

「CISO の明日はどちらだ !?」
イベントレポート

元インテル 副社長兼最高セキュリティおよびプライバシー責任者 (CSPO) が語る！

企業における情報セキュリティのあり方、 CISO の役割について



Cylance Inc. 最高セキュリティおよびトラスト責任者
マルコム・ハーキンズ

発行：エムオーテックス株式会社

企業における情報システムのあり方、CISO の役割について

INDEX

- I. 私たちが今日直面している最も重大な脆弱性とは一リスクに対する誤解
- II. 誤解の原因は「経済」と「心理学」。CISO は両方の問題を評価する必要がある
- III. CISO は内部・外部両方の課題に対応する必要がある
- IV. CISO に必要なスキルその1：技術センスとビジネスセンス
- V. CISO に必要なスキルその2：リーダーシップ
- VI. リスクと制御
- VII. セキュリティ制御の9ボックス
- VIII. サイバーリスクを企業リスクと紐付ける
- IX. リーダーシップの法則
- X. セキュリティチームにおけるモットー
- XI. セキュリティエグゼクティブの役割
- XII. CISO の3スタイル
- XIII. 長年にわたる教訓のまとめ



〔マルコム・ハーキンズ氏について〕

Cylance Inc. の最高セキュリティおよびトラスト責任者(Chief Security and Trust Officer)として、情報リスク、セキュリティ、プライバシーポリシーにおける組織的責任を担う。また、サイバーリスクとベストプラクティスに関する啓蒙活動も世界各国で精力的におこなっている。以前はインテルコーポレーションの副社長兼最高セキュリティおよびプライバシー責任者を務めた経験をもつ。

- 受賞歴 -

2010 年 RSA カンファレンスの Field of Security Practices 賞で「エクセレンス賞」受賞

2012 年 Computerworld 誌「IT トップリーダー 100 人の 1 人」に選出

2012 年 (ISC)2「Information Security Leadership 賞」を受賞

2013 年 グローバル CISO エグゼクティブ・サミットで「Breakaway Leaders」の上位 10 人の 1 人に選出

2015 年「Security Advisor Alliance Excellence in Innovation 賞」受賞

- 実績 -

下院、上院、連邦政府機関と連携する無党派のサイバーセキュリティシンクタンクである Institute for Critical Infrastructure Technology のフェローを務める。2012 年 12 月に自著「Managing Risk and Information Security: Protect to Enable®」を出版。2014 年に出版された「Introduction to IT Privacy」の執筆協力者でもある。

企業における情報システムのあり方、CISO の役割について

I. 私たちが今日直面している最も重大な脆弱性とは—リスクに対する誤解

本日はCISOの役割についてお話ししたいと思います。

わたしはこの業界に長年身を置いています、リスク、コンプライアンスに関しては17年間従事していました。今はサイランスでチーフセキュリティ及びトラスト責任者ですが、その前は長年インテルで最高セキュリティ、プライバシー責任者を務めていました。しかし、私はセキュリティのテクノロジストではありません。テクノロジー業界には長年いますが、大学では経済学を専攻し、ビジネス領域でキャリアを積んだうえでセキュリティ業界に入りました。その観点からお話をさせていただきます。

私がよくする質問が1つあります。「私たちが今日直面している最も重大な脆弱性とは何か」ということです。よく返ってくるのは「エンドユーザー」という答えです。コンピューターを使っているのはエンドユーザーであり、エンドユーザーがミスをしてしまう、リンクをクリックしてフィッシング詐欺やソーシャルエンジニアリングに引っかかってしまうからという回答です。



もちろん、エンドユーザーは管理しなくてはならない対象の1つですが、問題の核心ではありません。問題の核心は何かというと、「リスクに対する誤解」です。すべてのエグゼクティブ、そして意思決定者、さらにセキュリティチームの意思決定者であってもリスクを誤解しています。なぜかという人は先入観を持っているからです。

