

BJA Webinar on Cybersecurity – How to Prepare Your Company for a Cyber Crisis

Presented by:



Deloitte.



Belgium-Japan Association
Chamber of Commerce
日白協会兼商工会議所



PLEASE NOTE: THIS WEBINAR WILL NOT BE RECORDED.

24 June 2021

SPEAKERS

WELCOME AND INTRODUCTORY REMARKS



WIM EYNATTEN
Deloitte

International Tax Partner and Japanese Desk Leader; BJA Board Member and Chairman Legal & Tax Committee
weynatten@deloitte.com



THOMAS DE MUYNCK
Jones Day

Partner
Mergers & Acquisitions
tdemuyneck@jonesday.com

ARE YOU READY TO DEAL WITH A CYBER CRISIS?



WIM HERMANS
Deloitte

Partner
Cyber and Strategic Risk
Deloitte Consulting & Advisory
whermans@deloitte.com



TAKESHI TSUJI
Deloitte

Senior Manager; Japanese CPA;
Risk Advisory, Deloitte North South
Europe and Central Europe
taktsuji@deloitte.de

SPEAKERS

EU LEGAL FRAMEWORKS AND DATA BREACH RESPONSE



DR. JÖRG HLADJK
Jones Day

Partner
Cybersecurity, Privacy & Data Protection
jhladjk@jonesday.com



MICHIRU TAKAHASHI
Jones Day

Of Counsel
Intellectual Property
mtakahashi@jonesday.com

INSURANCE AS A TOOL FOR CYBER RESILIENCE



STÉFANIE DELEY
Aon

Cyber Expert Advisor & Broker Financial Lines
Commercial Risk Solutions
stefanie.deley@aon.com



SOGO YASUDA
Aon

Senior Client Director – Japan Global
Solutions (Germany)
Commercial Risk Solutions
sogo.yasuda@aon.de

Deloitte.



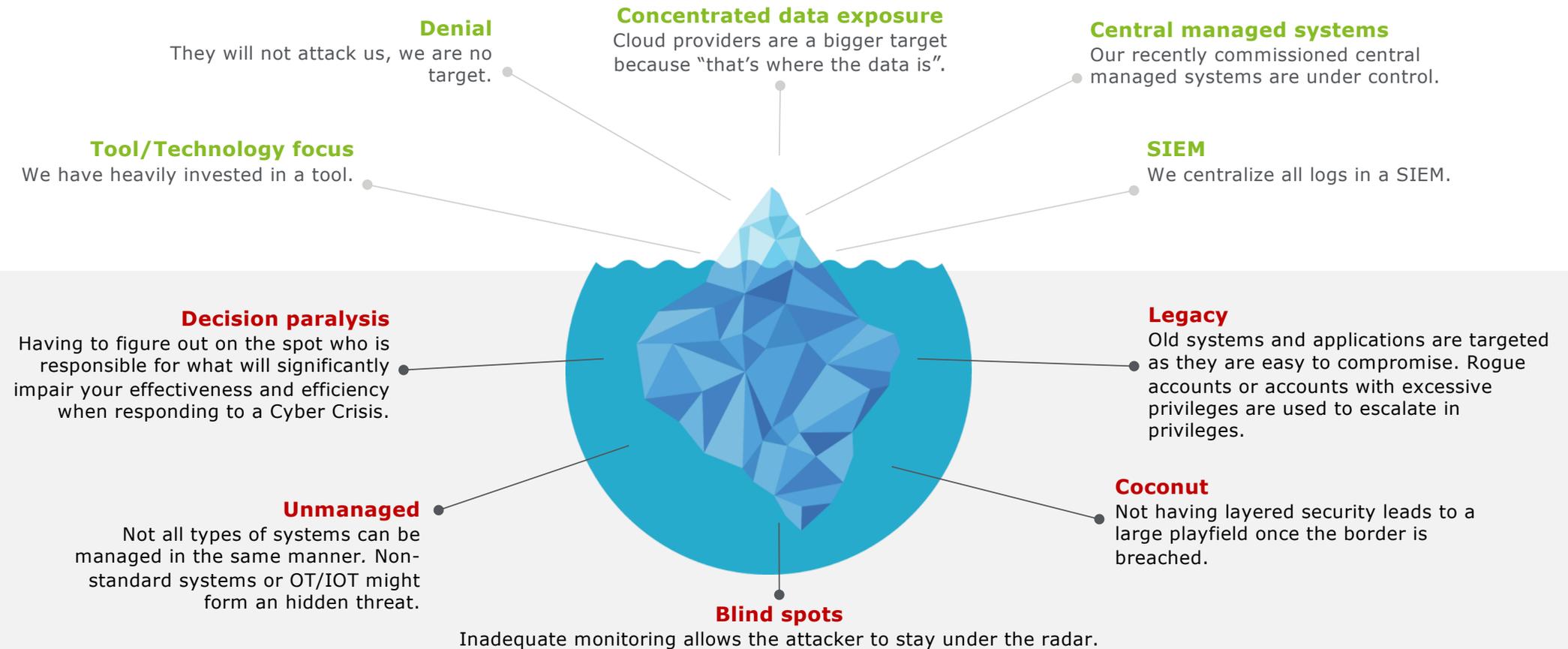
Cyber Crisis Readiness

Wim Hermans – Deloitte Belgium

June 2021

Are you ready to deal with a cyber crisis?

Know what is beneath the surface!

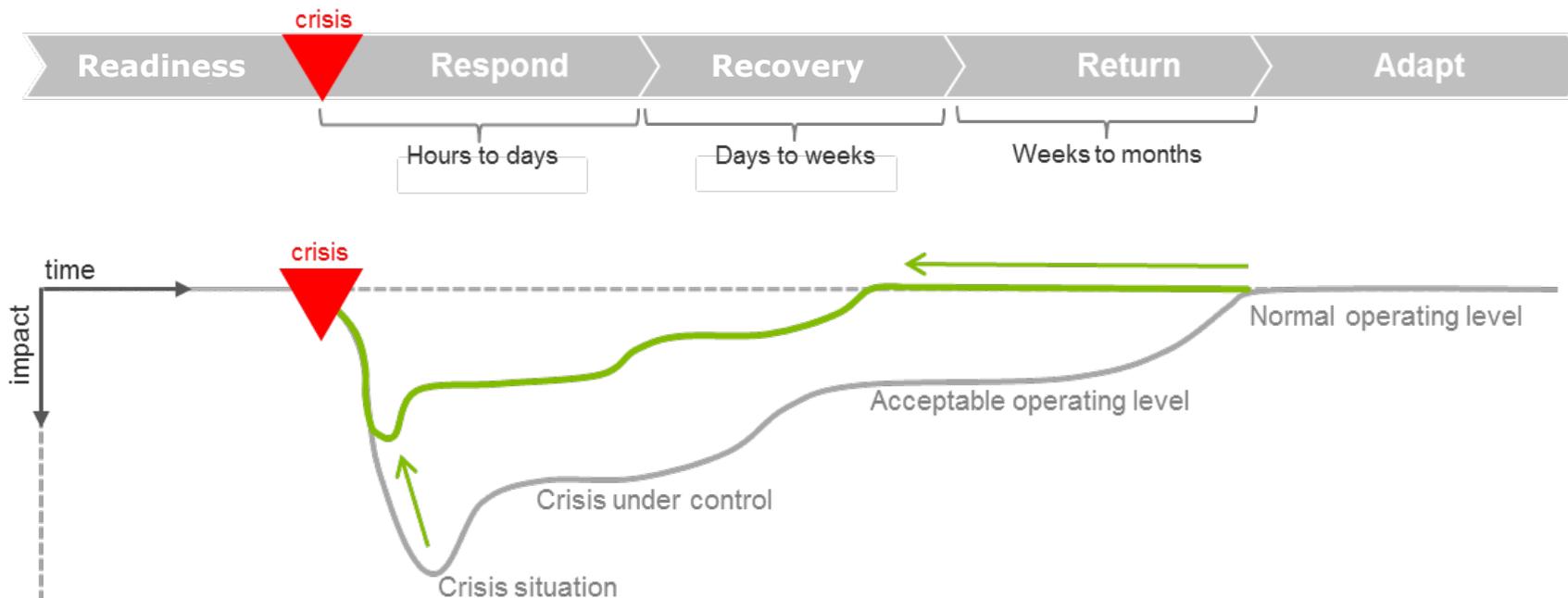


Are you ready to deal with a cyber crisis?

Survive & emerge stronger

As an organisation if you want to survive a cyber crisis you will need to focus on reducing:

- the **impact** on their processes and service delivery
- the **time required** to respond to a crisis (**respond**), recover to a minimal acceptable level of service (**recovery**) and return to normal operations (**return**)



Are you ready to deal with a cyber crisis?

Enterprise wide impact of a Cyber Crisis

The financial impact of ransomware depends on different factors such as the type of company, the IT landscape and the scope of the incident. The figures below give an indication based on Deloitte's real-life experience in helping clients through a ransomware crisis."

Recovery towards a minimal service level

🕒 **2 TO 4** WEEKS

€ **100K TO 500K***

Strategical improvements

Get your trust back in your digital landscape

🕒 **1 TO 5** YEARS

€ **MULTIPLE MILLIONS***

Tactical improvements Avoid similar attack in the future

🕒 **1 TO 6** MONTHS

€ **HUNDREDS OF THOUSANDS***

*these costs are mostly related to potential external resources needed to achieve a full recovery of the systems. Additional financial impacts can exist, such as stocks decline, loss of income and production rate, potential legal charges, etc...

FACTS

Maersk, victim of a ransomware in 2017, estimated the recovery costs between 250 and 300 millions of dollars, after having reinstalled the totality of their infrastructure.

OVERALL IMPACT

Financial loss

Loss of customer trust and reputation

Potential legal impact (GDPR, ...)

