サイバー・リスク：
その問題と企業への影響

Cyber Risk: Issues and Implications for Your Business

デジタル化する市場における課題と機会、エクスポージャーの管理、デジタル化への依存と関連リスクの管理方法

Challenges and opportunities in today's digital marketplace, including exposures, digital dependence and methods for managing related threats.

2011 年度 RIMS 理事長 **Scott B. Clark, AAI**

はじめに

本日皆様の前でお話ができる機会をいただき大変うれしく思っています。私、日本は初めてですので、来れたこと自体がうれしく、またこの素晴らしい国についてもっと学びたいと思います。また、RIMS 日本支部の濱地様には私の日本での受け入れを引き受けていただきました。この場を借りてのお礼を申し上げます。

本題に入る前にまず私の職歴について、RIMS での最近の出来事について、そして 2011 年の私の理事長としての任期中の目標についてお話します。

職歴

現在私はフロリダ州のマイアミ・デイド郡の教育委員会のリスク・ベネフィット・オフィサーです。この職務は 11 年間務めており、全米でも第四位に入る大きさの学区の直面する様々な戦略的、実務面でのリスクを管理してきました。マイアミ・デイド郡でのリスクマネジメントの仕事自体は 25 年にわたって携わってきています。幸いなことにリスクマネジメントの制度の枠組みを構築することができ、これまで 34 万 5000 人の生徒たちが世界水準の教育を受けてきました。とてもやりがいのある仕事でした。

マイアミ・デイド郡の教育委員会以前は、まず 1982 年から自己保険の仕事につきました。次にマイアミ大学で学生に対し無償で提供する保険に関する授業を運営して

INTRODUCTION

It is a great honor to have this opportunity to speak with you today. This is my first trip to Japan and I am excited to have the opportunity to be here and to explore your great country. I would like to thank Yoshi-san for his generous hospitality during my stay.

Before we delve into our topic this morning, I would like to dedicate a few minutes to my professional background, to the latest news from RIMS and to the goals I have set as RIMS president for the 2011 term.

PROFESSIONAL BACKGROUND

My current position as the risk and benefits officer at the school board of Miami-Dade County, Florida is one that I have held for 11 years and that has afforded me the opportunity to look at strategic and operational risk issues for the 4th largest school district in the United States. I have been in risk management with Miami-Dade County for 25 years and have been fortunate enough to be able to shape the risk management program there, and to ensure that 345,000 children enjoy a world-class educational environment. It's been an extremely rewarding position.

Prior to joining the school board of Miami-Dade County, I began my career working in self insurance in 1982. Following that I became involved in student outreach at the University of Miami

いました。そこで1986年新しくできたマイアミ・デイド郡の教育委員会のリスクマネジメント部での仕事にスカウトされたのです。今日、リスクマネジメントの機能は組織の隅々にまで効率、革新、成長のためのツールとしてゆきわたっています。

RIMSについて

昨年、私の前任者であり、公的機関のリスクマネジャーであるテリー・フレミングさんが日本支部の大会に来てからRIMS内部でも多くのことが変わりました。皆様がRIMSの様々な情報やウェブサイトを過去1年の間に利用されたとしたら、もっとも目についたのは新しいロゴとキャッチフレーズだったと思います。新しいデザインは理事会のメンバーの間での慎重な議論の結果決まったもので、RIMSの成長戦略とリスクマネジメント自体の進化を意味しています。

これらの目につく変化とともに2010年はメンバー数が5%超と大きく伸びた年でもありました。この伸びはRIMSの年次総会で2010年の早い時期に成功への戦略を立てたことで可能になったと思います。

キャリア開発の面でRIMSは昨年いくつかの新しい研修コースを開設しました。グローバル保険マネジメント、プロジェクト・リスクマネジメント、サプライチェーン・リスクマネジメント、そして大きな成功をおさめたERMの開発・導入ワークショップなどです。

商品とサービスに関してはRIMSストア、キャリア・センター、リスク・ワイヤ、賞を取ったリスクマネジメント・モニター・ブログ、RIMS年次大会のセッションを選ぶ方式の見直し、より使いやすいウェブサイトなどがあります。また、ERMと戦略リスクマネジメントの強化のため戦略リスクマネジメントのエキスパートであるキャロル・フォックスを採用し、彼女に新しいERMと戦略リスクマネジメントの開発部門を任せました。

RIMS品質フォーラムが5年連続でニューヨーク市で開催されたことを受けて、初めてカナダのトロントでRIMS品質フォーラムを開催し、これまた高い評価を受けました。また、「議会におけるRIMS」も再度開催され、われわれの多くの立法関連の活動も強化されました。慎重に検討を重ねた後、2011年1月にはPAC（政治活動委員会）の設立を公表しました。この委員会は今年中に活動を開始し、その報告がバンクーバーで開かれる年次総会で行われます。

where insurance classes were being offered. It was while there that I was recruited to the newly formed Risk Management Department at Miami-Dade County Public Schools in 1986. Today the Risk Management function is firmly embedded in the fiber of the organization as a tool for efficiency, innovation and growth.