II. 誤解の原因は「経済」と「心理学」。CISO は両方の問題を評価する必要がある

そもそもなぜリスクに誤解が生じるのか、2つ原因があります。1つはどれだけの予算を自分は持っているのか、どれぐらいのリソースを使えるのかといった「経済」と、もう1つが「心理学」です。例えば、何かについて「メリットがある」「新しい」「格好いい」と思った時に、経済的なリスクは見落としがちです。このような時にフィッシングに引っかかりやすくなるわけです。リスクをあまり考えずに、新しいものに飛びつくということが起きてしまうのです。

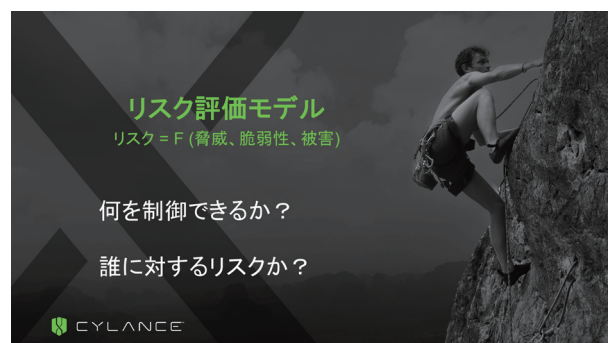
以上から、CISOというのは企業、組織、そしてチームの中で経済と心理学的な問題の両方を評価すべき立場にあります。

典型的なリスク評価モデルは3つの要素の関数です。その要素は「脅威」、そして「脆弱性」、そしてそれらによる「被害」です。

このリスク評価モデルにおいて、脅威である攻撃者をコントロールすることはできません。しかし、被害に関してはテクノロジーを導入することで最小化することができます。つまりCISOがコントロールできるのは

「脆弱性の管理」です。

しかし、ここで大切なのは、「誰に対してのリスクなのか？」を自問することです。組織に対してのリスクなのか。それとも顧客に対するリスクなのか。組織、企業によって、あるいは管理する対象によっては社会に対してのリスクかもしれません。これらのリスクをCISOがきちんと把握できているかが課題となるのです。



III. CISO は内部・外部両方の課題に対応する必要がある

CISOが直面する課題の領域は2種類あります。

まず「外部の課題」、これはサイバー犯罪者集団の攻撃によるインシデントのような、日々ニュースで取り上げられる課題のことです。

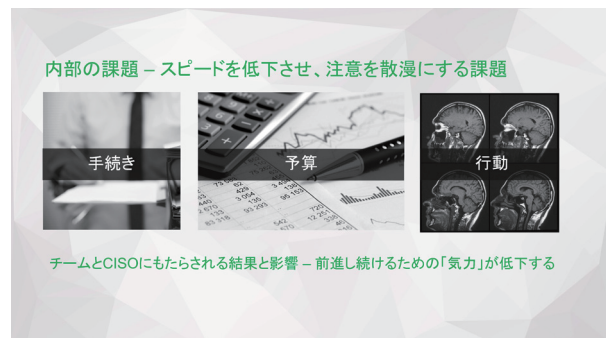
では、もう1つの領域とはどのようなものでしょうか。

私はセキュリティ・テクノロジーの専門家ではないにも関わらずビジネスセンスを買われ、インテルでセキュリティそして事業継続の役割を担いました。



そこで重要だったのは予算、手続き、そして人間の行動を熟知していることです。こういった「内部の課題」という領域で、経済・心理学のダイナミクスを管理することで、適切な意思決定と適切な予算建てを行い、そしてIT部門にやるべきことを指示して技術的な脆弱性に対応してきました。

