ISMSやCSIRTの機能を有機的に取り込み、情報セキュリティガバナンスを構築せよ

近年、大規模な個人情報漏えい事故が多発しており、企業における情報セキュリティ対策が社会的な関心事項となっている。一方で、2015年6月1日、東京証券取引所が上場企業に対して、コーポレートガバナンスの実現に向けた主要原則となる「コーポレートガバナンス・コード」の適用を開始した。デロイト トーマツ リスクサービス マネジャーの森島直人氏は、個人情報管理のさらなる強化を前提とした上で、「情報セキュリティについても、コーポレートガバナンスの向上が社会的に求められるようになってきている」と指摘、「現在の企業には利害関係者に対する情報開示を意識した情報セキュリティ態勢を構築し、運用していくことが求められている」と強調する。

デロイト トーマツ リスクサービス
マネジャー
森島 直人 氏

ガバナンスの中心となるのは“外部統制(＝モニタリング)”

まず森島氏は、「ガバナンスは3つの構成要素から成っている」と説明する。1つめがコントロール、2つめがマネジメント、3つめがモニタリングだ。

1つめのコントロールは管理策と呼ばれるもので、業務上してはいけないこと、あるいはしなければならないことを定めた具体的なルールのことだ。次にマネジメントは、たとえばリスクを評価して、ルールの維持管理をしていく仕組みのこと、そしてモニタリングは、組織外の利害関係者が、企業のルール及びその維持管理体制を継続して監視する仕組みのことだ。

現在では経営者が結果責任を問われやすい環境にあり、攻めの経営判断を下すことが非常に難しい状況だ。たとえば収益拡大のために新しい個人情報の収集を伴う事業を開始する場合や、コスト削減のためにクラウドサービスやBYODの導入を検討する場合、情報漏えい時の結果責任追及を想定してやっぱり止めようという話にもなりかねない。

「そこで普段から利害関係者と積極的なリレーションを構築しておくことで、自分たちの情報セキュリティに対する考え方を伝えると同時に、それに対してフィードバックをもらってセキュリティ対策に反映していくことも可能となる。それが企業価値の向上と、有事における企業価値の毀損を低減していくことになり、ひいては経営者を結果責任から守ることにも繋がる。そのためにも利害関係者を巻き込んでいく必要がある」

情報セキュリティにおけるガバナンスの仕組みは、3つの軸で整理する

企業と利害関係者とのリレーションにおいては、企業には、自社の「状況を伝える」ことと、利害関係者からの「要請を把握する」ことの2つの取り組みが求められることになる。

「伝えることについては、特に経営戦略や経営課題、あるいはリスクやガバナンスに関わる情報などの“非財務情報”について積極的、主体的に開示していくべきだとコーポレートガバナンス・コードに記されている。一方、要請を把握していく内容については明記されていないが、基本的には利害関係者の要望に応えていくことになる」

情報セキュリティにおけるガバナンスのあり方を考えるためには、利害関係者とのリレーションを、状況を伝える／要請を把握するという軸、平時か／有事かという軸、利害関係者の種類という3つの軸から整理していくことが重要となる。特に社内体制は、状況を伝える／要請を把握する、有事か／平時か、の2軸で考えることで整理するのがよいだろう。

企業が行う情報セキュリティ対策のフレームワークとして、ISMS(情報セキュリティマネジメントシステム)がある。リスクとコストのバランスを取りながらセキュリティレベルを最適化していくための仕組みで、ISMS適合性評価制度の要求仕様であるISO/IEC 27001:2013や、ISMSに関するベストプラクティス集であるISO/IEC 27002:2013といった標準規格がある。

「ISO/IEC 27001:2013では、Planのフェーズでリスクの把握と対応策の策定を実施する際、利害関係者の情報セキュリティに関する要求事項をインプットとして把握するよう求めている。また、Checkのフェーズでも、マネジメントレビューにおいて利害関係者からのフィードバックを考慮するよう求めている。つまりISMSの規格の中にも、ガバナンスに関する要求事項が入っているということ」

こうしたISMSの要求も考慮して、企業には利害関係者の要請を一元的に把握する仕組みを構築することが求められる。

たとえば株主なら経営企画部、個人顧客ならコールセンターなど、企業内には各利害関係者からのフィードバックを受ける様々な部署があるが、それらに集まる情報を一元的に集約し、情報セキュリティ部や品質管理部など関係各所に伝えていく体制が必要だ。

