日本企業の
情報セキュリティ予算の捉え方

– コストセンターか、または戦略的投資か –

2017年度　情報セキュリティリスク調査
Kaspersky Lab

目次

はじめに

サイバーセキュリティを取り巻く状況は進化し続けており、世界中の企業では常に自社をその状況に適合させる必要に迫られています。企業にとっては分野や規模に関係なく、セキュリティはますます IT 予算の重要な部分になりつつあると考えられます。

Kaspersky Lab が実施する企業の情報セキュリティリスク調査（Global Corporate IT Security Risks Survey）は、世界中の企業の情報セキュリティ状況に関する年 1 回の調査です。7 年目となる今回の調査では、これまでの調査結果を基に、情報セキュリティへの支出、企業が直面する脅威、およびこの脅威のターゲットになることによる財務的影響に関して質問をしています。さらに今回の調査では、脅威の変化に企業がどのように対処しているかについても調べるために、企業の意思決定者に情報セキュリティ予算への意識について質問をしています。

今回の調査で重要な質問は、企業では情報セキュリティをコストセンター（仕方なく支払っている避けがたい害悪）と見なしているのか、それとも戦略的投資（拡大しつつある脅威に直面した状況において、事業継続に重要で大きなメリットが得られる要素）と見なしているのかということです。

この質問が重要である理由は、調査において IT 予算が世界規模で圧迫されていることが判明したためです。IT 予算に占める情報セキュリティの割合は、2016 年の平均 17 % から 2017 年の 20 % まで増加している一方で、これを金額に直してみると、大企業における昨年の情報セキュリティ予算の平均は 2,550 万ドルに達していましたが、今年はわずか 1,370 万ドルと大幅に減少しています。

脅威は拡大し続けているにもかかわらず、情報セキュリティチームはより少ない予算で対処しなければならないという問題に直面しています。IT 予算が全体的に減少する一方、インシデントの数は増大しつつあり、世界中の企業ではいずれ脅威に対する保護が重要な問題となる可能性があります。この状況下で成功するために重要なことは、情報セキュリティの支出に対する企業の意識です。このレポートでは、大企業および中小企業が直面している脅威、そして情報セキュリティの支出に関する傾向について紹介しています。

調査の対象

Kaspersky Lab が実施した情報セキュリティリスク調査は、企業の IT 意思決定者に対する世界規模の調査であり、2011 年から年 1 回実施しています。最新のデータは 2017 年 3〜4 月に実施したもので、30 か国におよぶあらゆる規模の企業に勤務する合計 5,274 人を対象に実施しました。レポート全体を通して、企業規模を示す用語として 零細企業（従業員が 50 人未満の非常に小規模の企業）、中小企業（従業員が 50〜999 人の小規模および中規模の企業）、および大企業（従業員が 1,000 人以上の企業）を使用しています。このレポートには、全調査結果が記載されているわけではありません。日本の回答者は、中小企業と大企業に勤務する合計 224 名です。

日本における主な調査結果

- あらゆる規模の企業において、サイバー脅威への対処がさらに困難になり、そのコストが増大しつつあります。中小企業でのデータ侵害による平均的な影響の合計は 9 万 2,000 ドルでしたが、大企業ではこの 10 倍を超える 130 万ドルでした。
- 情報セキュリティに費やされる IT 予算の割合は増大しています。このことはあらゆる規模の企業に一貫して見られる傾向ですが、特に従業員が 1,000 人以上の大企業では、IT 予算の中で情報セキュリティの予算が、2016 年の 19 %から 2017 年は 26 %に増大しています。
- データ侵害の復旧コストが増大しているため、情報セキュリティへの支出を優先していない企業では、いずれ保護が重要な問題になる可能性があります。実際に当調査では、中小企業がデータ侵害を受けた際に平均 1 万 4,000 ドルの損失被害を受ける場合がある一方、大企業では信用格付けの下落 / 保険料の上昇へ対処するために平均 21 万 1,000 ドルを支出しています。
- 情報セキュリティへの支出を増大する理由として、株主/投資家（8 %）、顧客（17 %）を含む主なステークホルダーからの要求を挙げています。このことは、企業が情報セキュリティへの支出を最低限の戦略的投資と見なしていることを示しています。今年に入って、多数の企業が ROI には関係なくサイバーセキュリティに投資していることを認めており、その割合は 2016 年の 45 %と比較して 2017 年は 58 %と増大しています。