CISOはこの「内部の課題」「外部の課題」の両方の領域で勝利しなくてはならないのです。技術的側面に加えて、内部のダイナミクスにも対応することが重要です。

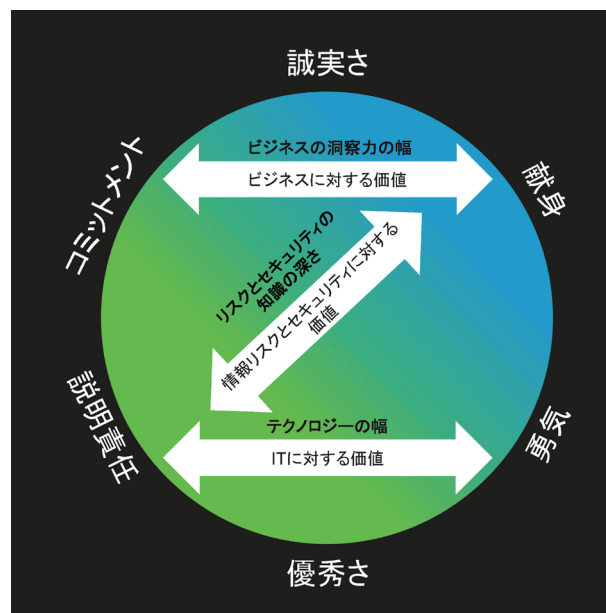


IV. CISOに必要なスキルその1：技術センスとビジネスセンス

私は、最初の本を書き出した時から2冊目の情報とリスク管理の本を書いていた時まで、CISO・CSOとしてどういったスキル・能力が必要なのかを考えていました。

これは「Z型」と私が呼んでいる図です。まず技術に関するセンスをテクノロジストとして、ITチーム/CTOとして持たなくてはなりません。そして、同時にビジネスのセンスも持たなくてはなりません。ビジネスの目的を理解し、それぞれの業務部門が達成しようとしているゴールを理解し、チームと丁寧に会話をし、彼らと共通言語を用いることも重要です。加えて、リスクとセキュリティの深い知識を持つことがZ型です。しかしCISOに必要なものはもう一つあります。自立性を持って誠実さを発揮できることです。戦術的な背景からテクノロジーを動かしたり、大きなリスクを伴う業務部門の取り組みを止めないといけない場合もあります。

さらに、CISOにはリーダーシップが必要です。リーダーシップについては詳しく後ほどお話しします。



これは1980年代の終わりにアメリカで非常に流行った映画で、ブレイクファスト・クラブという映画の写真(※)です。いわゆる落ちこぼれの高校生たちの話です。彼らは落ちこぼれなので、例えばスポーツしかできない落ちこぼれの高校生、綺麗な女の子や非行少年もいたりします。しかし異なった観点を一人ひとりが持っているのです。多様な観点を持ち寄ることで新しい洞察に到達することができました。

多様な観点があれば、我々が偏見を持ちながら意思決定をしがちであるということも見えてくると思います。

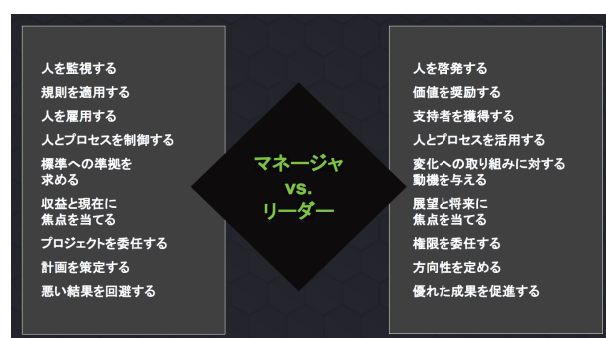
※[引用] <https://www.uphe.com/movies/the-breakfast-club>

V. CISOに必要なスキルその2：リーダーシップ

リーダーシップとは何か？

マネージャーの皆さんは、人事権を持ち予算を握ります。そして企業としてネガティブな結果とならないように管理をします。一方で、リーダーシップは異なる要素を持っています。人を啓発する、ポジティブな結果を奨励していく、変化を新しい方向に推し進めていく、そして組織を良い形に変貌させていく、それがリーダーシップの真髄です。

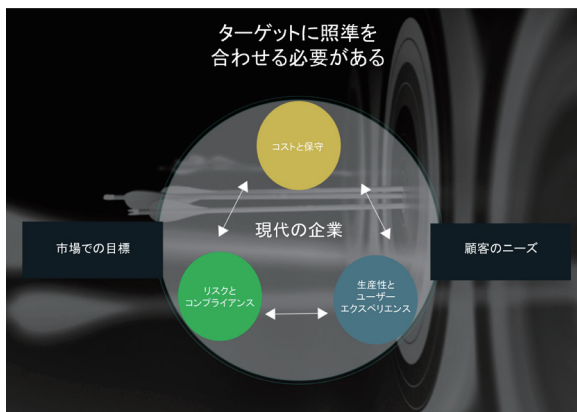
組織の中にはリスクと制御の要素というものがあります。これは財務、法務、あるいは技術的な要因全てに関わってきます。CISOの皆さまとお話をすると、この基本的なリスクと制御に問題を抱えていることが分かります。



