kyndryl

調査結果で見る

ITリスクの現状に関してITの意思決定者が語ること

昨今、ITリスクは取締役会で議論するトピックになりました。

企業が複雑で地理的に分散したハイブリッドITシステムに依存している環境では、ネットワーク障害やマルウェアによる攻撃などを含むシステム障害が、企業の生産性、評判、および収益に壊滅的な影響を与える可能性があります。

そのため、多くの企業の取締役会では経営層に対し、このようなインシデントに対する対応状況について詳細を提示するよう求めています。

その影響の大きさを考慮して、私たちは企業におけるITリスクの認識と、サイバーレジリエンスを高めるための取り組みについて調査しました。ITの意思決定者とリスクおよびコンプライアンスの専門家で構成される調査対象者に対して世界各国でアンケートを実施し、彼らが経験した困難、最も懸念されているITリスクは何か、また、こうしたリスクに対する特定、防御、対応、復旧のために企業が行っている取り組みについて聞きました。

この調査結果は、2023年ITリスクの現状レポートの一部をご紹介するものです。

今回の調査結果から、特に企業のITシステムが混乱に直面してしていることが明らかになりました。何がこうした障害の軽減に取り組む際に妨げとなるかについても理解を深めました。また驚くべきことに、ITリーダーたちが自社の組織においてITの混乱に対処し、復旧させるための能力が備わっていると、自信をもっていることがわかりました。

今回の調査結果は、自社のITリスク軽減戦略を検証するためにご活用いただけるものです。さらに、サイバーレジリエンスを実現するための9つのステップを以下にご紹介します。

調査データについて

キンドリルは第三者調査会社と協力して、大企業（従業員1,000名以上）のITの意思決定者300名に対し、オンラインで調査を実施しました。回答は2023年3月から4月に収集されました。

回答者の拠点：

- → 65% 北米
- → 19% 英国
- → 16% インド

業界別内訳：

- → 18% 金融サービス
- → 17% 政府機関
- → 17% 製造業
- → 14% 通信
- → 14% メディア
- → 20% その他

著者について

Kris Lovejoyは、キンドリルのセキュリティ&レジリエンシー担当グローバル・プラクティス・リーダーです。

企業は重要なビジネスプロセスを運用するうえで、IT部門に依存している

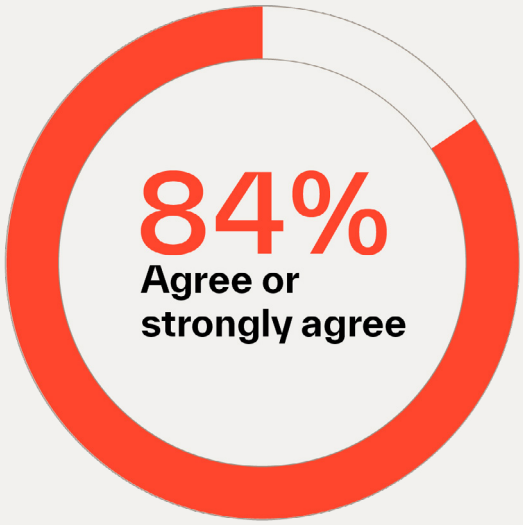
ITリスクに対する導入として、日常的な業務におけるIT部門への依存について回答者に尋ねました。

84%の回答者が、自社が重要なビジネスプロセスを運用するためにIT資産に大きく依存していることに「同意する」または「強く同意する」と回答しました。

デジタル変革が広く普及していることを考えると、この結果は驚くべきものではありません。

こうした回答が特別際立ったものではなかったことのほうがより驚くべきかもしれません。

質問：あなたの企業は、重要なビジネスプロセスを運用するためにIT資産に大きく依存していると考えますか。



ほとんどの企業がITシステム障害を経験

私たちはITシステムの重要性だけでなく、関連する障害についても調査しました。92%が、過去2年間に自社でITシステムに損害を与えたり混乱させたりするインシデントを経験したと回答しました。ビジネスとITリスクは切り離せないことが分かります。