Multiple months to a year of recovery time cause inability to produce and deliver goods

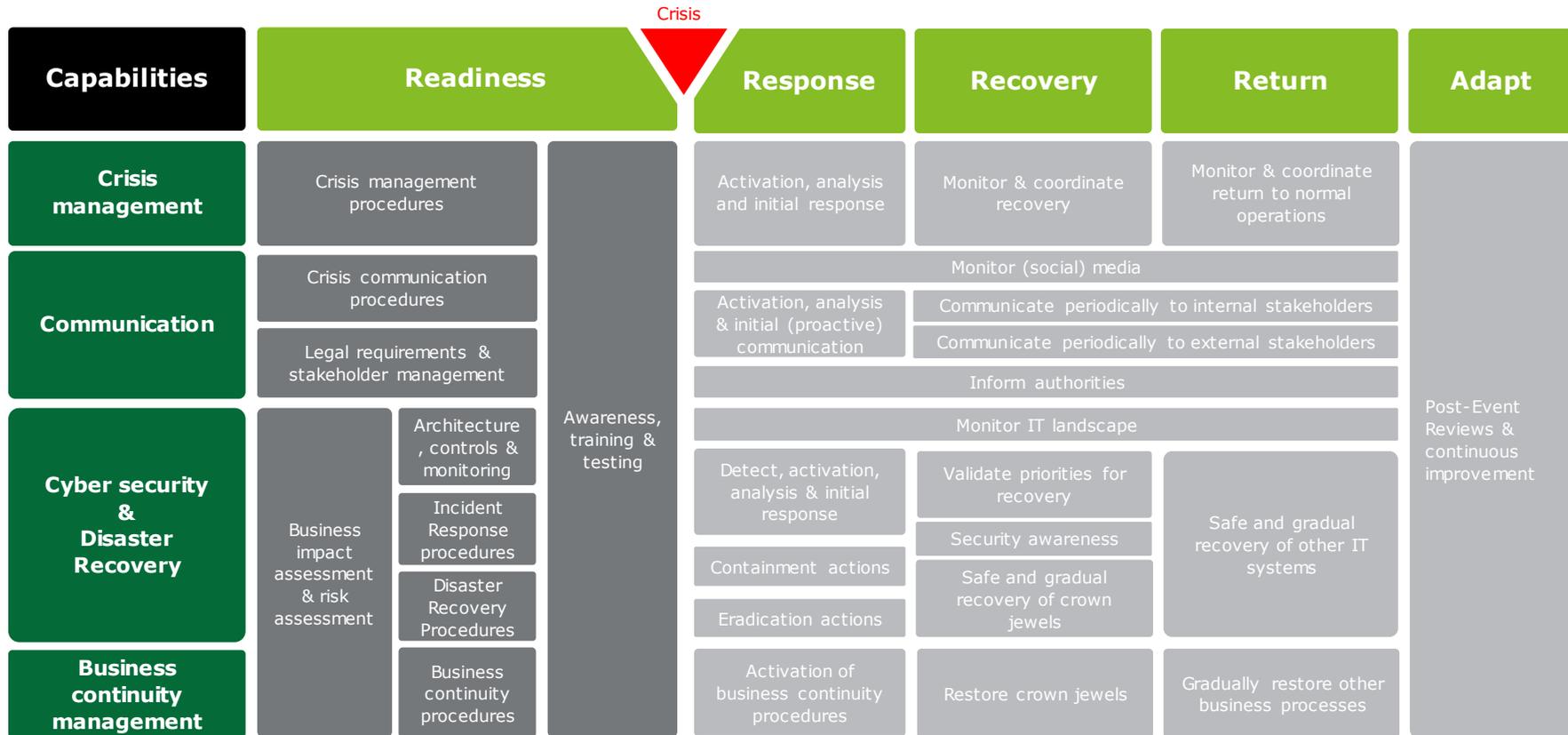
(Temporary) unemployment

"There is no such thing as a divide between technology and business in any company anymore, particularly when it comes to Cyber. You have got to operate as one."

Andy Powell, CISO at Maersk

Are you ready to deal with a cyber crisis?

Required capabilities



Are you ready to deal with a cyber crisis?

Cyber crisis readiness streams

Every organization should **establish capabilities** to **effectively and efficiently prepare** for and manage a cyber crisis. Depending on your maturity and desired capabilities, we recommend to prioritize the following four areas:



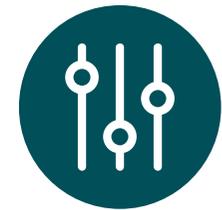
Technical testing of core security capabilities



Cyber Crisis Management and Communication process



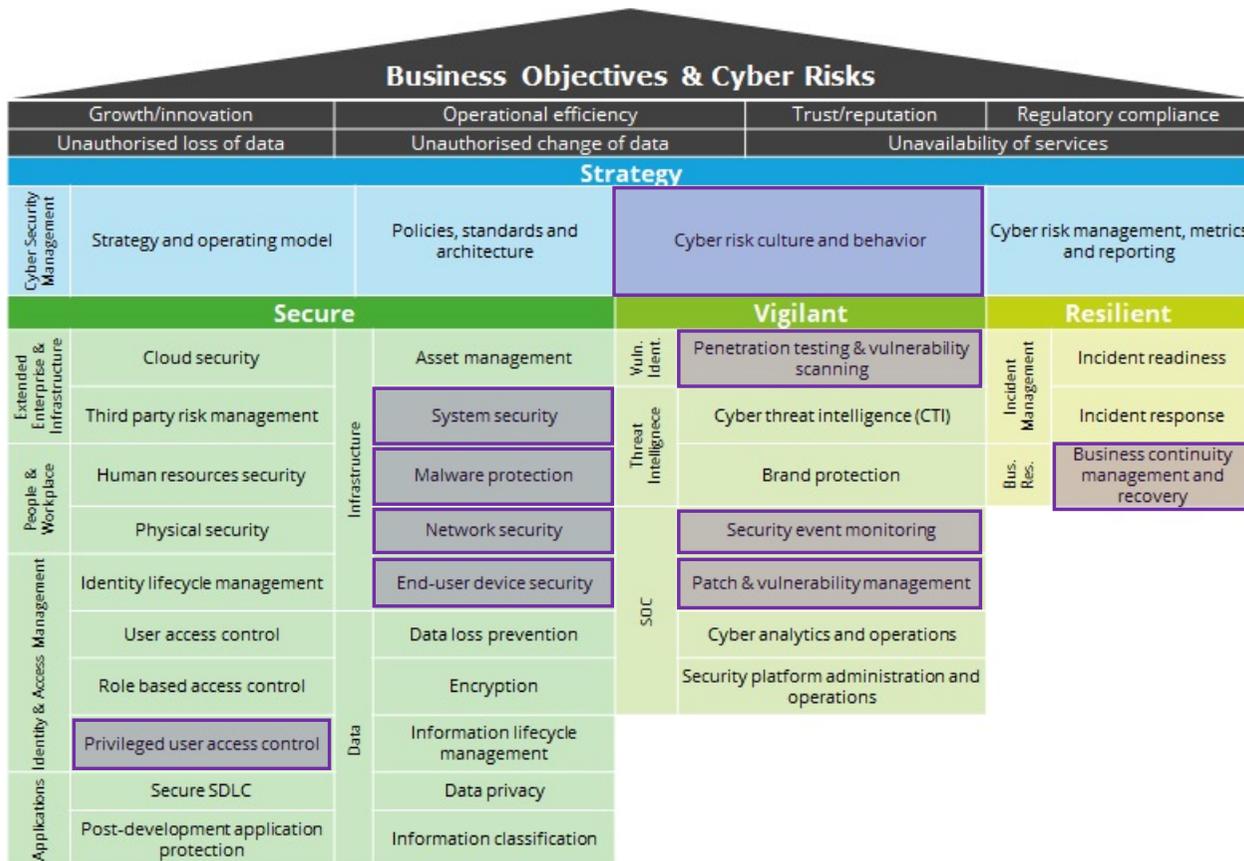
Cyber Incident Response



Cyber Crisis Simulation Exercises

Are you ready to deal with a cyber crisis?

Stream 1 - Technical testing of core security capabilities



Deloitte has developed the Cyber Strategy Framework (CSF) to provide a comprehensive view on the complex domain of Cyber:

Strategy

Ensures that the necessary organization and structure is in place to prioritize, implement and optimize the security measures most relevant for the organization.

Secure

Focused on preventing security incidents and crises from happening.

Vigilant

Focused on timely detection of security incidents.

Resilient

Focused on responding to security incidents.

Capabilities that will help prevent a Cyber Crisis (ransomware)

Are you ready to deal with a cyber crisis?

