Rencontres du Risk Management AMRAE 2020

Atelier B8

Les étapes clés pour construire une politique de gestion des risques numériques

MAÎTRISE DU RISQUE NUMÉRIQUE
L'ATOUT CONFIANCE

Un guide coréalisé par l'AMRAE et l'ANSSI

Une approche ambitieuse

OBJECTIF

Proposer une **démarche rationnelle** pour définir et mettre en œuvre **un management efficace** du risque numérique

CIBLE

Dirigeants

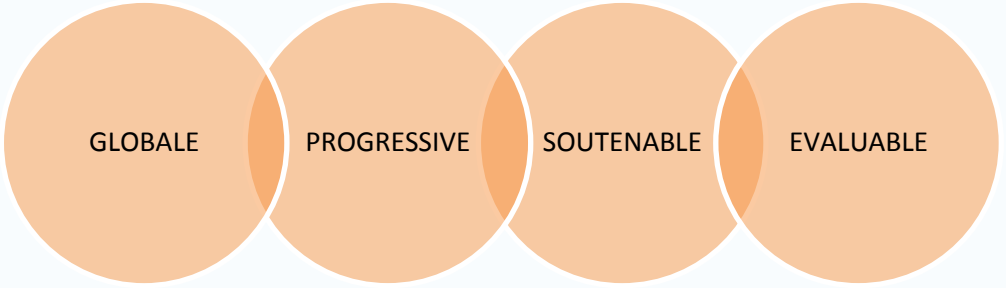
Directeur admin. taille moyenne

Risk managers / CISO

FONDAMENTAUX

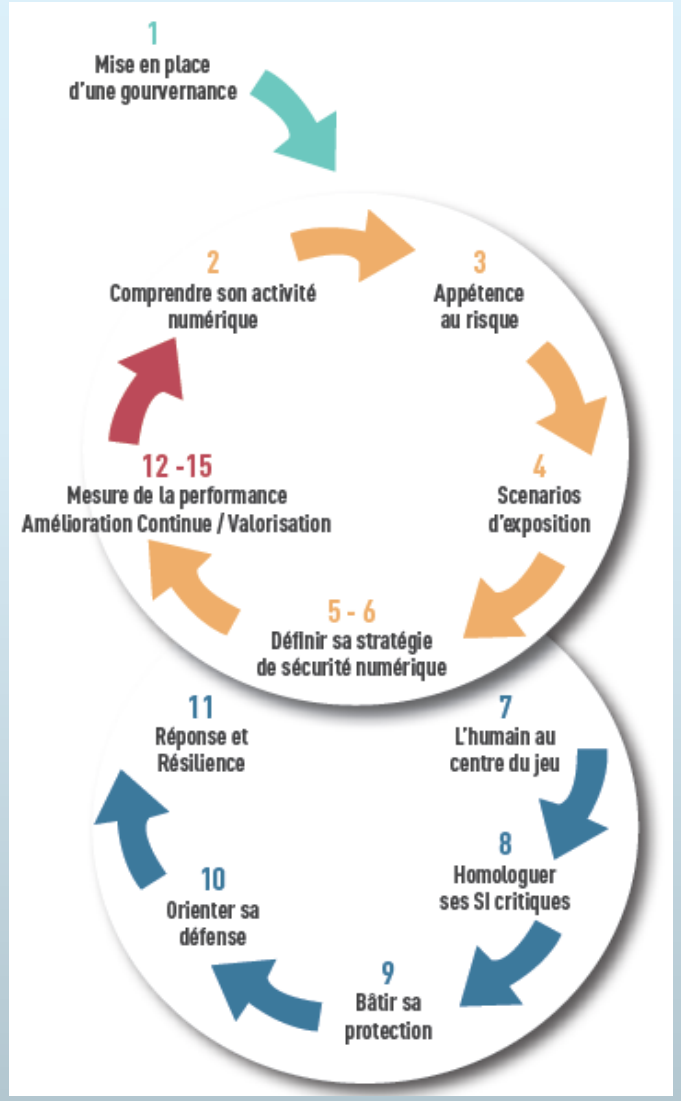
- 4 phases
- Maîtrise du risque numérique / des coûts
- Valorisation des investissements

VALEURS



Synthèse des cultures AMRAE & ANSSI

Synthèse des cultures AMRAE & ANSSI



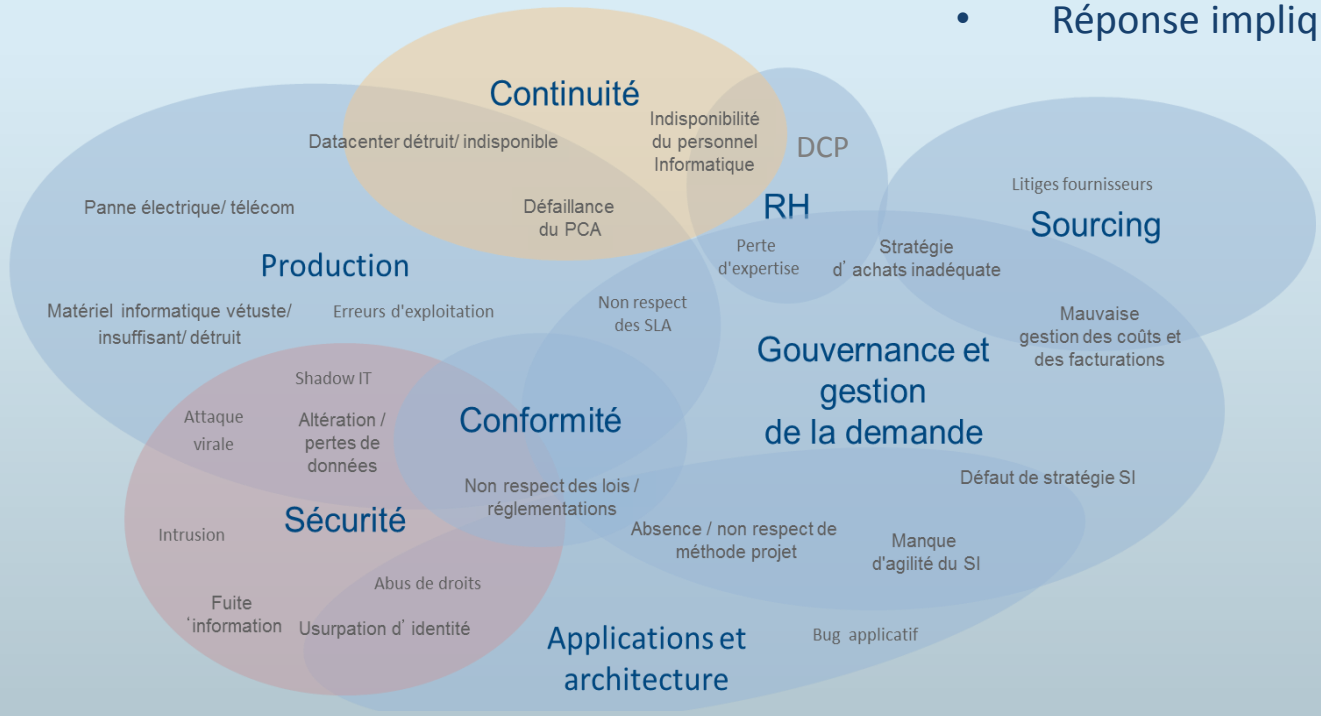
Prendre la mesure du risque

On passe d'un risque technique …

- Risque centré sur les activités transverses ou de support
- Enjeux de disponibilité, intégrité, confidentialité

… vers un risque d'entreprise

- Risque centré sur les activités métier
- Enjeux financiers, juridiques, d'image et de confiance
- Risque non externalisable
- Réponse implique et mobilise l'ensemble de l'organisation