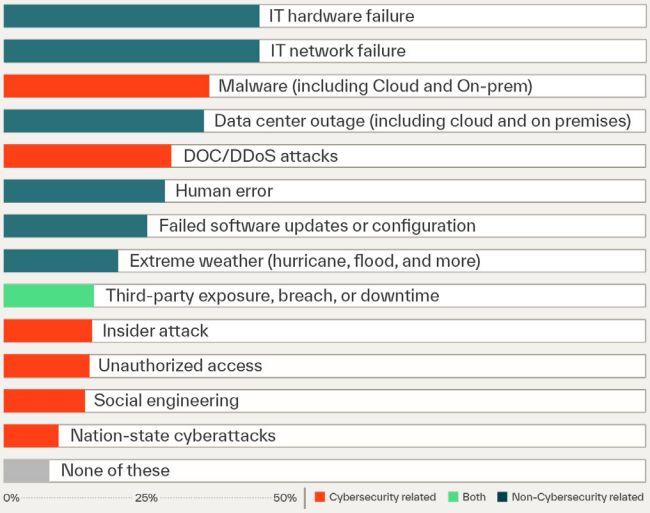
多くの回答者が3つか4つの異なるタイプのインシデントを経験していたことが分かりました。サイバー攻撃がニュースの見出しになる機会が増えていますが、この調査結果を見ると、ITリスクはより広範に及ぶことを示唆しています。

71%がサイバーセキュリティ関連の問題を経験したと回答し、88%がサイバーセキュリティ関連以外のインシデントを経験したと回答しています（複数回答）。実際に、インシデントの上位5件のうち、3件は以下のようなサイバーセキュリティ関連以外のものでした。

- → ITハードウェア障害
- → ITネットワーク障害
- → データセンター障害

注目すべき点として、人的エラーも依然として重要な障害の原因であり、調査の選択肢である13のうち6位の問題にあたります。金融サービス業界では常に上位3つに入ることが分かりました。

質問：過去24カ月間に、以下のような有害事象によって、ITシステム／データに障害が発生しましたか。



ITシステム障害は企業ブランドに悪影響を与え、罰金やその他の問題を引き起こす

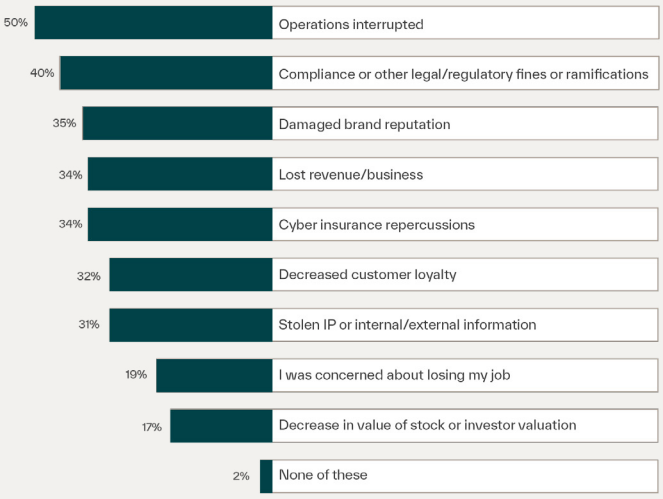
ITが日常の業務でどれほど重要な役割かを示す例として、ITインシデントによって生じる最も頻度の高い影響として、業務の中断が指摘されたことが挙げられます。

コンプライアンスやその他の法的または規制上の罰金、それに関連する影響の経験は、2番目に多い回答となりました。特に金融サービス、政府機関、メディア業界の回答者に顕著でした。

業務の中断とコンプライアンスの2つは、「最も多く経験した」のカテゴリーだけでなく、「将来IT資産が使用不可なったり侵害されたりした場合に最も懸念される影響」のカテゴリーでも上位2つに入りました。たとえば、サービス妨害（DoS）攻撃による障害やデータ漏洩には莫大な罰金が科せられる可能性があります。

35%は、IT障害が原因で自社のブランドとしての評判を損なったと回答しました。これはメディア系企業の回答者が多く、そうした影響があったと回答したうちの63%がメディア系企業でした。常に動き続けるニュースサイクルと顧客のソーシャルメディアアクティビティにより、こうしたインシデントがこれまで以上に注目を集めるようになったことが分かります。

質問：あなたの組織は、過去24ヶ月間に有害事象による影響があった場合、次のうちどれを経験しましたか。



ITリスクに先手を打つには常に課題が存在する

私たちは、世界的なITスキル不足がリスク軽減に向けた課題の上位に挙げられると予測していましたが、実際は異なりました。インシデントの影響に対処するうえで、回答者が直面する最大の課題として指摘したのは、暗号化されたクリーンなバックアップからシステムやデータを復元する能力の欠如でした。これは、キンドリルのサービスについてお問い合わせのお客様でもよく見られます。このような状況下では、次のことを推奨します。