ABOUT RIMS

Since my fellow public sector risk manager and predecessor, Terry Fleming, visited your chapter in 2010 there have been some substantial developments within RIMS that I would like to share with you. As you engage with RIMS and our various resources and website, the most apparent development over the past year will likely be RIMS' new logo and tagline. The new appearance was decided upon after very careful consideration by the board of directors, and it emphasizes the Society's growth strategy, as well as the evolving nature of the risk management discipline as a whole.

In addition to this most obvious development, 2010 was also a year of growth in membership, which rose more than five percent. We believe this growth was supported in no small part by RIMS Annual Conference & Exhibition, which set a tone of success early in 2010.

On the professional development front, RIMS introduced several new courses last year including Global Insurance Management, Project Risk Management, Supply Chain Risk Management and the highly successful Enterprise-wide Risk Management: Developing and Implementing workshop.

On the product and services side, 2010 saw recognition and enhancements to the RIMS Store, Career Center, RiskWire, the award winning Risk Management Monitor blog, and the session selection process for RIMS Annual Conference, as well as a redesigned, user-friendly website. We showcased our commitment to furthering our focus on ERM and strategic risk management with the hiring of a strategic risk expert – Carol Fox – who will lead our newly developed Strategic and Enterprise Risk Practice.

After five consecutive years of successful RIMS Quality Forums in New York City, we produced our first RIMS Canada Quality Forum in Toronto, which was a resounding success. We also hosted another effective RIMS on the Hill and many of our legislative initiatives gained traction. In January 2011, after a great deal of research, we announced the creation of a political action committee (PAC). We're pleased to announce that RIMSPAC will be launched in 2011 and highlighted at the annual conference in Vancouver.

RIMSの理事長としての任期の目標

ご紹介してきました通り、RIMSでは多くのことが起きており、この勢いに乗って2011年は生産性が高い、大きな変化の年になるでしょう。私自身は今年はRIMSの屋台骨である地方支部に注目しています。私自身地方支部での活動がRIMSでの出発点でしたし、地方支部と本部のリーダーたちの対話をより深めることを第一の目標にしています。米国の、そして各国の支部からのフィードバックを通じて、各支部がどのような問題に直面していて、RIMSがどのように支援できるか知りたいと思います。いろいろな層の会員を支援するために支部長たちとの定期的なウェビナーも開催しています。

今年は地方のRIMSの法令や規制に関する活動も活発化させようとしています。これまで通り、国レベルでの情報発信は続ける一方で、より多くの地方で「議会におけるRIMS」のイベントを開催します。このような集まりを通じて、各地方にとってもっとも重要な法令や規制が何かを探るとともに、各支部のリスクマネジャーたちとの交流も活発化させられます。そのことによってRIMSへの参加意欲も高まると思います。

我々の提供するサービスについては、キャリアのどの段階にあるリスクマネジャーに対しても有用であるように心がけています。戦略レベルのリスクマネジメントを担当している人でもERMを担当している人でも、われわれの多様なサービスの中から各自のニーズとキャリア開発にぴったりとあったツールを見つけられるでしょう。

新しいロゴに象徴されるように、2011年は進化の年になるでしょう。日本でも専門性をさらに高めるための支援を惜しみません。そのことによってリスクマネジメントが世界的に強化されていけばよいのです。また、バンクーバーで開催される年次総会では学生のための特別イベントや教育セッションを設けて、学生の間での交流を進めていきます。

本日のテーマの紹介

本日の話のテーマは世界中の全ての組織が直面している問題です。今の時代は技術に頼らざるを得ない時代で、結果としてサイバー・リスクは今後10年間、場合によってはそれ以上の長い間組織が直面する最も重大な課題の一つとなっています。今日、ビジネスと技術の間には複数の接点があるため、このようなリスクは複数の原因によっ

GOALS FOR TERM AS RIMS PRESIDENT

As you can see, it's been a big year for RIMS and I anticipate that this momentum will carry us into a productive and impactful 2011. I have outlined some specific goals for the coming year, specifically including a focus on RIMS chapters, which I believe to be the backbone of this Society. I personally began my involvement in RIMS by becoming active in my local chapter and one of the goals central to my presidency will be that of fostering a discourse between national and local leadership. I will be looking for feedback from the chapters, in the United States and abroad, about the issues you face and how RIMS can help. To this end, I will be hosting periodic webinars with chapter presidents to ensure that we are well equipped to support you at all levels.

In 2011 I also plan to expand the scope of RIMS' regional foothold in legislative and regulatory matters. We will continue to be a watchful advocate on the national front, but will also increase the number of regional RIMS on the Hill events. These gatherings allow individual chapters to concentrate on issues that affect them locally and also taps into what I view as one of the most valuable aspects of choosing to be part of this organization—your ability to engage with your fellow risk managers at the chapter level.

On the resource side, I intend to ensure that our offerings speak to risk managers at all stages in their careers. Whether you are working in a strategic and enterprise risk management capacity or not, our resources will be sufficiently varied so that you will be able to find professional development tools tailored to your needs and growth.

