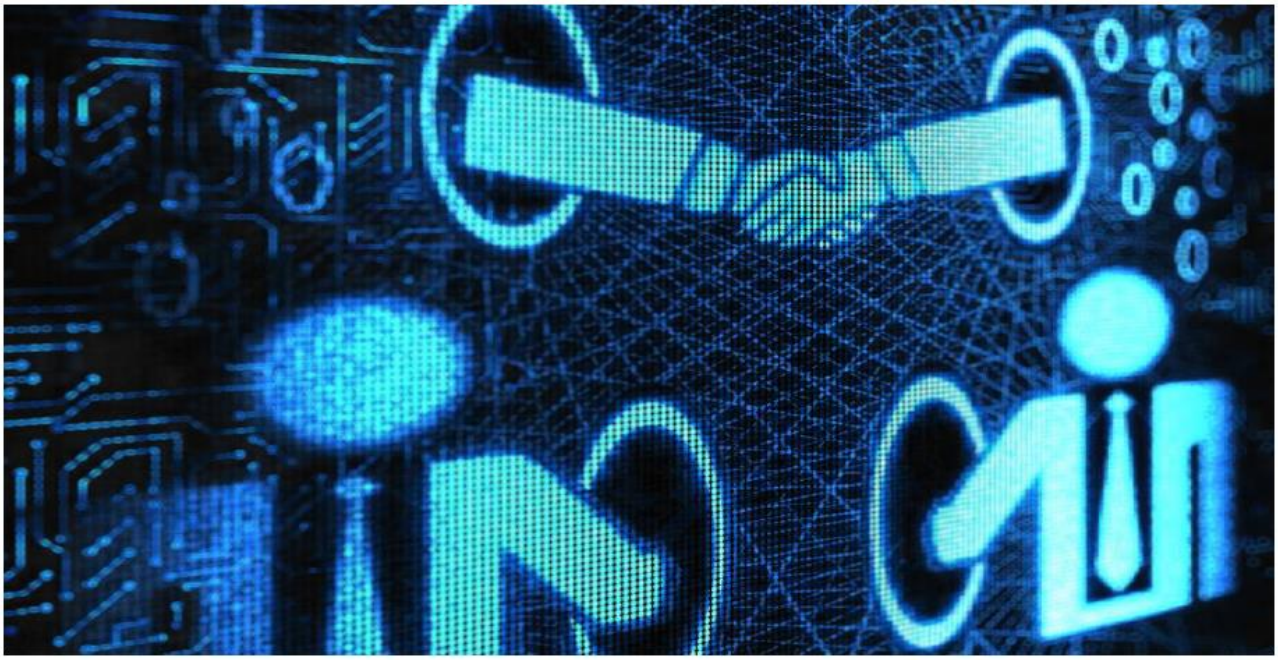

2016 年サイバー・レジリエンスを備えた企業に関するエグゼクティブ・サマリー

実施: Ponemon Institute LLC

後援: Resilient (an IBM Company)

発行日: 2016 年 11 月

2016 年 サイバー・レジリエンスを備えた企業に関する エグゼクティブ・サマリー

Ponemon Institute、2016 年 11 月

Cy-ber Re-sil-ience *(ˈsībə rəˈzilyəns) n.– サイバー攻撃時の主目的とインテグリティーを守る企業の能力。*

第 1 部: 概要

Resilient (an IBM Company) および Ponemon Institute は、強固なセキュリティー体制を築くためのサイバー・レジリエンスの重要性に関する 2 回目の調査の結果を発表いたします。世界中の 2,000 人を超える IT および IT セキュリティーの専門家を対象とした本調査[1] において、半数以上 (回答者の 51 %) が、セキュリティー態勢を強化する上でサイバー・レジリエンスが非常に重要または不可欠であるとしています。

