Cyber-attack trends and efficient response to incidents

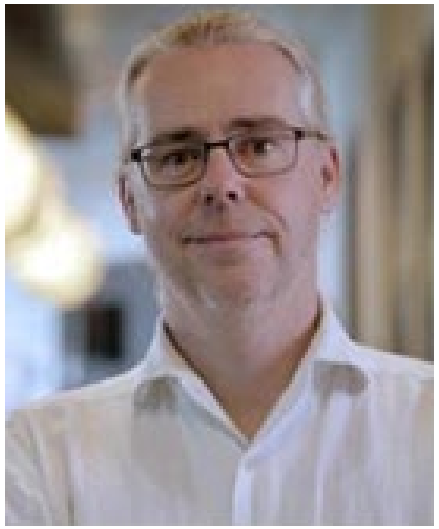
A story about leadership, actual client testimonials and key questions to consider

31 May 2022
Karel Dekyvere – Director Cyber & Privacy

サイバーアタックの傾向と対策

A story about leadership, actual client testimonials and key questions to consider

31 May 2022
Karel Dekyvere – Director Cyber & Privacy



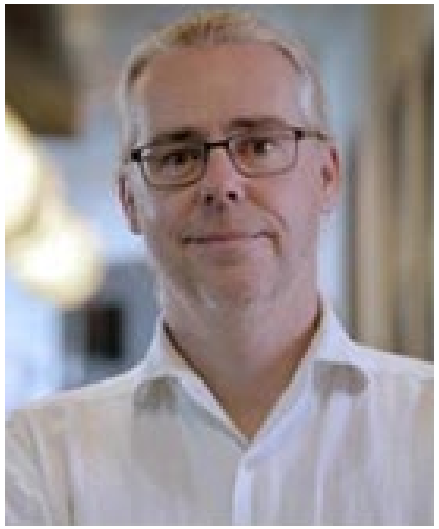
Karel Dekyvere
Director Cyber & Privacy
Kdekyvere@kpmg.com

Karel Dekyvere is part of the Cyberdefense team at KPMG, helping customer in building and maintaining business aligned security solutions.

In his previous career he was the Chief Information Security Officer (CISO) at Microsoft, focused on physical and information security. He has nearly 30 years of experience in security services, of which 20 years at Microsoft.

His past endeavours include a broad range of activities around security: Penetration testing, architecting security solutions, creating information management policies, building response capabilities, and assisting customer in incident recovery

Karel co-authored the Belgian Cyber security guide, and the Belgian security cookbook for small and medium business. He also published several articles and interviews for national newspapers and TV.



Karel Dekyvere
Director Cyber & Privacy
Kdekyvere@kpmg.com

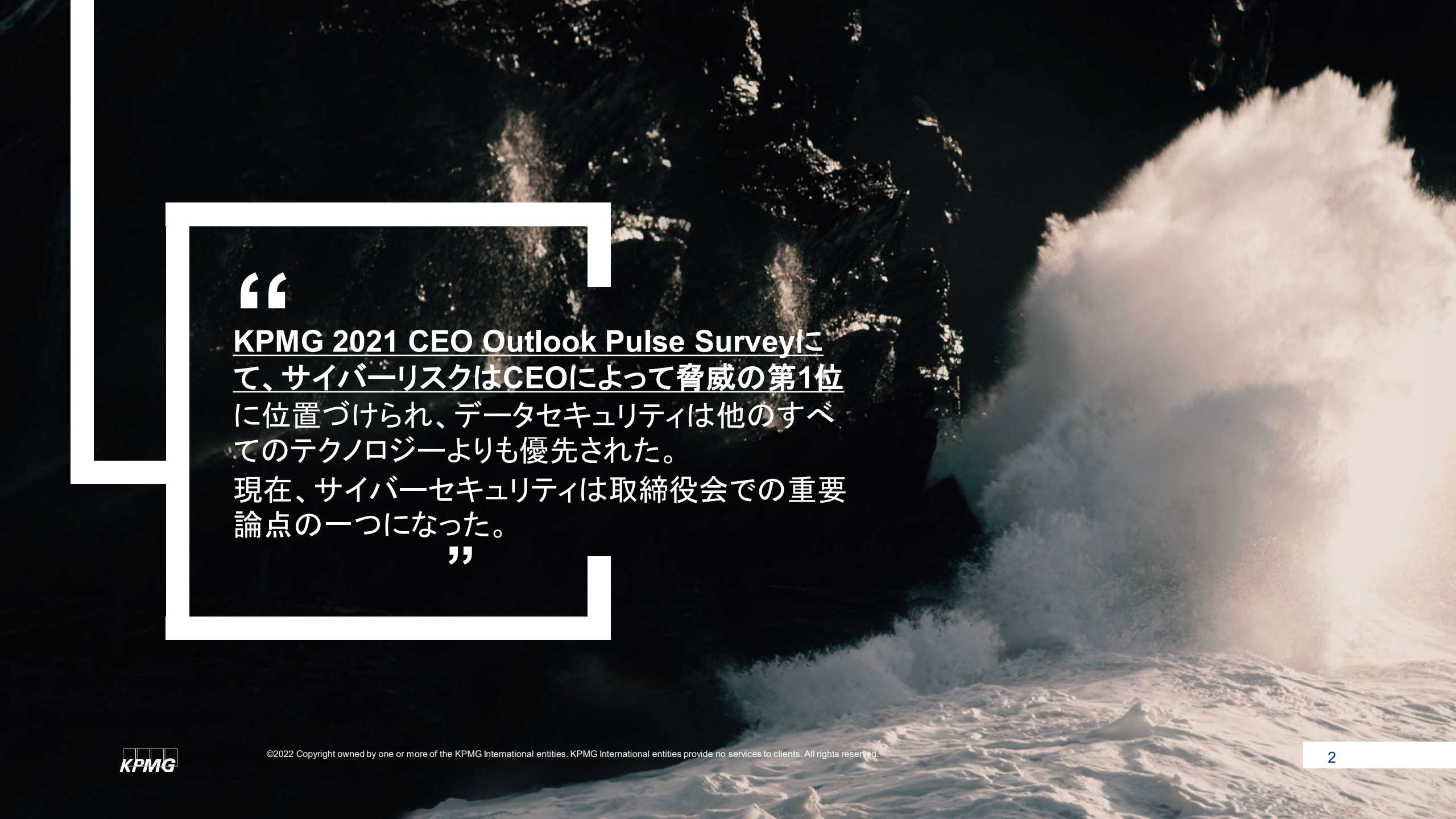
KPMGベルギーのサイバーディフェンスチームの一員として、ビジネスに沿ったセキュリティソリューションの構築と維持活動を多く支援。