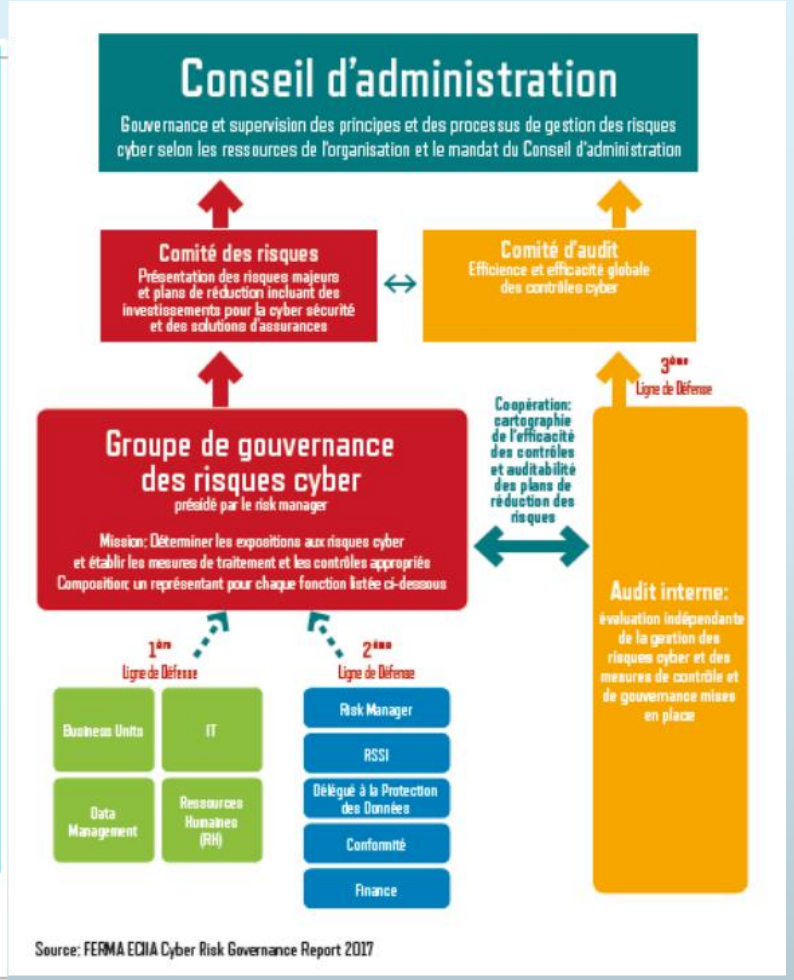


Comprendre et s'organiser

ECIIA – European Confederation of Institutes of Internal Auditing

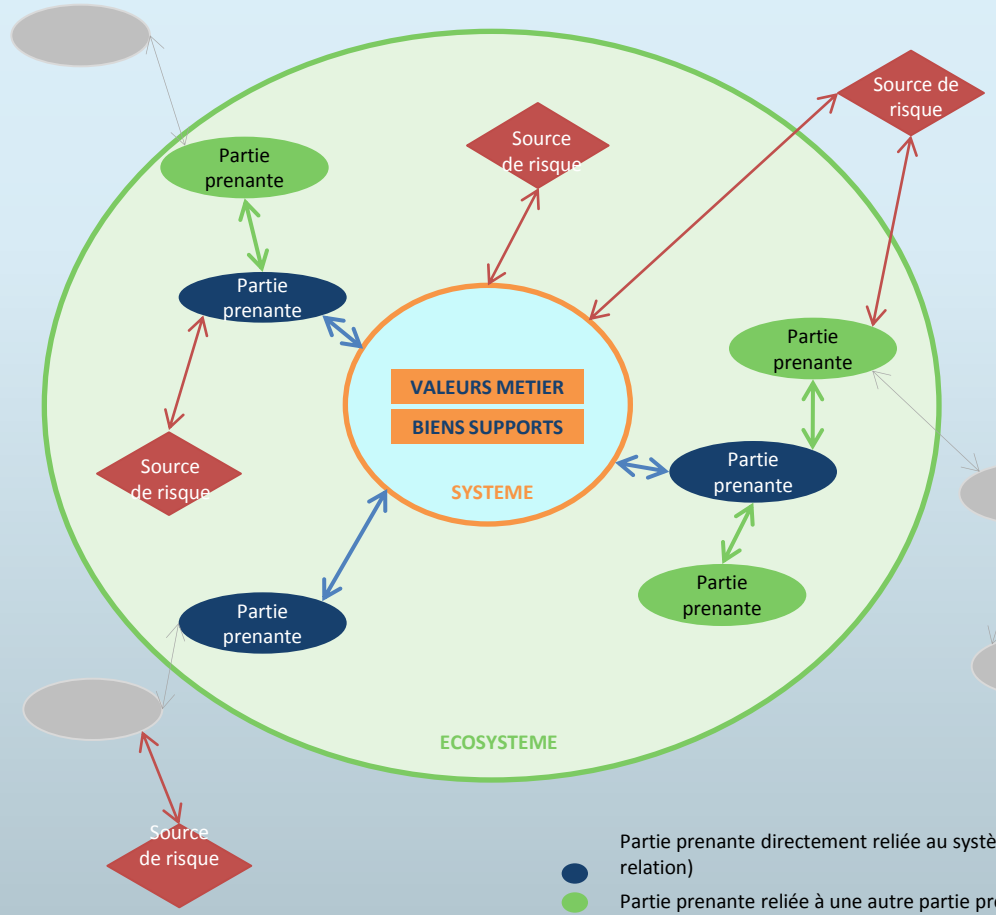
FERMA – Federation of European Risk Management Associations

European Commission
Directorate General for Communications Networks, Content & Technology (DG CONNECT)



Source: FERMA ECIIA Cyber Risk Governance Report 2017

Maîtriser son écosystème numérique



Pour chaque partie prenante, évaluer 4 critères :

EXPOSITION

Dépendance
La relation avec cette partie prenante est-elle vitale pour mon activité ?

Pénétration
Dans quelle mesure la partie prenante accède-t-elle à mes ressources internes ?

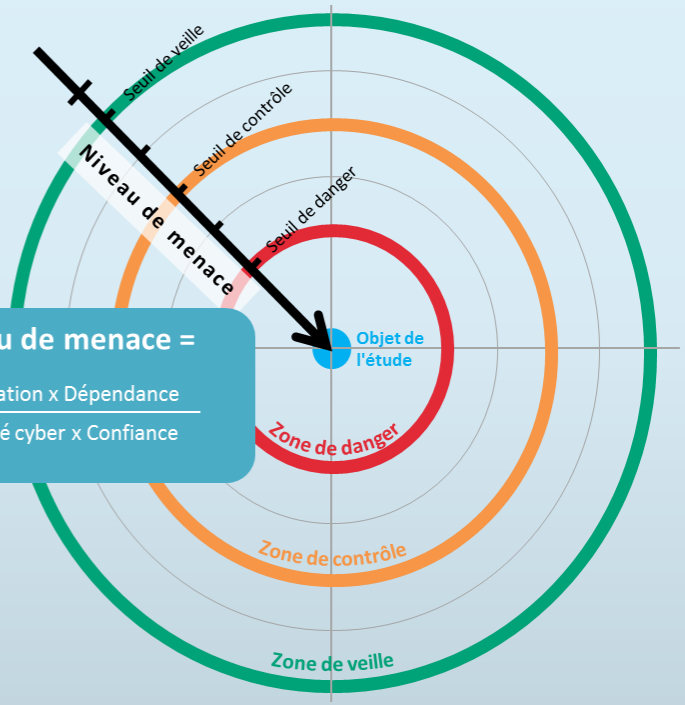
FIABILITE CYBER

Maturité cyber
Quelles sont les capacités de la partie prenante en matière de sécurité ?

Confiance
Est-ce que les intentions ou les intérêts de la partie prenante peuvent m'être contraires ?