CSIRTの活動では、情報開示の仕組みを作っていくことが大事

現在、発生したインシデントによる影響を最小限に抑えるために、CSIRT(Computer Security Incident Response Team)の設置を検討する企業が増えている。CSIRTでは、被害を受けることを前提として、インシデントの発見直後から終息までの損害額を最小化することを主なミッションとする。ISMSのような標準規格はないが、一般的に日常的活動、インシデント対応、事後活動という3つの機能を提供する。

このうち中心となるのがインシデント対応だ。検出と報告 → トリアージ(＝対処すべきインシデントの優先順位付け) → 意思決定と対処という3つのステップで行い、状況に応じてトリアージ、意思決定と対処の2つのフェーズを繰り返す。

そのインシデント対応の前段階として日常的活動があり、何か起きた時にすぐに動けるようなルールや体制作りなどを行う。そして事後活動では、原因究明やインシデント対応時の手順の見直しなどを行い、日常的活動やインシデント対応にフィードバックしていく。

「ISMSは、平時に利害関係者からの要請を把握する機能を持っている。一方、CSIRTは有事の際に、自社の対応状況を伝える役割と、利害関係者からの反応をキャッチする役割も果たすものだ。情報セキュリティにおけるガバナンスを強化していく上では、こうした仕組みを機能の一部として認識し、有機的に取り込んで全体的な構成を設計することが重要だ」

なぜリスクを開示するべきなのか、利害関係者とのコミュニケーション手法とは

コーポレート・ガバナンスの重要な要素の1つとして、外部の利害関係者への情報開示がある。たとえば最近、有価証券報告書に、わざわざ事業関連リスクとして情報漏えいやウイルス感染のリスクを記載する企業が増えてきているという。なぜリスクをわざわざ開示する必要があるのか。デロイト トーマツ リスクサービス シニアマネジャーの北野晴人氏はリスク開示の果たす役割を明らかにするとともに、インシデントが発生していない平常時に、企業が各利害関係者に対して、どのような方法で情報を開示していけばいいのかについて解説した。

デロイト トーマツ リスクサービス
シニアマネジャー
北野 晴人 氏

リスク管理の一環として求められる情報開示

一般的に情報セキュリティ対策に必要なコストは、直接的な利益を生み出すものではない。とはいえ万一リスクが顕在化した時の影響が大きい場合には、相応のコストを投下して、受容可能なレベルにまでリスクを低減しておく必要がある。企業が成長戦略を採る時には、今までになかったリスクが発生する。いわば"利益を生み出すために取るべきリスク"だ。

「その時に、どこに、どのようなリスクがありそうなのかをまったく知らずに取り組むのは、知らない道をブレーキのない車で走るようなもの。自社の成長戦略の中にどのようなリスクが潜んでいるのかを考えた上で、実行していく必要がある。情報セキュリティに対するリスクは、実はこの成長戦略に伴うものである場合が重要である。そこでリスク管理の一環として、情報セキュリティに対するリスクも開示していくことが必要となってくる」

それではなぜ、情報を開示することがリスク管理に繋がるのか。

「企業は、株主／法人顧客／個人顧客といった利害関係者とのコミュニケーションによって"情報の非対称性"を緩和しなければ、せっかく成長戦略を採っても、市場そのものが成長に向かわなくなる恐れがある。」

利害関係者に提供すべき3つの情報

利害関係者のうち、まず株主は投資判断に影響を及ぼす情報、もしくは情報セキュリティの株価の対する影響に着目している。次に法人顧客は、取引上の必要性から自社が提供している機密情報がきちんと保護されているか、また個人顧客は自分の個人情報がきちんと守られているかを注視している。

「利害関係者に提供すべき情報は、大きく3つの観点から分類できる。1つめが"リスクの所在"で、どこに、どのようなリスクが、どれぐらいの大きさで存在しているのか。2つめが"リスク管理の取り組み"で、そのリスクをコントロールするために、自社がどのような取り組みをしているのか。そして3つめが"モニタリングと継続的改善"で、その取り組みによってどのような効果が出ているのか。各利害関係者の関心事に応じて、これらの情報を届けていくことが重要だ」