The coming year will be one of advancement and progress, as illustrated by the new RIMS logo. We will be committed to harnessing the expertise here in Japan to strengthen the risk management community worldwide. We will also increase student interaction in RIMS by hosting special events and sessions aimed at student outreach during our annual conference in Vancouver.

INTRODUCE TOPIC

Our topic today is one with which every organization in every corner of the world must contend. We live in an era of technology dependence and, as a result, cyber risk is one of the most crucial issues organizations may face in the coming decade and perhaps beyond. Because of the multiple points of intersection between modern business and technology, these risks emanate

てもたらされます。脅威は法令面から起きることがあります。例えば財務報告の規制の IT 管理の条項に違反している、あるいはデータ・セキュリティの法令違反などです。サービス・プロバイダーが原因の脅威もあり得ます。例えば下請けの契約書の文言がいい加減であったために予期しない巨額の債務が発生してしまったり、競合企業が知的財産の権利侵害で訴訟をしてくる場合などがあります。2001 年 9 月 11 日の悲劇のような大規模災害によって起きることもあります。あの時、一部の会社はバックアップ用のデータにアクセスすることができなくなってしまいました。企業では IT インフラが適切に管理されていなければ企業自体が技術的なリスクの原因となりえます。私が住んでいるマイアミではハリケーンが学区と 345,000 人の生徒が授業を受けるうえでの大規模リスクです。

年間ベースで見ても数十億ドルの損失がデータのねつ造、個人情報の盗難によって発生しており、組織はこれらのリスクによってもたらされる損失に直接、間接的にさらされています。本日はどのようなリスクに対する露出があるか、いくつかの事例をもってご紹介し、皆様の組織でどのように対応策を取ればいいかを具体的に説明します。

第 1 部：エクスポージャー

インターネットを通じたコミュニケーションはほとんどの組織で当然のこととなっています。その結果、リスクマネジャーたちはますます多様なエクスポージャーに直面しています。いわゆるサイバーリスクは e コマースをやっている企業にのみ関係があると思われていましたが、機密情報を電子化して送っている企業はデータの不正利用、サイバー攻撃、企業イメージの失墜にさらされているのです。

例 1：データの不正利用

まずデータの不正利用についての驚くべき統計をご紹介します。ある調査によると、世界中の企業の 85%がデータの不正利用を経験している一方で、それら企業の 46%ではそのような不正が起きた後でも暗号化などの対策をとっていないというのです。

情報を守るということは、企業イメージの失墜、経済的損失、行政による介入、顧客からのボイコットなどから自社を守る上で最重要の対応です。データの不正利用によって発生しえるコストや費用の度合いは日々変化しており、正確に把握することができないものです。しかし、様々な組織がすでに法務費用、個人の信用調査、損害賠償、罰金、違約金、払い戻しなどで多大な損害をこうむっているという事実は知られています。

from a number of sources. Threats could be posed by the regulatory environment, such as non-compliance with IT control provisions of financial reporting regulations or with data security legislation. Threats can arise from service providers (for example, unmanageable expenses arising from a poorly drafted outsourcing contract) and competitors (for example, IP infringement claims). Threats can also arise from catastrophic events such as the tragedy of September 11th, 2001, following which some companies were unable to promptly access their back-up data. Additionally, a corporation itself could be a source of technological risk if its IT infrastructure is not properly managed. In my world in Miami, hurricanes pose a significant threat to the school district and our ability to serve the educational needs of 345,000 students.

With events such as data breaches and identity theft causing tens of billions of dollars in extra business expenses annually, organizations face an array of direct and indirect costs from these risks. Today I will take you through some examples of exactly what those exposures are, as well as specific steps which can be taken to address them within your organizations.

Part 1: Exposures

With Internet communications embedded in the processes of most organizations, risk managers face an increasing array of exposures. While cyber risks long have been associated with e-commerce firms, any firm that holds confidential information in an electronic format is exposed to the threat of data breaches, cyber attacks and risks to reputation.

Example 1: Data Breaches

First I would like to draw your attention to some startling statistics related to data breaches. Studies show that 85% of businesses worldwide have experienced a data security breach at some time and that of those businesses, 46% fail to implement encryption solutions even after suffering a breach.

The security and safeguarding of information is paramount to protecting an organization from embarrassment, reputational damage, financial loss, regulatory intervention and even public boycotting. The depth and breadth of the potential costs and expenses from a breach are still developing and not fully known. What we do know, however, is that organizations have already incurred significant cost and expense, from legal fees, credit-monitoring for individuals, reparations, fines, penalties and redress funds.