VI. リスクと制御

一般的なビジネスリスクとして企業が直面するものは10個あるといわれています。例えば、誤りのある財務記録、不正行為といったものです。これは組織の根幹を揺るがす危機になることを多くのCFOは理解しています。従って、CISOは技術的リスクをビジネスリスクの分脈に沿って明確にしていける必要があるわけです。そしてプロセス/制御という観点から、リスクを管理していくのです。

しかしリスクは全て排除できるものではないため、何らかのリスクは残ります。



そのためリスクがビジネスのプロセスとして受け入れられるか否かを判断するわけですが、その判断をするのは誰なのでしょう。

この業界に入る前から、セキュリティチームはターゲットを明確にする必要があると思っていました。会社のニーズを内部要因・外部要因から理解する必要があります。セキュリティとビジネスのバランスを取る必要もあります。ですからこういった計算式のような働きを行っていかねばならないのです。それは、その制御をすることがコストにどう影響するのか、組織にどういった影響が出るのか、そもそも市場に対する目標設定はどうされているのか、その全てを理解したうえで、あるべきセキュリティ・制御を実装し、そして単に守るというだけでなく「Protect to Enable」、すなわち何かを実現するためのセキュリティが必要なのです。

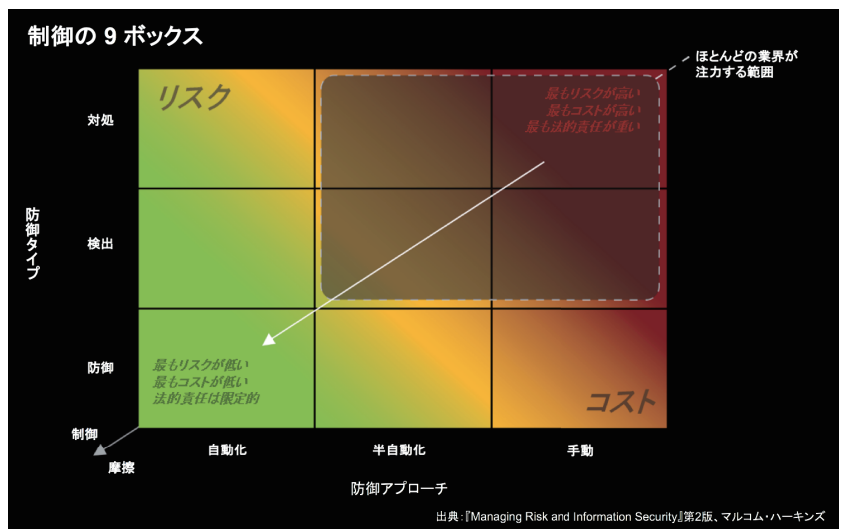
VII. セキュリティ制御の9ボックス

私は9つのボックスから構成される、セキュリティ制御のシンプルなフレームワークを作りました。物理的、論理的リスクの制御のタイプは防御、検出、対処の3種類が縦軸にあります。また、その3つの制御タイプに対し、3つの制御アプローチが横軸に置かれています。アプローチを自動化で対応するのか、半自動化なのか、あるいは手動なのかというアプローチを意味するものです。

手動はコストがかかるにも関わらず、組織内におけるほとんどのセキュリティは半自動化、あるいは手動という制御アプローチで行われ、検出あるいは対処という制御タイプで

対応されています。これは何故でしょうか？それは、処理が多ければ多いほどセキュリティ業者の利益が上がる仕組みがあるためです。このためセキュリティ業者は、この問題を解決するモチベーションがありません。経済的あるいは心理的な理由からセキュリティ業者は、リスクが最小化されていない環境に顧客企業を置いておこうという思惑があります。