KPMG参画前は、マイクロソフトベルギーにて最高情報セキュリティ責任者 (CISO) を務め、物理および情報セキュリティの構築に貢献。セキュリティ 分野において合計 30 年近くの経験を持ち、そのうち 20 年間はマイクロソフトにて勤務。

主な活動内容は、ペネトレーションテスト、セキュリティソリューション設計、情報マネジメント方針策定、セキュリティ対応態勢構築支援、インシデント復旧支援などが含れる。

また、ベルギーサイバーセキュリティ 指針と、中小企業向けセキュリティ クックブックを共同執筆。さらに、サイバーセキュリティに関するベルギー全国紙への寄稿やテレビ出演なども多数経験。

“Cyber security is now a common topic of boardroom debate. In the KPMG 2021 CEO Outlook Pulse Survey, cyber risk was ranked as the number one organizational threat by global CEOs, with data security taking a priority over all other technology investments.”



“

KPMG 2021 CEO Outlook Pulse Surveyにて、サイバーリスクはCEOによって脅威の第1位に位置づけられ、データセキュリティは他のすべてのテクノロジーよりも優先された。

現在、サイバーセキュリティは取締役会での重要論点の一つになった。

”

Cyber is a top business risk

KPMG Global Annual CEO Report

2016	2017	2018	2019	2020	2021
1. Cyber security	1. Operational risk	1. Territorialism	1. Operational risk	1. Territorialism	1. Cyber security
2. Regulatory risk	2. Emerging technology	2. Cyber security	2. Emerging technology	2. Cyber security	2. Regulatory risk
3. Emerging technology	3. Reputational/brand	3. Emerging technology	3. Reputational/brand	3. Emerging technology	3. Tax risk
4. Strategic	4. Strategic	4. Environmental change	4. Strategic	4. Environmental change	4. Supply chain risk
5. Geopolitical	5. Cyber security	5. Operational risk	5. Cyber security	5. Operational risk	5. Environmental change

Legislative focus is placing pressure on Boards

1. WW Cyber Security Acts

2. Privacy Mandatory Breach Notification

3. Critical Infrastructure & regional conflicts

サイバーセキュリティは第1位のリスク

KPMG Global Annual CEO Report

2016	2017	2018	2019	2020	2021
1. サイバーセキュリティ	1. 事務リスク	1. テロリズム	1. 事務リスク	1. テロリズム	1. サイバーセキュリティ
2. 規制リスク	2. 革新的技術	2. サイバーセキュリティ	2. 革新的技術	2. サイバーセキュリティ	2. 規制リスク
3. 革新的技術	3. 評判・ブランドリスク	3. 革新的技術	3. 評判・ブランドリスク	3. 革新的技術	3. 税務リスク
4. 戦略リスク	4. 戦略リスク	4. 気候変動リスク	4. 戦略リスク	4. 気候変動リスク	4. サプライチェーンリスク
5. 地政学的リスク	5. サイバーセキュリティ	5. 事務リスク	5. サイバーセキュリティ	5. 事務リスク	5. 気候変動リスク