情報セキュリティインシデントのコスト

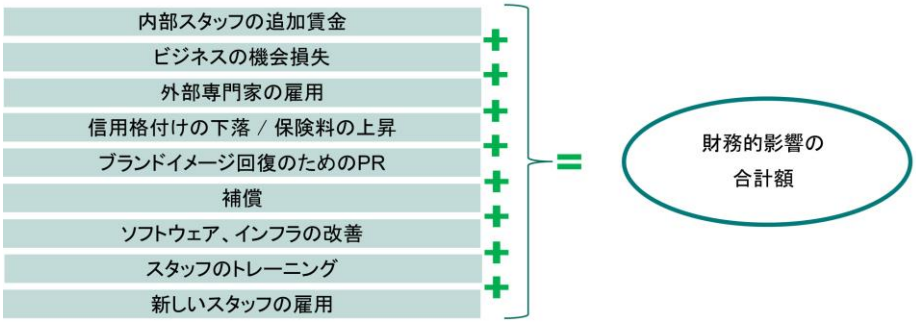
サイバーセキュリティインシデントのコストは変化しており、企業は侵害の影響として複数の考慮すべき事項（PR から新しいスタッフの採用に至るまで）に対処する必要があります。今年に入ってから、データ侵害の財務的影響が引き続き拡大しており、企業がサイバーセキュリティへの支出をコストセンターと見なしているのか、または攻撃による金銭的な著しい不利益を回避するための投資と見なしているのかによって、波及効果が変わります。

重大なデータ侵害にかかるコストの増大

企業の意思決定者を不安にさせる攻撃、例えば英国の NHS、米国ソニー・ピクチャーズ エンタテインメントに対する攻撃、または 米国放送局 HBO で発生したゲーム・オブ・スローンズに関する部外秘ファイルの漏洩などは非常に大規模であり、中には何百万という記録が含まれていました。ただし、これらの攻撃は例外的で、企業に対するサイバー攻撃の大部分はメディアのトップ記事になりません。専門メディアでは報道される可能性もありますが、たいていは気付かれることもありません。

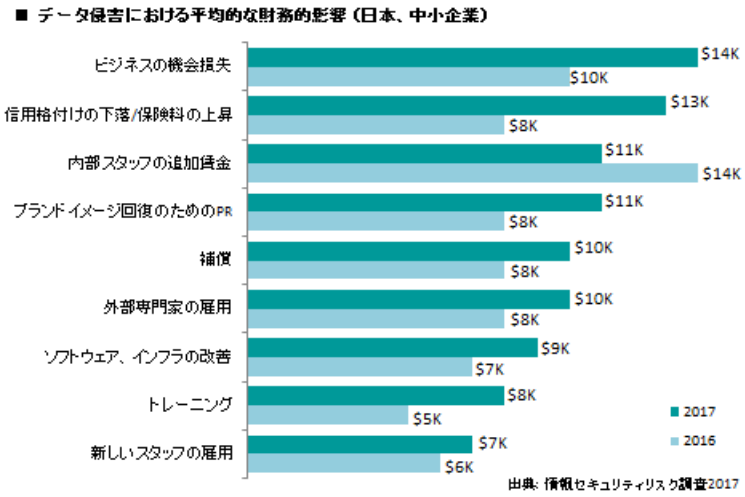
大規模な攻撃が見過ごされる場合がありますが、大部分を占める小規模な攻撃では、企業は極端なダメージを受ける可能性があります。それでは、「典型的な」データ侵害に対して企業が見積もるコストはどれくらいでしょうか。当調査では、最近 12 か月間に経験したデータ侵害の影響に対して、支出した金額または損失した金額の概算について質問を実施しました。

