リスクマネジメント協会2016年次大会 RIMS JAPAN CHAPTER CONFERENCE

ERM（エンタープライズ・リスクマネジメント）におけるサイバーリスク戦略

DEVELOPING A CYBER RISK STRATEGY

2016年度RIMS理事長 ジュリー・ペンバートン
Julie Pemberton

ジュリー・ペンバートン 自己紹介

本日は、みなさまの前でこのようにお話をする機会をいただき、誠にありがとうございます。私は、ジュリー・ペンバートンと申します。RIMSの2016年度の理事長です。私はRIMSに参加して16年以上、リスクマネジメント、保険の仕事に携わるようになってから既に25年以上になります。

私が勤務するアウターウォール社での私の仕事は、エンタープライズ・リスクマネジメントとグローバルに保険を管理することです。アウターウォール社は、「OUTR」という銘柄略称でニューヨーク証券取引所に上場しています。我社は、米国、カナダ、アイルランド、英国において自動両替機、ATM、レンタルビデオ等小売店における自動販売機を販売している会社です。設立当社は、我社で最も知られている自動両替機コインスターの名前を使いCoinstar Inc.としていました。その後、我社は年商20億ドルまで成長しました。

私の現在の職域は、私が以前「チキータバナナ」の会社で勤務していた時と同じです。当時のチキータバナナは社員数約25000名、米国、英国、アフリカ、ラテンアメリカ、スイス、バミューダに拠点を置き、60カ国で商品を販売していました。チキータ社の前には、グローバルなブローカーであるAON社に在籍し、多数の業界の様々な企業からのリスクマネジメントに関する要請に対応しました。

広い範囲でリスクマネジメントに携わってきた私が迷いなく言えることは、「リスクの専門家という職業は、今後も進化し続けるとともに、その責任範囲はますます広がっていく」ということです。

JULIE PEMBERTON INTRODUCTION

Thank you so much for giving me the opportunity to speak with you today.
My name is Julie Pemberton and I am RIMS 2016 President. I've been a member of the Society for more than 16 years and have worked in the risk management and insurance industry for more than 25.

In my current role with Outerwall, I lead the enterprise risk and insurance practice globally. Outerwall is a public company listed on the New York Stock Exchange under the ticker symbol "OUTR." We are a leading provider of automated retail solutions in the United States, Canada, Ireland and the United Kingdom. The company was founded as Coinstar Inc. with its most mature line of business bearing the same name. The company has grown to annual revenue of more than $2 billion US dollars.

In my immediate prior role, I led the same functions for Chiquita Brands, Inc. At that time, Chiquita had approximately 25,000 employees with product in more than 60 countries and a business footprint in the United States, United Kingdom, Africa, Latin America, Switzerland, and Bermuda. Prior to my employment with Chiquita, I worked for a global broker (AON Risk Services, Inc.) and in that role I served a vast array of industries with various client needs related to risk management.

I've experienced a broad view of risk management and I can say without doubt, our world as risk professionals continues to evolve – and our responsibilities continue to grow.

リスクが顕在化した際の影響の軽減に加え、好まざる事象の発生を阻止するだけでなく、リスクを受け入れ、リスクテイクすることによりビジネスを成長させるという考えを創造し、そのリスクマネジメント手法を開発しています。

どの発明も、どのスタートも、プロセスもガイドラインもプロトコール、基準も全ては発想から始まるのです。

今年度のRIMSの活動は、近年改訂した活動指針である「世界のリスクマネジメント社会に対し、教育、保証、主張すること」を実践します。

RIMSの第62代理事長として以下の活動を行います。
- 快活で情熱的な会員の皆様と会い、多くを学びます。
- RIMSがリスクマネジャーの将来に焦点を当てた活動をするよう導きます。
- 皆様のリスクマネジメントに関する創造性の障壁を取り去り、皆様の発想力を促進させます。
- 皆様の考えが所属組織で貴重な資源として受け入れられるようサポートします。

OUTERWALL

私が現在携わっている職務に関し、もう少しご説明させていただきます。

私の仕事は、グローバル・エンタープライズリスクマネジメントのプロセスを実行するために、経営陣、戦略計画、コンプライアンス、情報セキュリティ、内部監査、法務、そしてオペレーションの各部門と関わることが必要です。また、私のチームは各部門における保険の設計と購入、そして保険金請求が発生した際の処理を行っています。

私はこれまでの経歴で、様々な保険をカスタマイズしてきました。例えば、以下のような内容です。
- D&O保険
- 信託
- 労災
- 犯罪
- スペシャルリスク
- 財産
- 貨物
- 船舶
- 空輸
- 医療事故
- そして、サイバーリスクです。

トピックの紹介

このリスクマネジメント及び保険の領域で最後に掲げた「サイ

In addition to mitigating the impact of risk, we are initiating creative ideas and developing solutions to not only prevent unwanted risks but to embrace and enable risk taking that optimizes business growth.

Every invention. Every startup. Every process, guideline, protocol and standard starts with an idea.

This year, RIMS will stay true to its newly revised mission statement….to educate, engage and advocate for the global risk management community.

As RIMS 62nd President, I look forward to:
- Meeting with and learning from our bright and enthusiastic membership;
- helping RIMS focus on the future of our profession;
- Unlocking and advancing your risk management creativity; and
- helping you convert your ideas into valuable resources for your organization.

OUTERWALL

Let me tell you a bit more about my role with Outerwall.

My job requires me to partner with senior leadership, strategic planning, compliance, information security, internal audit, legal, and operations to execute upon global enterprise risk management processes. My team also designs and places insurance programs for the organization and manages related claims that occur.