- → 復旧プロセスの自動化とオーケストレーションに投資する
- → バックアップから復元する際の人的エラーを最小限に抑えるための最適な方法を評価、確立する
- → インシデントへの対応計画を繰り返し、また、頻繁にテストする

リスク軽減に向けた課題の上位3つは、IT資源の拡大と新たな脅威に常に対応する能力という結果が明らかになりました。スキルのあるITスタッフの不足は4位に挙げられています。

質問：有害事象の影響を管理する上で直面する課題の上位3つは何ですか。

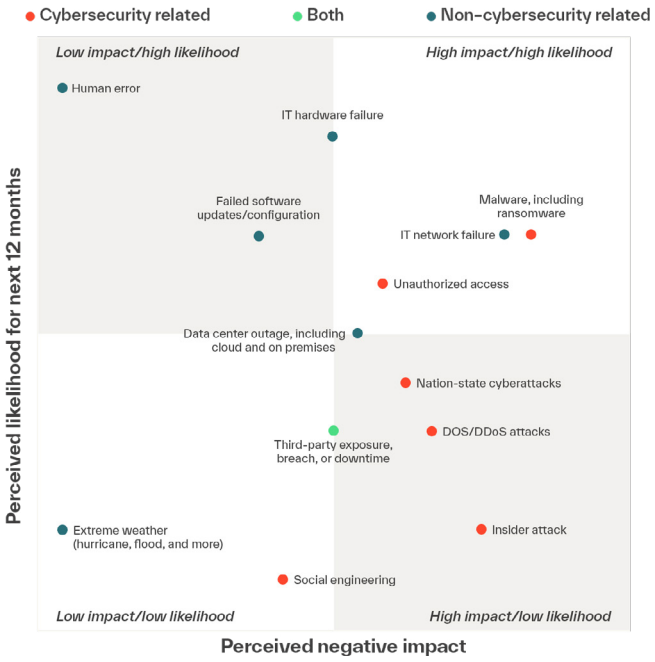
今後12か月で、マルウェアイベントは最も高い可能性と悪影響のある IT リスクとして認識されている

回答者に、今後12か月間で最も懸念されるインシデントと、それらのインシデントが発生した場合に企業に及ぶ影響のレベルについて尋ねました。

人的エラーが発生する可能性が最も高いと考えられていますが、予測される影響は他のほとんどのインシデントより低いと回答されました。一方、マルウェアは最も懸念され、最も脅威となるITリスクとして際立っていました。

マルウェア、特にランサムウェアに対する危機意識の高まりを考えると、この結果は驚くべきことではありません。前述の暗号化されたクリーンなバックアップからデータを復旧する際の課題という点で、この問題に意識が高まる理由もうなずけます。企業がバックアップを課題と認識しているかどうかに関係なく、ランサムウェア攻撃者がバックアップをターゲットとする事象が増えていることが、複雑化の原因と見られます。このような状況では、バックアップを侵害されると、企業はシステムを復元できないだけでなく、マルウェアの有無を確認することすらできなくなります。その結果、リスクと潜在的なの影響が急拡大することになります。

発生の懸念が高く、潜在的に大きな影響を持つもう1つのリスクは不正アクセスで、重大な悪影響をもたらすと考えられています。 ゼロトラストの原則は、不正アクセスに対処するための継続的に重要な役割を担います。ゼロトラストでは、企業は価値の高い資産を特定し、特権アクセスを識別し、多要素認証などのテクノロジーを活用して検証することが求められます。

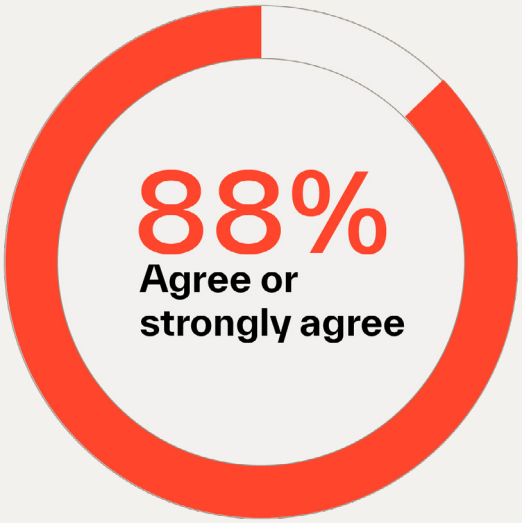


リスクを認識する一方で、ITの意思決定者は依然として自信をもっている

冒頭で、ITの意思決定者が世界的なインシデントや指摘された課題の存在を理解したうえで、自信をもっていることに驚いたと述べました。実際に88%が企業のIT資産を混乱させる悪条件、攻撃、または侵害に対処し、復旧するための十分な準備ができていると回答しています。