Stream 2 - Cyber Crisis Management and Communication process

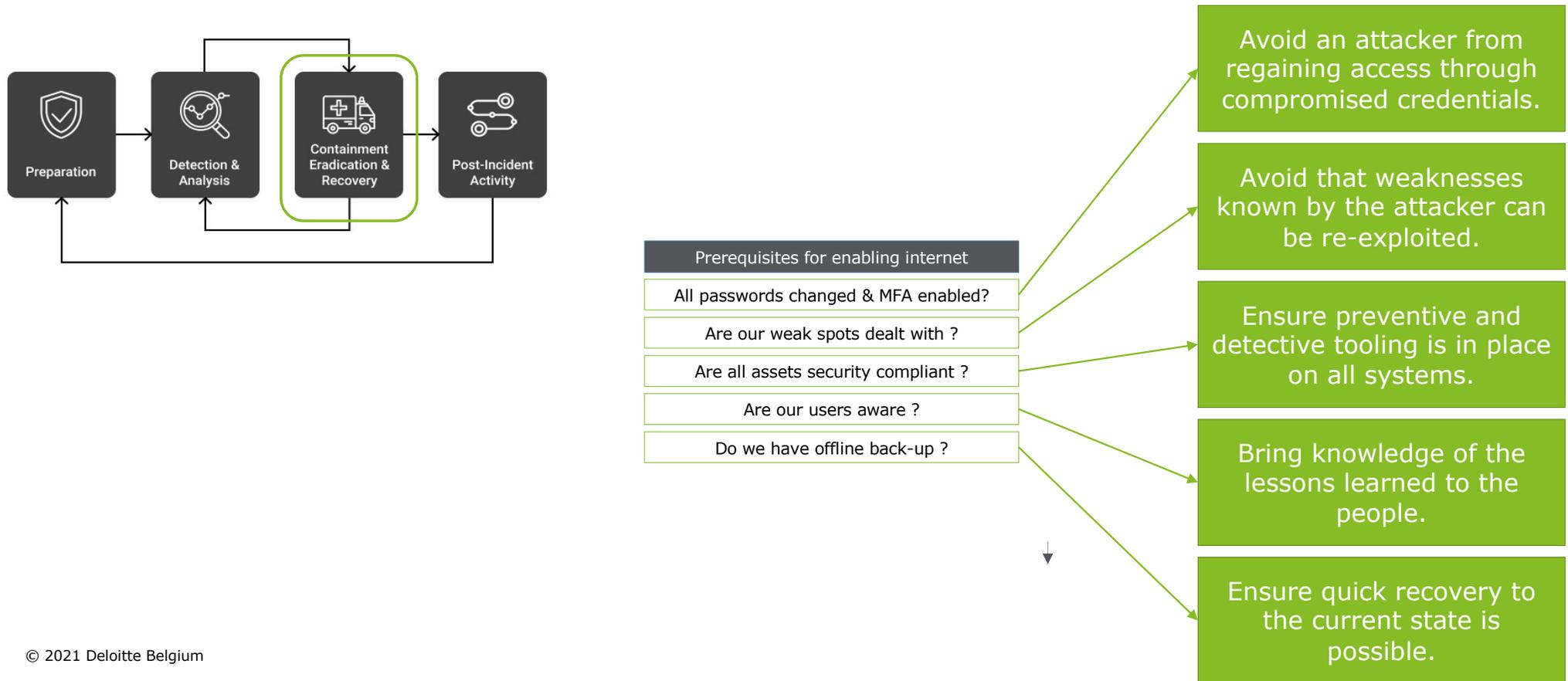
Deloitte has developed a pragmatic **crisis management methodology**. Each of the following are specific facets of a client's crisis management that may need to be assessed and guided during the course of a real life event. These evaluation topics are based upon industry accepted practices from Crisis Management standards (BS 11200:2014), practices utilized internally by Deloitte, and experiences from crisis management professionals.

Evaluation Topic	Topic Description
 Response Organisation	Pre-defined group(s) of senior leaders responsible for all aspects of planning, coordinating, managing, and executing an organization's response.
 Crisis Management Plan	A set of organized guidelines and procedures developed in advance of a crisis to assist an organization in responding to events more effectively.
 Common Operating Picture	Situational awareness capability for effective decision making, rapid staff actions, and appropriate response execution. <i>[adapted from Department of Homeland Security (DHS)].</i>
 Decision Making Process	Structured approach for analyzing the situation, identifying issues, assessing options, and taking decisive actions to support the Real-Time Response <i>(adapted from BS 11200)</i> .
 Control Hierarchy	Formal structure within an organization's crisis management program that defines decision rights, leadership succession, and other management controls during a crisis.
 Crisis Communications	Actions taken by an organization to communicate internally and externally during a crisis <i>(adapted from BS 11200)</i> .
 Information Management	Formal documentation that the client uses to track the details of the event and response actions throughout the crisis.
 Ongoing Crisis Monitoring	A process for collecting and analyzing pertinent information on a continuous basis throughout the crisis to support the response teams.
 Private – Public Coordination	Integration between public and private sector entities to respond to events that may involve critical infrastructure and key resources.

Are you ready to deal with a cyber crisis?

Stream 3 - Cyber Incident Response

Every organization should **establish a cyber incident response process** to **effectively and efficiently prepare** for and manage a cyber incident. A cyber incident response lifecycle breaks incident response down into four main phases, where interconnection is the key to success:

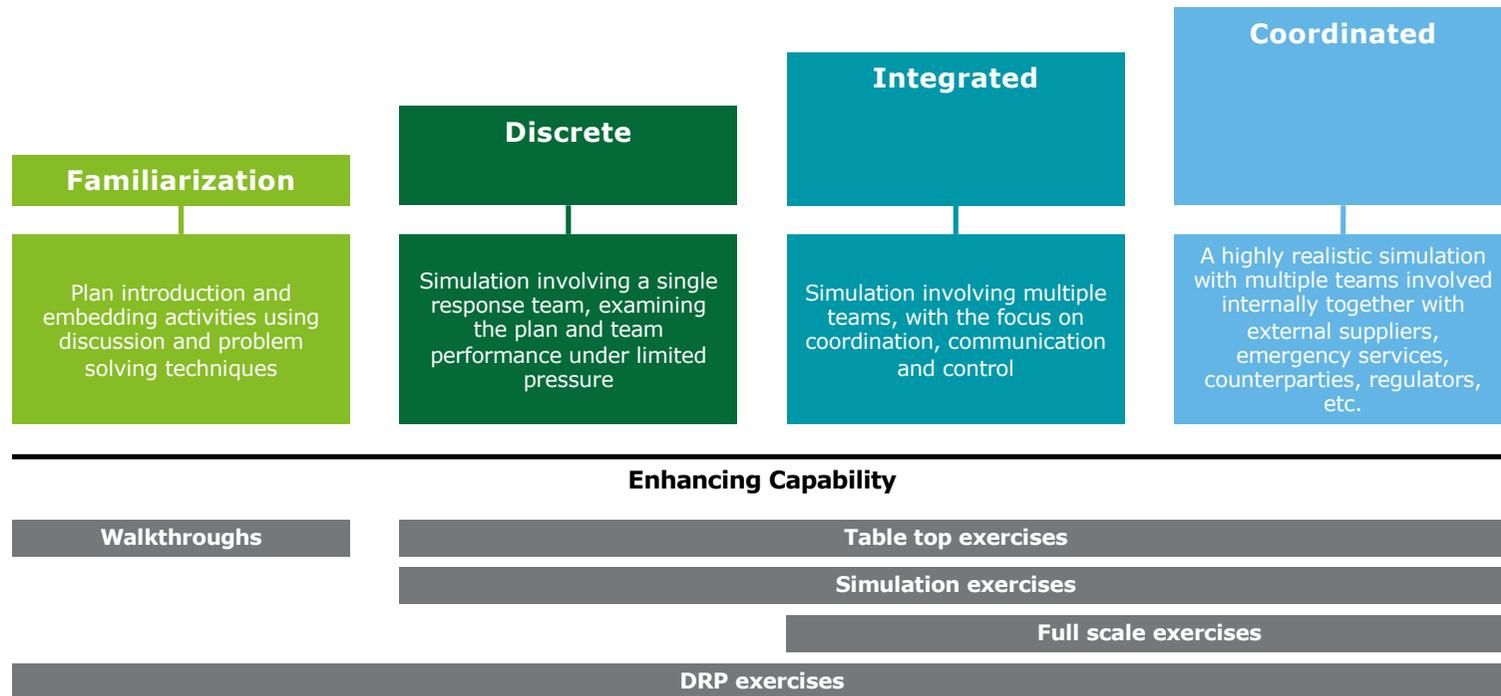


Are you ready to deal with a cyber crisis?

Stream 4 - Cyber Crisis Simulation Exercises

Types of exercises

It is crucial that Business Continuity Management and Crisis Management Plans are tested against reality. This ensures the performance and effectiveness of the processes and procedures during a disruptive event. **Different types of tests can be organized in a different order of complexity.** It is recommended to start with less complex tests in order to be familiar with roles and responsibilities, procedures, etc. in case of a disruptive event resulting into a crisis.



Are you ready to deal with a cyber crisis?

Key questions to consider

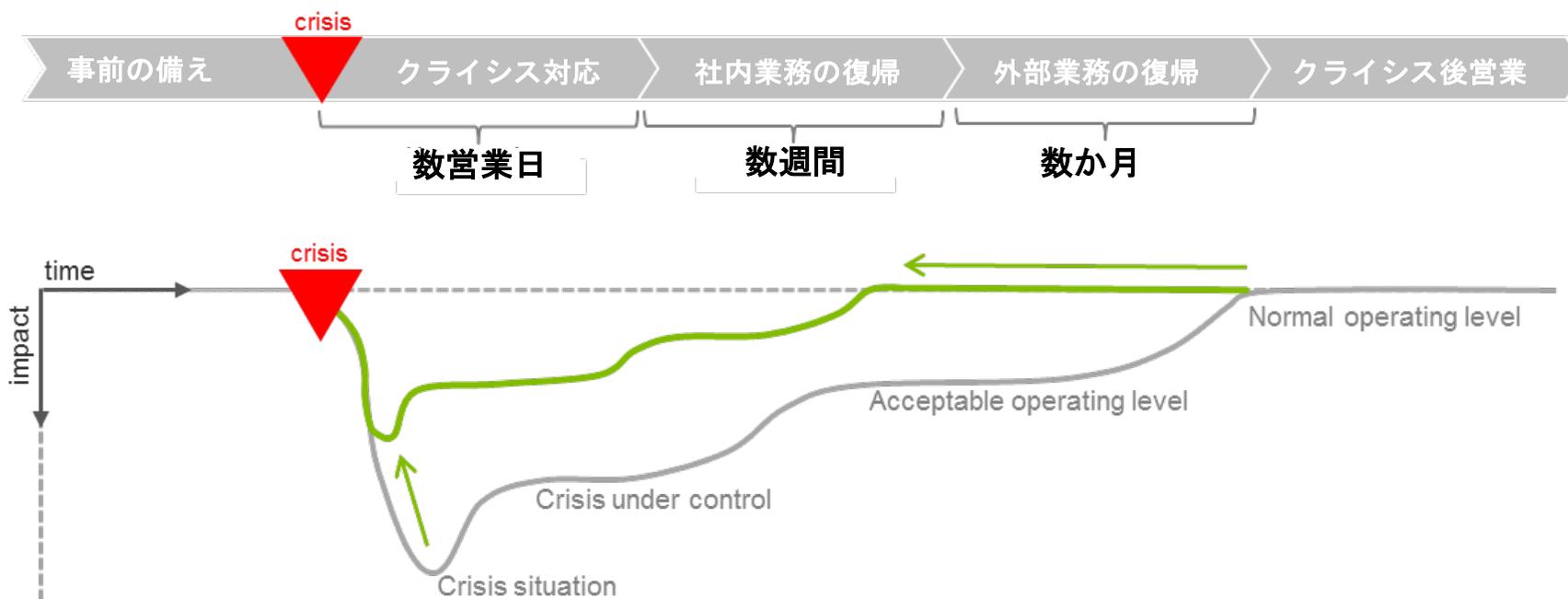
-  Are you aware what cyber capabilities are most important for your organization?
-  Are these capabilities at the required maturity level?
-  How to keep the business running for days or weeks whilst recovering IT systems and data?
-  How to rebuild IT services from scratch?
-  How confident are you with the plans you have?