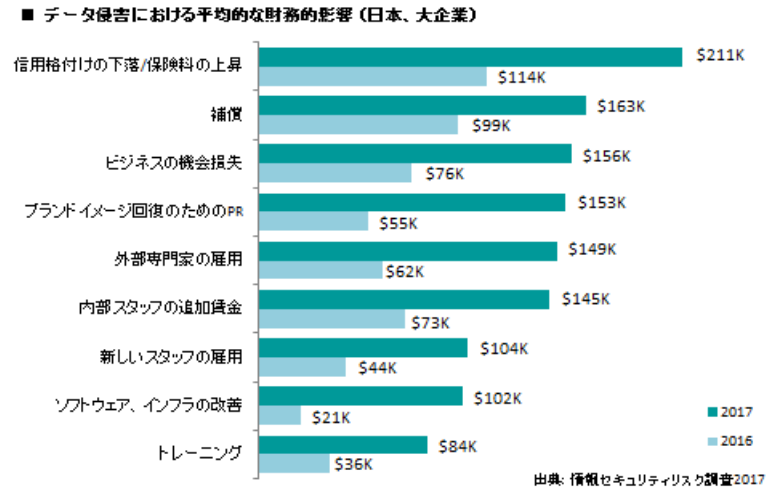
従業員が 50 人以上の全企業に対し、データ侵害の後、以下の各カテゴリで生じたコストの概算を尋ねました。



次に、その金額を合計して組織の財務的影響を算出し、企業全体の平均的なコストを計算して企業におけるデータ侵害の典型的なコストを推定しました。

中小企業 および大企業別の結果を下に示しています。日本では、規模が異なればその状況も非常に異なっていることがわかります。例えば 中小企業 の場合、データ侵害による平均的な影響の合計金額は 9 万 2,000 ドルに達していますが、大企業ではこの金額の 10 倍超の約 130 万ドルでした。この結果は、あらゆる規模の企業においてサイバー脅威に対処するにはコストがかかることを示しています。





データ侵害による平均的な財務的影響の合計金額は、中小企業 と比較して大企業の方が大幅に多いことは予想できることですが、コストの内訳を知るのは興味深いことです。

昨年は中小企業と大企業の双方にとって、内部スタッフの再配置による追加賃金が最大のコストでしたが、今年は状況が変化しており、中小企業 と大企業では状況が多少異なっています。日本の中小企業 で上位に挙げられた問題点は、ビジネスの機会損失と信用格付けの下落 / 保険料の上昇に対するダメージです。一方、大企業では信用格付け / 保険料へのダメージと補償によって多大なコストが発生しています。

さらに大企業では、セキュリティ侵害の影響として特にトレーニングへの支出が増大し、その金額は平均 8 万 4,000 ドルです。企業がセキュリティインシデントを経験した後は、スタッフのサイバー脅威に対する認識を向上させる必要があることに気付きます。

中小企業では攻撃を受けた結果として、特にビジネスの機会損失に対して脆弱で、大企業は社内で高い能力を保有していることから、脅威に対処するための支出と受けるダメージの間の均衡状態が変化します。ただし、補償は重大な問題として残されたままであり、データ侵害あたりの補償金額は平均 16 万 3,000 ドルに達します。

進化を続ける法律の財務的影響

2017 年は、世界全体で大企業のデータ侵害による平均的なコストは 11%増大していますが、このコスト増大の原因は何でしょうか。当調査により、大幅なコスト増大は、信用格付け、PR コスト、補償の観点から、評判の低下を防ぐ必要からくるものであることが判明しました。政府が新しい法律を導入することを急いでいるため、コスト増大は引き続き発生する可能性があります。企業は経験したデータ侵害を公表し、個人情報を保護するための適切な透明性を示す必要があります。