ここには制御の摩擦も存在します。制御の摩擦は人・データ・ビジネスのスピードを劣化させることになります。制御が事業を抑止する働きを



持つと、そのビジネスは制御を避けて進もうとするため、セキュリティのリスクが高まります。リスクが高まれば、セキュリティ業界は利益が上がるという仕組みです。

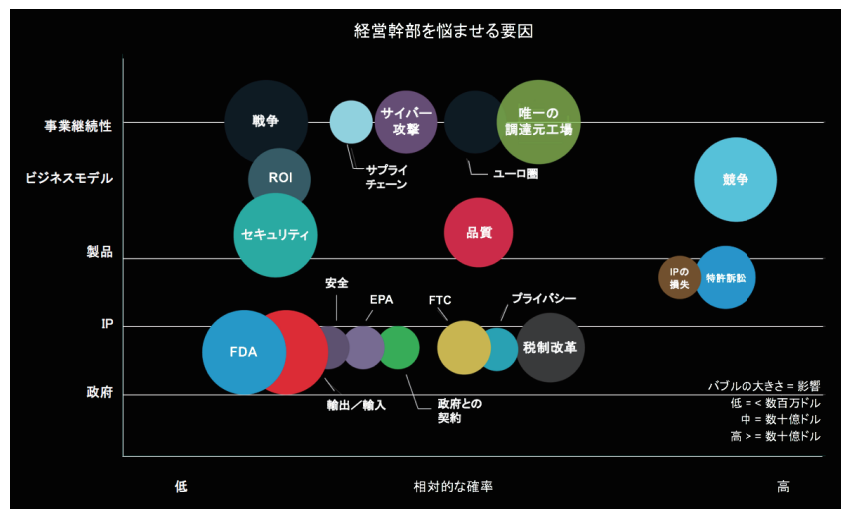
過去数十年間においてなかなかセキュリティ業界では改善が見られなかったのは上記の理由によるものです。これらを変えていくためには、この問題の根本的な解決が必要です。そして、コストを削減していくためにも「自動化」を進め、「防御」という形にリスク対応策をシフトしていくべきです。

VIII. サイバーリスクを企業リスクと紐付ける

取締役レベルになるとCEOも含め、常に企業としてのリスクを考えています。数十億ドルに及ぶ要素という、例えば税金の問題があるかもしれません。また、ヘルスケア業界であればFTA承認がなければ新たな薬事の承認を得ることができません。品質の問題、あるいは競合という問題もあるかと思えます。

こうしたマクロリスクを取締役は理解しています。そこで、CISOはこの取締役が抱えるリスクとサイバーリスクを繋げていかなければいけません。そして直接的・間接的なサイバーリスクを理解し、このマクロリスクと呼ばれる数十億ドルにも及ぶリスクに対応できるよ

うになる必要があります。これができるようになれば取締役レベルとのビジネスにおける対話がスタートします。なぜサイバーリスクが重要事



項なのか、そして注目すべきことであるのかを説明できるようになるわけです。

IX. リーダーシップの法則

ここで再びリーダーシップが問題になります。リーダーシップは従業員を共通の目的に向けて一つにまとめ上げ、意欲を高めていく行為といえます。チームの意欲を高め、IT組織の意欲を高め、課題に直面していくのです。これは外部要因と内部要因の両方の領域に対応する気持ちを高めていくことにつながります。

ここに挙げるリーダーシップの法則は非常に説得力があるものだと思います。

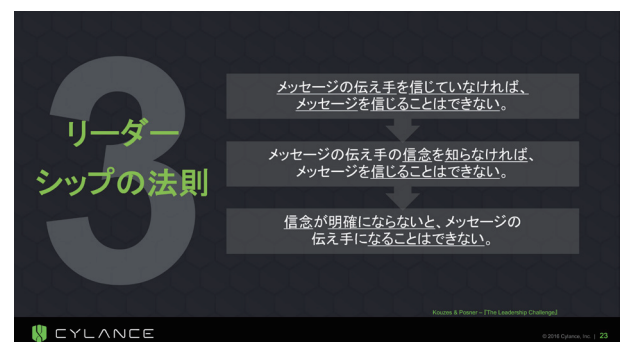
その1は「メッセージの伝え手を信じていなければメッセージを信じることはできない」ということです。情報セキュリティについて語る時、エグゼクティブはその主要な側面を理解しないとイケません。セキュリティリーダーはビジネスの主要な側面を理解しないとイケません。その両方が成立して初めて、セキュリティリーダーのメッセージはオーディエンスにとって信じられるものになります。