1つめのリスクの所在については、自社が行っている事業に対して、特に影響が大きいと思われるリスクを2つか3つ程度特定して、それが事業にどんな影響を及ぼすのかを開示しておくことが重要だ。

2つめのリスク管理の取り組みを行うに当たっては、リスクを網羅的に管理するためのフレームワークとしてISMS（情報セキュリティマネジメントシステム）が有用だ。ISMSでは、リスク管理責任者は誰か、従業員にどのような教育を施しているか、物理的な対策はどうか、技術的な対策はどうかなど、組織／人／物理／技術の各観点から求められる安全管理措置を明らかにしている。さらに前向きな姿勢を示すためには、インシデント発生後の対応に当たるCSIRT（Computer Security Incident Response Team）の活動を取り上げることも有効だ。

そして3つめのモニタリングと継続的改善については、リスク管理の取り組みをどうやってモニタリングして、継続的に改善しているかを伝えていく。具体的には、どのようなリスクが顕在化しているのか、また実際の対策によって事故がどれだけ減ったのか、あるいは増えたのか。また増えたなら今年は新たにどのような対策を取るのか。

「ここで大事なのは、各利害関係者に届く情報は、広報から、営業担当者から、個人窓口からというように別々のルートを通っても、一元化したソースから発信され、同じ情報が開示、提供されるということだ。相手によって表現の仕方や情報の深さが異なることがあっても、伝わる情報の内容には齟齬がないようにしておく必要がある」

利害関係者に対する情報開示は既存の枠組みの中で考える

それではこうした平時の情報セキュリティ管理に関する情報開示を、どのような手段によって行えばいいのか。

「まずは既存の枠組みで情報を伝えることを考える。1つが有価証券報告書、そしてもう1つがコーポレート・ガバナンスに関する報告書だ」

現在では内閣サイバーセキュリティセンター（NISC）が事務局を務める情報セキュリティ政策会議が、上場企業におけるサイバー攻撃によるインシデントなどを事業リスクとして投資家に開示することを検討しており、今後有価証券報告書でより具体的な情報開示が求められる可能性もある。

また企業の取り組みが顧客や投資家などのステークホルダーから適正に評価されることを目指すものとして、経済産業省が策定した「情報セキュリティ報告書モデル」がある。

コーポレート・ガバナンスに関する報告書も、情報開示の1つの手段として挙げられる。これは上場企業に対して、東京証券取引所からコーポレート・ガバナンスの状況を投資者により明確に伝える手段として要請されるもので、この中にリスクに対する取り組みを記載して、開示をするという方法も採ることができる。

「まだ現在では情報セキュリティリスクに対して、既存の枠組みを使って情報開示をしていく標準的な方法が確立されているわけではない。ただ2015年5月にNISCが公開した『サイバーセキュリティ戦略（案）』では、サイバーセキュリティを経営上の重要課題として取り組んでいることが、ステークホルダーから正当に評価される仕組みなどを構築することが謳われている。今後、こうしたものも踏まえて、徐々に標準化されていくだろう」

情報セキュリティ事故のときの情報開示方法は、3つのフェーズに分けて考える

情報セキュリティインシデントの発生時には、事件・事故を起こした企業に対して、外部のさまざまな利害関係者から「知りたいこと」が噴出する。デロイト トーマツ リスクサービス シニアマネジャーの亀井将博氏は、「インシデント発生時の情報開示は、3段階で考える必要がある。また自社の状況を伝えるだけでなく、利害関係者から寄せられる要望を把握しようという姿勢も重要だ」と指摘する。そのために日頃から企業に求められる取り組みとは、どのようなものなのか。

デロイト トーマツ リスクサービス
シニアマネジャー
亀井 将博 氏

インシデント発生時には、適切な情報開示と伝達方法が求められる

インシデントの発生時、利害関係者のうち株主なら、短期的および中長期的な企業価値への影響が最大の関心事となる。顧客企業なら、業務取引上、提供している自社の情報は安全か、契約そのものを継続しうるのかを判断できる情報の入手が最優先となる。そして個人顧客は、自分の情報が漏れていないか、もし漏れていたならどんな被害を受ける可能性があるのかを知りたいと考える。誠意ある謝罪も大きな関心事だ。

「各利害関係者で知りたい情報は異なっているが、必ず伝えるべき内容とその方法の適切性については共通している。内容については、被害の範囲と事故の原因を適切に開示することが重要で、方法については発表のタイミングや誰が記者会見を行うのかなどがポイントとなる」