サイバー攻撃への対処と準備

生き残りと急速なリカバリー

組織として、サイバー危機から生き残るためには、以下の内容を低減させる必要がある。

- ビジネスのプロセスとサービス提供へのインパクト
- サイバー危機への対応プロセスの時間・通常社内業務運営までの回復期間・最低限のサービス提供が可能となるまでの時間及び通常外部業務への回復までの営業日



サイバー攻撃への対処と準備

サイバー危機の全社的影響度

ランサムウェアの財務的なインパクトは各社の業種業態、IT環境や事故の範囲によって影響度が異なります。以下の数値は Deloitte がご支援したランサムウェア攻撃の結果のリアルな数値となります。

最低限のサービス提供体制への復帰

🕒 2 TO 4 WEEKS

€ 100K TO 500K*

評判や風評被害からの回復を含めた戦略的改善

🕒 1 TO 5 YEARS

€ MULTIPLE MILLIONS*

類似の事案発生防止を含めた戦略的改善

🕒 1 TO 6 MONTHS

€ HUNDREDS OF THOUSANDS*

*このコスト見積もりは、株価の下落や収益や生産量の減少や潜在的な法的対応も含めて、どのような体制を企業が構築できるか、裏を返すと外部業者にどの程度依頼するかによるため、概算としています。

「特にサイバー危機に関してはどんな会社も、もはやテクノロジーとビジネスを切り分けることはできない。一体として運用すべきである。」

Andy Powell, CISO at Maersk

FACTS

2017年にランサムウェアの被害にあったロジスティック企業の「Maersk」はITシステムの再構築と導入に、250億円から300億円がかかった。

全社的なインパクト

財務的損失

顧客および関係者からの評判と信頼の喪失

潜在的法的損害 (GDPR, ...)

複数月から一年のサービスと製造の提供不可期間の発生

(一時的な) 雇用停止、解雇

サイバー攻撃への対処と準備

サイバー危機管理の準備プロセス

全ての組織は効果的効率的にサイバー危機に関する準備と対応に関する能力を備えるべきである。各社での成熟度と期待する能力にも依存するが、Deloitteは以下の4つのエリアを優先的に実行することを推奨する。



技術的なテストの核となる
防御能力の保持

サイバー戦略やカルチャーに
基づく、
保護・監視・回復能力



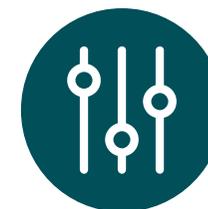
サイバークライシスマネジメントと
コミュニケーションプロセス

事案発生時の組織体制、対応部署、
コミュニケーションルートや情報統
制の整備



サイバーインシデント対応

インシデント対応については、4つ
の相互に連携するプロセス（準備・
捜査と分析・封鎖、殲滅と回復・事
後対応）で実行すること



サイバー危機
シミュレーション

役割と責任や手順を確
認するために、まずは
簡単な方法でのシミュ
レーションをすること

Thank you for your attention

A large green circle is centered on the page. Inside the circle, the word "Questions?" is written in a bold, black, sans-serif font.

Questions?

Contacts



Wim Hermans

Partner | Cyber and Strategic Risk
Deloitte Consulting & Advisory

Gateway building | Luchthaven Brussel
Nationaal 1 J, B-1930 Zaventem

D: +32 2 600 66 32 | M: +32 496 57 41 60

whermans@deloitte.com | www.deloitte.be



Takeshi Tsuji (辻 武志)

Senior Manager | RA European representative for Japanese enterprises (RA 欧州代表) | CPA of Japan (日本公認会計士)
Deloitte Risk Advisory North South Europe & DCE

Schwann Straße 6, 40464, Deutschland

M: +49 151 5807 3858

taktsuji@deloitte.de | takeshi.tsuji@tohmatu.co.jp

Deloitte.

BJA WEBINAR ON CYBERSECURITY – HOW TO PREPARE YOUR COMPANY FOR A CYBER CRISIS

Cybersecurity Incidents – EU Legal Framework and Data Breach Response

Brussels
June 24, 2021

Dr. Jörg Hladjk
Partner
Cybersecurity, Privacy & Data
Protection
Jones Day
Brussels



TABLE OF CONTENTS

- 1 EU Notification Requirements**
- 2 Involvement of Law Enforcement**
- 3 Pitfalls and Best Practices for Incident Response Plans**

1. EU NOTIFICATION REQUIREMENTS

1 LEGAL FRAMEWORK

GDPR

NIS Directive I

Proposal for NIS Directive II

1 GDPR – PERSONAL DATA BREACH (I)

GDPR Definition

Breach of security leading to...



... the accidental or unlawful destruction,
loss, alteration, unauthorized disclosure of, or access to,
personal data transmitted, stored or
otherwise processed





1 GDPR – PERSONAL DATA BREACH (II)

- Notification to **supervisory authority** unless it is **unlikely** to result in a risk to the rights and freedoms of the individuals concerned
- **Content:** type of incident (where possible, categories and number of data subjects, data categories and number of data records), name and contact details of the data protection officer or other contact person, likely consequences of the incident, measures taken or proposed to remedy the incident and, if necessary, measures to mitigate the effects

Timing

- Without undue delay, where feasible, within **72 hours** to the supervisory authority;
- After having **become aware** of the breach ("reasonable certainty" that a security incident has occurred that compromises the protection of personal data)

1 GDPR – PERSONAL DATA BREACH (III)

- Communication to **individuals** if it is *likely* to result in a *high risk* to the rights and freedoms of the individuals concerned
- When ? “**Without undue delay**”
- Within the 72 hours’ timeframe, the probable risk for those affected should also be checked - determination of whether notification is required and which **measure(s) to remedy** it - examples:

Loss of control over
personal data

Restriction of Rights

Discrimination

Identity theft or fraud

1 GDPR – PERSONAL DATA BREACH (IV)

Communication to individuals

Higher threshold than for reporting to the supervisory authorities

Content of the communication: similar to notification to authorities

Delay possible if investigation would be hindered by early disclosure (legitimate interest of law enforcement)

Exception: encryption etc.

1 GDPR – PERSONAL DATA BREACH (V)

Processor must notify controller “without undue delay”

Principle “controller is “aware” of the incident as soon as the processor has informed”

Processor: must support those responsible with their obligations

Contractual rules often similar, better specify the exact number of hours (e.g. 24 or 36 hours)

1 NIS DIRECTIVE I – PURPOSE AND SCOPE

Purpose: achieve a high common level of security of network and information systems within the EU

Scope of Application

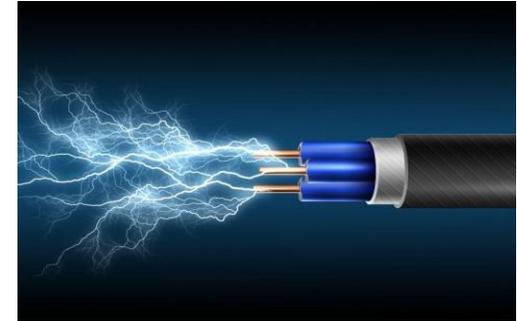
- **Operators of Essential Services (OES):**

- Energy (electricity, oil, gas)
- Transport (air, rail, water and road)
- Banking
- Financial market infrastructures
- Healthcare
- Drinking water supply and distribution
- Digital Infrastructure (IXPs, DNS, TLD)

- **Digital Service Providers (DSP):**

- Online Marketplaces
- Online Search Engine
- Cloud computing services

1 NIS DIRECTIVE I – NOTIFICATION REQUIREMENTS



Operators of Essential Services

- To notify the competent authority or the computer emergency response team (CSIRT) of incidents having a **significant impact** on the continuity of the essential services they provide;
- To provide **information** enabling the competent authority or the CSIRT to determine any **cross-border impact of the incident**.

Digital services providers

- To notify the competent authority or the CSIRT of **any incident** having a **substantial impact on the provision of a service** that they offer within the EU;
- To provide information enabling the competent authority or the CSIRT to determine the **significance of any cross-border impact**.

1 PROPOSAL FOR NIS DIRECTIVE II – BACKGROUND



- December 16, 2020: Commission presented a proposal for a Directive on measures for a high common level of cybersecurity across the Union (“**Proposal for NIS Directive II**”).
- **Extension of industry sectors:** (i) public administration; (ii) space, (iii) waste management, (iv) postal and courier services, (v) manufacture, production and distribution of chemicals, (vi) food production, processing and distribution, (vii) manufacturing and (viii) digital providers.
- One of the objectives: **Clarify reporting obligations** for companies in the event of a security incident.
- **Specific procedure, content and timeframe** for reporting security incidents.