しかしメッセージの伝え手を信じるためにはその人物が何を信念としているかを理解しなくてはなりません。これは私の同業者の間でも課題になっています。例えば、セキュリティ組織の担当者となった時に、「自分たちが何を信じているのかははっきりしていない、明確にリスクが理解できていない、どうすればIT部門がそれを管理できるのかをきちんと説明できていない」というのが一例です。また、文化的なトランスフォーメーションが必要だったにも関わらず、ビジネス面・リスク面についての会話が十分ではなかったというケースもあります。

自分の信念が明確にならないと、リーダーとしての発信はできません。信念に関してはインテルにおける私の長年の課題でもありました。リスク管理の方法は分かっている。そしてビジネスについても分かっている。

X. セキュリティチームにおけるモットー

多くの企業は模範・テーマといったものを掲げています。例えば「大胆になり、大きな構想を持ち、迅速に行動する」というものが挙げられます。なぜこのようなモットーがあるかというと、ビジネスは常にスピード



テクノロジーについても学んで理解することができました。しかし2006年・2007年頃、情報リスクとセキュリティについて役員会で説明を依頼された際、私に与えられた時間は30分と限られていました。この時、私は自分の信念と向き合うことを決意し、私のチーム・ビジネスにとっての重要事項とその内容を理解してもらい、何をすべきかが分かるように伝えることに注力しました。

今振り返って考えてみると、私のミッションは目的と理念を考えた時に変化しました。私はそこで「Protect to Enable」ということを考えました。それはつまり「人・データ・ビジネスの利用を実現するための防御がミッションである」ということです。人々の生産性を妨げるものを阻止しなくてはならないという理念です。

そして、役員会ではパラダイムをコントロールすることが重要だと説明し、企業にとってのリスクは何なのかを話しました。こうやって、私は外部要因と内部要因、両方の領域で成果を上げることができるようになりました。

を求めるからです。ただ、このような内容のモットーはセキュリティチームにあまり関連するものではありません。しかしビジネスは常に方向性を持ったスピードを求めます。

しかし、このモットーをセキュリティチームに置き換えたとき、重要なのは「大胆になり、大きな構想を持ち、迅速に行動する」ことではなく、まずは「勇敢になる」ということです。

多くのセキュリティ部門はリスクを恐れています。

一方で、勇敢なセキュリティ組織は、リスクを含んだ施策も実現します。例えばクラウドを早くから導入し、AIもいち早く活用します。新しいテクノロジーをどんどん導入していくのです。勇敢に導入していかないと、人々を動かすためのプロテクションについて学ぶことができないからです。

またセキュリティリーダーは「飛躍的な構想」を持たなくてはなりません。24年間インテルにいた私はこのことをよく理解しています。コンピューターとサイバーリスクはどちらもムーアの法則に基づいて何十年間も飛躍的に増加しているのです。

しかしサイバーリスクに対してのコントロールは直線的にしか増加していません。結果として、リスクが増大しているのが今の状況です。

このような背景から、私はセキュリティについてはチャレンジして飛躍的に考える必要があると訴えています。また、セキュリティのための行動は目的を持って行わなくてはなりません。皆さんは企業のミッションを理解することが必要です。

先ほど挙げた「Protect to Enable」という考え方があります。活用す



るものは、人・データ・そしてビジネスです。そのための防御を株主が求め、そして業務部門のリーダーにも求められる。このように目的を持って行動することがCISOに必要とされる資質です。

XI. セキュリティエグゼクティブの役割

異なるCISOの側面として、おそらくほとんどのセキュリティエグゼクティブが自分たちの役割を過小評価していると思います。情報セキュリティというのは、リスクという万華鏡における1側面しかありません。他の側面としてはプライバシー・世界的な法令順守や規制もあります。また事業継続性と災害復旧、製品やサービスのセキュリティも網羅しなければなりません。