最近紙面をにぎわせたウェブサイトのウィキリークスもサイバーリスクへの露呈がいかに複雑で速く変化するかを示しています。ウィキリークスによって公表された情報のうち最も注目を集めたのは政府関係の情報でしたが、この問題は企業も重大な損失をもたらす情報流出の対象であることを意味しています。

例 2：サイバー攻撃

それでは話を変えて違った種類のリスク、すなわちサイバー攻撃についてお話しします。一般的な分類では戦争には四つの種類があります。陸、海、空、宇宙での戦争です。しかし、これにもうひとつの戦争、すなわち「サイバー空間」を加える定義もあります。

サイバー攻撃はいろいろな形をとります。例えばあなたが飛行機で米国を横断している最中に、空を飛んでいる全ての飛行機が地上の管制官と連絡が取れなくなったと想像してみてください。その後に来る混乱と失われる命が想像できますでしょうか。

あるいは外部の誰かがウォール街の IT システムを完全に止めたらどうでしょうか。もっと恐ろしいのは例えば全世界の株式取引所を中断した場合です。ハッカーが送電網をかく乱したり、軍事技術が効かないようにしたり、石油のパイプラインと精製所を機能不全にしたらどうでしょうか。

ここで紹介したような出来事は極めて現実的なもので、対応策を講じていない組織には大きな影響をもたらすものです。これらの出来事は全て、少なくとも理論上は悪意を持った当事者がいわゆるロジック・ボム（論理爆弾）とよばれるコードを意図的にソフトウェア・システムに組み込み、特定の条件がそろった時に機能するよう設定しておけば実現できることなのです。

実際に過去に起きているのです。2007 年、エストニアで、そして 2008 年グルジアでのサイバー攻撃は国の議会、外務省、銀行、新聞社を含むほとんどのウェブサイトを停止させています。多くの人たちがこの攻撃はクレムリンによって実行されたと批判しましたが、追跡の結果たどりつけたのは一部のロシアのサイバー犯罪者たちだけでした。

より最近ではグーグル、アドビその他の有名企業に対し、ウイルス対策会社マカーフィーの分析によると暗号化、ステル

Recent headline-grabbing leaks by the controversial website WikiLeaks again have highlighted for companies the complex and fast-changing nature of cyber risk exposures. Although the highest-profile information released by WikiLeaks has centered on government documents, this example reflects concerns which have been raised about corporations also becoming the target of potentially damaging information leaks.

Example 2: Cyber Attacks

Now I would like to switch gears and discuss some of the perils associated with a different breed of risk – cyber attack. In a traditional sense, there are four domains of war: land, sea, air and space. However, some now believe there is a fifth domain: cyberspace.

Cyber attacks can come in many forms. Imagine you are midflight on an excursion across the country when every plane in the sky looses contact with air traffic control. Imagine the chaos that would ensue and the lives that would be lost.

Or consider another scenario in which outsiders shut down tech-reliant Wall Street, or worse, interrupt stock exchanges worldwide. What if hackers could disrupt the electrical grid, compromise military technology or disable oil refineries and gas pipelines?

The threats posed by these events and others are very real and they have consequences for organizations who don't prepare for them. These scenarios could all, theoretically, be accomplished if enemies were to implement so-called "logic bombs," a piece of code intentionally inserted into a software system that can set off a malicious function when specified conditions are met.

And it has happened before. In Estonia in 2007 and Georgia in 2008 cyberattacks shut down most of those country's websites, including those of the parliament, ministry of foreign affairs, banks and newspapers. Many blamed the Kremlin for the attacks, but they could only be traced to independent Russian cybercriminals.

More recently, an attack was launched on Google, Adobe and dozens of other high-profile companies using never-seen-before

ス・プログラミングを組み合わせ、公開されていないインターネット・エクスプローラーのセキュリティ・ホールを経由するという全く新しい種類の攻撃が行われました。この攻撃の第一の目的は中国の人権擁護活動家たちのｅメールアカウントをハッキングすることであったとグーグル社は結論づけています。

より恐ろしく大きな損害をもたらしうるサイバー攻撃は米国の軍に対するものです。2008 年、ウイルスに汚染されたフラッシュ・ドライブが中東にある米軍基地のノートパソコンに接続されました。ここからウイルスが検知されることなく侵入し、機密情報のあるコンピューターシステムから重大な機密情報を正体不明の相手に流出させてしまいました。米国国防省長官のウィリアム・リンは、これは米軍のコンピューターシステムにこれまで起こった中で最悪の出来事であると述べました。

例３：メディアへのエクスポージャー

本日ご紹介する最後の脅威はメディア・評価のエクスポージャーで、知的財産の流出、中傷、プライバシー侵害などをきっかけに起きるものです。知的財産に関するリスク、例えば著作権や商標の侵害は予測が難しくかつ、インターネット上で関連法がどのように適用されるべきかが明確に定義されていないため、動きの激しい分野です。例えばどうすれば著作権に違反するか、明確な定義はまだ確立されていません。あるサイトにあなたの著作権物へのリンクが張られた場合､著作権法違反になるのか。インターネットを経由した音楽の共有もこの未定義の領域に属し、世界中で規則が決まっていく中ではじめてわれわれは企業イメージや知的財産のリスクをどう評価するかが分かるのです。

第二部：デジタルへの依存

リスクがどのようなものか、より明確になったところで、なぜこのことが皆様の組織の将来にとって重要かを説明します。

これらのリスクの重要性は、技術システムが当該企業の売り上げにとって重要か、また業務がどれだけこれらのシステムに依存しているかによって決まります。技術を使う全ての組織が何らかのリスクを抱えるのです。例えば食品メーカーであれば自社の ERP システムやジャストインタイムのコミュニケーション・システムが機能しなくなれば大きく機能が損なわれます。ですから全ての企業の取締役会は技術に関連するリスクを評価し、各社が直面する個別のリスクに対応した IT 統治に関する方針を定めるべきなのです。

tactics that combined encryption, stealth programming and an unknown hole in Internet Explorer, according to anti-virus firm McAfee. The primary motive for the attack, Google concluded, was to hack into the email accounts of Chinese human rights activists.