この調査では、サイバー・レジリエンスを、サイバー攻撃を管理、緩和、および対処するために、一貫的に予防、検知、および対応するための能力と定義しています。これは、サイバー攻撃を受けた際に、その主目的とインテグリティーを守る企業の能力です。サイバー・レジリエンスを備えた企業とは、データ、アプリケーション、および IT インフラストラクチャーに対する多くの深刻な脅威に対して予防、検知、被害拡大防止を行い、そうした状況から復旧できる企業です。

ここでは、調査の結果を以下のトピックに従って説明します。

- サイバー・レジリエンスの状況
- サイバー・レジリエンスを達成する上での障壁
- サイバー・レジリエンスが直面する脅威
- サイバー・レジリエンスを達成するための要素

サイバー・レジリエンスの状況

サイバー・レジリエンスの状況は改善されていません。2015 年には、『概要』で説明した定義に基づいて、自社のサイバー・レジリエンスが高い (低レジリエンスを表す 1 から高レジリエンスを表す 10 のスケールの中で 7 以上) と評価した回答者は 35% にすぎませんでした。この評価は、2016 年には 32% に低下しました。過去 12 カ月間で自社のサイバー・レジリエンスが改善されたという回答は、大幅に改善した (回答者の 9%) および改善した (回答者の 18%) を合わせて、全体の 27% にすぎません。改善した場合の要因として挙げられたのは、スタッフへの研修の実施 (回答者の 54%) または管理セキュリティー・サービス・プロバイダーの導入 (回答者の 42%) です。

サイバー・レジリエンスの主な構成要素は改善されていません。サイバー・レジリエンスの主な構成要素は、予防、検知、および対応ですが、回答者は、いずれの要素にも改善を認めていません。

- 昨年は、38% の回答者がサイバー攻撃に対する自社の予防能力を高いと評価していましたが、今年は、40% の回答者がサイバー攻撃に対する自社の予防能力を高いと評価しています。

- サイバー攻撃を迅速に検知する能力、および被害拡大を防止する能力のそれぞれに関し、自社の能力が高いと評価した回答者は、前者については昨年の 47% から 49%、後者については昨年の 52% から 53% に増加しました。

- サイバー攻撃からの復旧能力が高いと評価した回答者は、昨年は 38% でした。一方今年、自社の能力が高いと評価した回答者は 34% にすぎません。

---

[1]本調査は、米国、英国、フランス、ドイツ、オーストラリア、アラブ首長国連邦、およびブラジルで実施されました。昨年度の調査は、米国、英国、およびドイツで実施されました。

本調査の対象企業の多くが、過去 1 年以内にデータ漏えいを経験しています。回答者の 53% が、過去 2 年以内に、機密情報や社外秘のビジネス情報を含む 1,000 を超えるレコードの紛失または盗難を伴うデータ漏えいを自社が経験していると答えています。データ漏えいが発生した企業では、回答者の 57% において、過去 2 年以内に複数回のデータ漏えいが発生しています。

サイバー・レジリエンスを達成する上での障壁

サイバー・レジリエンスの最大の障壁は、依然として不十分な計画と準備です。2015 年には、回答者の 65% がこれを最大の障壁と見なしていました。今年は、回答者の 66% がこれが最大の障壁であると回答しています。

インシデント対応計画は今もなお不足しています。回答者の 79% は、有能なサイバー・セキュリティーの専門家によるサイバー・セキュリティー・インシデント対応計画 (CSIRP: Cyber Security Incident Response Plan) の重要性を認めています。それにも関わらず、企業全体にわたる一貫した CSIRP が適用されていると答えたのは、回答者の 25% にすぎません (2015 年の 18% からは増加しています)。

さらに、インシデント対応の改善に向けた取り組みが必要です。サイバー・インシデントを解決するための時間が増加したという回答は、大幅に増加した (回答者の 16%) または増加した (回答者の 25%) を合わせて、41% になります。時間が短縮されたという回答は、短縮された (回答者の 22%) または大幅に短縮された (回答者の 9%) を合わせて、31% にすぎません