日本では大企業のデータ侵害による平均的なコストは 2016 年の 58 万ドルから 2017 年の 130 万ドルと 2 倍以上に増大しています。日本政府はデータ侵害の問題を認識しており、2017 年 5 月に施行された改正個人情報保護法など、データセキュリティ規制を強化するための対策を講じた結果、関連するコストが急増しています。

法律の立案と制定には時間を要しますが、IT 状況の急激な変化とサイバーセキュリティ脅威の拡大に直面するなかで、これは大きな問題です。日本の多数の企業にとってこの法律が施行されるのが遅すぎたため、その間に注目を集める多数の事件が発生しました。その 1 つの例として、2016 年に旅行代理店の JTB が大規模なデータ侵害を経験し、その結果、ほぼ 800 万人にも及ぶ顧客の個人情報（名前、住所、パスポート番号を含む）が盗まれた事件が挙げられます。これは世界規模の課題の前兆となるケースであり、脅威は急激に拡大しましたが、世界の企業や法律の対応は緩慢でした。別の例として、2018 年 5 月に施行予定の EU 一般データ保護規則（GDPR）は、企業が EU 市民のデータを取り扱う方法を大幅に制限するものです。

世界全体で法律は改定されていますが、サイバー脅威は急激に進化しています。このため、企業は引き続き法律と現実のギャップを意識して、顧客と自社の評判を保護するために、適宜防衛対策を準備しておく必要があります。また、企業は自社データと顧客のセキュリティ対策として、ポリシーを変更するか、期日までに新しい規制に準拠するための検討を開始する必要があります。

自社にもおよぶサードパーティの弱点

さらに重要なことは、サイバー犯罪者が最初の段階でデータ侵害を達成するために使用する、攻撃経路の種別を詳細に調査することです。これは通常、どの種別の攻撃が最もコストがかかるデータ侵害を引き起こすのかを理解するのに役に立ちます。

当調査によると、中小企業の場合、最も重大な経済的影響を受けると予想されるのは、次のインシデントです。

1. サードパーティのホスティングインフラに影響するインシデント（14 万ドル）
2. コンピューティング以外の接続デバイスに伴うインシデント（11 万 2,000 ドル）
3. 内部システムからの電子的なデータ漏洩（11 万 1,000 ドル）
4. 標的型攻撃（10 万 8,000 ドル）
5. サードパーティのクラウドサービスに影響するインシデント（10 万ドル）

一方で大企業の場合、状況は多少似ていますが異なる点もあります：

1. データを共有しているサプライヤーに影響するインシデント（180 万ドル）
2. サードパーティのホスティングインフラに影響するインシデント（160 万ドル）
3. コンピューティング以外の接続デバイスに伴うインシデント（160 万ドル）
4. データの電子的な漏洩（120 万ドル）
5. サードパーティのクラウドサービスに影響するインシデント（120 万ドル）

ここでわかることは、ビジネスパートナーのセキュリティ失策によって引き起こされた攻撃は、あらゆる規模の企業にかなりのダメージを与える場合があることです。このことは、クラウドや他のインフラを通してサードパーティと協力している企業の経験からも明らかであり、サプライヤーとデータを共有している企業の場合にも当てはまります。 別の企業に対して、自社のデータまたはインフラへのアクセス権限を付与した場合は即座に、その企業の弱点が自社の弱点にもなります。ただし、前に説明したように、これは大部分の組織が適切な配慮をしていないために発生することです。

注目すべき別の種別の攻撃として、コンピューティング以外の接続デバイスに影響するインシデントがあります。モノのインターネット（IoT）は、今日のデータトラフィックに関して最も急速に普及している分野であり、企業セキュリティの潜在的な弱点が増大していることを示す別の例です。特に IoT デバイスでは、工場出荷時のパスワードと脆弱なセキュリティ対策が広く使用されていることにより、Mirai のようなボットネットの格好のホストにされてしまいます。このボットネットは、多数の脆弱なデバイスを利用して、大規模な DDoS 攻撃を実施することができます。