A more frightening example of a potentially devastating cyberattack involved the U.S. military. In 2008, an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The bug spread undetected on both classified and unclassified computer systems, exposing highly sensitive information to an unknown adversary. The U.S. Deputy Secretary of Defense William Lynn called the incident the most significant breach of U.S. military computers to have ever occurred.

Example 3: Media Exposures

The final threat we'll touch on today is that of media and reputational exposures, which can arise from intellectual property, defamation and invasion of privacy. The intellectual property exposures, such as copyright or trademark infringement, are an unpredictable and rapidly evolving area because the law as it applies to the Internet is not clearly defined. For example, no clear definition has been established for standards of copyright infringement. Does a link from another site to your content infringe on your copyrights? The litigation involving Internet-based music sharing is delving into this new territory and as it plays out across the globe, the ways in which we interpret risks to reputation and intellectual property will evolve.

Part 2: Digital Dependence

Now that we have a clearer understanding of what the risks are, let's talk for a moment about why they matter so much to the future of your organization.

The severity of these risks depends on how important technology systems are to a company's revenues and its internal dependence on those systems. All organizations that utilize technology bear some risk. A food manufacturer, for example, might have significant vulnerability if its enterprise resource planning software and just-in-time communication channel were to become unavailable. Thus the boards of all companies should evaluate technology-related risks and implement IT governance policies tailored to the specific risks faced by their companies.

今日ではほとんどの組織が大きく技術、先端情報システムに依存しており、これらのシステムが機能しなくなるリスクを抱えています。業務を遂行する上で、技術への依存度は高まっており技術が機能しなくなるか新技術への投資をやめると事業にマイナスの影響が出かねません。

われわれはコストを下げるため、顧客サービスの向上、事業で競争していくためにますます技術に依存するようになっています。技術の威力と信頼性が､顧客を引き寄せ、つなぎとめ、効果的に競争する上でキーになっています。このような恩恵を継続して受けるため、われわれは技術インフラに相当な投資をし続けるでしょうし、投資ができなくなればどのような業界であっても事業にマイナスの影響が出るでしょう。さらに、様々な業務に必要な複雑なシステムや技術を統合する上での課題にも直面するでしょう。

内部技術のエラーや機能不全、我々が依存する外部の技術インフラ、つまり電気、電気通信、インターネットなどの大規模な中断はわれわれの技術ネットワークをかく乱します。一時的、継続的あるいは複数の技術の機能不全は顧客サービスに影響を与え、コストの上昇を招きます。

われわれは技術システムと関連するデータに依存しており、それらは自然災害、テロ攻撃、電気通信の中断、コンピューター・ウイルス、ハッカー、その他のセキュリティ上の問題に常にさらされいてます。だからわれわれには防御策が必要なのです。

第三部：関連する脅威を管理するための実用的な方法

これまでの例でも見てきたとおり、IT の進歩は全ての産業に変化をもたらしたといえます。企業によってはうまく適応したところもありますが、多くの企業では直面する新たなリスクから自分の会社を十分財務的に保護できているとはいえません。これらのリスクは技術系の企業だけが直面するものではありません。インターネット、そして IT を業務に必要なものと位置付けた会社は大きなサイバー・リスクに直面しているのです。しかし、多くの会社ではサイバー・リスクがより大きなリスクになったことを把握しきれていないのです。

犯罪的な面からみると、組織化された犯罪組織が新しい技術を取り入れ企業のネットワークにより巧妙に侵入し、機密情報や貴重な知的財産を盗むようになっていま

Today most organizations are highly dependent on technology and advanced information systems and there is a risk that such technology or systems could fail. We are increasingly dependent on technology in our operations, and if our technology fails or we are unable to continue to invest in new technology, our business may be adversely affected.

We have become increasingly dependent on technology initiatives to reduce costs and to enhance customer service in order to compete in the current business environment. The performance and reliability of the technology are critical to our ability to attract and retain customers and our ability to compete effectively. These initiatives will continue to require significant capital investments in technology infrastructure to deliver these expected benefits and if we are unable to make these investments, our businesses and operations could be negatively affected no matter what industry we function within. In addition, we may face challenges associated with integrating complex systems and technologies that support the separate operations.

Any internal technology error or failure or large scale external interruption in technology infrastructure we depend on, such as power, telecommunications or the internet, may disrupt our technology network. Any individual, sustained or repeated failure of technology could impact our customer service and result in increased costs.

Because of our dependence, our technology systems and related data—which are vulnerable to natural disasters, terrorist attacks, telecommunications failures, computer viruses, hackers and other security issues—must be protected.