取締役会に対して、法的整備に関する圧力も高まりつつある

1. サイバーセキュリティ関連法案

2. プライバシー違反発覚時の強制開示

3. 重要インフラ及び領域の保護

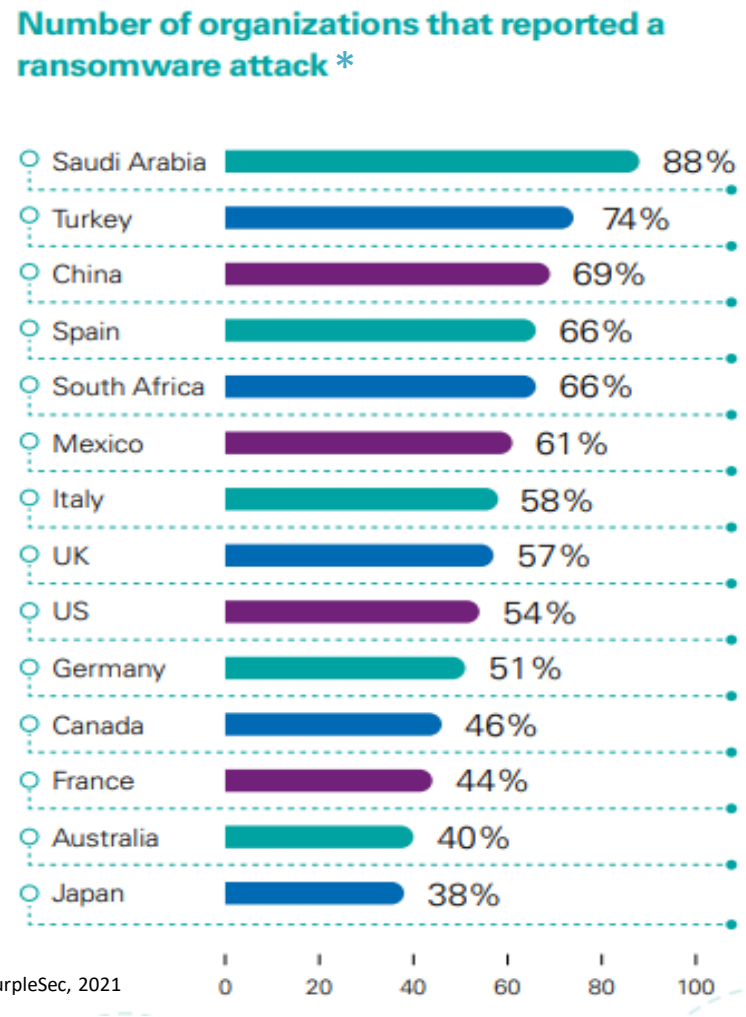
KPMG

The Cyber Threat Landscape

KPMG

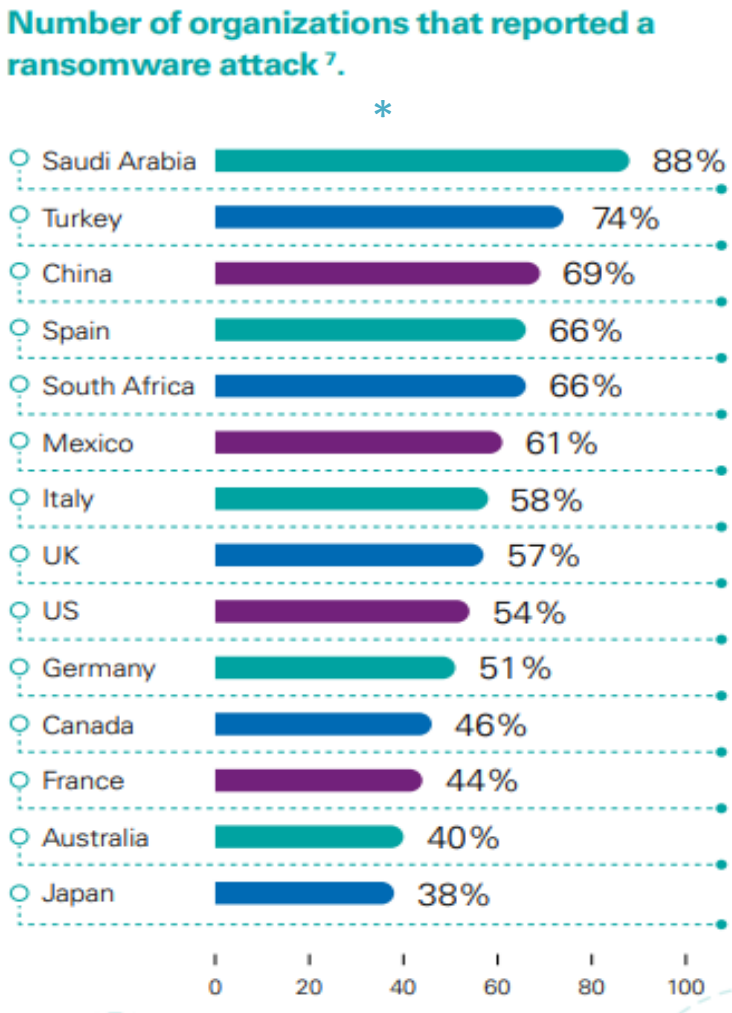
サイバー脅威の概況

The growing threat landscape



*2021 Ransomware Statistics, Data, & Trends, PurpleSec, 2021

サイバー攻撃は増加傾向にある



*2021 Ransomware Statistics, Data, & Trends, PurpleSec, 2021

Cyber threats and risks for consumers and organizations

Business threats and risks

320 billion
emails sent per day

DDoS Attacks
expected to reach
1.4 million
by 2022

28%
of cyberattacks are due to insider threats

Consumer threats and risks

50% more
smartphones which account for the largest threat vector

447 million
million consumer records stolen in 2018

Personal health information is
50x more valuable
than credit card info on dark web

60 million
affected by identity theft in 2018 (up from 15M in 2017)

90%
of all hacks are done by phishing

Cloud security
By 2022 **100x** more data is stored online than in 2019

顧客及び組織におけるサイバーの脅威

3200億通
一日辺りのメール送受信

50% 以上
のスマートフォンが脅威にさらされている

4.47 億人
の個人情報が2018年時点で漏洩

DDoS攻撃の成功数

1.4億回
by 2022

個人の病歴や健康状態の情報は、クレジットカードの**50倍**の価値がある

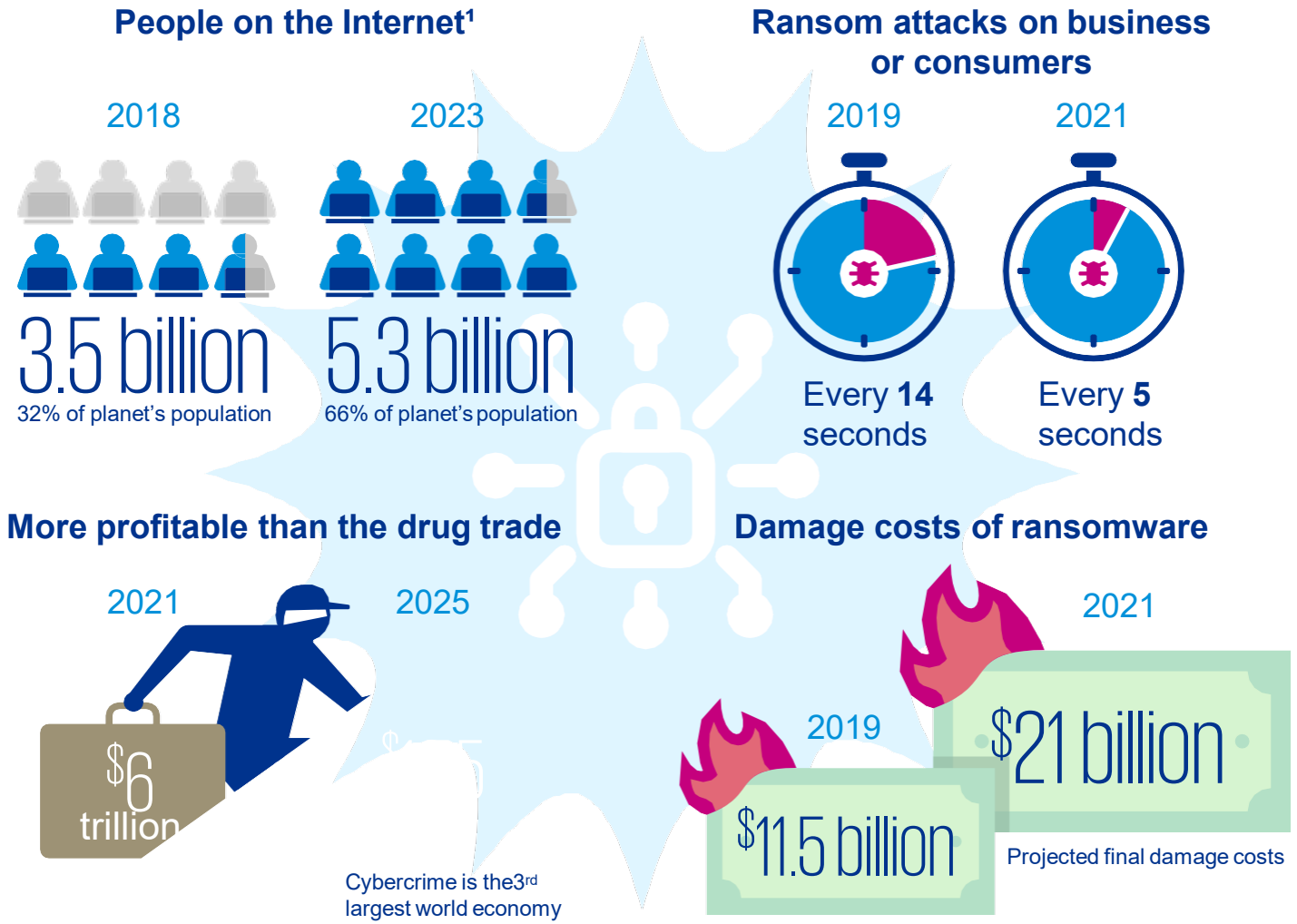
6千万件
の個人認証情報が盗難にあっている(2017年時点の1.5千万件より増加)