サイバー・レジリエンスの新たな敵となっているのは、複雑性です。2015 年に、IT プロセスの複雑性が高水準のサイバー・レジリエンスへの障壁になっていると回答したのは回答者の 36% でした。この数値は 2016 年には大幅に増加し、46% に達しています。また、ビジネス・プロセスの複雑性が増加したと考えている回答者も (2015 年の 47% から今年の 52% に) 増加しています。

サイバー・レジリエンスが直面する脅威

サイバー・レジリエンスに対する最大の脅威は人的ミスです。サイバー・レジリエンスに影響を与える可能性がある IT セキュリティーの脅威を 7 つ挙げるとしたら、最大の脅威は人的ミスであり、それに続くのが、APT 攻撃 (Advanced Persistent Threats) です。回答者の 74% が、発生したインシデントには人的ミスが関係していると回答しています。IT システム障害およびデータ流出についても、回答者の 46% および 45% がそれぞれ深刻であると答えています。

企業 IT ネットワークまたはエンドポイントでもっとも頻繁に発生する被害はマルウェアとフィッシングです。サイバー・セキュリティーの侵害の結果としてビジネス・プロセスまたは IT サービスの中断が発生したという回答は、非常に頻繁に発生 (回答者の 16%) または頻繁に発生 (回答者の 28%) を合計して、44% になります。

最も頻繁に発生するインシデントまたは被害は、マルウェア (回答者の 74%: これは、2015 年の 67% から増加)、およびフィッシング (回答者の 64%: これは、2015 年の 55% から増加) です。それに続いて多いのが通信エラー (回答者の 53%) です。

サイバー・レジリエンスを達成するための要素

サイバー・セキュリティーを改善する上で重要な取り組みと考えられているのは、インシデント対応プラットフォームの確立と脅威情報の共有です。サイバー・レジリエンスが向上したと答えた回答者の 58% が、インシデント対応プラットフォームの確立がサイバー・レジリエンスの改善のキーであると考えています。

回答者の 53% は、自社が、政府機関や同業他社との間でデータ漏えいおよびインシデント対応に関する情報共有の取り組みやプログラムに参加していると回答しています。回答者の 81% は、それにより自社のセキュリティー体制が改善されたと回答し、75% は、自社のインシデント対応計画の有効性が高まったと回答しています。回答者の 53% が、脅威情報を共有することでインシデント対応の適時性が向上したと回答しています。

脅威情報の共有に参加していないと答えた 47% の回答者から挙げられた理由は、利益が見込めない (回答者の 42%)、リソース不足 (回答者の 42%)、およびコスト (回答者の 33%) です。

サイバー・レジリエンスの重要性に関する上級経営陣の認識は変わっていません。サイバー・レジリエンスが収益やブランド評価に与える影響についての認識の傾向には、改善が見られません。2015 年には、回答者の 52% が、自社のリーダーがサイバー・レジリエンスが収益に影響を与えることを認識していると回答していましたが、今回このような回答はやや減少し、47% になりました。同様に、2015 年には回答者の 43% が、サイバー・レジリエンスがブランド評価に影響を与えると回答していましたが、この数字は 2016 年もほとんど変わっていません (回答者の 45%)。企業リスクがサイバー・レジリエンスに影響すると認識しているのは、回答者のほぼ半数 (48%) で、これは、2015 年の 47% から微増しています。

サイバー・セキュリティー予算に充てる資金は若干増加しています。2015 年には、サイバー・セキュリティー予算の平均は 1000 万ドルでした。この数字は、平均 1140 万ドルに増加しました。より多くの資金がサイバー・レジリエンス関連の活動に割り当てられるようになりました。2015 には、IT セキュリティー予算の 26% がサイバー・レジリエンス関連の活動に割り当てられていました。　この割合は、2016 年には 30% に増加しました。

企業のサイバー・レジリエンスの有効性を 10% 高めるために許容される予算増加幅は 7% です。有効性を 90% 向上するために許容される予算増加幅は 37% です。

