュリティの監視はさらに困難になるおそれがあるため、委託先管理をより効果的にする必要があります。Proofpoint Inc.の最新の調査によると、保険会社は現在、他の産業セクターに比べて多数の、電子メールによるセキュリティの脅威に直面しています。[2] 実際に、KPMGの「データ損失のバロメーター」(2012年)では、保険セクターは、社会工学的な攻撃・システムおよび(または)人為的ミスによるリスクが最も高い状態であると説明されています。別のKPMGの調査では、金融サービス会社は、業界の中でもソフトが最も脆弱であることが示されています。[3] 費用はかかりますが、システムのアップグレードが必要です。

最後に、おそらく最も重要なことですが、保険会社は揺るぎない効果的な対応を構築する方法を理解する必要があります。脅威はすべて極めて現実的なものですが、知的で緻密に行動することにより対抗しなくてはなりません。これには、サイバー攻撃に対する純粋な技術的準備だけでは不十分です。脆弱なエリアの理解、改善すべき領域の特定・優先、会社およびオペレーション両方のコンプライアンス担当への説明を行うために、人・プロセス・技術を組み合わせた視点から、情報リスクをビジネス上のメリットに変える必要があります。我々の経験によれば、これは主に以下の6つの側面において行動することを意味しています。これらの側面は合わせて、組織におけるサイバー面での成熟度についての包括的かつ詳細な視点を提供します。[4]

リーダーシップとガバナンス

リスクに関する適正な評価、オーナーシップおよび効果的な管理を示す取締役会。

情報のリスク管理

組織全体で包括的かつ効果的な情報のリスク管理を実現する取組み、およびそのリスク管理の普及・提供に共に携わる人材。

運用と技術

特定されたリスクに対処し、情報漏洩の影響を最小限に抑えるために実施される統制措置の水準。

人的要因

適切な人材、スキル、行動(思考)方法および知識が認められ、また確保されるセキュリティ文化の水準と統合。

---

1 サイバーセキュリティの自己評価に関するガイドライン(Cyber Security Self-Assessment Guidance)、カナダ金融機関監督局、2013年10月28日、http://www.osfi-bsif.gc.ca/Eng/Docs/cbrsk.pdf

2 Proofpoint、脅威への洞察:貴社は標的にされているか(Threat Insight:Are You Being Targeted)、第1部:産業、Poofpoint Inc. http://www.proofpoint.com/threatinsight/posts/are-you-being-targeted-part-1-industry.php

3 KPMG、英国におけるサイバー面の脆弱性インデックス(UK Cyber Vulnerability Index)2013年

4 KPMGのサイバー面の成熟度評価(UK Cyber Maturity Assessment, CMA)は、情報資産を保護する組織の能力およびサイバー攻撃への準備に関する詳細な検討を提供しています。参考:KPMGサイバー面の成熟度評価:貴社のサイバー脅威、2013年5月

事業継続性と危機管理

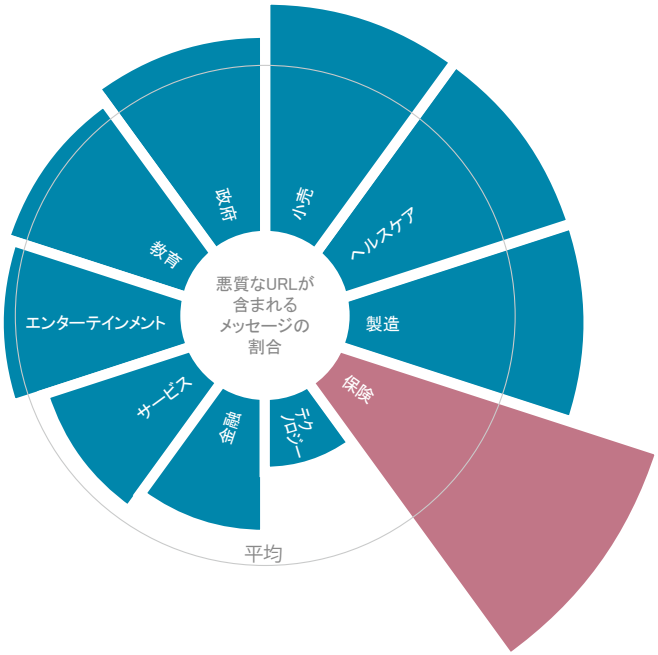
セキュリティを脅かす事象への準備および適切な危機・利害関係者の管理を通じて影響を阻止あるいは最小化する能力。

法務とコンプライアンス

関連する、規制上および国際的な認証基準。

銀行部門は、サイバー犯罪による脅威に阻止・対抗できることを示してきました。保険会社は、銀行に匹敵する防御を確実に整備できるよう、緊急に対策を強化する必要があります。

保険業界は、より多数の電子メールによる脅威に直面しています



出典：www.proofpoint.com/threatinsights

詳細情報の入手先

Stephen Bonner
KPMG UK
電話：+44 20 7694 1644
メール：stephen.bonner@kpmg.co.uk

Jon Dowie
KPMG UK
電話：+44 20 7311 5295
メール：jdowie@kpmg.com

Kevvie Fowler
KPMG Canada
電話：+1 416 777 3742
メール：kevviefowler@kpmg.ca

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
e-Mail: financialservices@jp.kpmg.com

この文書はKPMGインターナショナルが2014年4月に発行した「Frontiers in Finance」の「Cyber crime: Insurers in the firing line」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。