28%
のサイバー攻撃に内部者が関与

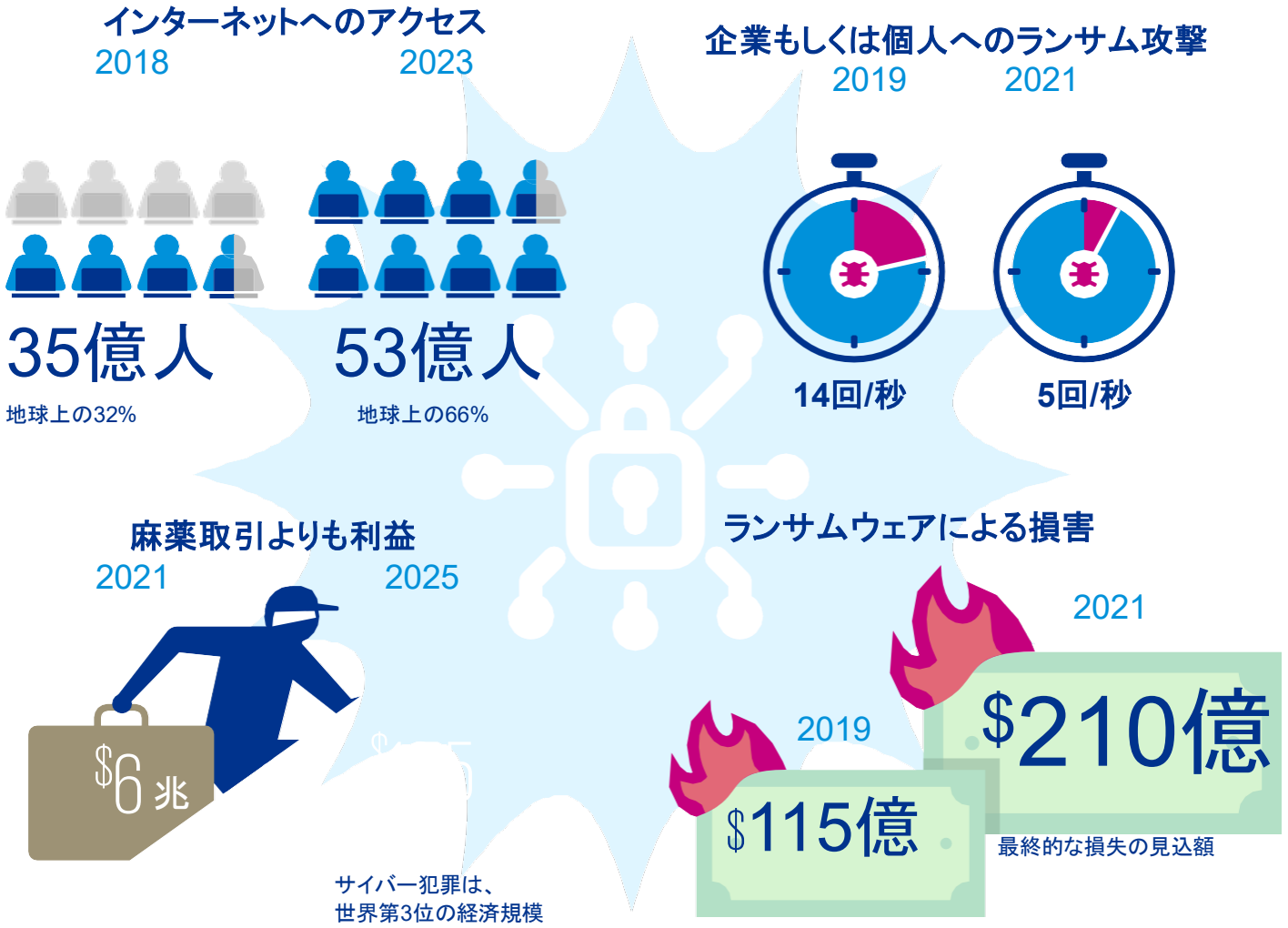
90%
のハッキングは、フィッシングによって行われている

Cloud security
2019年と比較して
2022までに **100倍**
のデータがオンライン上に保管される

Explosive growth



爆発的増加



Moving from IT componets to digital assets

Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans

Garther, July 21, 2021

Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security (CPS) Incidents by 2024

Garther, Sep 30, 2020

Gartner

ITシステムからデジタルアセットへの移行傾向

Gartnerは、2025年までにサイバー攻撃者がオペレーション技術環境を武器化して人間に危害を加えたり殺害すると予測
Garther, July 21, 2021

さらに、CEOの75%が2024年までにサイバーフィジカルセキュリティ(CPS)インシデントに対して個人的に責任を負うと予測
Garther, Sep 30, 2020

Gartner

KPMG

Current state of play

最新状況

Crime landscape overview

Commodity crime

Commodity attacks are usually perpetrated by attackers who either do not have the skills to perform more advanced attacks or who prefer to perform many, easy attacks and benefit from a low success rate rather than spend a lot of time to customize a small number of more profitable attacks against specific targets.