Niveau de menace =

$$\frac{\text{Pénétration x Dépendance}}{\text{Maturité cyber x Confiance}}$$

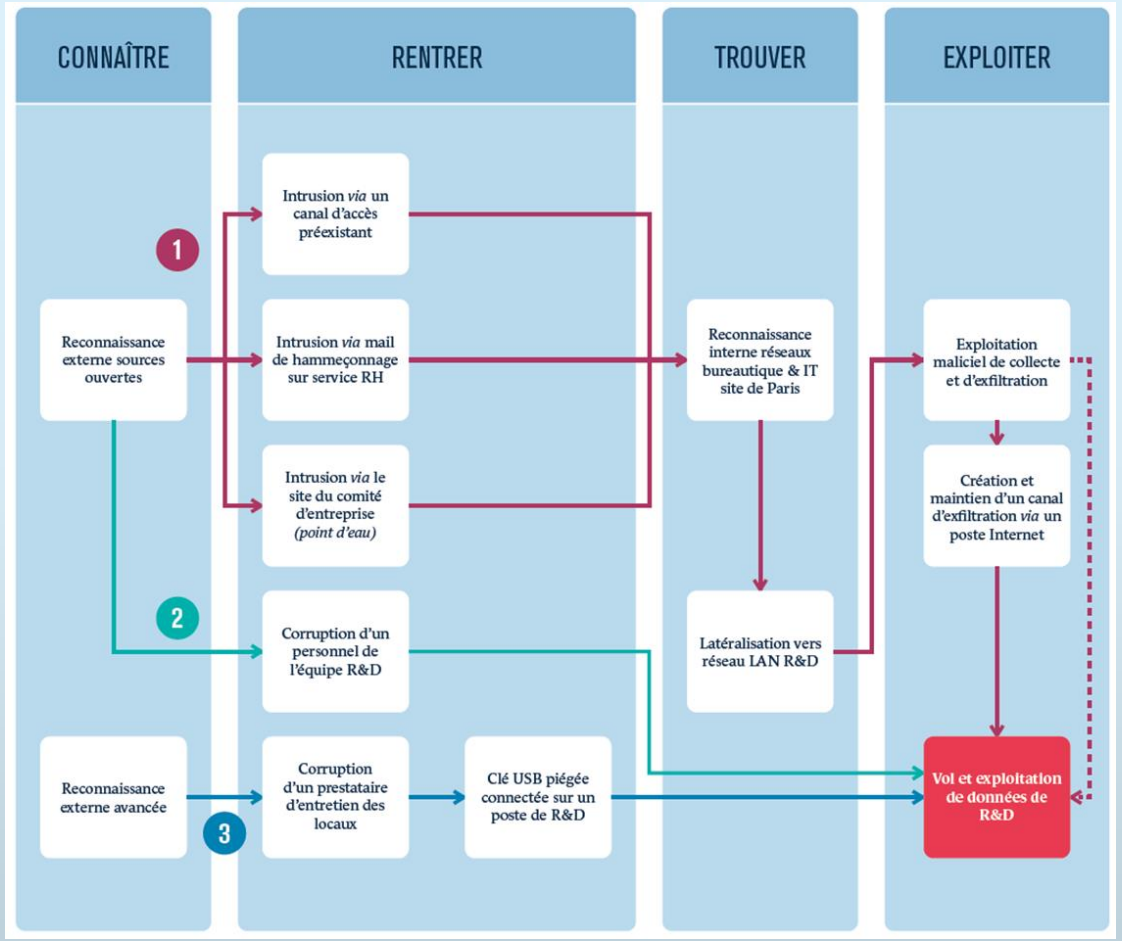


- Partie prenante directement reliée au système (1er niveau de relation)
- Partie prenante reliée à une autre partie prenante (2e niveau de relation)

Identifier les pires scenarios

Identification des Scenarios

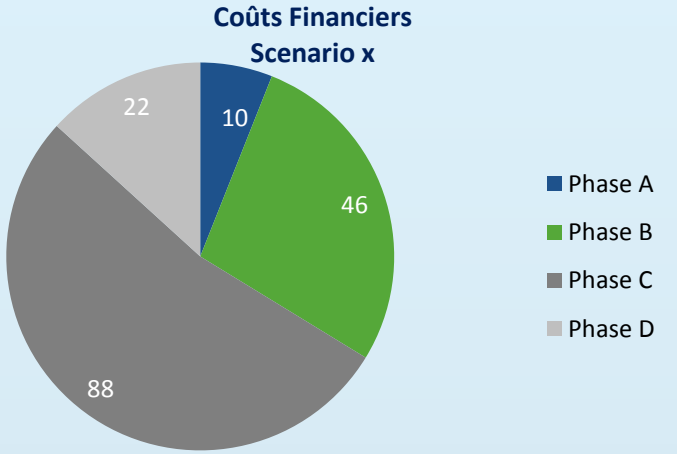
- Focus sur les scenarios catastrophiques
- Bien identifier les hypotheses sous jacentes