Throughout my career, I have customized many areas of insurance including:
- directors & officers
- fiduciary
- employment practices
- crime
- special risks
- property
- cargo
- marine
- aviation
- medical malpractice,
- AND, cyber risk.

TOPIC INTRODUCTION

It's this last area of risk management and insurance – Cyber

バーリスク」が現代社会において、世界中のリスクマネジャーが最も懸念しているリスクです。そして、それにはそれなりの理由があるのです。

昨年、Allianz Global Corporate & Specialty 社が、「サイバーリスクへのガイド」という報告書を作成しました。同社は、世界をリードする企業のサイバー犯罪による被害額を算出しました。

その金額は驚異的です。ここ日本だけでも、その費用の概算は9億800万ドル（約1000億円）です。中国約600億ドル、私の国アメリカは1080億ドル（約13兆円）です。このチャートにある国々は、確実にこのリスクの影響を受けています。

日本の年金機構、ヤフー、一時は世界最大のビットコイン交換所であったマウントゴックス社、ソニーピクチャーズ社などがこの情報セキュリティ侵害の被害額の中心となりました。

私の調べでは、日本はサイバーリスク対策の主導者として大きな飛躍を遂げているように思われます。2020年のオリンピックに向けての活動が1つの良い例です。日本は、有識者としてハッカーを招聘し自分達のデータシステムの耐久性を検査しています。これは、有効的な戦略です。

日本は、技術分野において常に世界のリーダーとして君臨してきました。日本のビジネスリーダーは、日本が技術分野のリーダーであり続けるには、資源を投入し世界で最も優秀なサイバーセキュリティ国となることが必須であるということに気づき始めたのです。

Identity Finder and Ponemon 研究所が発行した「2014年度の巨大情報セキュリティ侵害事件」では、米国最大手チェーンストア「Target」社を取り上げ、同社がサイバーリスクの重要性を強調するキッカケとなった壊滅的サイバー攻撃を紹介しています。

E-Bay, JP Morgan, Chase, Home Depot などでほぼ同時期に発生したデータの流出、機密情報の漏えいなどの情報セキュリティ侵害をキッカケに、各企業はこれまで以上にサイバーセキュリティーへの懸念が増加しました。

Identity Finder 社のIT専門家に対する調査では、61%の企業がサイバーセキュリティーへの予算を平均34%増加したと答え、67%の企業は自社のシステムを情報セキュリティ侵害から守るために十分な予算を組み込んでいると答えました。

その他にも、情報セキュリティ侵害としてオペレーションシステムの変更や情報セキュリティ侵害によるその他影響などが報告されました。

Risk – that has become THE top concern for risk professionals around the world. And, there is good reason why.

Last year Allianz Global Corporate & Specialty produced a report titled, “A Guide to Cyber Risk.”
The company estimated the annual cost of cybercrime for the world’s top leading economies.

The numbers are staggering. Here in Japan alone, the cost was estimated at $908 million (US dollars). In China, $60 billion and in my home country, the United States, $108 billion. All of the countries on this chart are certainly experiencing the full-force of this risk.

Cyber breaches like the ones at the Japanese Pension Service, Yahoo Japan Corporation, the Tokyo-based Mt. Gox – which was once the world’s largest Bitcoin exchange – and Sony Pictures contributed to this number.

From my research, it seems that Japan is making great strides in its cybersecurity initiatives. The country’s work surrounding the 2020 Olympics is a great example. Inviting ethical hackers to come in and test the strength of their data systems is an effective strategy.

Japan has always been the world’s leader in technology. Business leaders here are now realizing that in order to remain the best in this sector, it’s critical that they devote their resources to becoming the world’s leader in cybersecurity.

A report by Identity Finder and Ponemon Institute titled “2014: Year of Mega Breaches” looked at Target, a retail giant in the United States, and their catastrophic breach’s impact on the way companies now address cyber risk.

In the wake of their data breach and a host of other high-profile breaches at eBay, JP Morgan, Chase and Home Depot that happened around the same time, companies have grown more concerned about cybersecurity than ever before.

In that Identity Finder survey of IT professionals, 61 percent of companies increased their cybersecurity budget by an average of 34 percent.
Sixty-seven percent made sure IT had the budget necessary to defend it from breaches.

Other findings included changes made to operations and other impacts the breach had on the company.

企業は、このサイバーリスクの対策に取組んではいます。しかし、問題は「企業はこれらのリスクに対する防止策の設置を適時に実施できているか?」ということです。

昨年、RIMSはサイバー調査報告書2015を発行しました。この報告書は、RIMSの米国のメンバーである様々な業界を代表したリスク専門家284名からの回答で、それら専門家が所属する組織は年収10億ドル（1200億円）を超える企業です。

それらの回答者に、「あなたの組織は2015年度サイバーセキュリティにどの程度予算を当てていますか?」という問いかけに、25%が100万ドル以上（1億円以上）と答えました。

こちらの図表で、これらの企業が何に予算を使っているかが分ります。情報セキュリティのモニタリング及び分析、そして検査システムがこのリストの上位を占めました。

このような情報セキュリティ侵害による影響への注意や注目度を考えると、一般的な企業は、情報セキュリティ侵害が発生しないよう防止に力を注ぐべきだと考えると思います。

しかし、こちらのような傾向を見ると、Thycotic Black Hat 2015「ハッカー調査書」では、87%のハッカーは、「企業がサイバーリスク対策への投資を増加させても、企業の重要機密データに侵入するのは、以前よりも簡単とは言わないまでも、2年前と同様程度に簡単なことだ」と指摘しています。