Part 3: Practical methods for managing related threats

As we've seen in the preceding examples advances in information technology have transformed virtually every industry. While some businesses have readily adapted, many haven't sought to adequately protect themselves financially from the new exposures they face. The risks are not limited to technology companies. All businesses that have made the internet and new information technology an essential part of their operations face significant cyber exposures. Many companies have failed to recognize that the threat to their businesses from cyber risks has escalated sharply on several fronts.

On the criminal front, organized gangs have adopted new technology and used it to launch more powerful attacks against corporate networks to extort protection payments or to steal

す。規制面を見ると、立法府はより厳しいプライバシー保護を求め、企業はより多くの資源を投入して個人情報や財務情報を保護したり、セキュリティが機能しなかった場合の通知を顧客に行うようになっています。訴訟に関しては、データ保護がうまくいかなかった場合、より高額の補償を求められ、集団訴訟の可能性もより高くなっています。最後に、セキュリティが破られ顧客の情報が流出した場合、企業は最も重要な顧客を失うことも十分ありえます。

このような新たな脅威に備えて保険業界はサイバーエクスポージャーに特化した商品を作りだす一方で、既存の契約ではこのようなリスクはカバーしないようにしました。現在のところ少数ではあるもののこのような保険を購入し、サイバーリスクに備えた企業もあり、サイバーリスク保険はこれから伸びる保険商品とみられています。ただ、サイバーリスクをカバーしていく上で保険業界は常に進化していかねばなりません。技術が速いペースで進化し、企業と企業のリスクが新しい、予期せぬ方向へと動いていく中で、保険会社も継続的に変化していくリスクに対応し、技術の進化を把握し、適応し、変化を機会へと変えていかねばなりません。

企業はこのようなリスクを保険でカバーするとともに、サイバーリスクに優先順位を付け、対応するための明快な仕組みを持つ必要があります。私はここでセキュリティ戦略の強固な土台を築くための非常に分かりやすい５段階のステップをご紹介します。

第一のステップは情報資産の特定です。組織が使っている情報の主要な種類、例えば社会保障番号、クレジットカード番号、患者の記録、デザインなどを考え、何を守るべきかの優先順位をつけるのです。

第二のステップはこれら資産の場所の確認です。これらの情報、資産がどこにあるかのリストを作成します。例えばファイル・サーバー、ワークステーション、ノートパソコン、リムーバブル・メディア、PDA、電話機、その他のデータベースなどです。

このようにして場所が分かったら、第三のステップでこれらの情報をカテゴリーに分けて評価します。情報資産のレーティングです。例えば 1-5 までのランクを以下のような基準で割り振ります。（1）公知の情報、（2）内部情報だが機密情報ではない、（3）注意を要する内部情報、（4）隔離するべき内部情報、（5）最も厳重な管理を要する情報。このような分類をすることによって、組織は公開されたり改変されたらどれくらいの損害を被るのかを基準にした情報のランク付けをすることができます。

さて、ここまで来ると私が脅威モデリング演習と呼ぶ作業ができるようになります。最高レートと評価された情報資産が直面する脅威を評価するのです。一つの方法はマイクロソフト社の S.T.R.I.D.E. メソッドの利用です。簡単で、分かりやすく、主要な脅威を全てカバーできます。それぞれの資産ごとに以下の S.T.R.I.D.E. カテゴリーを記載した表計算シートを作成します。

なりすまし
データの改ざん
取引の中断
情報の開示
サービス妨害
アクセス権限の改変

表計算シートに第二のステップで特定したデータの場所を記入します。各セルに当該の脅威が実際にその場所にある資産に影響する確率と、攻撃が成功した場合組織に与える影響の度合いを記入します。１を「起きる確率は極めて小さい」、「影響はほとんどない」、10 を「起きる確率は十分ある」、「致命的」として、１から 10 までの数値を記入します。「確率」と「影響度」の二つの数字を掛け合わせて、各場所の合計数値をセルに入力します。表計算シートには１から 100 までの数字が並ぶことになります。

この作業が終わると、データを確定させ対策を検討します。まず第三のステップで実施した資産のランクの数字と各セルの数値を掛け合わせます。このようにして出た数字が組織の情報に対して存在する全てのサイバー脅威の評価ということになります。一般的なセキュリティの計画としては合計の数値が一番高いリスクから対策を始め、低いスコアのリスクはより低い優先順位とします。理想的には全てのリスクを低減させたいのですが、まずは大きなリスクへの対応を実行してください。

このようにすれば能動的な戦略の土台が築かれますが、同時に対策を講じたにもかかわらず、データが破損した場合どのような影響が出るか、どのようにするべきかについても準備しておくべきです。

confidential information or crucial intellectual property. On the regulatory front, lawmakers have enacted stricter data-privacy standards, requiring businesses to take significant measures — and commit significant resources — to protect personal and financial data and to notify customers of security breaches. On the litigation front, businesses face greater liability and the increased likelihood of class action suits should their data protection measures fail. Finally, businesses face the very real possibility of a fatal loss of clients and customers should a security breach result in the exposure of confidential personal or client information.