特に亀井氏は伝える内容について、インシデントの発生直後は、徹底的に被害者にフォーカスを当てた情報開示が重要だと強調する。

「つまり被害を拡大させないようにしている姿勢を見せることが非常に大切だ。それが引いては会社を救うことにもなる。」

日頃から有事に備えた情報開示の態勢作りをしておかなければ、いざという時に適切な対応を採ることができない。そこで有効となるのが、CSIRT（Computer Security Incident Response Team）だ。

インシデント発生時の情報開示は、3段階で考える

CSIRTは、インシデントの発生を前提として、情報開示の整備や訓練などの日常的活動、実際のインシデント発生時の対応、証跡分析や原因究明などの事後活動を行うインシデント対応チームだ。

中でもCSIRTの中心的な活動となるのがインシデント対応で、このフェーズではインシデントを検出してトリアージ（＝対処すべきインシデントの優先順位付け）を行った後、抑制→除去→回復というステップを踏んで、事件・事故の終息を目指すことになる。

まず1つめの抑制のフェーズでは、被害の拡大を抑制しようとしている姿勢を見せることが大切だ。もしサービスを継続し続けると個人情報の漏えいがさらに進んでしまうかもしれない場合には、売上を諦めてサービスを停止する。その判断を迅速に行うためには、あらかじめ想定されるインシデントを明らかにし、その際にどんな対応を採るのかを決めておく必要がある。

また有事／平時を問わず、各利害関係者に伝える情報は首尾一貫していなければならない。そこで次にポジションペーパーを作成する。ポジションペーパーとは、有事の際に何を言うのか、何が言えるのかを整理したものだ。その後、告知・速報を行うが、これは基本的に被害者に向けた情報開示で、また今後被害に遭う可能性のある人たちに向けた警戒情報も含まれる。

抑制のフェーズが一段落ち着いたら、次は2つめの除去のステージでお詫び・釈明を行う。ここでは単にお詫びや釈明をするだけでは不十分で、現在の状況を説明できなければならない。

そして3つめの回復のフェーズでは、まず再発防止策の策定とその公表を行い、そしてサービス再開を告知する。

企業には利害関係者の要望を把握するための取り組みも求められる

一方インシデントの発生時には、自社から利害関係者に対して情報を開示するだけでなく、利害関係者からの要請を把握することにも関心を払わなければならない。特に個人顧客の論調を能動的に把握することは重要で、今の時代はソーシャルメディアに記載されている情報には十分な注意が必要だ。

「たとえば異物混入が発生した時、今の消費者はお客さま相談室に連絡すると同時に、その状況を画像と共にTwitter上に投稿したりする。企業側では今受けたクレームが同時、即時に公開されているかもしれないということを念頭に置いて対応しなければならない」

その際に有用となるのが、デロイト トーマツ リスクサービスが提供する「Webモニタリング アラート」というサービスの中の「バズアラート」だ。いわばTwitter上の論調確認ができるもので、たとえば「トーマツ　デロイト」という文字列を設定しておけば、24時間Twitter上の投稿を監視して、投稿数の急上昇があった場合にはアラートを上げてくれる。

先にCSIRTの活動の1つとして日常的活動を挙げたが、この中の取り組みとして情報開示の整備や訓練がある。インシデント発生時の情報開示に備えて、常日頃から情報開示に向き合っておく必要があるということだ。

この時に有用なツールとして、リスク評価の成果を表したリスクマップがある。横軸が発生可能性スコア、縦軸がインパクトの大きさを示し、横軸を右に行くほど発生確率が高い／対策が弱いインシデント、また縦軸を上に行くほど、発生時のインパクトが大きいインシデントということになる。

「必ずこうしたリスクマップを使ってくださいということではなく、組織内での意識の共有が非常に大事だということ。意識の共有がなければ、インシデント発生時に迅速に行動することはできない。また自社の現在のガバナンス機能を知る上では、以下のようなチェック項目で自己採点することも有効だ」

※本記事は、2015年7月30日に掲載されたビジネス+ITからの転載です。

お問い合わせ先

Deloitte.
デロイト トーマツ

デロイト トーマツ リスクサービス株式会社
〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル
Tel:03-6213-1300　URL：www.deloitte.com/jp/dtrs