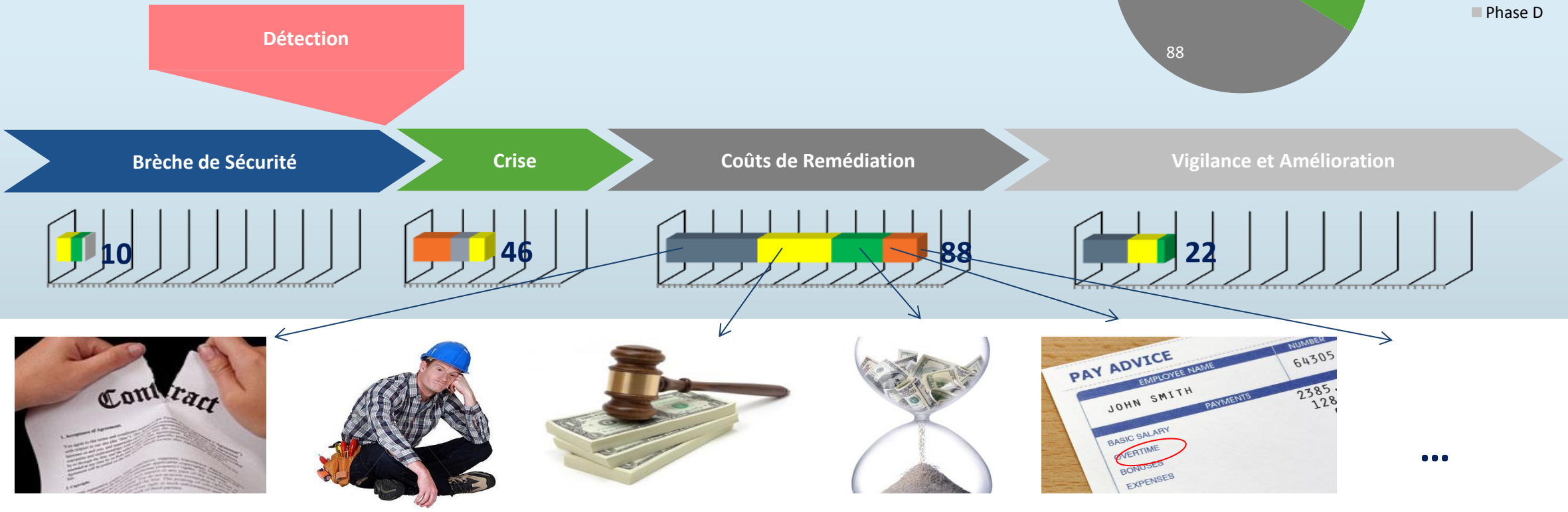


Quantification Financière

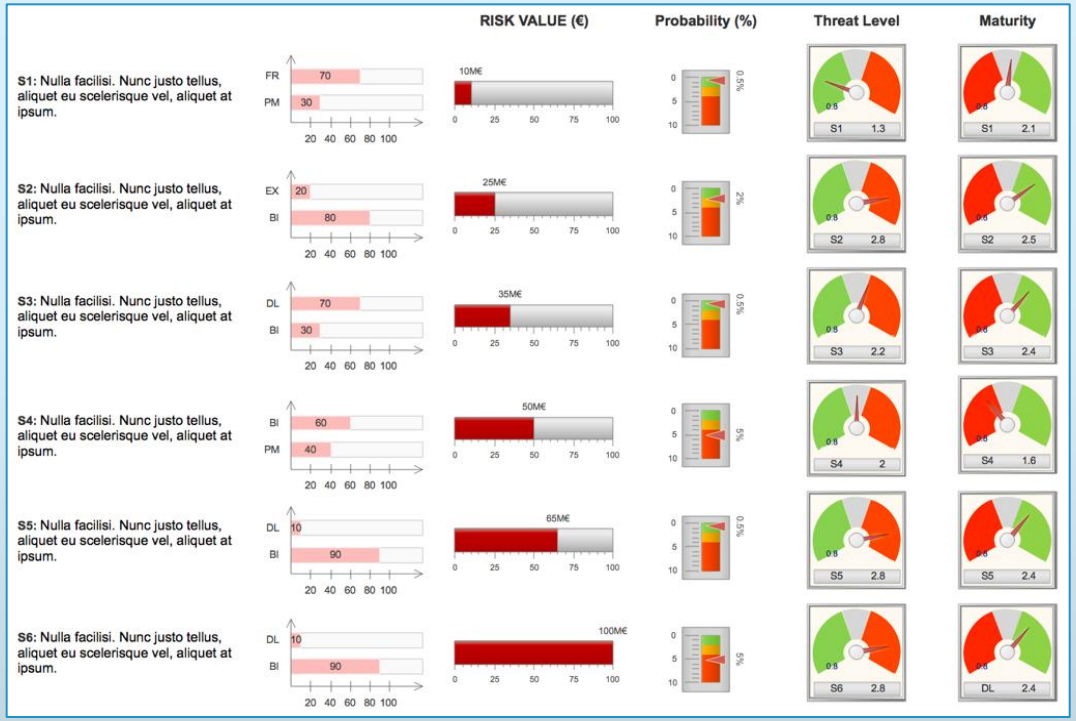
Quantification financière des scenario

- **Séparer les scenarios** en différentes phases
- **Simplifier la liste** des fonctions impactées
- **Adresser les coûts** affectés à chaque phase