The insurance industry has responded to the emerging exposures by creating products to specifically address the new cyber exposures, while excluding those risks from traditional policies. To date, a small proportion of businesses have taken advantage of those new products to insure against cyber risks, making cyber coverage a specialty market with significant potential for growth. The insurance industry, however, cannot remain static when it comes to covering cyber risks. As technology continues to evolve rapidly, transforming business and business exposures in new and unexpected ways, insurers must continuously adapt their products to meet the evolving exposures and to keep pace with rapidly changing technology and its risks and organizations must remain in tune with those adaptations so that they can take advantage of them.

In addition to insuring against these exposures, organizations need a clear methodology for prioritizing and addressing cybersecurity risks. I would like to outline five very clear steps you can take to develop a solid foundation for a security strategy.

The First is to identify information assets. Consider primary types of information that an organization handles—for example, social security numbers, payment card numbers, patient records, designs—and make a priority list of what needs to be protected.

The next step is to locate these assets. Identify and list where each item on the information asset list resides, be it on file servers, workstations, laptops, removable media, PDAs and phones or other databases.

Once you have located them, the next step is to place them in categories. Assign a rating to your information asset list. Consider a 1-5 priority scale, with the following categories: (1) public information, (2) internal, but not secret, information, (3) sensitive internal information, (4) compartmentalized internal information, and (5) regulated information. This type of classification allows the organization to rank information assets based on the amount of harm that would be caused if the information was disclosed or altered.

Now you're ready to take part in what I call a Threat Modeling Exercise. Rate the threats that the top-rated information assets face. One option is to use Microsoft's S.T.R.I.D.E. method, which is simple, clear and covers most of the top threats. Develop a spreadsheet for each asset, listing the following S.T.R.I.D.E. categories:

Spoofing of identity
Tampering with data
Repudiation of transactions
Information disclosure
Denial of service
Elevation of privilege

In the spreadsheet, list the data locations identified in Step 2. For each cell, make estimates of both the probability of this threat actually being carried out against the asset at the location in question and the impact that a successful exploitation of a weakness would have on the organization. Use a 1-10 scale in which 1 is "not very likely" and "minimal impact" and 10 is "quite probable" or "catastrophic." Then multiply those two numbers together and put the total for each location into cells. The spreadsheet should be populated with numbers from 1 to 100.

Once you have done this, you can finalize your data and start planning. To do this, multiply the total in each cell in all the worksheets by the classification ranking assigned to the asset in Step 3. The final total will give you a rational and comprehensive ranking of all the cyber threats posed to the organization's information. A reasonable security plan will start by tackling the risks with the highest totals and then assign a lower priority to mitigating those with lower totals. In an ideal world, you will find a way to lessen all your risks-but be sure to take care of the big threats first.

Now that you have a foundation for a proactive strategy, you must also consider the steps you would take and the consequences that would result if that data is compromised, despite the steps you've taken to prevent it.

過去に起きたこれらのセキュリティの破たんを考慮してください。どれもがあなたの会社で簡単に起こり、全ての顧客の個人情報や信用情報が公開されてしまいかねないケースです。

- ハッカーがネットワークに侵入、顧客データを全て盗み、これらを公開するか第三者に売却すると脅かしてきた。
- 顧客情報を保存した社員のノートパソコンや USB メモリーが盗まれた。
- コンピューターが誤動作する、あるいは社員の誤操作で顧客情報をメールで大量配信してしまう、資料に印刷してしまう、あるいはホームページに掲載してしまう。

このようにして個人情報が流出してしまったとします。どうしたらいいでしょうか？

対応策としてとるべきと思われるステップは以下のようなものです。

- 盗まれたデータの性格や盗難の経緯によっては、情報セキュリティ上の問題があったことを全ての顧客に知らせます。具体的にはコールセンターを準備し、警告書、プレスリリースやポスターの作成、広告や記事で顧客に対してどのようなセキュリティ上の問題が起きたかを知らせます。
- 顧客の個人情報が流出した場合は、それぞれの顧客について信用状況をモニターするサービスを無償で提供するべきかもしれません。
- あなたの会社には顧客の情報を保全する義務があるので、この義務違反ということで訴訟され、相当な法務費用や訴訟が数年間続くこともありえます。
- あなたのセキュリティ・システムが、どのように破られたかのデジタル鑑定分析を行うと、その費用が発生します。また、このようなことが将来起こらないように新しいセキュリティ・システムを設置せねばならないでしょう。
- これらのことが起きている間、毎日の業務は影響を受け、問題が解決するまでその影響は続くでしょう。

あなたの会社にこれらの費用を負担することができますか？

典型的な財物保険、あるいは一般的な損害賠償保険はこれらのリスクのどれもカバーしてくれません。したがって全ての費用は自己負担となります。例えたった 1,000 件の情報の損失の場合でも、20 万ドル（約 1500 万円）の費用がかかりえます。件数が 5,000 件であれば 100 万ドル近くになります。これらのコストはゆすりによる損害額を含まないものです。

Consider these past security breaches, each of which could easily happen to your company exposing all your customers to identity theft and credit problems:

- A hacker breaks into your network and steals all your customer data and threatens to post it publicly or sell it
- An employee's laptop or USB flash drive is stolen containing your customers' information
- A computer malfunction or employee action accidentally distributes customer information in a mass e-mail, on printed material, or posts sensitive data on a website

Now you have a privacy data breach, what do you do?