1 PROPOSAL FOR NIS DIRECTIVE II - NOTIFICATION REQUIREMENTS

“Essential” and “Important” entities must notify, without undue delay, and in any event within 24 hours after having become aware of the incident the following stakeholders:

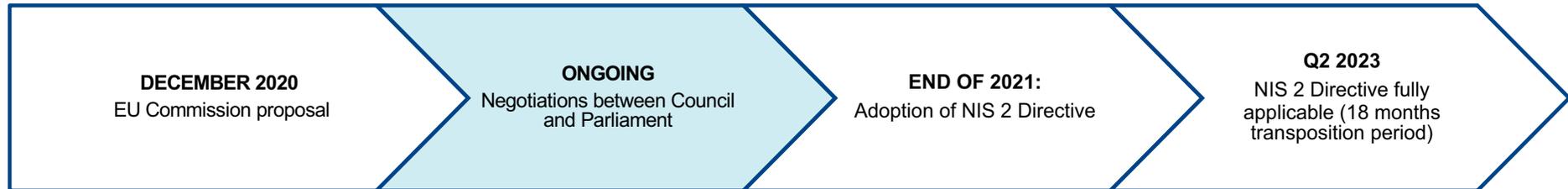
1. Competent authorities or the CSIRT of any incident having a significant impact on the provision of their services

2. Where appropriate, the recipients of their services if the incidents are likely to adversely affect the provision of the services



1

PROPOSAL FOR NIS II DIRECTIVE - LEGISLATIVE PROCESS



- Bart Groothuis appointed as rapporteur in Jan. 2021
- Proposal currently awaiting EP committee decision



2. INVOLVEMENT OF LAW ENFORCEMENT

2

MULTIPLE LAW ENFORCEMENT AUTHORITIES (I)

Challenges



- Pros/Cons: If involvement of law enforcement in one country is required/desired, how will law enforcement in other countries react? Public? Regulators?
- Which law enforcement authority to notify first? (Risk of loss of control over investigation)
- Benefit of obtaining support/information from law enforcement authorities
- Confidentiality/privilege waiving risks
- Liability risks (timing of law enforcement involvement may suggest earlier notice was necessary)
- Cost

2

MULTIPLE LAW ENFORCEMENT AUTHORITIES (II)

Best Practices

- Carefully weigh pros/cons before involving any law enforcement authorities
- If law enforcement notification is required, consider whether other law enforcement authorities should be notified (discretionary)
- Coordinate notification/involvement of multiple law enforcement to extent possible



3. PITFALLS AND BEST PRACTICES FOR INCIDENT RESPONSE PLANS

3 INCIDENT RESPONSE PLANS – COMMON PITFALLS

Great plan but...

- Participants don't understand or follow it;
- Does not identify decision-makers (tasks assigned to groups or functions)

Not an enterprise wide plan

- IS/IT response procedures

Escalation triggers from IS to enterprise level Incident Response Team

- Are not clear; or
- Are purely discretionary

Legal team not involved early enough to address key legal issues

- In particular notification obligations; evidence preservation

Decentralized communications/notifications

- Risk inconsistent statements/approaches

3

INCIDENT RESPONSE PLANS – BEST PRACTICES



BJA ウェビナー: サイバーセキュリティ - サイバー危機から企業を守るために -

サイバーセキュリティ事故
- EUの法的枠組みとデータ侵害対応 -

ブリュッセル
2021年6月24日

Dr. Jörg Hladjk パートナー 弁護士
Jones Day ブリュッセル

高橋美智留 オフカウンセル 弁護士
Jones Day 東京



JONES
DAY®

サイバーセキュリティ事故 – EUの法的枠組みとデータ侵害対応 – プレゼンテーション要約 (I)

1 通知要件

2 法執行機関の関与

3 事故対応計画

サイバーセキュリティ事故 – EUの法的枠組みとデータ侵害対応 – プレゼンテーション要約(II)

1 通知要件

- GDPR: 監督機関への個人データ侵害の通知及び個人へのコミュニケーションに関する法的枠組
- NIS指令I: 所轄官庁またはCSIRT (Computer Security Incident Response Team)へのセキュリティ事故の通知に関する法的枠組 – 産業分野 (例、エネルギー、銀行、ヘルスケア)
- NIS指令IIの提案: (案) 所轄官庁、CSIRTまたはサービスの受け手へのセキュリティ事故の通知に関する法的枠組 – 産業分野の拡大 (例、宇宙、化学製品の製造、生産および販売)

サイバーセキュリティ事故 – EUの法的枠組みとデータ侵害対応 – プレゼンテーション要約(III)

2 法執行機関の関与

- 課題、例
 - 機密性
 - タイミング
- ベストプラクティス、例
 - 法執行機関が関与する前にメリット、デメリットを検討
 - 複数の法執行機関の調整

3 事故対応計画

- 一般的な落とし穴、例
 - 事故対応計画で意思決定者が特定されていない
 - 企業全体の計画ではない
- ベストプラクティス、例
 - 企業レベルの事故対応チームの策定および実施
 - コミュニケーションの中央集中化

Any presentation by a Jones Day lawyer or employee should not be considered or construed as legal advice on any individual matter or circumstance. The contents of this document are intended for general information purposes only and may not be quoted or referred to in any other presentation, publication or proceeding without the prior written consent of Jones Day, which may be given or withheld at Jones Day's discretion. The distribution of this presentation or its content is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the author and do not necessarily reflect those of Jones Day.



One Firm Worldwide®

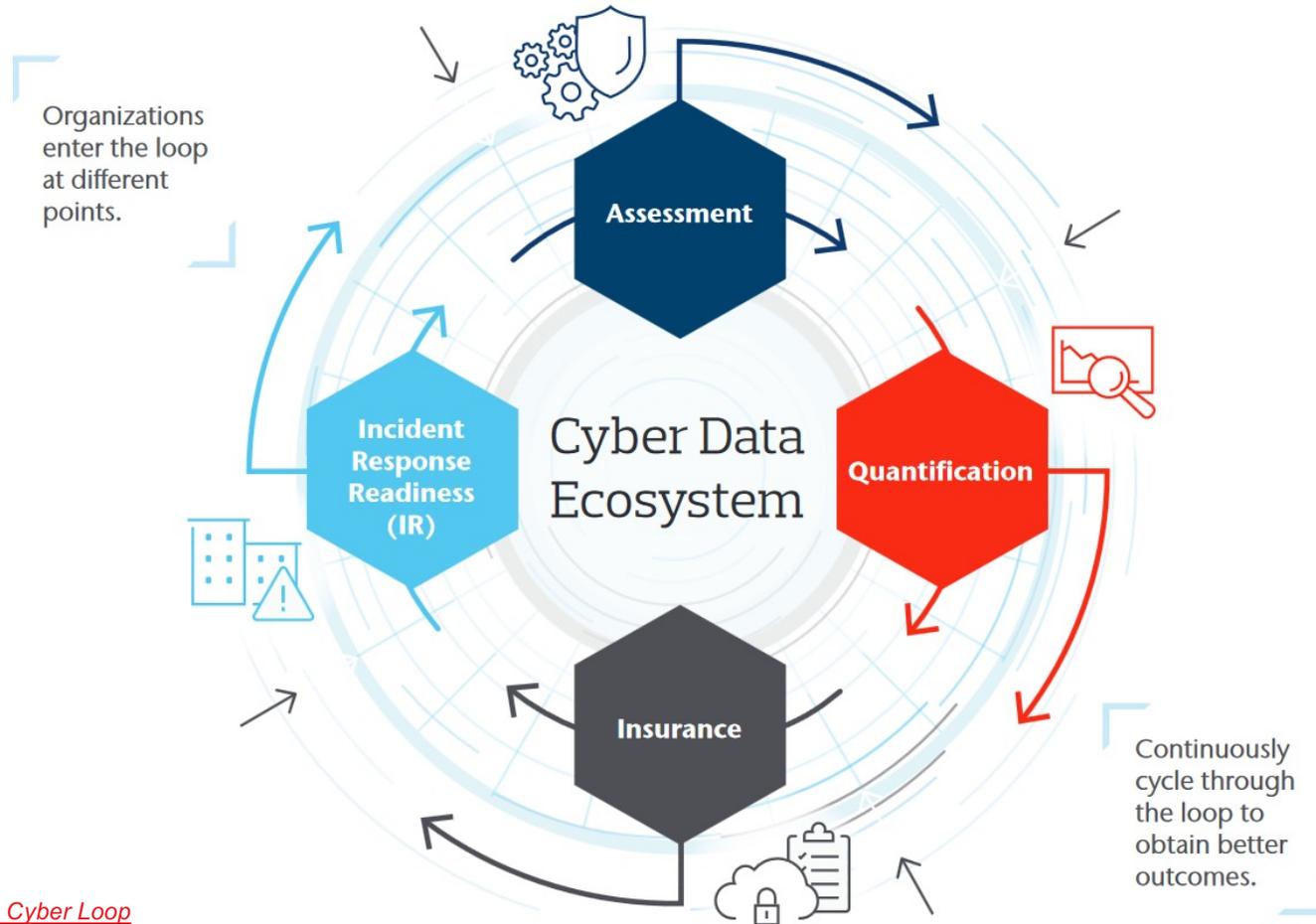
Insurance as a tool for a better cyber resilience

BJA Webinar on Cybersecurity – how to prepare your company for a Cyber Crisis
24/06/2021

Prepared by Aon's Cyber Solutions

AON
Empower Results®

The Cyber Loop: Managing cyber risk requires a circular strategy



Source: [Aon's White Paper The Cyber Loop](#)

Prepared by Aon's Cyber Solutions
Proprietary & Confidential

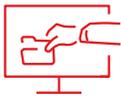
Cyber Risk Trends to Watch



Remote Workforce - Remote Desktop Protocol (RDP) software, remote access security, reliance on third party IT service providers, and digital communication as the primary venue to share information.



Vendor Risk - The SolarWinds compromise and the recent Microsoft Exchange vulnerabilities demonstrate the complexity of technology supplier relationships and how they may potentially add risks that may impact cyber security posture.



Cyber Extortion - Ransomware attacks may result in corporate downtime due to encrypted networks as well as potential liability consequences in terms of regulatory fines or third-party lawsuits.



Uncovered Technology Professional Indemnity (PI) - The emergence of technology services and product exposures in more traditional industries represents a potentially “uncovered” PI exposure that may not be contemplated from liability and financial loss standpoints.



Breach Regulations - GDPR fines rose by nearly 40% in 2020 with €158.5M in total and the largest fine in 2020 of €35 million issued by the German regulator. Italy’s regulator imposed more than €60M in aggregate. The highest GDPR fine to date remains the €50M fine imposed by the French regulator.