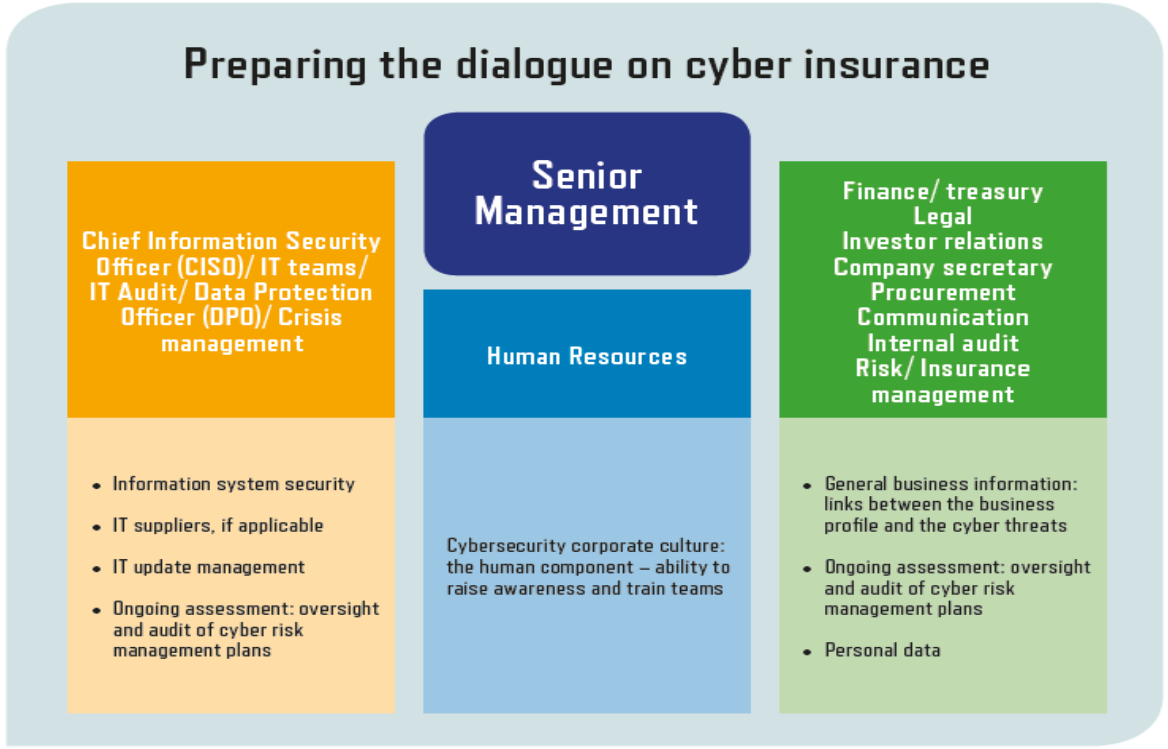
Définir une stratégie de sécurité

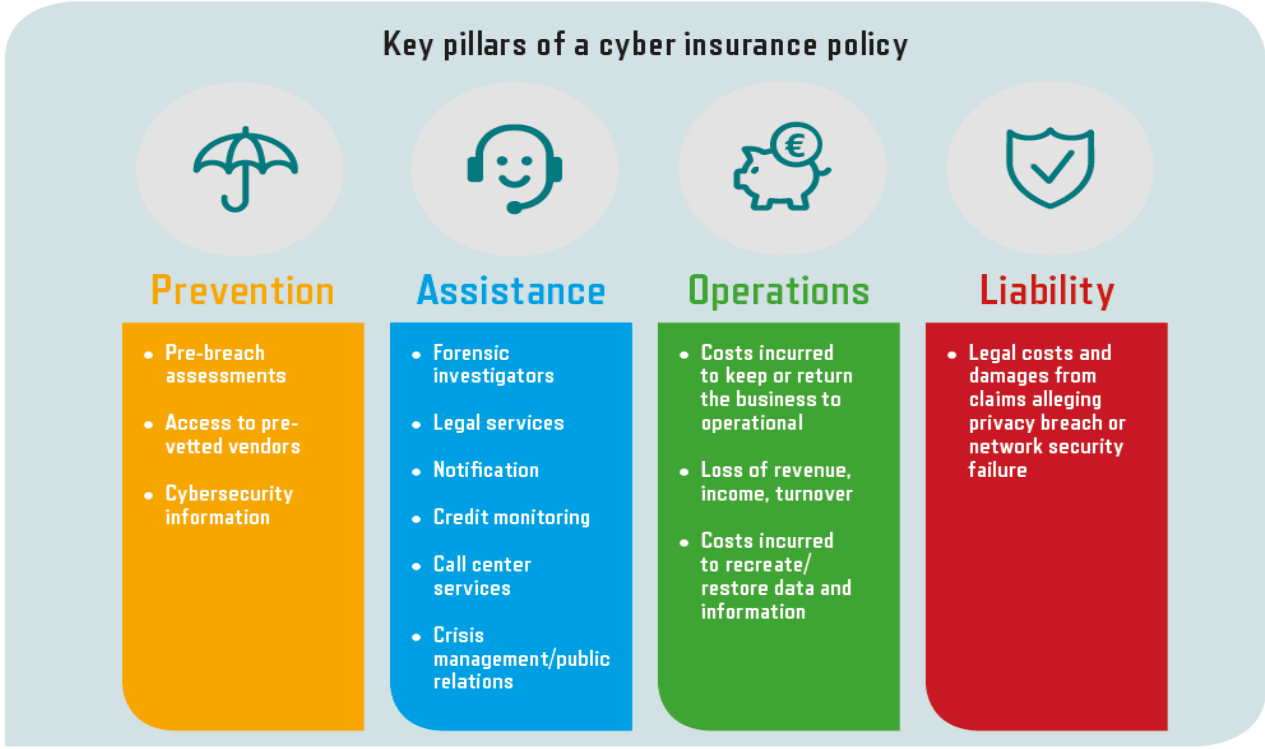


Cyber risks, a view from the industry - Ferma Forum 2015 - Cyber risks workshop

Mesure de sécurité		Scénarios de risque	Responsable	Complexité	Coût estimé	Echéance	Priorité
Nature	Mesure						
Facteur humain	Sensibilisation renforcée aux méthodes d'hameçonnage	R3 / R4	Responsable sécurité	+	€5k	3 mois	P3
Protection des données	Protection renforcée des données de fabrication et de livraison sur le SI (pistes : chiffrement, cloisonnement)	R1 / R5	Responsable informatique	++	€15k	3 mois	P1
Résilience	Plan de continuité d'activité avec un partenaire / sous-traitant	R2	Responsable opérationnel	+++	€30k	1 mois	P2
Résilience	Contrat d'assurance cyber / responsabilité civile	R1 / R2 / R3 / R4 / R5	Responsable financier	++	€5k / an	1 mois	P1

Definir sa couverture d'assurance





Quelques règles simples:
-connaitre son besoin
-l'exprimer clairement avec l'aide de son courtier
-avoir un dialogue de qualité avec son assureur

L'humain au centre du jeu

FORMATION

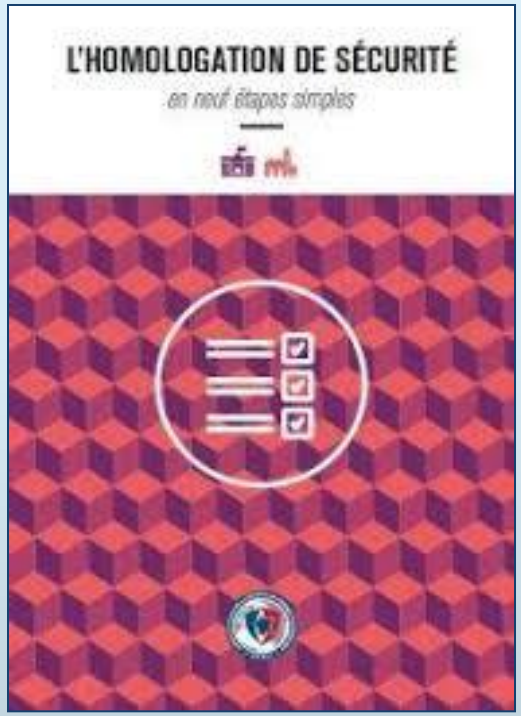
SENSIBILISATION

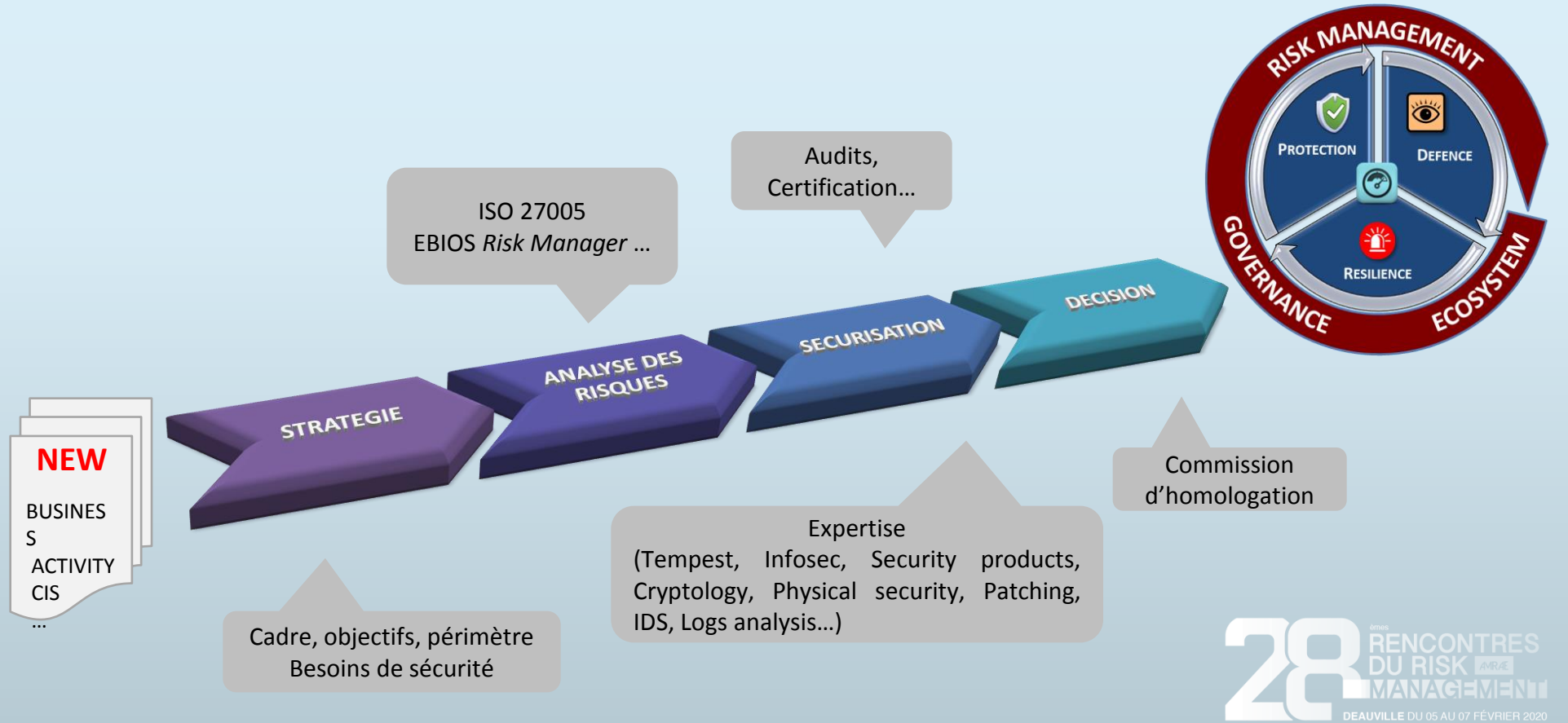
ENTRAINEMENT

SecNumacadémie.gouv.fr
Formez-vous à la sécurité du numérique

Resilience FRANCE
HAUT COMITÉ FRANÇAIS POUR LA RESILIENCE NATIONALE

L'homologation de sécurité





Bâtir une sécurité en profondeur

*Se **protéger** contre les attaques en rendant le SI et son écosystème les moins vulnérables et exposés possibles*