Tailored attacks

A targeted attack is any malicious incident aimed at a specific individual, company, system or software. It may extract information, disturb operations, infect machines or destroy a specific data type.

A targeted attack uses a type of crimeware or malware program designed to attack the target. First, perpetrators typically analyze the target, the underlying security mechanisms and potential post-attack ramifications.

Highly targeted attacks

According to a Forbes article, “Cyberwarfare will explode in 2020 (because it’s cheap and effective)”. Cyberwarfare is a new business model, it is cheaper, easier, faster and thought to be the most effective warfare seen to date.

Cyber attacks have become more advanced. 2020 saw the first noted instance of a bad actor using AI to mimic a voice (known as deepfake) in a scam. It convinced a CEO to part with US$243,000.

サイバー犯罪の概況

一般的攻撃

攻撃者自身が高度なスキルを有していない場合や、特定標的に対してより収益性の高い攻撃の為にカスタマイズするための時間を費やすより、一件あたりの成功率が低くても多数の比較的単純な攻撃を実行する方が有利と判断した場合に採用される攻撃パターン

標的型攻撃

特定の個人、企業、システム、またはソフトウェアを狙った悪意のある攻撃パターンであり、情報搾取、操作妨害、ウィルス感染、特定データ破壊等を効率的に実行

攻撃対象の為に個別に設計されたクライムウェアまたはマルウェアプログラムを利用する為に、攻撃者は通常、ターゲットの基盤となるセキュリティメカニズムや攻撃による潜在的影響を分析する

高度な標準型攻撃

フォーブスの記事によると、「安価で効果的なサイバー戦争は2020年に勃発するだろう」と指摘している。サイバー戦争は新しいモデルであり、より安価・簡易・迅速な攻撃が可能であり、歴史的な戦争よりも格段に効果的であると考えられる

2020年には、悪意のある攻撃者がAIを使用したディープフェイクと呼ばれる手法で詐欺師の音声を模倣した最初の事例が見られた。被害にあった企業のCEOは243,000米ドルを支払うこととなった

Seven phases of a cyber attack

1

Reconnaissance
Research, identify and select targets.

2

Weaponization
Pair remote access malware with exploit into a deliverable payload (i.e. creating Phishing emails).

3

Delivery
Transmission of weapon (i.e. Phishing email) to target.

4

Exploitation
Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems.

5

Installation
The weapon installs a backdoor on a target's system allowing persistent access.

6

Command and control
Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.

7

Action on objective
The attacker works to achieve the objective of the intrusion.

サイバー攻撃の7つのステップ

1

偵察
調査、識別、対象選定

2

最適な攻撃手段の決定
リモートアクセスの為のマルウェアの送付手段 の策定
(例：フィッシング用メール作成等)

3

デリバリー
ターゲットへの武器(フィッシングメールなど)の送信

4

1101100
100
100

情報収集
攻撃手段の送信後、攻撃用コードが発動され、脆弱なアプリケーションやシステムを特定

5

インストール
攻撃対象システムにバックドアを設置し、永続的なアクセスを可能する

6

指示とコントロール
外部サーバーは、ターゲットのネットワーク内で「ハンズオンキーボードアクセス」を提供する攻撃手段と通信

7

目的別攻撃
攻撃者は、侵入後の目的に沿って攻撃目標行動を実行.

The Mammoth case

A case that could be yours!

マンモス社*の事例

*欧州の主要インフラ・装置企業

A case that could be yours!

A typical client story...

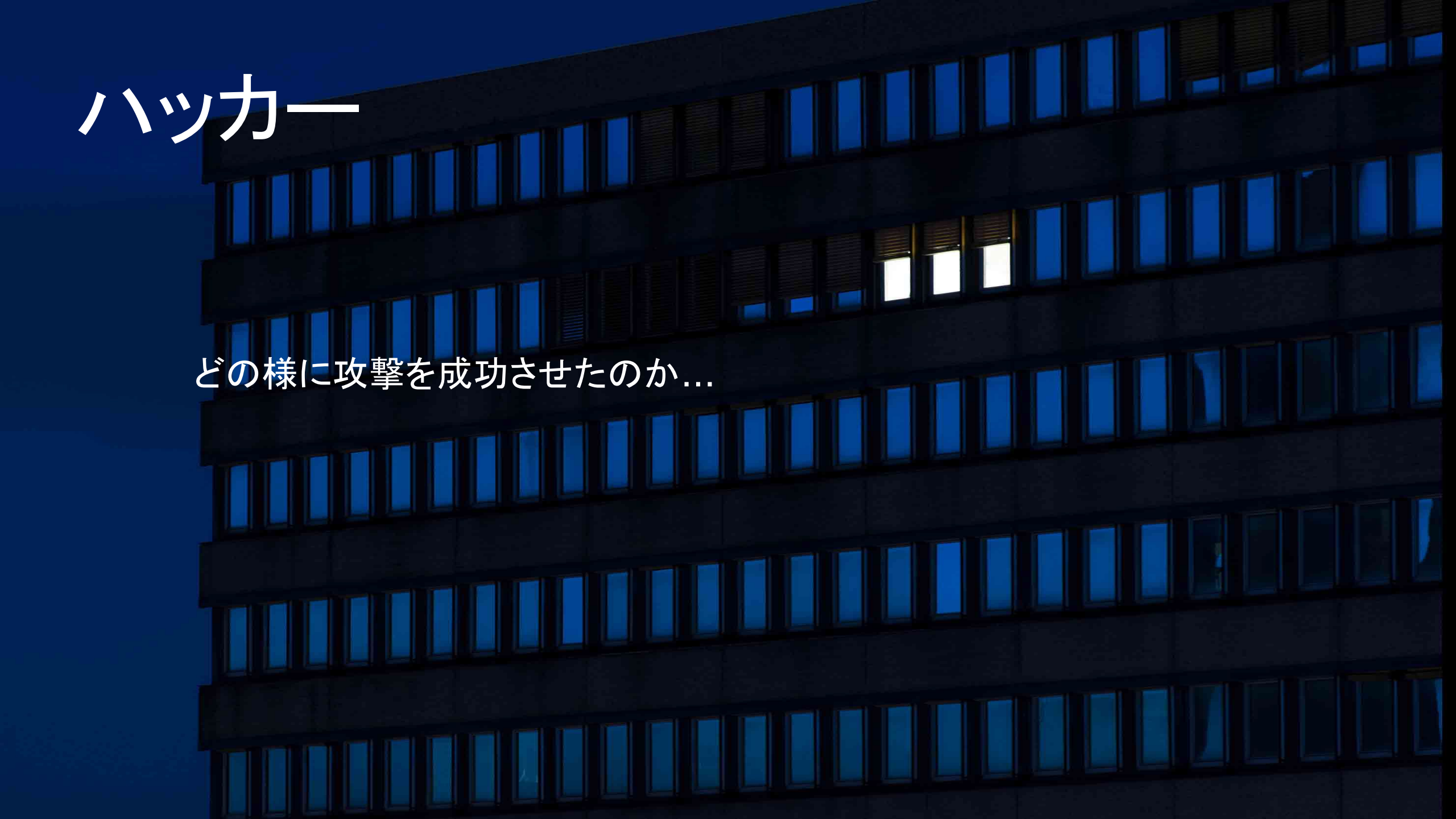
サイバー攻撃の典型例...