The Ransomware Threat in 2021

the business of ransomware is changing

more
frequent

more
targeted

more
sophisticated

more
costly

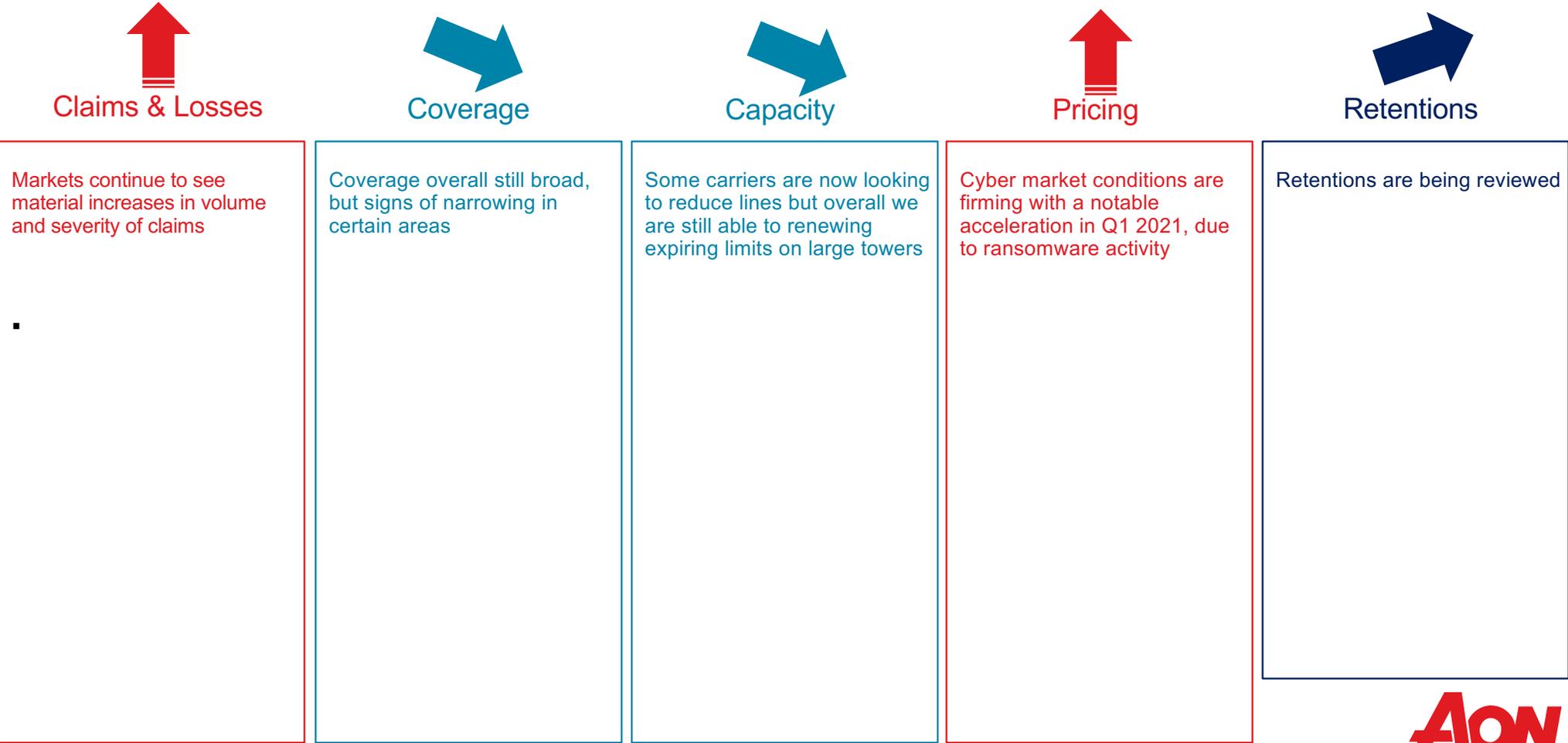
- Global ransomware damage costs are predicted to reach €17 billion this year, **an increase of 57X** from 5 years ago
- Ransomware is the **fastest growing type of cybercrime** and a top cyber threat facing organisations in 2021¹.
- Attackers are moving away from the **“spray and pray”** to **target practice** and **big-game hunting**
- Targeting victims that can yield a greater financial pay-off².
- Attacks are growing in sophistication.
- **“Double extortion”** attacks
- Taking **copies of data** and threatening to release it publicly
- Threaten to **delete data** entirely
- **Cold calling** victims trying to restore systems³
- Some of the most sophisticated ransomware attack groups and malware variants are now averaging over **€650,000 per payment**⁴

1,4) <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/>

2) <https://www.wired.co.uk/article/ransomware-trends-2021>

3) <https://www.itproportal.com/news/ransomware-attacks-set-to-see-huge-growth-in-2021>

International Cyber Insurance Market Trends as of Q1 2021



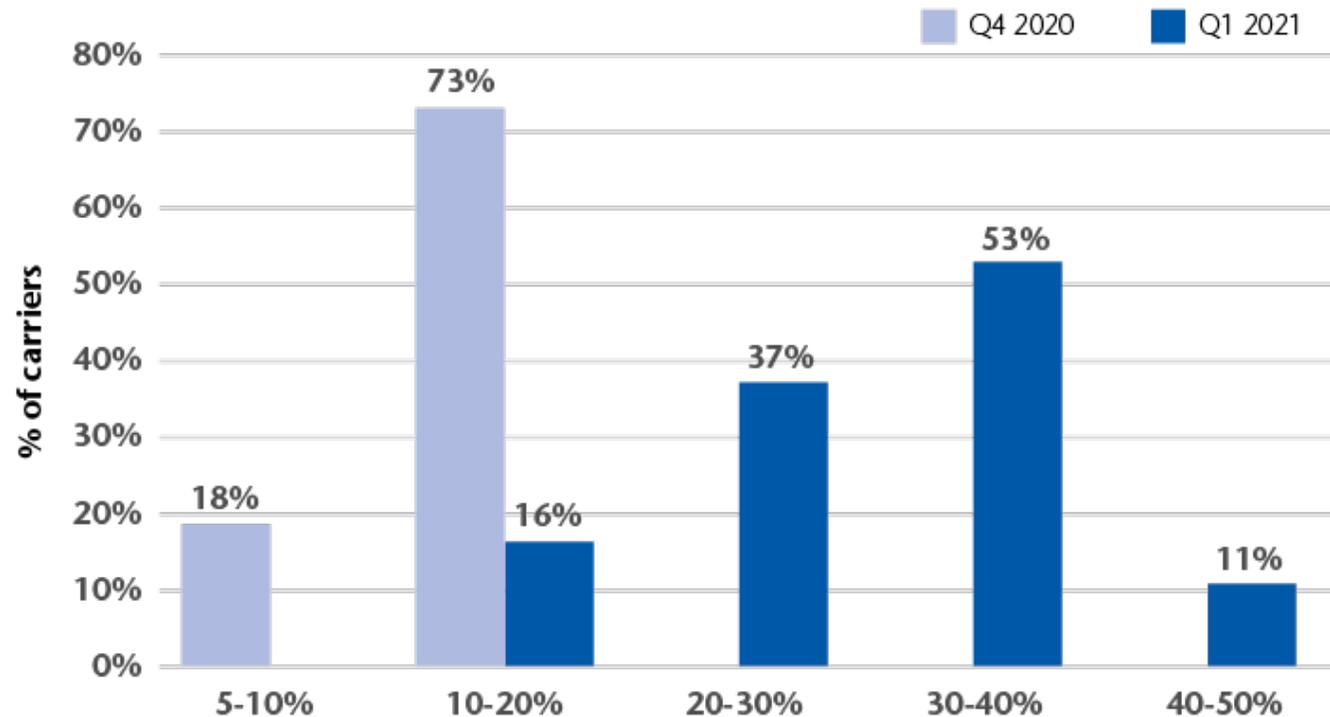
Cyber Pricing Trends | Result Rate Guidance Changes Across the Entire Portfolio Q4 2020 vs Q1 2021

Key Commentary:

Aon pricing data is real-time on a historical basis and examines the year-over-year price change on a quarterly basis.

- 2020 Q4 Average rate change from carriers was of **+12%**
- 2021 Q1 Average rate change from carriers was of **+35%** which represents a **23% increase** versus the previous quarter.
- Majority of respondents suggested they are seeking rate increases **greater than 30% throughout Q2 2021**.

However, cyber rates are rapidly changing.



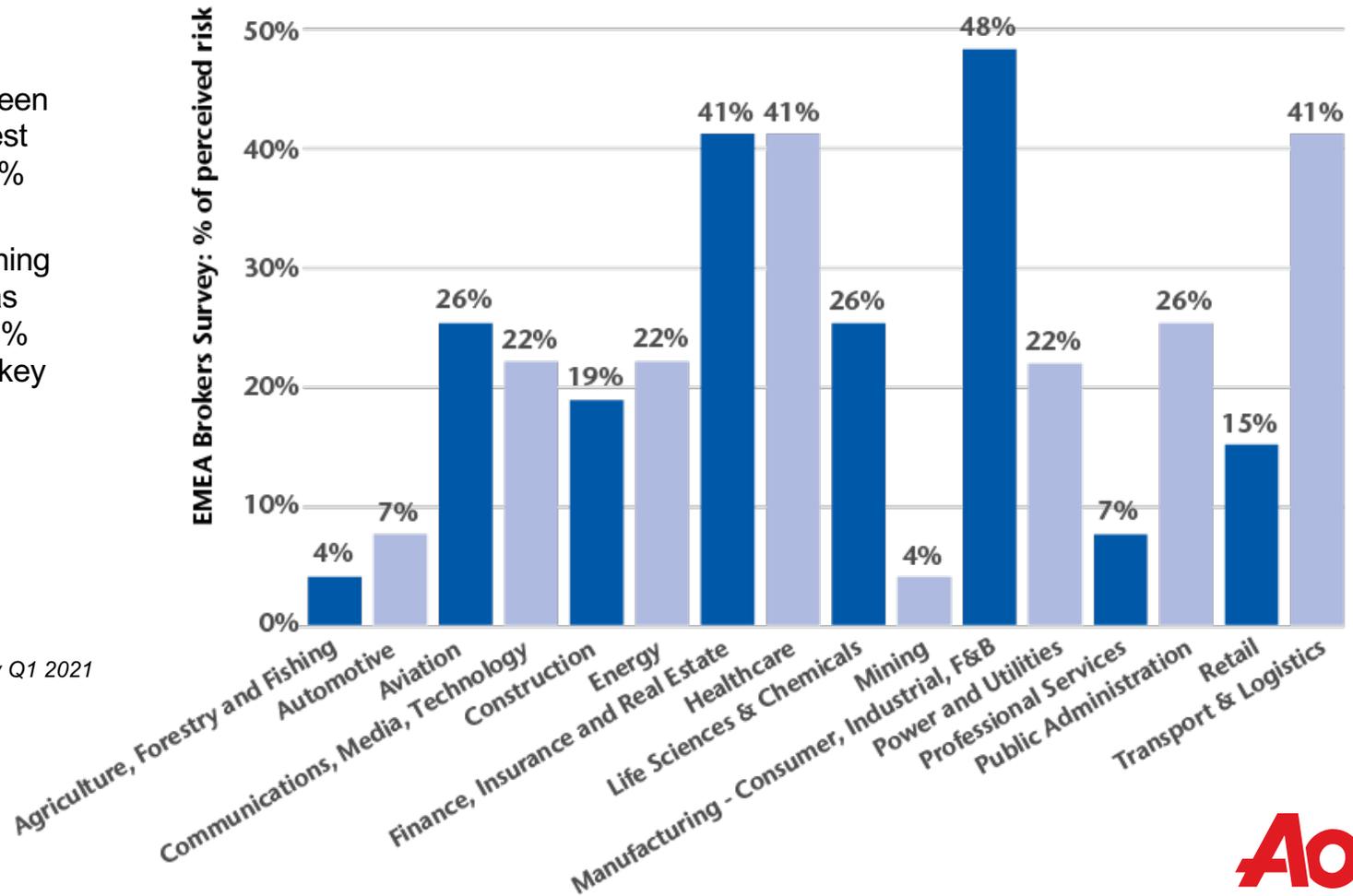
*Guidance is provided through Aon's proprietary survey of the major Cyber insurers Aon trades with. This is not proposed pricing, or guidance specific to a particular insured's programme. This is portfolio level guidance offered by underwriters who participated in the survey.