1990

PROTECTION

GOUVERNANCE

DÉFENSE

***Détecter** les signaux faibles ou une attaque avérée et **répondre** pour en minimiser les impacts*

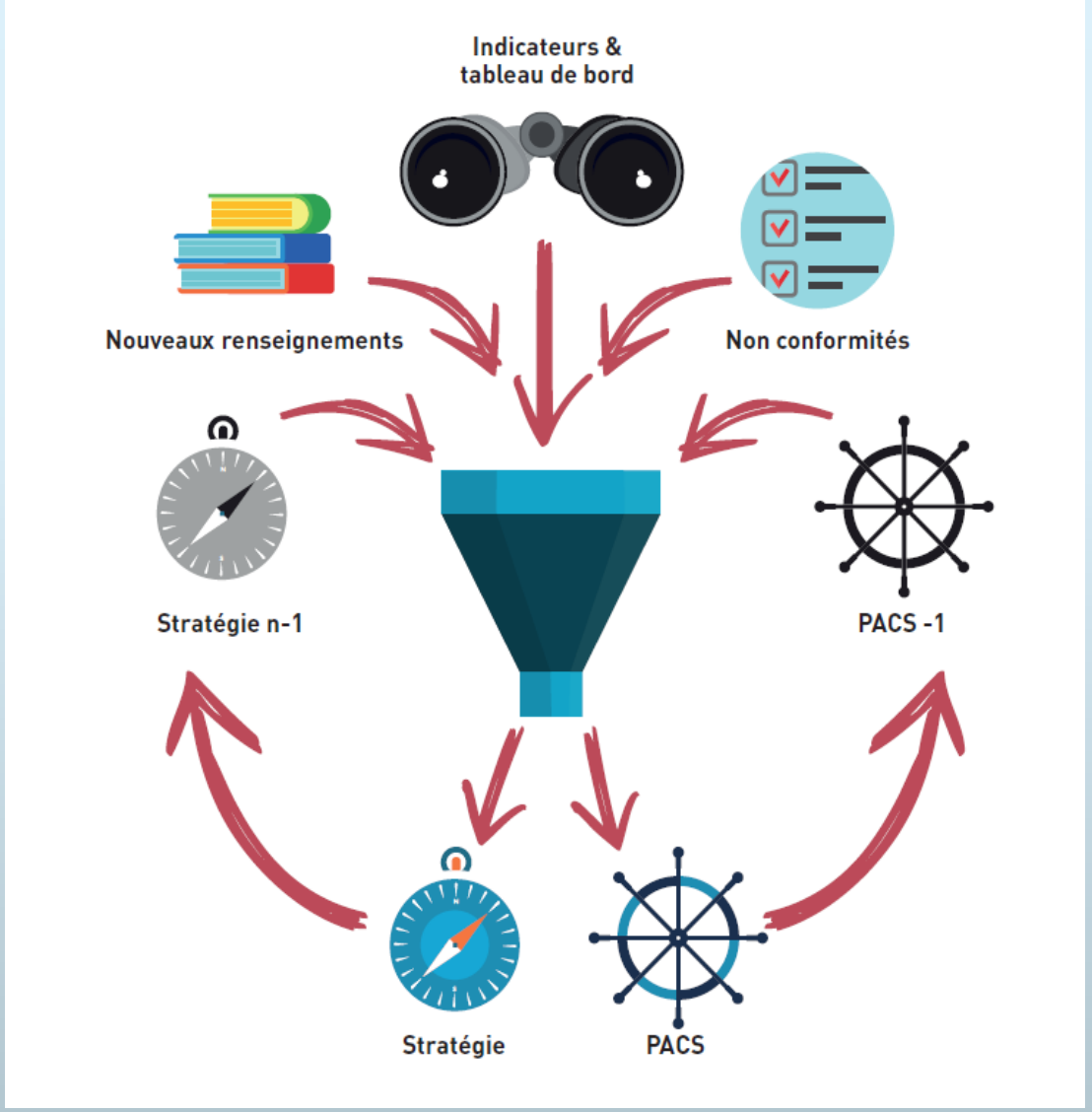
2000
2015

***Anticiper**, suivre le niveau de sécurité et **renforcer** en continu le dispositif*

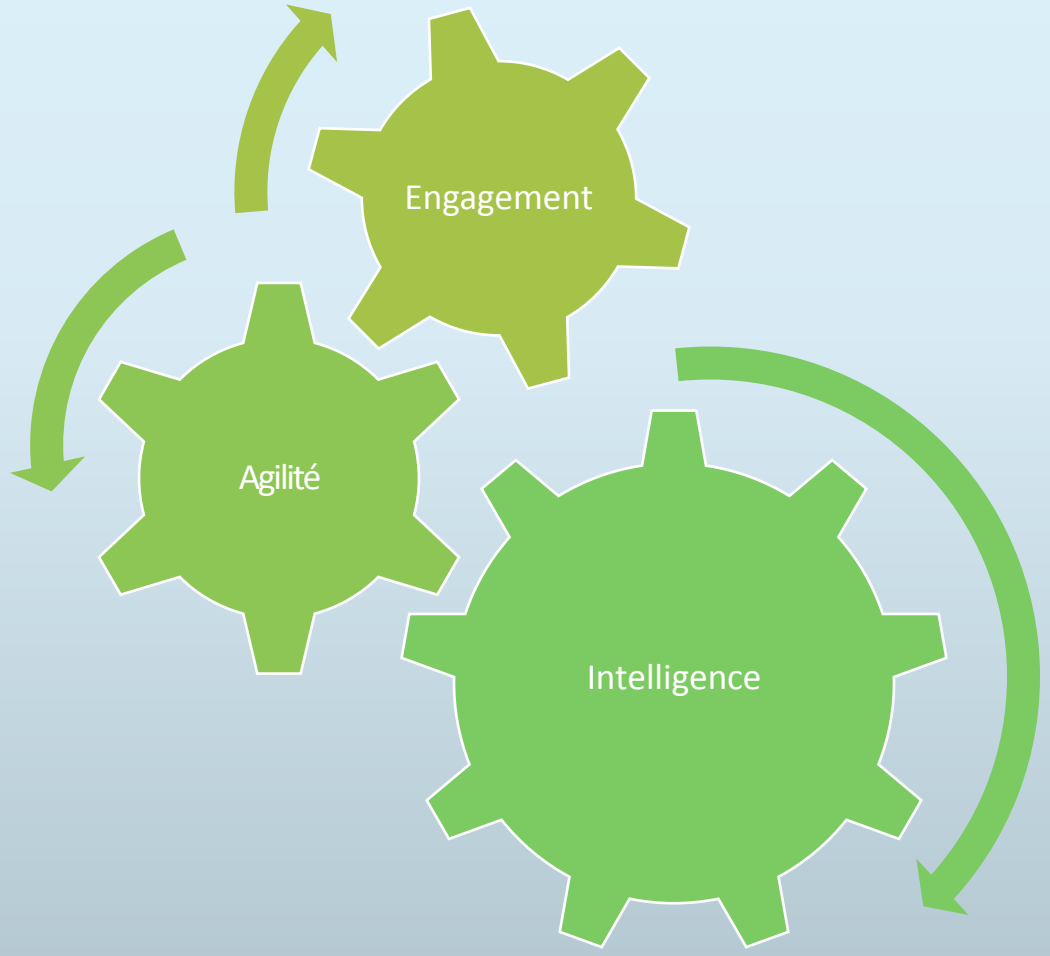
RÉSILIENCE
2020

*Assurer la **continuité** d'activité avec un niveau de dégradation tolérable, puis la **reprise** nominale progressive*