コンピューティング以外の接続デバイスでの攻撃を経験したことのある中小企業と大企業では、特に保険料と関連コストが大幅に増大していることも報告されています。保険会社でも、これらの種別の攻撃がもたらすリスクを過小評価している傾向があります。さらに、攻撃に伴う保険料の再評価では、解消するのにコストがかかる企業のセキュリティにおけるギャップも明らかになります。これらのデバイスの弱点が、企業の弱点となる可能性もあります。

リスク低減に対する投資

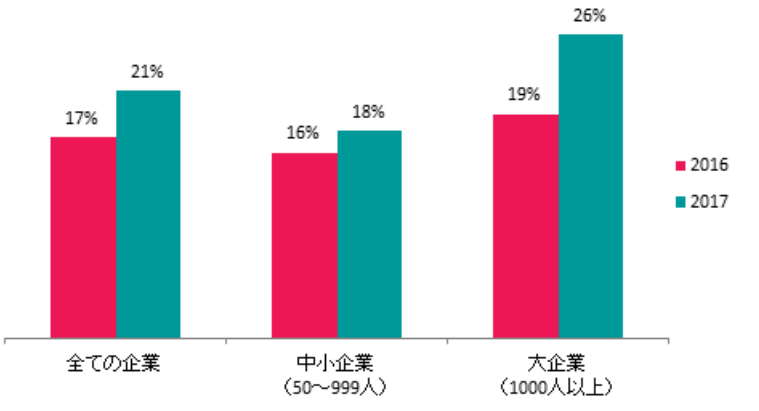
当調査で示しているように、セキュリティ脅威は非常に重要で拡大しつつあります。これらの脅威に直面し、議論の核心が 情報セキュリティをコストセンターと見なしているのか、それとも企業に実際的な価値をもたらす分野であると見なしているのかという場合、それは 情報セキュリティ予算そのものを指しています。これらが示しているのは 情報セキュリティに対する企業の意識であり、企業の重要な位置にあるリーダーは、保護という分野および許容範囲のリスクはどの程度であるのかについても認識しています。

情報セキュリティ予算：少ない予算に占める大きな割合

今年に入って、コスト削減と外注化への取り組みにより、世界の大企業における IT 予算全体が削減されている傾向が見られます。それにもかかわらず（または、それが理由で）、情報セキュリティに費やされる IT 予算の割合は増大しています。このことはあらゆる規模の企業に一貫して見られるパターンですが、特に従業員が 1,000 人以上の大企業では、IT 予算のうち情報セキュリティ予算が 2016 年の平均 19 %から 2017 年は 26 %にまで増大しています。リソースが不足している日本の 中小企業 の場合でも、セキュリティに割り当てられる IT 予算の割合は増大しており、非常に低かった 2016 年の 16 % から多少健全ともいえる 18 % に増大しています。

これは、情報セキュリティの重要性に関する認識度が健全な成長を遂げていることを示しています。つまり、企業が情報セキュリティをコストセンターとしてではなく一種の投資であると考え始め、実際の必要性についても理解しているということです。