Source: Aon EMEA Cyber Carrier Survey Q1 2021

Forward Looking Guidance | Industry Vertical Perceived at Greatest Risk During Q1 2021

Key Commentary:

- Manufacturing clients have been identified as having the highest perceived risk (elected by 48% of broker respondents).
- Agriculture, Forestry and Fishing clients have been identified as having the lowest risk (only 4% of brokers selected this as a key risk industry).



Source: Aon EMEA Cyber Broker Survey Q1 2021

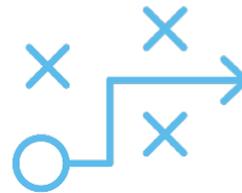
Key Pillars of a Cyber Insurance Policy



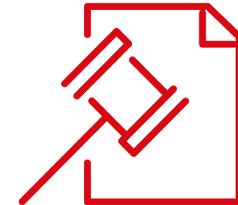
- Pre-breach assessments
- Access to pre-vetted vendors
- Cybersecurity information



- Forensic investigators
- Legal services
- Notification
- Credit Monitoring
- Call Center Services
- Crisis Management/ Public Relations



- Costs incurred to keep or return the business to operational
- Loss of revenue, income, turnover
- Costs incurred to recreate/restore data and information



- Legal costs and damages from claims alleging privacy breach or network security failure

Market Standard Cyber Coverages Overview



- Network Business Interruption
- System Failure
- Dependent Business Interruption / System Failure
- Cyber Extortion
- Digital Asset Restoration



- Privacy and Network Security Liability
- Privacy Regulatory Fines and Penalties
- Media Liability
- PCI Fines and Penalties
- Breach Event Expenses

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber security, risk and insurance management, investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

Cyber security services provided by Stroz Friedberg Limited and its affiliates. Cyber risk services provided by Aon UK Limited and its affiliates.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

© Aon plc 2019. All rights reserved.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The information contained in this document should not be considered or construed as legal or tax advice and is for general guidance only. Accordingly, the information contained herein is provided with the understanding that Aon, its employees and related entities are not engaged in rendering legal or tax advice. As such, this should not be used as a substitute for consultation with legal and tax counsel.

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

aon.com/cyber-solutions

サイバーの環境下における保険の活用方法

BJA Webinar on Cybersecurity – how to prepare your company for a Cyber Crisis
24/06/2021

Prepared by Aon's Cyber Solutions

AON
Empower Results®

サイバー攻撃への準備と拡大するリスク環境

1. サイバー・リスクへの取組み・対処:

「現状把握・分析」→「リスクの定量化」→「リスク・ヘッジ(保険化)」→「事故時の対応準備」←
各社毎、このサイクルをどこから始めるかは異なる。同サイクルを継続実施が、対策強化に繋がる。

2. 注意すべきサイバー・リスクの傾向:

(1) リモートな職場環境

職場がリモートになることにより、アクセスのセキュリティー、第三者のIT業者への依存増加、全てのコミュニケーションがデジタル越しになる、など。

(2) サイバー恐喝

ランサムウェア攻撃は会社の事業停止・減速だけでなく、規制に対する罰金、第三者との訴訟など多くの賠償義務の発生が潜在している。

(3) 規制違反

GDPRによる罰金は年々大幅増加傾向。2020年は前年対比で約40%上昇し総額€158.5M。同年の一件あたり最大はドイツ当局による€35M。総額はイタリアで€60M以上。過去最大はフランスで€50M。

(4) 取引先リスク

送電やソフト障害など、業者の脆弱性や業者間の複雑な業務交流によりリスクが高まる外部環境。

(5) 補償されていない技術系職業賠償責任

急速な技術発展により(伝統的業界を主に)賠償義務・同責任の所在と中身が明確になっていない。

2021年におけるランサムウェア脅威

ランサムウェアの手法は変化している

発生頻度の 大幅増加

- 全世界のランサムウェアによる被害コストは€17 billionになると見込まれる。これは5年前に**比べ57倍**
- ランサムウェアはサイバー犯罪で最も急速に伸びており、**2021年、企業が最も脅威に感じているサイバー・リスク¹**。

ターゲットの 一層の明確化

- 攻撃手は漠然と網羅的に攻撃することから、**具体的な個別攻撃、そして大物狙いに手法・標的を変えている**。
- 高額な支払いが出来るに標的を定めている²。

攻撃方法の 一層の洗練化

- 攻撃は洗練・高度化している。
- 「**二重恐喝**」の攻撃
- **データをコピーし公表すると脅す**
- **データを全て削除すると脅す**
- 「システム回復する」と連絡してくる。³

コストの 高額化

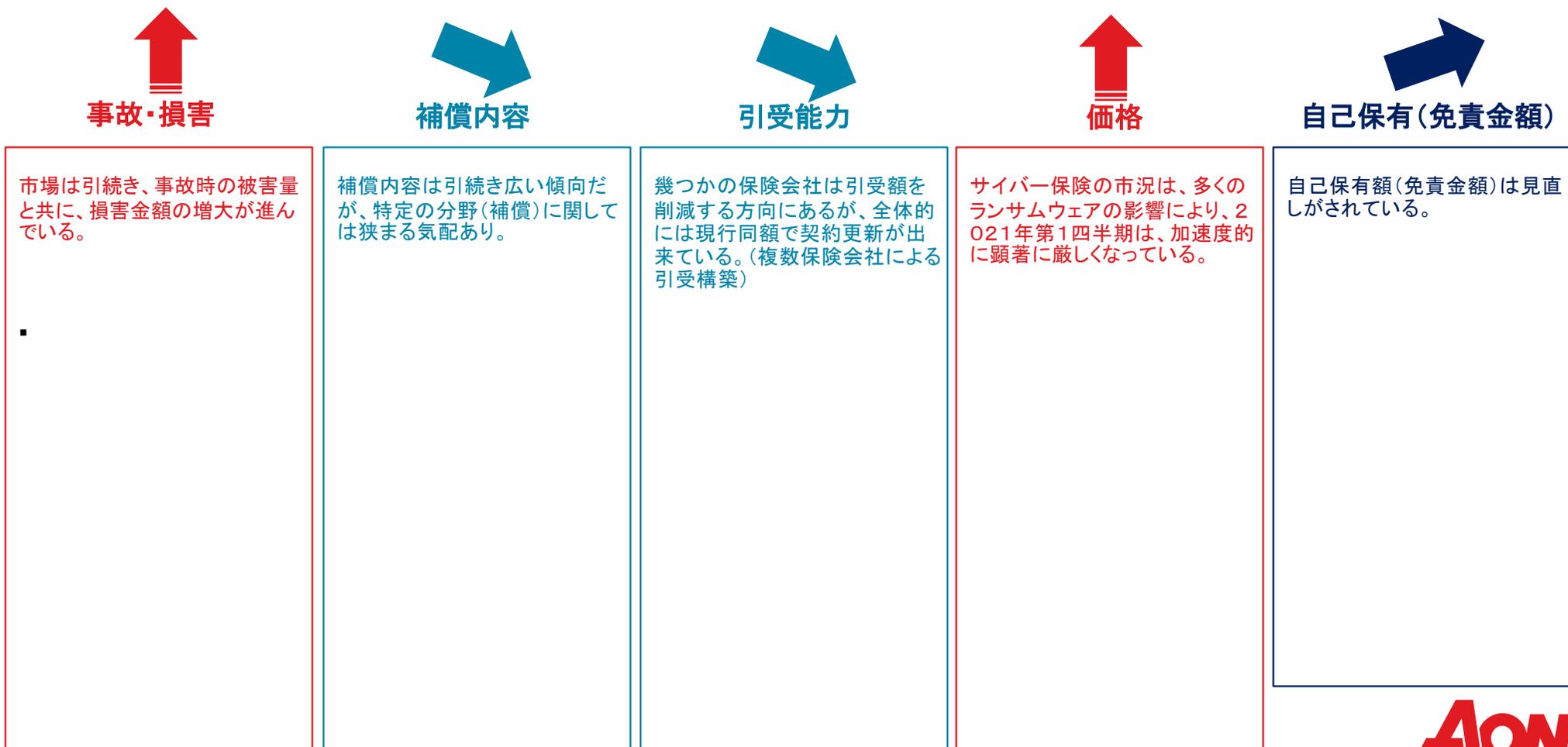
- 最近の高度化されたランサムウェア攻撃や、**一支払い当たり€650,000を超える⁴**
- (CrowdStrikeによると)**100社以上の日系企業がランサムウェアの攻撃に遭っており、33社が平均1.3億円支払った**。