今日、全ての企業は、リスクの多くは現代社会ではデータがデジタル化されていることにあるという事を理解しています。

私達のサイバーリスクに対する考えは進化しています。以前は、「サイバーリスクは、もし発生したらではなく、いつ発生するかを考える」と言われていましたが、私達はその考えを進展させました。現代の課題は、「いつ発生するか?」ではなく「発生した際にいつ発見することができるか?」なのです。企業は、情報セキュリティ侵害は対応せずに保有するには大きすぎるリスクであることを十分理解しているのです。

先ほど、私達リスク専門家の役割が拡大していることを簡単に説明しました。サイバーリスクは、典型的な例です。企業やその組織のリスク専門家は、全てのリスクに対し事前に対応する必要があります。しかし、統計で説明したとおり、サイバーリスクに関しては特に前々に準備、対応する必要があるのです。

サイバーリスクへの対策が必要であることは必然です。もし、皆さんが所属する組織に事業活動をモニタリングし、サーバーリスクが顕在化した際の計画を立てているセキュリティチームがあるとすれば、それは大変幸運なことです。その場合、そのチーム

Companies ARE adapting but the question is, “Are we making changes and implementing these preventative measures fast enough?”

Last year, the Society published RIMS Cyber Survey 2015. The survey features input from 284 of RIMS’ Professional Members in the United States. Majority of respondents represent organizations with excess of $1 Billion US in revenue, representing a wide-range of industries.

When we asked this group “How much will your company spend to protect cybersecurity exposures in 2015?” 25 percent planned to spend over $1 million dollars.

On the chart you can see where they planned to spend that money. Active monitoring and analysis of information security AND scanning tools topped the list.

One would think that with all this attention and awareness about the damage of a cyber breach, companies, in general, would be better prepared to prevent them from occurring.

But, then you see a statistic like this. “Thycotic Black Hat 2015 Hacker Survey” says:
Eighty-seven percent of hackers indicated that it is just as easy, IF NOT EASIER, to compromise privileged account credentials as it was two years ago, despite increased corporate cybersecurity spending.

Today, every organization knows that many of its biggest risks come from the digital world.

There has been an evolution in the way we think about cyber risk. We used to say “it’s not a question of IF you will experience a breach, but WHEN.” We have evolved our thinking. The question now is not when it will happen, but when will we discover it has happened. Organizations recognize that the potential to experience a breach is too great not to plan.

I talked briefly before about how risk professionals’ roles are expanding…cyber risk is a great example.
Organizations and their risk professionals must be proactive about all risks but as the statistics that I pointed out suggest, especially cyber.

Having a cyber risk strategy is a necessity. You may be fortunate enough to have an information security team who monitors your data and plan for events. In this structure, that team would be the owners of data risk. Not all companies have

がデータリスクのリスクオーナーになります。しかし、全ての組織にこのようなチームがあるわけではありません。このような専門チームが無い場合は、リスクの専門家がサイバーリスクを認識し、それを管理するための司令塔にならなければなりません。

皆さんが所属する組織がどのような組織体系であっても、リスク専門家は組織の資産としてのデータや組織としてのサイバーリスクにおける優先順位を経営者、経営陣や保険のアンダーライターに説明できなければなりません。

この知識無しに、組織を守るために必要な保険の購入や現場社員と防止対策を検討することはできません。

皆さんが日々クレジットカードを取り扱う小売店で働いてるかどうかは一切関係ありません。どのような業界においても、知的財産に関わるデータや社員の個人情報といった管理しなければならない重要な情報を処理、保存しているのです。

データを管理するということは非常に気が重い仕事です。それは、現代社会では、私達はテクノロジーに頼りきっているからです。2012年のFinancial Timesに、「企業は一日に2.5エクサバイトまたは10億ギガバイトの情報を創出している」という記事が掲載されていました。これは既に3年以上前の話です。今日ではどのような数値になっているか、想像してみてください。

情報セキュリティ侵害の定義

企業は、情報セキュリティ侵害への対応を計画する必要があることは理解しています。なにから始めればよいのか?を見つけるのが課題かもしれません。サイバーリスク戦略を開発する際の基礎の1つは、全社員が「情報セキュリティ侵害」の意味、内容を十分理解するということです。

RIMSのエグゼクティブリポートである「サイバーワールドのERMベストプラクティス」では、情報セキュリティ侵害を「重要で保護された、または機密の情報が認可されていない個人または組織により閲覧、盗難される単独または継続的事象」と定義しています。

例えば、私のプレゼンテーションの中では、サイバー攻撃の逆、つまりサイバー攻撃を受ける側の立場という意味で「情報セキュリティ侵害」という言葉を使います。情報セキュリティ侵害とは、より広い範囲を意味します。サイバー戦略を検討する場合、初期の段階で組織に対し、「情報セキュリティ侵害の全てがサイバー攻撃によるものではない」ということを明確にする必要があります。

Ponemon研究所の報告書「情報セキュリティ侵害研究の費用：グローバル分析2015」では、情報セキュリティ侵害の根本的

this structure and sometimes the risk professional will be responsible to lead the effort of identifying and managing the risk.

Whatever your organizational structure, as risk professionals, we need to understand the data assets and top cyber priorities in our companies and must be able to explain both assets and priorities to senior leadership and to insurance underwriters.

Without this knowledge, we won't be able to purchase the right coverages to protect the organization or initiate conversations with operations about preventative measures.

Whether you are a retail business who routinely processes customers' credit card information or not, your business will process and possess sensitive data including intellectual property and employees' information – all of which must be protected.

Protecting data is a daunting task mainly because how reliant we all have become on technology. According to a 2012 Financial Times article, at that time companies were generating 2.5 exabytes, or 1 billion gigabytes of data a day. That was more than three years ago – imagine what that number is today.

DEFINING DATA BREACH

Organizations know that they need to plan for a cyber breach. Figuring out where to start might be an issue.
One of the fundamental steps in developing a cyber risk strategy would be to ensure that everyone understands exactly what a data breach is.