私はインテルで情報セキュリティに加えて、製品のセキュリティも担当していました。しかし今や、全ての企業はテクノロジー企業になっています。もしアプリやWebサイトを持つ企業であれば、それは顧客と繋がるためにテクノロジーを使っていることになります。そうすると当然、製品のセキュリティも統括することになります。例えばリアルな店舗しか持っていない企業でも、テクノロジーを製品やサービスに導入するということであれば、やはりテクノロジー企業です。すると情報セキュリティの課題が出てきますし、またプライバシーの



問題にも対応する必要があります。だからこそ私も同業他社や同僚に対して、CISOとして全体のビジネスを見て、全体の情報リスクの観点から管理する必要があると訴求しています。

XII. CISOの3スタイル

CISOあるいはCSOのキャリアアップにはいくつか異なるやり方があります。まずは、テクノロジストとしての役割があります。テクノロジーを理解して、技術を確立し、知識を積み重ねていく。しかし私のような人間はテクノロジストではなく、どちらかというビジネス側の人間で、リスクやコントロールのバックグラウンドをより理解しています。

先ほど挙げた通り、セキュリティのエグゼクティブはZ型でないと全ての範囲をカバーできません。テクノロジー側の人間はビジネスのセンスを磨かないといけません。もしビジネスリーダーであれば、テクノロジーのセンスも磨く必要があります。さらに企業の中には、他にもカバーしなくてはならない範囲があります。

セキュリティリーダーはCIOに業務報告を行うだけでいいのでしょうか？単に社内のポリシーやルールだけを責任範囲とする場合もあれば、全体の予算や意思決定が範囲となる場合もあるかもしれません。

その場合は、財務担当、もしくは法務担当に報告が必要かもしれません。

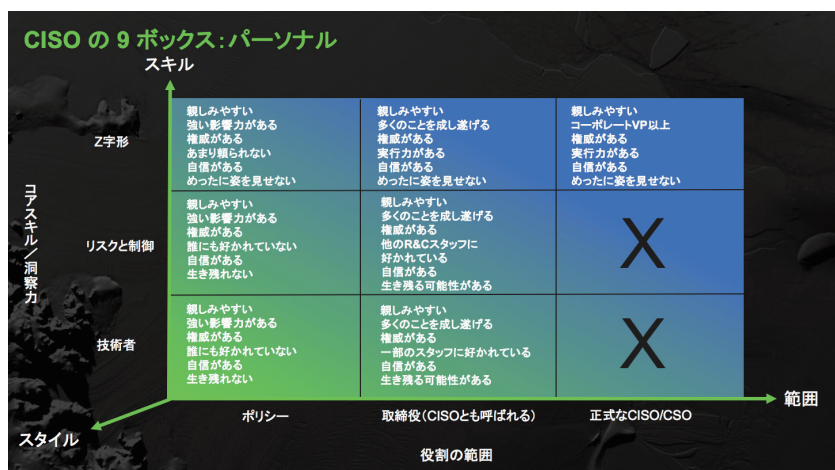
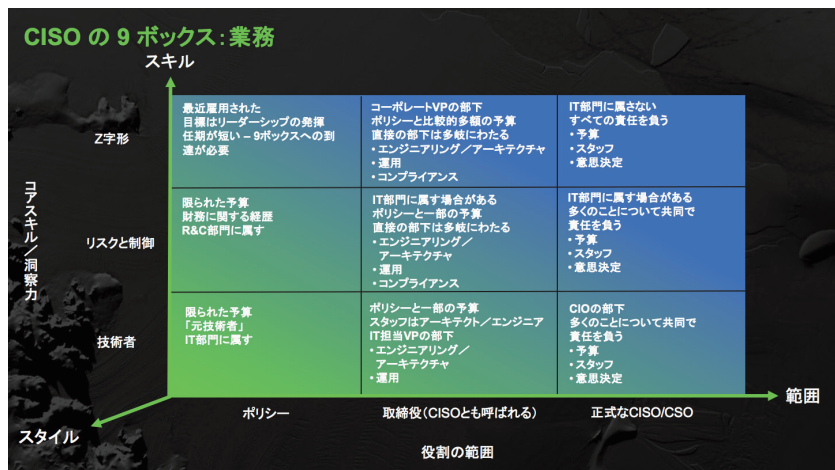
どのような責任範囲にも正誤はありません。しかし、全体的なビジネスリスクを管理する必要性を踏まえると、セキュリティエグゼクティブは自分の責任範囲をできるだけ拡大する必要があります。