The hackers

How they pulled it off…

ハッカー

どの様に攻撃を成功させたのか…



Incident investigation

5 compromised domain controllers

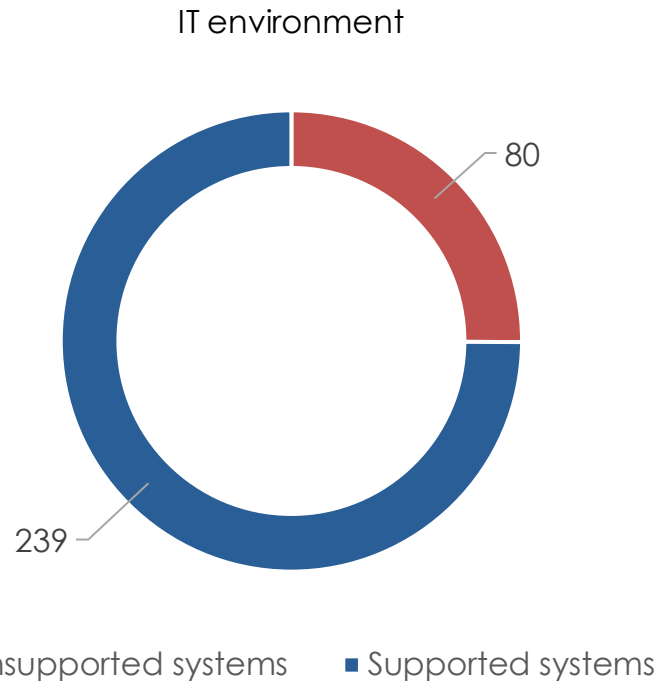
Execution of malicious scripts and connection to known malicious IP address