■ IT予算に占める情報セキュリティ費用の割合（日本）

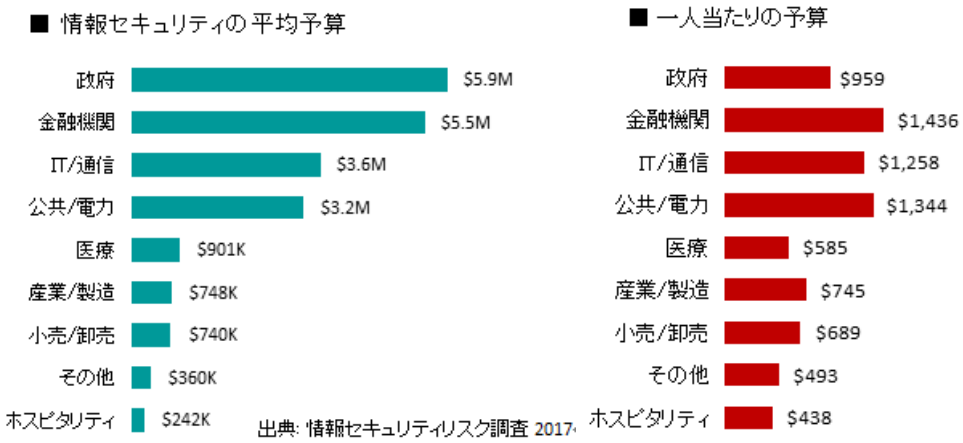


出典：情報セキュリティリスク調査2017

世界における 情報セキュリティ関連の上位支出分野：政府、金融、IT および通信企業

おそらく当然のこととも言えますが、政府に関係する組織（防衛を含む）や金融機関では、今年情報セキュリティに関する支出が最高額に達しており、両予算は 平均 500 万ドルを超えることが報告されています。IT および通信、公共および電力においても、情報セキュリティへの支出は平均額を超えています。これらの分野の企業では政府や金融機関が費やす 500 万ドル超と比較して、ほぼ 300 万ドルを費やしています。

興味深いのは、情報セキュリティに関して「1 人あたり」に費やされる金額を見てみると、政府機関は高支出リストにおいて下位に位置する傾向があります。IT および通信では、情報セキュリティに 1 人あたり平均約 1,258 ドルを費やしていますが、この金額は公共および電力では 1,344 ドル、金融機関では 1,436 ドルに増大しています。一方、政府機関では 1 人あたりわずか 959 ドルに過ぎません。



IT および通信、公共および電力においては、情報セキュリティに関する 1 人あたりの支出額が高くなっていますが、これらの企業では知的財産の保護が問題となることに関係していると考えられます。公共や電力企業の場合、これらの企業をターゲットとする悪意のあるグループの活動に対する脆弱性がますます増大していることが原因の可能性があります。

これらの企業の場合は間違いなく、情報セキュリティへの投資は単に投資すればよいコストでは無く、組織が機能し続けるための事業継続性計画において非常に重要であり、大きなメリットがある投資ということは間違いありません。

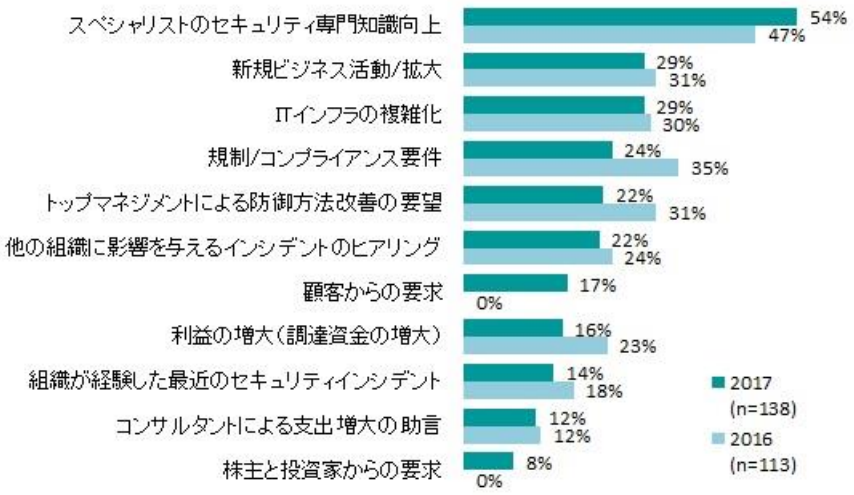
さらに興味深いのは、製造業ではこれと同じ意識を持っていないように見え、プロセスを稼働し続けるために産業用制御システム（ICS インフラ）に依存する傾向があります。ICS インフラに対する攻撃は、2017 年では 12 か月前と比較して 5%増大しています。ただし、これらの組織の情報セキュリティ予算は最低に位置しており、わずか平均 74 万 8,000 ドルに過ぎません。この金額は今年に入って大幅に減少しており、組織とその重要な事業プロセスに関して長期間にわたるセキュリティ上の懸念を引き起こしています。