RIMS Executive Report "ERM Best Practices in the Cyber World" defines data breach as an incident (or series of incidents) in which sensitive, protected or confidential information has potentially been viewed, stolen or used by an individual or entity unauthorized to do so.

For example, throughout this presentation I will use the phrase cyber breach as opposed to cyberattack. A breach is more encompassing. During the initial meeting to set the cyber strategy it's important that we remind our organizations that not all cyber incidents are the result of an attack.

The Ponemon Institute's "2015 Cost of Data Breach Study: Global Analysis" took a look at the root causes of data breaches.

原因追求をしています。そして、その結果調査対象となった11カ国から、サイバーアタックによる問題の発生は全体の47%に過ぎないと報告されています。情報セキュリティ侵害と分類された47%は、悪意的または犯罪的事象のどちらかでした。

その他の原因は、ほぼ同規模に2つの組織内部要因でした。1つはヒューマンエラー、もう一つはシステム故障です。

その他の表現、例えば「重要な記録」や何を基準に「システム故障」と呼ぶかなどは、十分に検討し賛同、理解を得たうえで次に進まなければなりません。

データの評価・査定

組織が、サイバーリスク戦略の必要性を理解し、その言葉や表現の理解を社内で統一した後、次のステップはデータの評価・査定プロセスを始めます。

包括的な評価と計画は、組織全体とそのデータを対象に全社的な視点で行わなければなりません。特に各業務部門やシステム、社員それぞれがつながっているかを徹底的に調査します。

このつながりを強化するために、サイバーリスクチームを設置することにより経営者や各部門の管理者から情報や協力を得やすくする体制を設置している企業もあります。

サイバーリスクチームを編成する場合は、技術部門のリーダーと法律のアドバイザーを含めることが重要です。さらに、組織のコアとなる部門のマネジャー、コミュニケーショングループ、人事部などからのスタッフもメンバーに入れることも重要です。このような人材が社内で集められない場合は、組織外部の専門家を含める必要があります。

サイバーリスクチームは、情報セキュリティ侵害対応の計画およびその実行の重要な役割を担っています。しかし、データ評価の初期段階では、組織における各データの特長に関する考えを提供するために召集されます。

このグループは、リスク担当者が組織の各部署がデータをどのように利用しているかをより理解し、データの機密性における優先順位を決定する手助けをします。

情報セキュリティ侵害発生前または発生時の対応にしても、このチームには各部署のリーダーが招集されているため、情報セキュリティ侵害に関する新しい戦略やその軽減対策規程に関する議論・決定を全社的レベルで実施することが容易になります。

And, for the 11 countries represented in the research only 47 percent of the breaches resulted from attacks. That 47 percent fell into a category of cyber breaches that were either malicious or criminal.

The remaining were almost split equally into two internal factors. The first was human error. The second was system glitches.

Other terminology – for example what is “a compromised record” or what constitutes a “system glitch” – should also be reviewed and agreed upon before moving forward.

DATA ASSESSMENT

Once the organization agrees that a cyber risk strategy is needed – and has agreed upon a common understanding of vocabulary and terminology – the next step is to begin the data assessment process.

A comprehensive assessment and plan should take an enterprise-wide view of the organization and its data. Special attention should be devoted to bridging the silos between internal operations, systems and people.

To achieve this, some organizations have formed a Cyber Risk Team as a means of getting input and support from leadership and business operations leaders.

When forming a Cyber Risk Team, you should ensure the team includes technology leaders and legal advisors. But, managers from key business operations, your communications group and human resources would also be important members of this team. If these areas of expertise are not represented in the skillsets of your internal team members, it may be necessary to engage outside resources.

The members of your Cyber Risk Team will play an important role in setting and executing the breach response plan. But, in the preliminary phase of data assessment, they’ll be called on to provide their unique perspectives on the organization’s data.

This group will allow risk professionals to gain a better understanding of how their individual departments use data and, also, help prioritize the sensitivity of data.

Whether it’s prior to a breach or in reaction to one, because leaders from various functional areas are included on this team, new strategies or protocols to prevent or remediate a breach can be easily communicated across the organization.

このチームにはリスク担当者の参加が不可欠です。なぜなら、リスク担当者は経営陣との連携役となりこのプロセスを実施するための資源を確保することができるからです。

最終的には、このチームが情報セキュリティ侵害に対する戦略や軽減対策を設置、実施するための承認は、上級経営者が行います。

データ（情報）の定義

データの定義をすることが次のステップです。このステップの目的は、データとは何か、どこに保管されているのか、誰がそのデータへのアクセス権があるのか、どこへ流れるのか、などをより理解することです。

データは、以下の3つの形で存在します。
- 紙
- 電子
- 人の記憶

データには、サイクルもあります。データは、そのサイクルのどこにあるのかを知ることが重要です。
- そのデータは、誰かから送られたのか？ または社内で作成されたのか？
- そのデータは、現在使用されているか？ 維持されているか？ 保管されているか？
- そのデータを使用した後、それはアーカイブされるのか？ 破壊・破棄されるのか？

データがこのサイクルでどの段階にあるかにより、組織の取り扱い方に大きな影響を与えます。危険なデータ、機密データはビジネスを行う上で貴重であるかもしれませんが、それが危機の根源となる可能性もあります。それらのデータは、取扱いに十分注意するほか、必要なくなった時点で確実に破棄されなければなりません。

データを定義し、重要度の順位付けをした後は、組織内における入手から保管、移動といったデータの流れの図を簡単に描くと非常に便利になります。

これは、データのフローチャートのサンプルです。このチャートには全てが含まれているわけではありませんが、みなさんの組織で、機密データに関する検討事項のいくつかは含まれているはずです。例えば、
- 何を機密データと考えるか？
- 誰が機密データを提供するか？
- どこに保管されているか？
- 誰がアクセス権限を持っているか？

組織がデータを管理するためには、4つの簡単なルールがあり

The make-up of the team will also require the risk professional to align with leadership, ensuring resources are committed for this process.