同業他社との比較について尋ねたところ、65%の回答者が他社に比べて自社組織のインシデントへの対策は十分であると回答しました。逆に他社に後れを取っていると回答したのはわずか8%でした。前述のとおり、92%がインシデントを経験したと回答したことを考慮すると、この高い自信は驚くべき結果といえます。この二重性は、その自信が正当かどうかを疑問視するほどではないにしても、少なくとも興味深いものです。

質問：次の内容にどの程度同意または反対しますか：私の組織は、企業のIT資産を混乱させるような不利な状況、攻撃、侵害を管理し、そこから復旧するための準備が十分に整っている。



ITリーダーがサイバーレジリエンスの実現に向けて計画すべき9つのステップ

私たちは、ITの意思決定者がITリスクの現状をどのように認識しているか、リスクを軽減するために以下のサイバーレジリエンスの4つの柱にもとづいて、企業がどのように行動しているかを評価するべくこの調査を実施しました。

- → **特定：** 潜在的な脅威を適切に軽減し、潜在的な規制を回避するためのITリスク体制を評価および理解する
- → **防御：** IT資産がインシデントから保護されるようIT資産の防御を強化する
- → **対応：** 混乱に対処し、影響を軽減する
- → **復旧：** 中断後の影響を軽減し、重要なIT環境を迅速に復旧する

回答者は一様に自社のパフォーマンスは良好であると評価しており、自信は高いといえます。すべてのアクティビティで平均して、75%が自社のパフォーマンスが「非常に良い」または「優れている」と回答しました。微妙な違いとして、経営層からセキュリティ投資に対する強い賛同を受けていると報告した回答者は、サイバーレジリエンス関連の活動で最高の評価をつける傾向が強いことが分かりました。

そこで経営層からの賛同を得るために、サイバーレジリエンスに向けて実行するべき9つの基本的なステップをご紹介します。

1 初期のうちから積極的に事業部門を巻き込む

IT部門は他の事業部門から切り離され、サイロ状態で運用されることがよくあります。サイバーレジリエンス戦略を成功させるための最も確実な方法は、サイロを打破することです。IT部門外のメンバーを募り、企業の使命におけるサイバーレジリエンスについて議論を進めましょう。それが企業文化の一部となるよう取り組みます。

2 リスク許容度を調整する

リスク許容度のレベルは、たいていの場合、業界によって決まります。たとえば、高い規制のある金融機関の許容度レベルは非常に低くなります。自社のリスク許容度を定義し、全社に伝えましょう。

3 実用最小限な会社 (Minimum Viable Company) を設立する

実用最小限の事業体とは、運営を維持し、事業目標を推進するために重要な企業の一部を意味します。サイバーレジリエンス戦略は、重要な部分の特定だけでなく、これらのシステムの基礎となるデータをどのくらいの速さでオンラインに復旧する必要があるかという影響の許容度の特定も必要です。

4 棚卸しを実施する

調査結果から分かるように、多くの企業は拡大し続けるIT資産という課題に直面しています。最小限の存続可能な会社にとって重要なIT資産を特定し、マッピングします。これらの資産は保護すること、最悪のケースではインシデント後に復旧することが最優先となります。

5 ゼロトラストフレームワークに移行する

権限システムにアクセスする必要がある人だけがアクセスを取得でき、必要のない人には取得できないようにする、デフォルト拒否の原則を推奨します。

6 危機管理計画を策定する

場合によっては、インシデントは避けられないこともあります。(例：混乱の最も予想される原因としての人的エラーなど。) 部門全体の役割と責任を定義し、コミュニケーション、文書処理プロセスを確立し、透明性を向上することで、インシデントの影響軽減に役立ちます。

7 混乱に備えてテストする

計画は策定しただけで、ほとんど実行されないことがよくあります。インシデントが発生した場合、テストされていない計画は、混乱や応答時間の遅れを招き、影響がさらに深刻化します。