Leaked usernames and passwords

Multiple compromised administrator accounts

3 compromised Citrix virtual systems

2 compromised file servers



インシデント調査

5つの侵害された
ドメインコントローラー

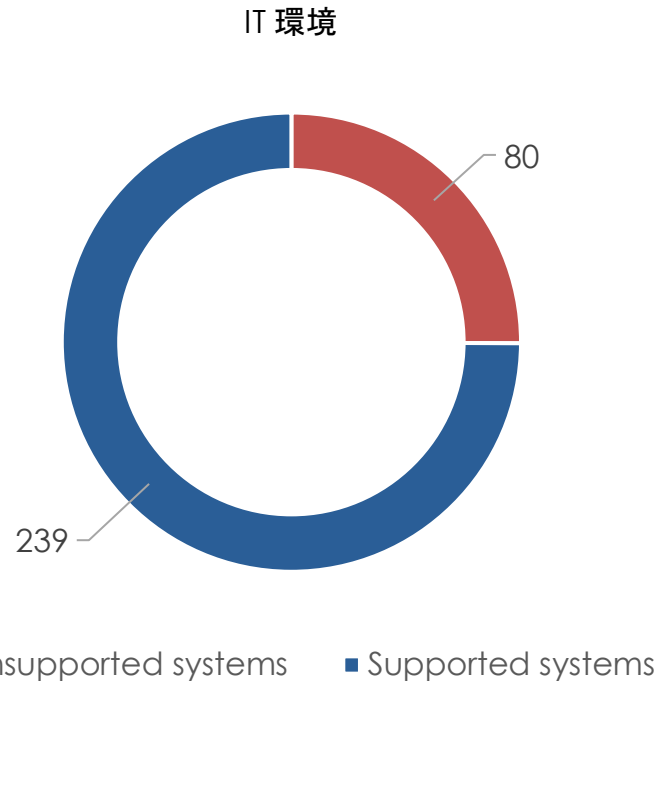
悪意のあるスクリプト
の実行と既知の
IPアドレスへの接続

ユーザ名とパスワード
漏洩

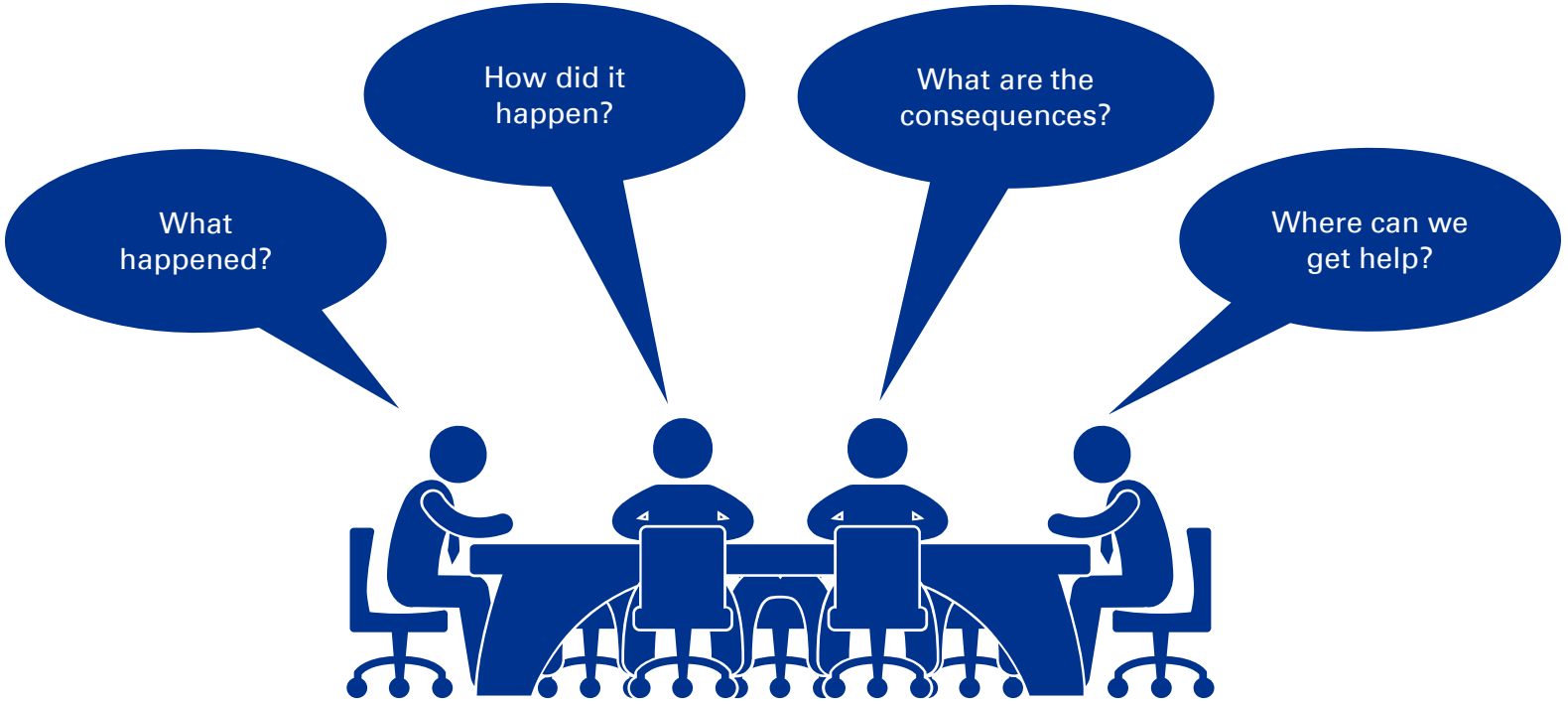
複数の侵害された
管理者アカウント

3つの侵害された
Citrix仮想システム

2つの侵害された
ファイルサーバ

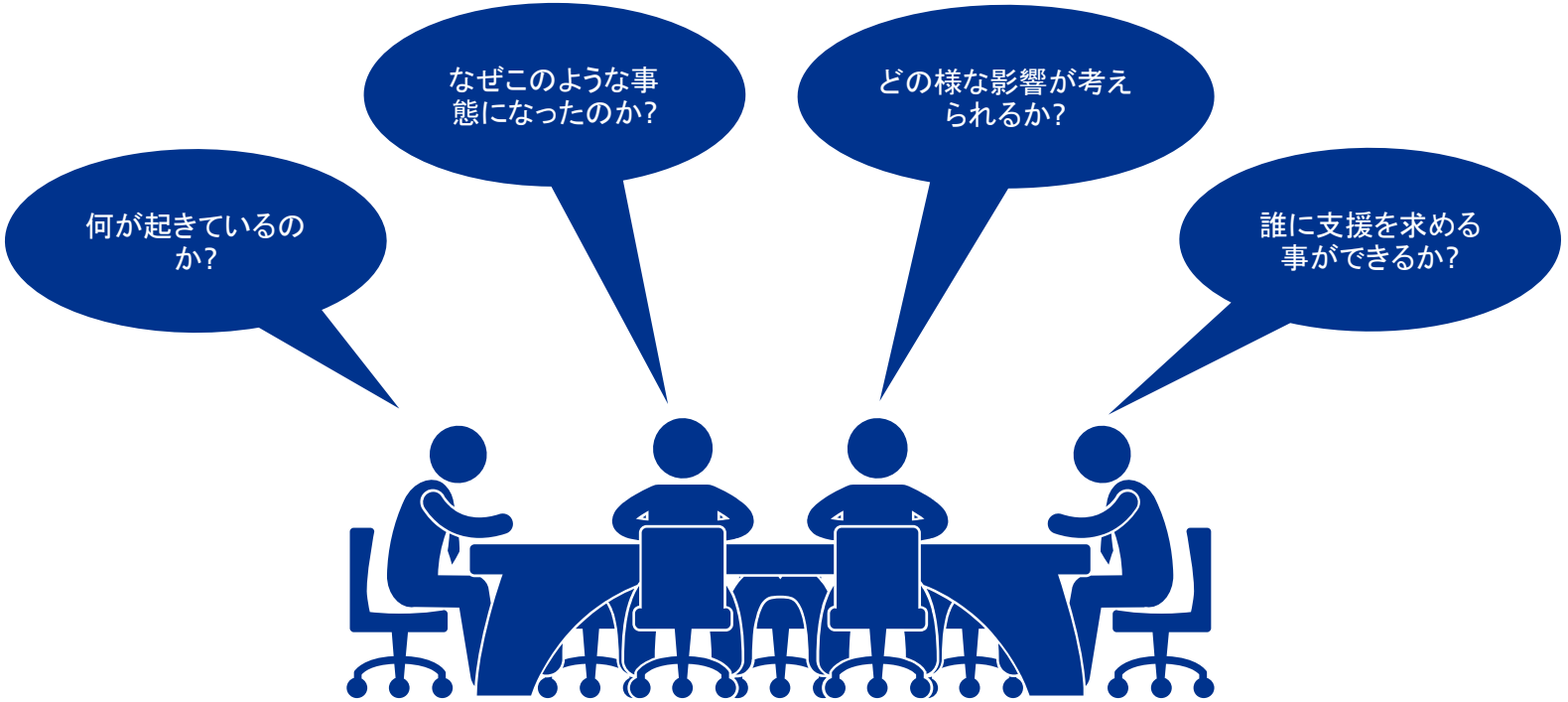


Mammoth grapples with the issue



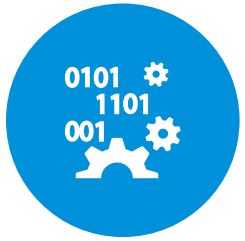
Why don’t we have a procedure for this?