Ultimately, it is senior leadership who will approve the strategies and remediation initiatives set forth by the team.

DEFINING DATA

Defining the data would be the next step. The goal of this is to better understand what the data is; where it is kept, who has access to it and where it is going.

Data exists in three basic forms:
- Paper;
- Electronic; and
- Human Memory

Data also has a lifecycle. Knowing where it is in that lifecycle is important:
- Is the data received from someone or is it created by us;
- Is it currently being used, maintained or stored;
- When we're finished with it, will it be archived or destroyed.

Where data is in its lifecycle will have an impact on how the organization treats it. Like hazardous material, sensitive data may be essential to your business but it can be toxic. It must be handled with care and properly disposed of when it's no longer needed.

After initially defining and classifying the data, it can be very useful to simply draw the flow of the data as it enters, resides and moves through the organization.

This is an example of a data flow chart. And, while it's not all-inclusive, it does provide you with some of the questions your organization should be asking itself about sensitive data. For example:
- What do we consider sensitive data?
- Who provides sensitive data?
- Where is it stored?
- And, who has access to it?

There are four simple rules that organizations should follow

ます。

1. 必要でないデータは収集しない。
2. データの収集が必要な場合は、必要なデータのみ集める。
3. データ収集が必要な場合は、管理し暗号化する。
4. データが必要でなくなった場合は、すぐに安全に破棄する。

データのリスク評価は、いくつかの目的を達成するために行います。

始めに、組織の脆弱性を露出させます。「脆弱性」はこのプロセス開始時点で定義する必要がある言葉の1つです。

次に、データ評価は、組織の内部、外部における脅威となるリスクを認識するのに有効です。

3つめとして、組織内における管理状況の違いを記録するためです。アメリカでは、業界によっては法律によりサイバー戦略の1部を報告することが義務付けられています。

データのリスク評価は、ある一定のケースではマイナス効果が発生する可能性があります。データリスク評価のレポートは、敵にこちらの戦略を見せる結果となる競合他社への利点、または業務怠慢の証拠を作成する結果となる場合があります。そのため、組織はこのレポートが外部へ知られたくない情報などが無いよう注意することが重要です。データリスク評価を始める段階で、外部の助言者を付けておくなどの対策が有効です。

情報セキュリティ侵害　対応

サイバーリスクチームを召集し、データの評価、順位付けを行いました。機密情報がどのように管理されているか、データが組織内をどのように動くかを確認することができました。

リスク担当者として次に実行すべきことは、戦略的且つ率先的に情報セキュリティ侵害対応計画を設置することです。計画を設置することにより、組織で実際に情報セキュリティ侵害が発生したとき、私達は速やかに対応できるようになります。

情報セキュリティ侵害計画は、情報セキュリティに関する様々な事象が発生した事実や状況に応じ判断するガイドラインまたは源となります。しかし、その計画はあまり焦点を絞りすぎたものではなく、多くのケースで活用できるものでなければなりません。計画は、柔軟性を持たせることが重要です。

多少の違いはありますが、情報セキュリティ侵害計画を立てていない組織はそのような事象が発生した際、最善の対応策ばかりでなく、軽減対応や復旧作業をするための正しい資金を見出すことができず、非常に苦しんでいます。そして、予算にない資金は使えない可能性もあります。このとき初めて経営者は情報セキュリティ

when it comes to managing data:

1. If the organization does not need it, do not collect it.
2. If data must be collected, collect only what is needed.
3. If data is needed, control it and encrypt it.
4. When data is no longer needed, get rid of it – SECURELY.

A data risk assessment is designed to accomplish several objectives:

For starters, it will expose vulnerabilities in the organization. “Vulnerability” could be another one those terms that is defined during the onset this process.

Second, a data assessment identifies threats to the organization. That would include both internal and external factors.

The third reason is to record control gaps within the organization. In the US, some industries are required by law to report pieces of their cyber strategy.

A data risk assessment can also have a negative effect in certain situations. Reports stemming from a data risk assessment may provide a roadmap for an adversary, an advantage for a competitor or be produced as evidence of negligence. It’s important for organizations to seek to protect such reports from unwanted discovery. Retaining outside counsel at the start of a data risk assessment can certainly help.

DATA BREACH RESPONSE

Now you have assembled a cyber risk team, identified and classified your data. You’ve mapped out how sensitive data is managed and how it moves throughout the enterprise.

The next step requires the risk professional to be strategic and to proactively develop a data breach response plan so that when the organization experiences a breach, we know exactly what our next move is.

The data breach plan is a guideline and resource that can adjust depending on the facts and circumstances surrounding a specific event. But it should be a repeatable plan that can be applied to most incidents regardless of its specific characteristics. Flexibility will be an important attribute of a plan.