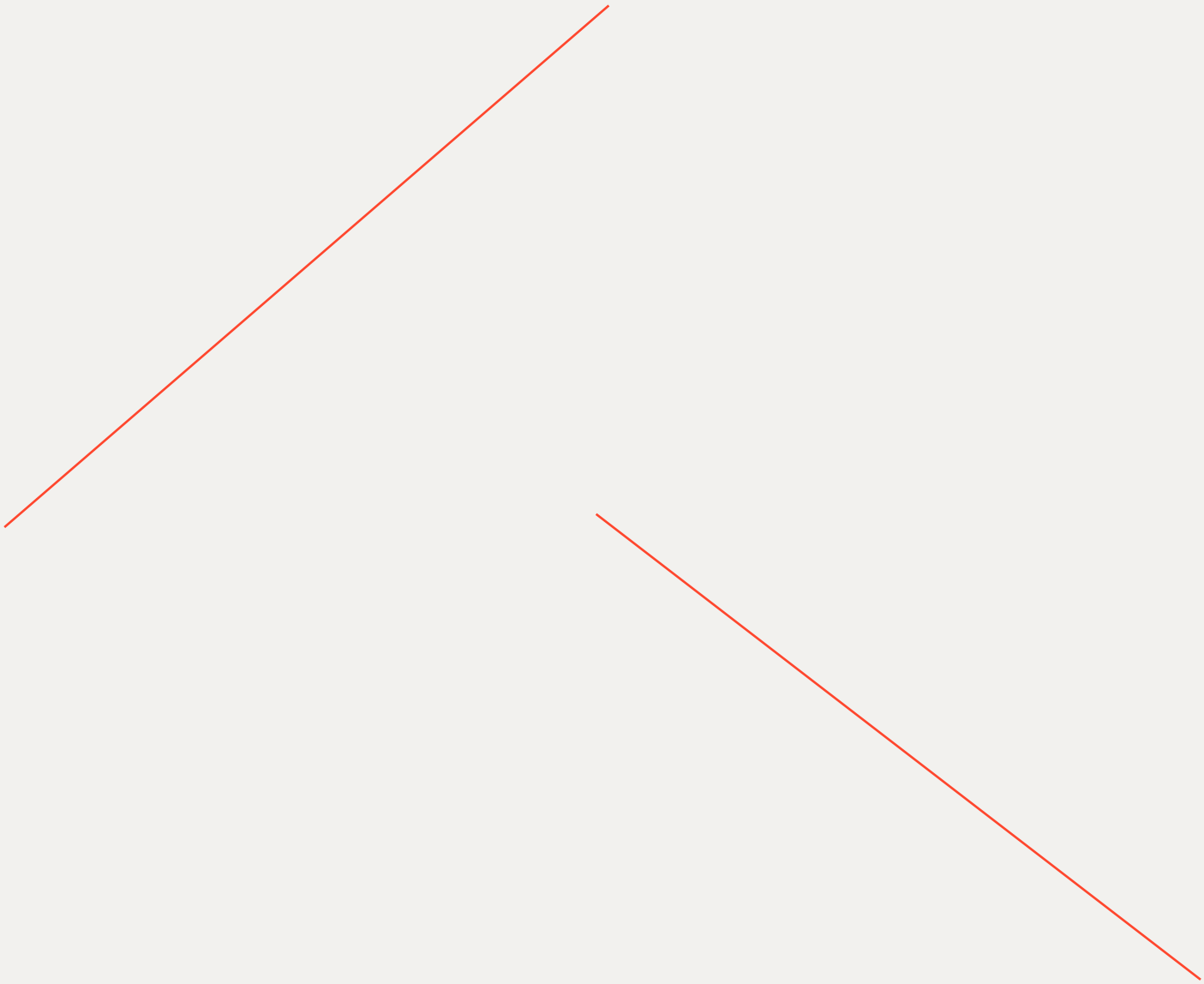
8 サイバーレジリエンス戦略を継続的にアップデートする

企業は生き物のようで、ビジネスの推進力は変化し、IT環境はより複雑化し、外的要因 (規制など) により変更を迫られることもあります。サイバーレジリエンス戦略の有効性を確保するには、継続的に戦略について議論し、アップデートする必要があります。

9 経営層レベルで認識を高める

最後に、サイバーレジリエンスが世界中で取締役会レベルの議論のトピックになっているという事実をもう一度振り返り、調査レポートをまとめます。

リスクを軽減するためITのリスクと計画について経営層と最新情報を共有することで、トップダウンで企業全体の足並みを揃え、サイバー対応のシステムがインシデントの間も稼働できるようにするために必要な変化をもたらします。



kyndryl