Amélioration continue

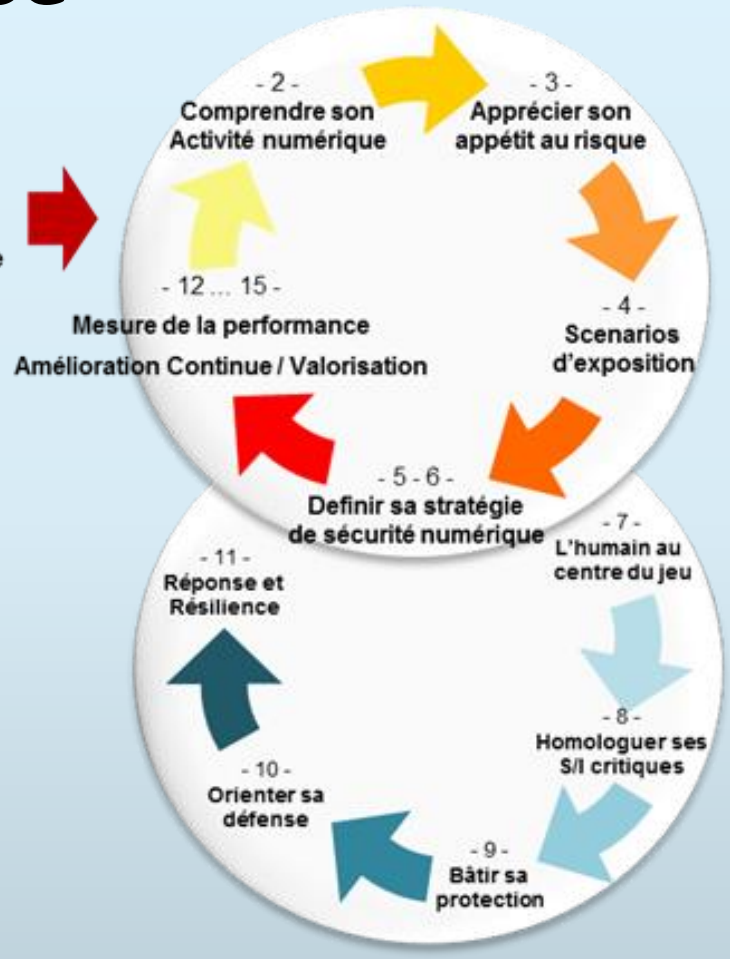


Piloter la performance



Comité des risques

-1 –
-Mise en place
-d'une gouvernance



Valoriser la démarche

Maîtrise du risque numérique

Investissements de sécurité

… approche *Cyber Business Partner*

D'un centre de coût ….

… à un avantage concurrentiel

Vers une réference internationale

Rencontres du Risk Management AMRAE 2020

Les étapes clés pour construire une politique de gestion des risques numériques (B8)

ACCÉLÉRATEUR D'ÉCHANGES

Expert en
Cargo Community System
depuis 35 ans

Une plateforme numérique internationale qui facilite et accélère les échanges d'informations sur la marchandise entre les acteurs du commerce international via des systèmes d'information intelligents

28èmes RENCONTRES DU RISK MANAGEMENT AMRAE
DEAUVILLE DU 05 AU 07 FÉVRIER 2020

EXPERIENCE

NOTRE MISSION

Créer un Port Community System destiné à gérer le passage portuaire de la marchandise

35 ans d'expérience dans les CARGO COMMUNITY SYSTEMS

Expert en projet R&D

- Blockchain
- Intelligence Artificielle
- RFID
- C-ITS
- Géolocalisation
- Code Barre

13 COMMUNAUTES PORTUAIRE EN FRANCE ET EN DOM-TOM

environ **4000** utilisateurs

1989

Système PROTIS

2005

AP+

2011

AirPort+

2018

Ci5

28èmes RENCONTRES DU RISK MANAGEMENT AMRAE

DEAUVILLE DU 05 AU 07 FÉVRIER 2020

15 METIERS CONNECTES

DE L'INFORMATIQUE AU NUMÉRIQUE

2015

Nouvelle gouvernance avec forte volonté de changement

Lancement de Ci5 et de ses nouvelles technologies :
blockchain, l'intelligence, artificielle , la gestion en mode SaaS, hébergement dans le cloud...

Nouveaux risques

Nouvelles menaces

Améliorer la sécurité, disponibilité et l'intégrité des données de nos clients

ISO 27001

L'ISO 27001

2016

Lancement de la certification ISO 27001 avec l'AFNOR

Nouvelle **organisation** avec la Création d'un service Qualité Sécurité et un **renforcement** de nos pôles **innovation, exploitation et édition**

Création du Système de Management Sécurité de l'information

Sensibilisation interne importante sur les bonnes pratiques, quizz, questionnaire

Réalisation **d'audits techniques** sur nos produits et **audit interne** par des experts ISO 27001

Veilles réglementaires sécurité, Innovation, transport

Partenariat d'excellence en matière de sécurité de l'information

L'évaluation et la gestion des risques de sécurité de l'information sont au cœur de la norme ISO 27001.

L' ANALYSE DE RISQUES :

Cinq étapes simples vers une évaluation des risques ISO 27001 efficace

- Valider un cadre de gestion des risques
- Identifier les risques
- Analyser les risques
- Evaluer les risques

MGI a utilisé la méthode EBIOS, méthode d'analyse de risque française de référence, qui nous a permis de réaliser une appréciation et un traitement des risques en fonction des contextes internes, externes, menaces et des critères ci-dessous :

Vraisemblance/ Gravité	1	2	3	4
1	acceptable	acceptable	acceptable	à maîtriser
2	acceptable	à maîtriser	à maîtriser	à maîtriser
3	à maîtriser	à maîtriser	à maîtriser	inacceptable
4	à maîtriser	inacceptable	inacceptable	inacceptable

COÛTS OU INVESTISSEMENTS

En France, la facture d'une cyberattaque s'élève en moyenne à **8, 6 millions d'euros**.

Une forte sensibilisation en interne pour éviter les virus malveillants de type ranconware ou intrusion physique

Un arbitrage délicat

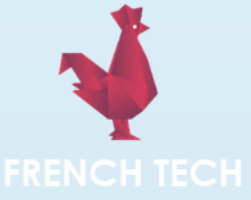
MGI a décidé de créer une organisation Qualité Sécurité avec le recrutement entre autre d'un chef de projet Qualité Sécurité également DPO qui pilote le SMSI et l'amélioration continue

Mise en place d'outils qui renforcent la robustesse des systèmes MGI : Anti spam et virus, gestion documentaire dans le cloud, vidéosurveillance dans les locaux, alarmes....

Réalisation d'audits d'intrusion dans nos systèmes

LA SÉCURITÉ N'A PAS DE PRIX !

Partenariats MGI



MGI VOUS ACCOMPAGNE VERS LE PORT VERT DU FUTUR

CONTACTS

Fabrine FRESTEL

f.frestel@gyptis.fr +33 04 91 14 12 30

Rencontres du Risk Management AMRAE 2020

Les étapes clés pour construire une politique de gestion des risques numériques (B8)