Despite the possible variances, organizations who fail to plan in advance often find themselves scrambling to identify the best response or the right resources to mitigate or recover from the event. Also, the funds for last minute, unplanned expenses might not be available. The first time management starts

侵害への対応は危機が発生した後では遅いことに気づくのです。

典型的な情報セキュリティ侵害計画と対応は以下のような流れです。

- 情報セキュリティ侵害の前計画
- 計画の実施
- サイバーチームのブリーフィング
- 調査と被害評価
- 改善と対策
- コンピュータ　フォレンジック（専門調査）補助
- マスコミ対応
- 義務的な違反通知
- 業務と環境のモニタリング

情報セキュリティ侵害が認識された場合、経営者は緊急事態としてその事象に対処しなければなりません。当然のように思われますが、情報セキュリティ侵害対応計画とその優先順位を理解し、明確にすることが重要です。

情報セキュリティ侵害が発生した場合、設置されたサイバーリスクチームは、以下の事を実行しなければなりません。

- 事象の処理、解決するために必要な資源を認識し、対応策を実施するための承認をできる限り早く取らなければならない。
- 情報を早急に収集し、どの情報まで組織にはあるか、どのような情報を得なければならないかを決定しなければならない。
- 情報の漏えいまたは喪失箇所を発見し、停止しなければならない。
- 情報の修復作業を実施しなければならない。
- ダメージがあればすぐに抑制しなければならない。
- 法律、規制、契約で決められた処置を取らなければならない。
- 被害を受けた個人または部門のサポートをしなければならない。
- 環境を修復し、データ喪失による影響に早期対応しなければならない。

組織は、情報セキュリティ侵害対応は非常に被害が集約する可能性があることを理解し、その上限に関しては現実的に考えなければならない。また場合によっては、外部の資源を活用しなければならないという事実を理解しなければなりません。

サイバー保険

情報セキュリティ侵害発生時に必要となる資源は、保険会社により提供されています。サイバー保険は、事象が発生する前の盾であり、事象発生後の組織の危機的財務状況を救うものです。

多くの場合、特にサイバーポリシーでセールスポイントとして記

thinking about a response should not be in the midst of a crisis.

A typical breach planning and response flow takes the following steps:

- Pre-Planning for Breach
- Execution of Plan
- Cyber Team Briefing
- Investigation and Damage Assessment
- Remediation and Resolution
- Computer Forensic Assistance
- Media Relations
- Mandatory Breach Notification
- Monitor Activities and Environment

Once the breach is recognized, management must address the issue with a sense of urgency. While it may seem obvious, it is important to understand and articulate breach response action priorities.

When a breach occurs, that Cyber Risk Team that you formed earlier must:

- Identify the resources needed for addressing and resolving the event and gain approval to launch a response effort as soon as possible.
- It must gather information quickly and determine what the organization knows and what it needs to find out.
- It has to identify and stop the immediate source of the data leak/loss.
- It must attempt to recover the information.
- Contain the damage, if any.
- Do what is required by law, regulation or contract.
- Assist those individuals or entities impacted by the situation.
- And, remediate the environment and exposures that caused or contributed to the data loss.

The organization needs to realize that a breach response may be a very resource intensive initiative and must be realistic about its limitations and, in some cases, concede to the fact that it may require assistance from outside sources.

CYBER INSURANCE

External resources needed at the time of a breach are provided by cyber insurers.
Cyber insurance is a backstop that is secured prior to a breach and could be crucial to the organization's financial needs post-breach.

Most of the time, the selling-point of cyber policies in

載させているのは、その会社の持つ外部専門家のネットワークです。そのため、情報セキュリティ侵害が発生した場合、サイバー保険を購入していれば、以下のような特典を受けることができます。

- 情報セキュリティ侵害に関するアドバイザーの紹介を得る。
- 情報セキュリティ侵害事象発生後の専門家紹介を得る。
- そして、財務的安心が得られる。

しかし、サイバー保険は比較的新しい商品です。多くの場合、財務的補填はコールセンターやフォレンジックの費用に対してのみ適応できます。また、風評被害による影響、ビジネスの中断による被害に対しても活用することができます。

それではここで、RIMS Cyber Survey 2015に戻ります。こちらを見ても分るとおり、リスクマネジャーや組織は、まだこのサイバー保険に関しては、懐疑的です。回答者の51%しか、単独のサイバー保険を購入していると答えていません。

私達は、そのサイバー保険にどのような内容が含まれているかも調査しました。ご覧の通り情報セキュリティ侵害の告知、データ回復、ネットワークの中断などがカバーされています。

情報セキュリティ侵害の最も重大なリスクである機密情報の盗難、風評被害、専門的責任に関しては、リストの下のほうにおかれています。私は、サイバー保険が高額なこともありますが、これら重大リスクが含まれていないことが、多くのリスクマネジャーがこの保険を購入していない理由であると思います。

また、情報セキュリティ侵害発生時の財務的影響の定量化は非常に困難であり、いくらの保険を購入するべきかがまだ不明瞭であるとも考えられます。

この情報セキュリティ侵害の影響における不明瞭さは、保険会社側でも同様であることが、填補範囲、保険料からわかります。情報セキュリティ侵害発生が流行する中、多くの企業が情報セキュリティ侵害対策を取っていますが、各事象の組織に与える影響度が異なります。このため、情報セキュリティ侵害による組織の損失を計算することはほぼ不可能な状態になっています。

しかし、日が経つごとに保険会社は提供内容を改訂し続けているため、組織のニーズに合った保険商品が開発されつつあります。

RIMSの調査に答えてくださったリスクマネジャーは、1、2年の間にサイバー保険を購入する検討をするかという問いかけに、74パーセントが「はい」と答えました。

さまざまな新しいリスクと同様に、そのリスクの内容を十分理解

particular are the external resources it funds. So, in cases of a breach, if an organization has purchased cyber insurance, it would possibly have access to:

- A cyber breach advisor
- A network of service providers that can assist post-breach
- And, maybe some financial relief.

But, I would mention that cyber insurance is a relatively new product. Many times, the financial support can only be used for expenses like setting up a call center or forensics. It can, however, also address reputation damage and business interruption.

If we go back to RIMS Cyber Survey 2015, we can see that many risk professionals and their organizations are still skeptical about cyber insurance.
Only 51% of the respondents purchase stand-alone cyber insurance policies.