世界的なプライバシー規制によって、資金は増加しています。IT セキュリティーの資金増加を促しているのはどのような規制かという質問に対して、ほとんどの回答者は、新しい EU General Data Protection Regulation (回答者の 51%) またはその国の国際法 (回答者の 50%) と回答しています。EU General Data Protection Regulation に対する自社の準拠レベルが高いと回答したのは、回答者の 22% にすぎません。

サイバー・レジリエンスを達成する上で重要ないくつかの要素があります。サイバー・レジリエンスを達成する上で最も重要な要素として回答者から挙げられたのは、緊急事態に対する準備、俊敏性、および強固なセキュリティー態勢です。予算およびリーダーシップの重要性は、最も低く評価されています。

ほとんどの企業は、あらゆる災害に備えています。回答者の 66% は、本調査の対象企業が、準備の一環として、厳しい気象事象、火災、および自然災害を対象とした総合的なレジリエンス戦略を策定していると回答しています。

サイバー・レジリエンスは、特定のテクノロジーを使用することで向上します。サイバー・レジリエンスを達成するには、人材やプロセスに加えて、適切なテクノロジーが不可欠です。回答者が最も有効だと考えているテクノロジーには、ID の管理と認証、侵入の検知と予防のシステム、インシデント対応プラットフォーム、アンチウィルスやアンチマルウェア、および保存されたデータの暗号化があります。

サイバー・レジリエンスを達成する上でキーとなるいくつかのテクノロジー機能が存在します。サイバー・レジリエンスを達成するために全体的または部分的に展開されている最も重要な機能として、エンド・ユーザーによる安全ではないインターネット・サイトまたは Web アプリケーションへのアクセスの抑制 (回答者の 79%)、安全ではないデバイスからのセキュリティー・システムへのアクセスの制限 (回答者の 78%)、機密データや社外秘データおよび基幹業務アプリケーションへの無許可アクセスの抑制 (回答者の 77%)、エンドポイントおよびモバイル接続の管理 (回答者の 72%)、セキュア・データのクラウドへの保管 (回答者の 70%)、および BYOD を含む、安全ではないモバイル・デバイスの管理 (回答者の 70%) が挙げられます。

サイバー・レジリエンスを達成する上でキーとなるいくつかのガバナンスおよび管理の手順が存在します。サイバー・レジリエンスを達成するために全体的または部分的に展開されている最も重要なガバナンスおよび管理の手順として、明確に定義された IT セキュリティー・ポリシー (回答者の 84%)、バックアップおよび災害復旧計画 (回答者の 82%)、インシデント対応管理計画 (回答者の 82%)、セキュリティー・リーダーから CEO および取締役会への (下位から上位への) コミュニケーション・チャネル (回答者の 77%)、システム・ユーザーの背景調査 (回答者の 76%)、エキスパートの IT セキュリティー担当者 (回答者の 74%)、および企業のシステム・ユーザーに対する研修および啓蒙活動 (回答者の 74%) が挙げられます。

本調査の詳細については、Ponemon Institute までお問い合わせください
(E メール: research@ponemon.org、電話: 1.800.887.3118)。

Ponemon Institute

情報管理の信頼性向上に向けた取り組み

Ponemon Institute は、独自の調査と教育を通して、企業と政府機関における信頼性に優れた情報管理と個人情報管理の実践を推進しています。当社のミッションは、ユーザーと企業の機密情報の管理と保護を左右するさまざまな重要課題に対して、豊富な経験を活かした高品質な調査を実施することです。

当社は、**Council of American Survey Research Organizations (CASRO)** の参加企業として、データの機密保持、個人情報保護、倫理に関する厳格な基準を遵守して調査活動を遂行しています。当社は、個人が特定できるようないかなる情報も収集しません (企業調査の場合は、企業が特定できるようないかなる情報も収集しません)。また、調査対象者に無関係な質問や不適切な質問をしないための厳格な品質基準を遵守しています。