ビジネスの話ができると同時にサイバーリスクを管理できるCISOになる必要があります。ここではCISOのスタイルというもう1つの側面が関係してきます。

CISOのスタイルは3つのタイプに分けることができます。「過信タイプ」「権威タイプ」「親しみやすいタイプ」の3つです。

「過信タイプ」は横柄とでもいうべき、自信があまりすぎるタイプの人です。他の役員とは上手くやれない方もいるかもしれません。「権威タイプ」は、何をしなければならぬのかを権威を持って対応していくタイプの人です。そして誰とでも仲良くやっていける「親しみやすいタイプ」の人もあります。

CISOのパーソナリティで何がベストなのかを考えてみましょう。それはおそらく、「過信タイプ」あるいは単なる「権威タイプ」ではなく、権威と親しみを持ち合わせているタイプでしょう。このようなタイプの人は、意思を強く持ちながら自分が何を信念としているのかを上手く伝えることができ、そして何かを成し遂げることがで



きます。その一方、親しみやすいパーソナリティも持っていて人と上手くやっていくことができるため、話をすると、他の組織・他の部門の人間であっても皆が耳を傾けたいと思うのです。こういったスタイルの人が、内部要因を上手く管理できるのです。

XIII. 長年にわたる教訓のまとめ

私のこれまでの学びは、4つの要素にまとめることができます。

まずは「制御の9ボックス」です。リーダーはやはり制御のパラダイムを変え、制御の9ボックスに基づいてコストを下げ、そしてリスクを下げるために防御型に持っていくべきだということです。そしてビジネスのスピードを上げるために無駄で必要のない摩擦を緩和していかなければいけません。

次に「リーダーシップの3つの法則」です。メッセージの伝え手として必要なのは、信頼を得ること、信念を明確にすること、信念を伝えることです。リーダーシップを発揮することで、セキュリティチームを引っ張っていくことができ、大きな課題に対応することが可能になります。

そして、「Z字型」です。自身をこのZ型に成長させて欲しいと思います。テクノロジストのバックグラウンドを持っていらっしゃる方であれば、ビジネスのスキルを身に付けてください。そして反対にビジネス側の方であれば、テクノロジーのスキルを身に付けて欲しいと思います。

長年にわたる教訓のまとめ

制御の9ボックス – リーダーは、前進と移動を区別することができる
リーダーシップの3つの法則 – 信念を明確にする
Z字形 – CISOは、自らの役割の範囲を広げて、スキルとスタイルを向上させる必要がある
1つの真の目的 – Protect to Enable® (物事を実現するためのセキュリティ)

© 2018 CyLance, Inc. | 33

最後に「一つの真の目的」です。真の目的を見つけてください。私はセキュリティチームのミッションが、「何かを実現するためのセキュリティである」という考えが見つかった時に、これが私の信念であり真の目的であると気づきました。この目的によって私の行動も変わり、セキュリティチームの行動も変わりました。そしてセキュリティチームが社内非常に重要視されるようになったのも真の目的に気づいたことがきっかけでした。



「CISO の明日はどっちだ!？」 イベントレポート 企業における情報システムのあり方、CISO の役割について

2019年1月21日 初版

講 演 者 Cylance Inc. 最高セキュリティおよびトラスト責任者 マルコム・ハーキンズ
レポート制作 エムオーテックス株式会社
監 修 Cylance Japan株式会社
発 行 元 エムオーテックス株式会社
〒532-0011 大阪市淀川区西中島5-12-12 エムオーテックス新大阪ビル
TEL:06-5460-8989 FAX:06-6308-8977

[本件に関するお問い合わせ先]

エムオーテックス株式会社 企画広報部 TEL:03-5460-1373 press@motex.co.jp