We also took a look at what those insurance policies included. You can see that resources like Breach Notifications, Data Recovery and Network Interruption were covered.

While the most significant losses of a cyber breach – Theft of Trade Secrets, Reputation Harm and Professional Liability – were at the bottom of the list.
I think this, coupled with the high costs of purchasing a cyber policy, is the reason many organizations elect to forgo the coverage.

Also, quantifying the financial impact of a breach is daunting and may leave risk professionals uncertain as to how much, if any, insurance to purchase.

Those same uncertainties are evident from the insurer's perspective in the coverage and pricing offered. In their defense, despite the epidemic of cyber breaches, each event impacts organizations differently. This makes calculating the potential loss resulting from a breach nearly impossible.

But, as each day passes, insurers continue to refine their offerings and are developing better products that meet organizations' needs.

If you look at this chart, when we asked respondents if their organization would consider purchasing cyber coverage within the next 12-24 months…74 percent said YES.

Like with any new risk, it takes time for us to fully understand

するには時間がかかります。それを定量化できるようになるには、更なる時間が必要です。

it and even longer to quantify it.

ストレステスト（耐久性テスト）

一般的言語の定義、データの評価、情報セキュリティ侵害対応計画を開発した後、事象の発生を仮定しその対応計画の効果を検証する必要があります。このプロセスで露呈した問題点などを考慮し、対応計画を向上させます。

その他、プロセスで再確認が必要な事項は以下の通りです。

- 事象発生時における各個人の役割と権限の明瞭化
  - ― 全員がそれぞれの責任を理解しているか?
  - ― 全員が情報のエスカレーションプロセスを理解しているか? 例えば、各自の役割が完了した際、誰にその内容を報告するか? また逆に誰が各自に情報を伝達するか?
  - ― 事象が発生した際、サイバー戦略において各担当者が責任範囲における行動をする際、その権限は与えられているか? 権限の範囲や承認を得るためのプロセスに時間がかかる場合、対応を遅らせてしまう場合がある。

情報セキュリティ侵害対応策をテストする際、サイバー保険を購入するのであれば、契約内容の表現も適合しているかを確認することを強くお勧めします。この作業が、リスクマネジャーの必須業務です。この作業により、保険の填補内容が目的どおりか否か、損失が発生した際組織を守るのに十分な内容かを評価するのに有効です。私は、この作業を皆さんの組織のサイバー戦略の一部として検討することをお勧めします。

その他、事象発生後に関する検討事項

どのような準備、対策を講じても、情報セキュリティ侵害事象発生を阻止することはできないことはしばしばあります。組織で情報セキュリティ侵害が発生した場合、保険金請求を複数の保険会社にしなければならない場合もあります。

この場合、損失の定量化、書面提出はこのプロセスで最重要項目となります。このプロセスの一部として、リスクマネジャーは以下の事象を検討する必要があります。

- 全ての保険契約内容を再確認する：サイバー、財産、賠償保険は全て再確認し、全ての手続きに準じて請求する。このプロセスにおいて、契約内容に適合していることを確実にするために填補カウンセルの協力を仰ぐことも可能。
- タイムリーに告知を発信すると共にコミュニケーションの継続を確実に行う

STRESS TESTING

Once you have established a common vocabulary completed your Data Assessment and developed your Data Breach response plan – you should test the response plan in a hypothetical event to determine its effectiveness. Any lessons learned during this process should be applied to improve your plan.

Some of the processes that you also want to review include:

- Clarity and authority of roles individuals will be responsible for during an event;
  - ― Does everyone know what they're responsible for?
  - ― Does everyone understand escalation processes? In other words, once their task is complete, who do they report findings to and, conversely, who should be delivering information to them.
  - ― Do the individuals responsible for an action in the cyber strategy have the authority to execute when the time comes? Limitations or a time consuming approval process set by senior leadership could delay the response time.

Just as you would test your breach response plan, if you purchase a cyber insurance product, I suggest stress testing the contractual terms as well. This can prove to be an integral part of risk management's responsibilities. It will help to evaluate whether the insurance coverage will perform the way it is intended to perform, and adequately protect the organization in the case of a loss. I recommend you consider this as part of your organization's cyber strategy.

OTHER POST BREACH CONSIDERATIONS

Sometimes all the preparation in the world will not be enough to prevent a data breach. Once an organization experiences a breach, you may need to initiate a claim with one or more insurers.

Documenting and quantifying losses will be critical to this process. As part of this process, risk professionals should consider the following items:

- Review all insurance policies: cyber, property, liability, should all be reviewed and compliant with notification provisions for all. You may want to engage coverage counsel in this process to ensure you are meeting contractual terms and conditions.
- Ensure that you're providing timely notification and

- 事象を時系列にまとめる。情報セキュリティ侵害事象が発生した時点までさかのぼることにより根本的な原因を見つけることができる可能性がある。
- 情報セキュリティ侵害の終息を確認する。機密情報へのアクセスが許可されるべきでない社員が完全にアクセスできないシステムが設置されたかを確認する。
- 財務担当者に協力を依頼し、被害を計上するアカウント番号、または情報セキュリティ侵害事象の記録をするための特定の経費管理コードを作成、または影響を受けた部署において特定の管理コードを作成し、この事象で受けた費用を記録する。保険金請求する際、発生した損失を分類ごとにまとめることは、言うまでもなく非常に重要である。
- 情報セキュリティ侵害事象による財務的損失を説明するための書類を確保する。例えば、事象が発生する前の営業予算や見通しに関する書類。そして、逆に事象発生の結果として使用されなかった経費予算も認識する。
- 最後に、風評、ブランド価値、今後の戦略への影響に関し、経営陣と共にブレインストーミングを行うための会議を実施する。