To clean up the mess, here are a few steps your company may have to take:

- Depending on circumstances and the nature of the stolen data, your company may wish to notify all your customers of the security breach. This potentially means paying for call centers, drafting written alerts and press releases, printing, postage, and advertisements/publications to inform your customers of the security breach.
- With your customers' information personal information exposed, your company may be expected to pay for credit monitoring services for each of them.
- Because your company had a duty to secure customer information, you could face lawsuits for this breach of duty, resulting in hefty legal fees and years of litigation
- Because there was a breach of your security system, your company will now have to pay for a digital forensics analysis to determine how the breach occurred, and new security systems to guard against future instances will have to be installed.
- During this whole process, your business's day-to-day operations will be interrupted while security breach issues are cleaned up

Could your company afford to pay these costs?

Typical commercial property and general liability insurance policies do not cover any of these losses, so you'd have to pay them all out-of-pocket. With only 1,000 records, a data loss scenario could possibly cost your company $200,000. And 5,000 compromised records could cost your company nearly $1,000,000. These costs don't account for the possibility of cyber extortion.

さらにこれらの費用は短期的な費用だけなのです。現在の、そして将来の顧客が危ないのです。彼らは自分たちの情報が危険にさらされていると感じるからです。このようなマイナスのニュースが流れると民間企業の株は大きく値を下げることがあります。

データ流出の影響の大きさを考えると、データのリスクを事前に管理していくことは極めて重要であり、最も効果的な対策です。

重要なデータを維持していく上で、社員への適切な訓練も重要です。一部の会社はサイバー・セキュリティの手続きについて社員が協力してくれるという誤った理解をしています。例えば IT 部門はパスワードなしには誰もコンピューター・ネットワークに入れないようにしているかもしれませんが、社員が最初に貰った暫定パスワードを各自のものに変えていなければ十分とはいえません。

優れたシステム・モニタリングも問題を見つける助けになります。システム・モニタリングはしばしば自発的というよりは受動的に実施されることがありますが、それではいけません。例えばネットワークのログを調べると怪しい外部への通信の記録があるかもしれません。毎日午前 2 時から 3 時の間、大量のデータが特定のインターネット・プロトコル・アドレスに送られているようなケースです。あるいは社員がいない国から社内ネットワークにアクセスがあった場合などです。

不正なアクセスや情報の不正利用を防止するためのセキュリティ・サービスやツールについては十分すぎるくらいのものが世間にはありますが、企業はお金で問題を解決しようとする前にじっくりと考える必要があります。最新技術を利用することも重要ですが、セキュリティは何層かにわたって設置され、適切に保守、管理がなされなければ効果を発揮できません。

どのようなリスクでも、損失や不正はある意味完全に防止することはできません。しかし、セキュリティの弱点を特定するための適切な措置を事前にとり、社員を教育し、戦略的な対応のためのプロセスを準備すれば、問題が起きた場合でも損害を最小限に食いとめられます。皆様の中でバンクーバーの年次総会に来られる方はサイバーリスクをはじめ、企業が直面する様々なリスクへの実用的な解決策のセッションが数多く提供されます。情報の共有、仲間同士のネットワーク、そして戦略的な問題解決、それこそが RIMS の価値なのです。

And that's only the immediate aftermath. Current and future customers are in jeopardy—for fear their personal information could be compromised. Public companies have seen their stock prices plummet from negative press.

Given the severity of the impact of a potential breach, managing data risks preemptively is extremely important and a best practice.

When sensitive data must be maintained, proper training of employees is also vital. Some companies mistakenly assume their employees will cooperate on cyber security procedures. For example, the information technology department might make sure nobody can get onto computer networks without a password, but such steps are lacking if employees never bother to change their default passwords into something that is less easily hacked.

Better system monitoring can also help to identify problems. Security monitoring is often something done reactively, rather than proactively and that shouldn't be the norm. For example, examining network logs might reveal suspicious outbound traffic, such as a heavy amount of data being transferred to the same Internet Protocol address every day between 2 a.m. and 3 a.m. Or someone might have connected to the corporate network from a country where your company has no employees.

There are a plethora of security services and tools to help companies prevent unauthorized access and misuse of their information, but companies need to think carefully before just throwing money at a problem. You may have bought cutting-edge technology but security should be layered, maintained and managed properly and proactively in order to be effective.

As with any risk, losses and breaches are inevitable. Taking the proper steps prior to an issue to identify possible shortcomings, train staff, and formulate a strategic recover process will significantly lessen the damages if or when a problem arises. For those of you who will be in attendance in Vancouver for the annual conference, there are a host of sessions being offered with practical solutions to issues such as cyber risk and many other exposures businesses have today. This is the value of RIMS, information sharing, peer to peer networking and strategic problem solving.