1,4) <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/>

2) <https://www.wired.co.uk/article/ransomware-trends-2021>

3) <https://www.itproportal.com/news/ransomware-attacks-set-to-see-huge-growth-in-2021>

全世界におけるサイバー保険市場の傾向(2021年 第1四半期)



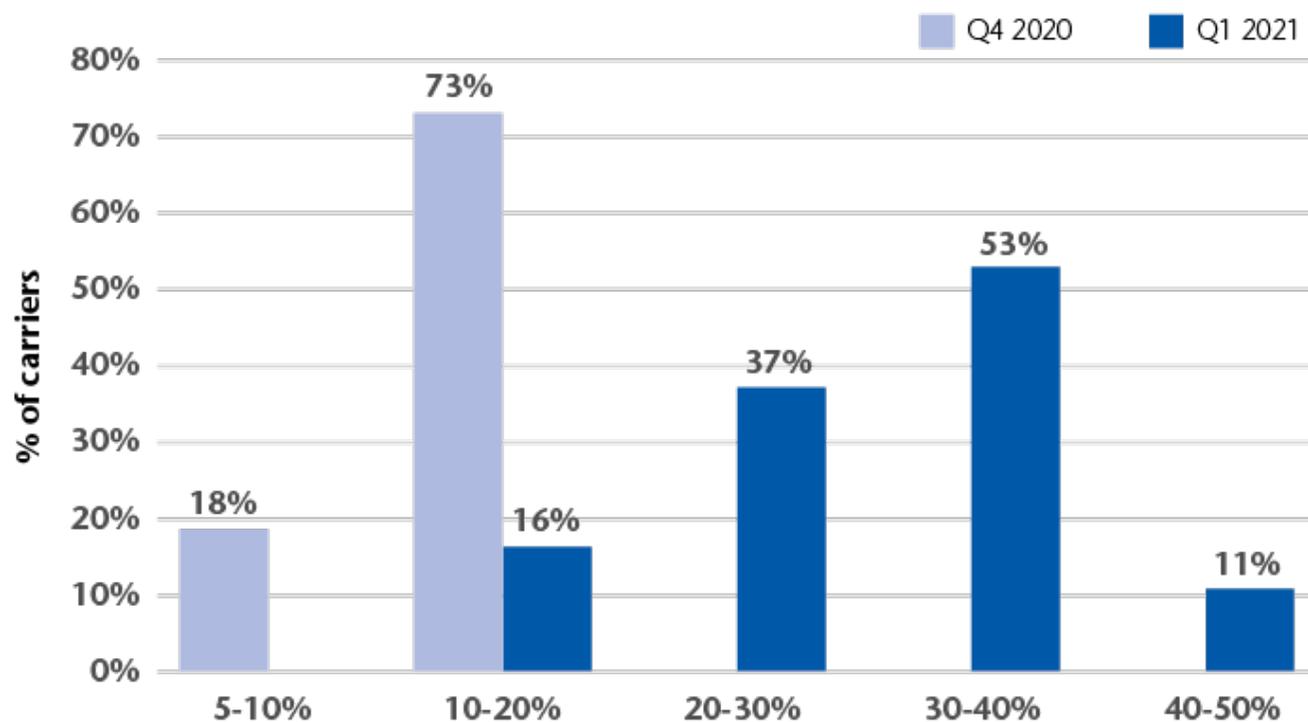
サイバー保険価格動向 | ポートフォリオ全体における価格変化の比較 (2020 Q4 vs 2021 Q1)

主要ポイント:

Aonの価格データはリアルタイムで時系列比較を実施。年毎に四半期単位でチェック。

- 2020 Q4 における平均的価格変化は +12%
- 2021 Q1 における平均的価格変化は+35%
- 即ち、増加幅は前四半期対比で+23%
- 調査対象の大層は、2021Q2には30%以上の更なる増加を見込むと回答。

*サイバー保険の価格は迅速に変化しています。

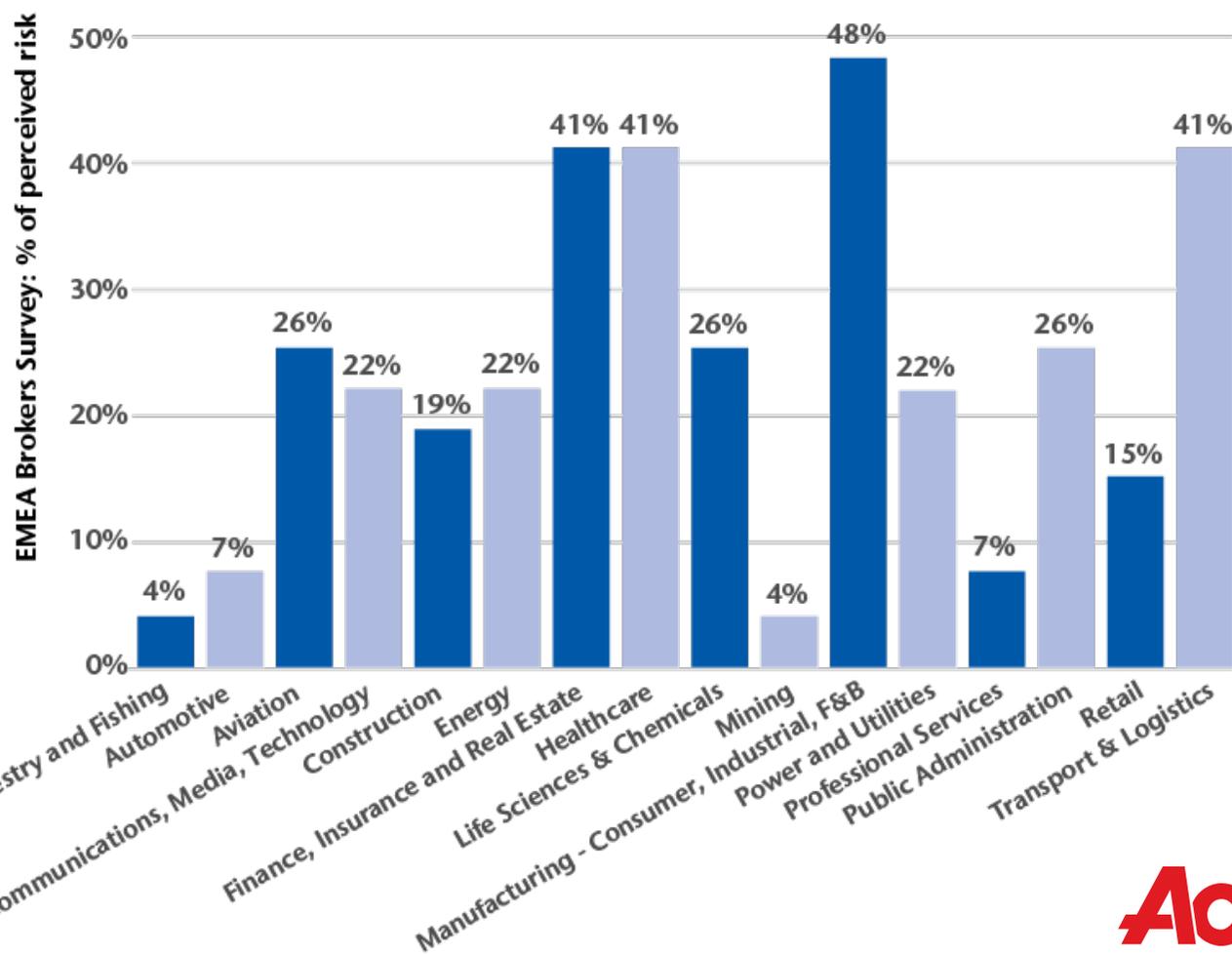


Source: Aon EMEA Cyber Carrier Survey Q1 2021

将来に向けた見込み | 業種別 事故発生 危険性予見 (2021 Q1)

主要ポイント:

- 最も事故が発生する危険性が高いと予見されるのは製造業。(全体回答者の48%を占める。)
- 農業、森林業、漁業が最も危険性が低い業種として予見される。(全体回答者の4%に留まる。)



Source: Aon EMEA Cyber Broker Survey Q1 2021

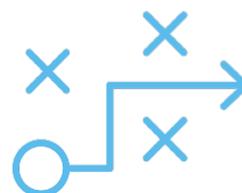
サイバー保険における重要な項目



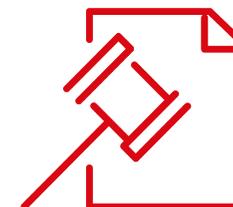
- 事故発生前の防止策解析
- 事前調査済業者へのアクセス
- サイバー・セキュリティ情報



- 科学的調査官
- 法務的サービス
- 各種通知・案内
- クレジット・モニタリング
- コールセンター・サービス
- クライシス・マネジメント/対外折衝



- 事業を通常に維持・回復するコスト
- 収入、収益や売上の減少
- データや情報の再作成・再構築にかかるコスト



- 事故による損害に加えプライバシー侵害やセキュリティ対策過失などによる法的費用

サイバー保険マーケット標準の概況

操業リスク



- (自社内)ネットワーク 操業停止・逸失利益
- (自社)システム障害
- (取引先) 操業停止・逸失利益 / システム障害
- サイバー恐喝
- デジタル化された財産の再構築

プライバシーと ネットワーク セキュリティリスク



- プライバシー及びネットワーク・セキュリティーに係る賠償責任
- プライバシー規制に係る罰金や罰則
- メディア 賠償責任
- PCI 罰金や罰則
- 法的抵触に係る諸費用

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber security, risk and insurance management, investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

Cyber security services provided by Stroz Friedberg Limited and its affiliates. Cyber risk services provided by Aon UK Limited and its affiliates.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

© Aon plc 2019. All rights reserved.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The information contained in this document should not be considered or construed as legal or tax advice and is for general guidance only. Accordingly, the information contained herein is provided with the understanding that Aon, its employees and related entities are not engaged in rendering legal or tax advice. As such, this should not be used as a substitute for consultation with legal and tax counsel.

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

aon.com/cyber-solutions



Empower Results® 64