これらのステップは、損失を定量化するために必須な作業です。このような作業により保険契約による組織の財務的回復を促進することができます。

最後に

最後に、データを管理するということを複雑で困難にしている要因はたくさんあります。

- 組織は、過去や他の経験から単純に被害想定をすることができない。
- ほぼ全ての情報セキュリティ侵害事象は独特であり、組織のサイバーセキュリティのレベルで常に新しい問題が発生する。
- そして、実際に発生するかわからないリスクに対し、予算を取るまたは資金を確保することは、経営者の理解を得るのが困難なこともあります。しかし、資金を確保していなければ、リスクマネジャーが努力して設置した計画に制限がかかったり上限ができてしまいます。

世界各国の経営陣は、現代社会はテクノロジーで埋め尽くされていることやデータは組織の最も重要な資産であることを理解しています。そのため、情報セキュリティ侵害発生頻度は、サイバーセキュリティを取締役会議の議題の上位に位置づけています。

ここまでお話したように、組織がこのリスクへの対応準備を確実にするために、リスクマネジャーが率先してできるステップやプロセスがあります。

- 情報セキュリティ侵害リスクに関する用語の定義。
- ERMの手法を活用し、全てのオペレーション部門を参加さ

ongoing communication.

- Create a timeline of events. Going back and pinpointing when the breach actually occurred might help find the root cause.
- Confirm the breach has ended. Has the organization taken the measures it needs to ensure that sensitive data is no longer accessible to those who shouldn't have it?
- Work with your finance partners to identify account numbers or charge codes specifically created to record costs related to the event or specific to the business areas affected by the breach. Cataloging expenses is unquestionably important when submitting insurance claims.
- Secure documentation that will help explain the financial loss of the breach. For example, sales budgets or forecast that were created before the breach. And, conversely, identify the costs that were put on hold as a result.
- Finally, brainstorm and facilitate discussions with leadership about the impact it will have on reputation, the brand or future strategy.

These steps will be crucial to quantifying losses and will expedite the process of recovering finances from insurance policies.

CONCLUSION

In conclusion, there are so many factors that contribute to the complexity and the challenges of managing data.

- Organizations can't confidently make assumptions from past or other experiences.
- Almost all data breaches are unique and are accompanied by a new set of questions surrounding the strength of the organization's cybersecurity.
- And, securing funding or resources for a potential risk, a risk that might not ever happen, can also be a challenge. But without that funding, there could be restrictions or limits to your planning efforts.

Board Directors around the world recognize that technology is everywhere and data is one of their most important assets. As such, the frequency of cyber breaches have put cybersecurity at the top of their agenda.

As we've discussed, there are some steps and processes a risk professional can initiate to ensure their organization is ready.

- Defining common terms
- Utilizing an Enterprise Risk Management approach to get

せ、サイバー戦略に貢献していただく。
- 評価のプロセスとして機密データの認識、理解、分類、マッピングを実施する。
- 計画を実施テストし、役割が認識され、全員が各自の責任を理解していることを確実にする。
- 簡単に適用できる情報セキュリティ侵害対応計画を開発する。
- 付保する。情報セキュリティ侵害が発生した場合でも普及、回復できるだけの資源を得られることを確実にするプロセス、そして
- 事象発生後の具体的な実行計画を持つ。

早急に情報セキュリティ侵害対応計画を新たに立てるということは、通常企業の最優先関心事項です。この計画は、組織が情報セキュリティ侵害の重大さを理解していること、そして事象回復に迅速に取組むことをステークホルダーや監督官庁に示すことができるからです。

リスク担当者には以下の事項全てが必須です。
- リスクマネジャーは、経営者の役割を受け入れ、組織のプライバシーや情報セキュリティグループなど各方面の専門家と良いパートナーシップを作らなければならない。
- リスクマネジャーは、計画をステークホルダーに明確に説明するために、分析力を磨くと同時に十分な技術的知識も持たなければならない。
- リスクマネジャーは、影響力、教育力、説得力を高め、サイバー戦略を実施する良い社内環境を整えることに関し、経営陣を納得させなければならない。
- そして、最も重要な点は、リスクマネジャーはただの伝達係ではないということ。私達は、組織を成功に導く解決策やアイデアを提供する準備をすることが重要である。

本日は、こちらで講演をする機会をいただき、誠にありがとうございました。RIMSの理事会そして日本支部の代表として今年度の理事長を務めることを光栄に思います。

ありがとうございました。

all business operations involved and contributing to your cyber strategy.
- Identifying, understanding, categorizing and mapping sensitive data as part of your assessment process.
- Testing your plan to make sure roles are identified and everyone knows their responsibilities.
- Developing a general data breach response that is easily adaptable.
- Insuring your organization. A process that will confirm that you have the resources you need to remediate and recover; and
- Then, having concrete action items post-breach.

Initiating a data breach response plan as soon as possible is always in the company's best interest. It shows both stakeholders and regulators that the organization understands the severity of the cyber breach and is quickly moving to remedy the situation.

Risk professionals are integral to all of this:
- We need to embrace a leadership role and create partnerships with subject matter experts in the organization's privacy and information security groups.
- We need to hone our analytical skills and, at the same time, have enough technical understanding to articulate the plan to stakeholders.
- We need to have the ability to influence, educate, persuade and convince management to establish an environment that supports the data breach strategy.
- And most importantly, risk professionals must be more than messengers. We need to be prepared to offer solutions and our ideas that contribute to the success of the organization.

I want to thank you again for allowing me to speak with you. It truly is an honor to represent RIMS Board of Directors and this Society here in Japan.

Thank you.