情報セキュリティに対する投資の動機付け

縦割り部門での幅広い支出において重要な点は、企業が情報セキュリティに貴重な予算を費やすための動機付けです。このことは、企業が情報セキュリティに費やす支出を無価値であると見なしているのか、または一種の投資と見なしているのかを理解する上で重要です。

今年に入って、日本の非常に多数の企業が ROI には関係なくサイバーセキュリティに投資していることを認めており、2016 年の 45%と比較して 2017 年は 58%と増大しています。これは、多数の企業が情報セキュリティへの投資の必要性について理解していることを示しています。

■ 情報セキュリティ予算を増やした主な理由（日本）



出典: 情報セキュリティリスク調査2017

企業は見返りは期待していませんが、情報セキュリティ支出を増大する理由として、株主、投資家（8%）、顧客（17%）を含む主なステークホルダーからの要求を挙げています。これは、企業が情報セキュリティへの支出を増やすことにより、戦略的メリットが生じることを徐々に認識し始めていることを示しています。さらに、企業がサイバー攻撃から自社を防御することができるようになると同時に、顧客に対しては自社データの取り扱いが安全であることを示し、投資家に対しては事業継続性を保証することができるようになります。

企業が情報セキュリティへの支出を増やす理由で多かったのは、スペシャリストのセキュリティに関する専門知識レベルの向上のためで、2016 年は 47%でしたが今年は 54%に増えています。

一方、新規ビジネス活動または拡大に起因するセキュリティ支出の増大の必要性は、昨年の 31%から 2017 年は 29%まで減少しています。この減少は特に 中小企業で顕著であり、脆弱であるマクロ経済の要因を反映したものであると考えられます。ただし、同種の大規模な企業と比較してみると、中小企業の情報セキュリティへの投資は増大しています。これは中小企業が他の組織に影響を与えるインシデントについて認識し、自社を適切に保護する必要性を感じているためです。

まとめ

今年に入って、世界中の企業が被害を受けた WannaCry や exPetr によるサイバー攻撃の大きな影響から、最近 HBO が受けた攻撃のような標的型ハッキングまで、サイバーを取り巻く状況は急激に変化しており、企業は自社の保護戦略をその状況に適合させる必要に迫られています。また企業では、サイバー犯罪へのプロアクティブな対処にかかるコストと、被害に遭った場合のコストを比較した算定を実施する必要性がますます増大しています。

当レポートでは、データ侵害がメディアのトップ記事にならない場合でも、企業はコストがかかるダメージを受ける可能性を示してきました。さらに、世界および日本における法律の改定が、セキュリティインシデントのコストを増大させていることも指摘しました。これは企業が適合する必要がある法律であり、そうしない場合は非準拠かつ安全ではないリスクとなることを意味しています。

このため、コストの算定がより重要になります。この結果として、世界中の企業は IT 予算におけるセキュリティの割合を増大させることを与儀なくされることになります。日本の非常に多数の企業が ROI には関係なくサイバーセキュリティに投資しており、2016 年の 45%と比較して 2017 年は 58%と増大しています。

企業がますますコストがかかるサイバーセキュリティインシデントに直面した際に、情報セキュリティを一種の投資としてとらえ支出の準備ができている場合、攻撃に対して自社を防御する最良の準備になるはずです。あなたはどちらの立場を選択されますか？

株式会社カスペルスキー
PR-1042-201710