問題への取組み



なぜ我々は、事前にこの様な事態への準備を怠っていたのか?

Compromised assets



Infrastructure

- Several systems (5 domain controllers, 2 file servers, 3 Citrix virtual systems) show evidence of compromise.
- Execution of malicious scripts and external connections are made to known malicious IP address.
- Unsupported and potentially unpatched systems, with known vulnerabilities, provide several opportunities lateral movement.

Compromised

Identity

- Leaked credentials (usernames and passwords).
- Multiple compromised administrator accounts.
- Unauthorized connections with compromised accounts to systems throughout the whole IT environment.

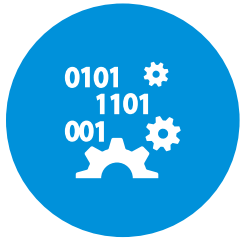
Compromised

Information

- Compromised files resulted in the detection and notification of the incident.
- Several files previewed within O365 environment.
- Insufficient logging to validate data exfiltration.

Potentially Compromised

侵害された資産



インフラ

- 5つのドメインコントローラ、2つのファイルサーバー、3つのCitrix仮想システムが侵害
- 悪意のあるスクリプトの実行と既知のPアドレスへの接続
- 適切にサポートされていない、またはパッチが適時にあてられていないシステムにおける脆弱性は、侵入後の導線を提供する事に繋がる

侵害

個人認証

- 漏洩したクレデンシャル(ユーザ名、パスワード等).
- 複数の管理者アカウントの侵害
- 侵害されたアカウントを用いたIT環境全体システムに対する不正接続

侵害

情報

- 侵害されたファイルが、インシデント検出と通知につながった
- いくつかのファイルは、オフィス365環境下にてプレビューされた
- データ漏えいを検証するにはログが不十分

侵害の可能性

Get well plan

1. Deploy SIEM platform and Azure ATP
2. Update Palo Alto firewall rules (network segmentation)
3. Patching of CITRIX systems
4. Embed Navision systems in shielded environment
5. Crawl identity stores for dormant and orphan accounts
6. Prepare internal and external communication plan

Infrastructure

1. Setup dark forest and restore a system in order to monitor the behavior of the system
2. Patching of all client and server systems
3. Rebuild Domain controllers
4. Strategic decision green/brown field recovery

Identity

1. List and investigate all administrative accounts
2. Enable multifactor authentication
3. Validate conditional access (warning mode only)
4. Enable Windows Hello for Business and Credential Guard for all systems

周到な事前準備の一例

1. SIEM(システムセキュリティ及びイベント管理プラットフォームとAzure ATP(クラウドベースEDRセキュリティ機能)を配置
2. Palo Alto(パロアルト)ファイアウォールによるネットワークセグメンテーション
3. CITRIX(仮想化ウェア)の適切なパッチ
4. シールド環境へのNavision(MS社ERPパッケージ)の導入
5. 休止中および孤立IDの情報収集
6. 内外部コミュニケーション方法の確立

インフラ

1. システム動作監視のためダークフォレストをセットアップとシステム復元
2. クライアントサーバ全システムのパッチ
3. ドメインコントローラの再構築
4. グリーン/ブラウンフィールド復旧の戦略的決定

個人認証

1. 全ての管理者アカウントの一覧化と調査
2. 多要素認証の有効化
3. 条件付アクセス検証(警告モードのみ)
4. 全システムへのWindowsHelloforBusinessとCredentialGuardの有効化

Incident still active - remain vigilant

インシデントは継続中ー警戒態勢

KPMG

Cyber security toolkit for Boards

KPMG

取締役向けサイバーセキュリティツール

Board responsibilities

Understand:

1. Risk landscape
2. Response plans
3. Critical systems
4. Regulatory obligations
5. Audit results

Guide and agree to:

1. Security strategy
2. Cyber risk management
3. Risk appetite
4. Accountable
5. Partnerships

Take board-level action to:

1. Raise cyber awareness
2. Challenge management
3. Ensure sufficient time at board
4. Enable management
5. Enable continuous enhancement

取締役の責任

現状理解:

1. リスクの全体像
2. 対応計画
3. 最重要システム
4. 規制対応
5. 監査

指示と合意:

1. セキュリティ戦略
2. サイバーリスクマネジメント
3. リスク選好
4. 説明責任
5. パートナーシップ

取締役レベルの行動:

1. サイバー攻撃に対する啓もう活動
2. チャレンジマネジメント
3. 取締役会における十分な協議
4. 有効性マネジメント
5. Enable continuous enhancement

Five key questions to asks

- As an organization and as board members, how would we know when an incident occurred?
- As an organization, what measures do we take to minimize the damage an attacker could do inside our network?
- As an organization, do we have a incident management plan for cyber incidents and how do we ensure it is effective?
- Does our incident management plan meet the particular challenges of ransomware attacks?
- How is data backed up, and are we confident that backups would remain unaffected by a ransomware infection?

5つの重要な問い

- 組織として、また取締役会のメンバーとして、インシデントがいつ発生したかをどのようにして知ることができるか？
- 組織として、攻撃者がネットワーク内で行う可能性のある被害を最小限に抑えるために、どのような対策を講じているか？
- 組織として、サイバーインシデント管理計画があり、それが効果的であることをどのように確認しているか？
- インシデント管理計画は、ランサムウェア攻撃の特定課題に対応しているか？
- データはどのようにバックアップされているか？また、バックアップはランサムウェア感染の影響を受けないと確信できているか？

御清聴ありがとうございました

Contacts:

Benny Bogaerts
Partner
T: +32 477 301449
E: bbogaerts@kpmg.com

Karel Dekyvere
Director
T: +32 475 700961
E: kdekyvere@kpmg.com

home.kpmg/socialmedia