Agenda

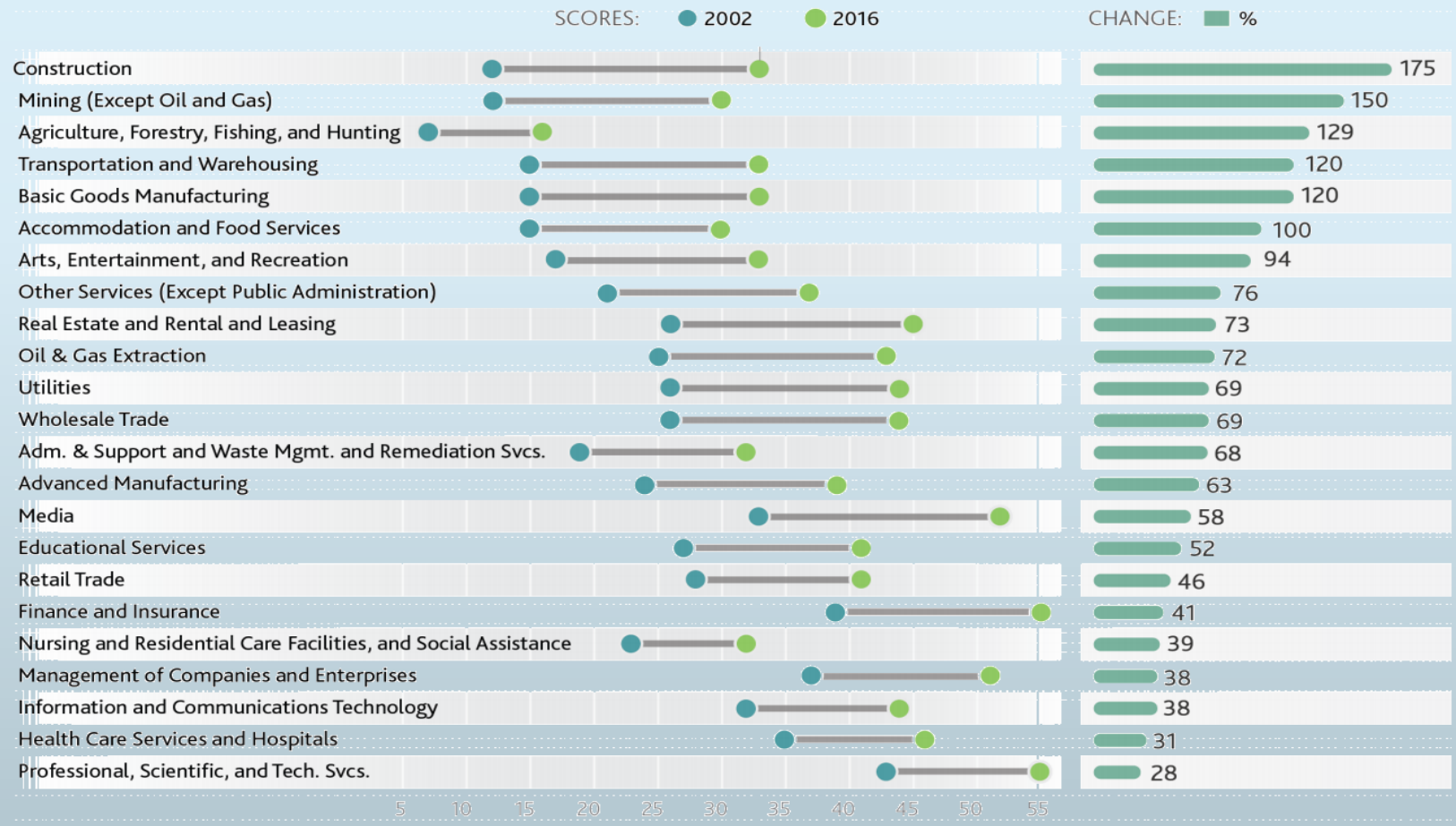
1. How Moody's assesses cyber risk
2. Our 2020 scenario
3. Some concrete examples

1. How Moody’s assesses cyber risk

Cyber risk is rising

Digitization, greater intersection of supply chains, connectivity and access to data are creating new vulnerabilities

Sector mean digitization scores and percent change, 2002 and 2016



Moody’s objectives

Two strategic pillars: capacity building in the rating agency and formation of an assessments group.

Build Cyber Expertise in Credit

Deepen Moody’s cyber risk capabilities and profile:

- Create a **framework** to incorporate cyber security risk into our credit risk analysis,
- Develop cyber **data sets, analysis and reports** that can be efficiently used in the MIS analytical process when considering the impact of cyber on credit ratings
- Develop and execute a robust, **data driven research agenda**
- Build Moody’s **brand recognition** around cyber through research, publishing, outreach and partnerships that will enhance our capabilities

Comprehensive Assessment

Create a new cyber risk product offering with cybersecurity company Team8 to assess how vulnerable businesses are to cyber attacks.

Moody’s cyber framework

A relative assessment which started at the sector level

1. **Two dimensions: vulnerability and impact**
2. **Relative assessment under a five-point scale**
3. **Assessment at the sector level**
4. **Only sector-wide mitigants considered**

Moody’s cyber risk framework

We have considered seven different factors

RISK FACTORS

Vulnerability

- Business size and profile
- Sensitivity of collected data
- Services and essential products

Impact

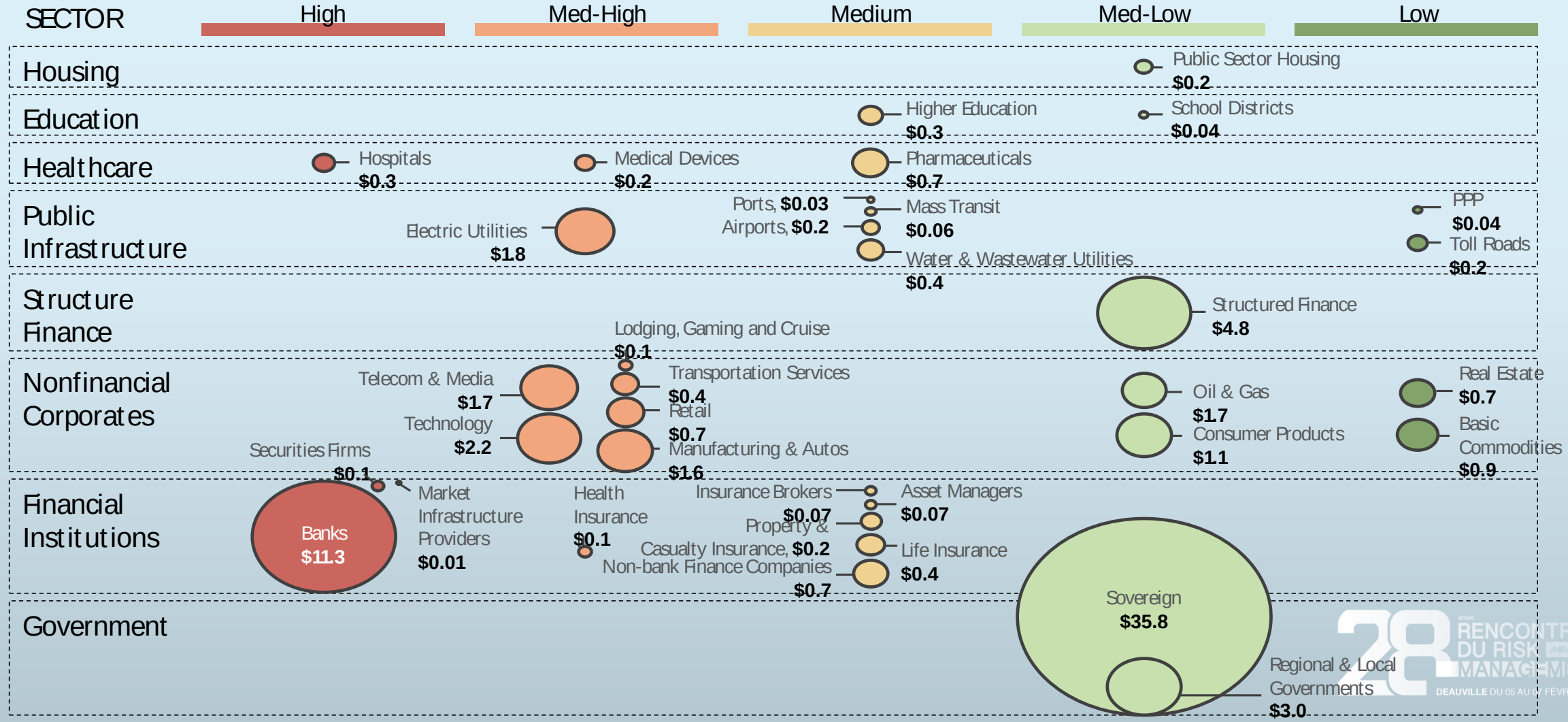
- Brand impact
- Legal regulations and consequences
- Manage crisis and recover
- Financial impact

RISK LEVELS

- High
- Med-High
- Medium
- Med-Low
- Low

Moody’s cyber risk framework

Cyber risk levels and Moody's-rated debt



Attacks are underreported

- Although reporting frameworks for cyber risk events have improved in recent years, they continue to focus on data disclosure, often with a focus on privacy
  - General Data Protection Regulation
  - NY SHIELD Act
  - California Consumer Privacy Act
- Attacks that cause disruption are underreported, with only the largest attacks becoming public through media coverage vs. disclosure rules
  - Securities and Exchange Commission's 2018 Guidance on cybersecurity disclosures adopted more prescriptive language to encourage more consistent and timely disclosures of cyber events.

Cyber risk management disclosures vary across sector

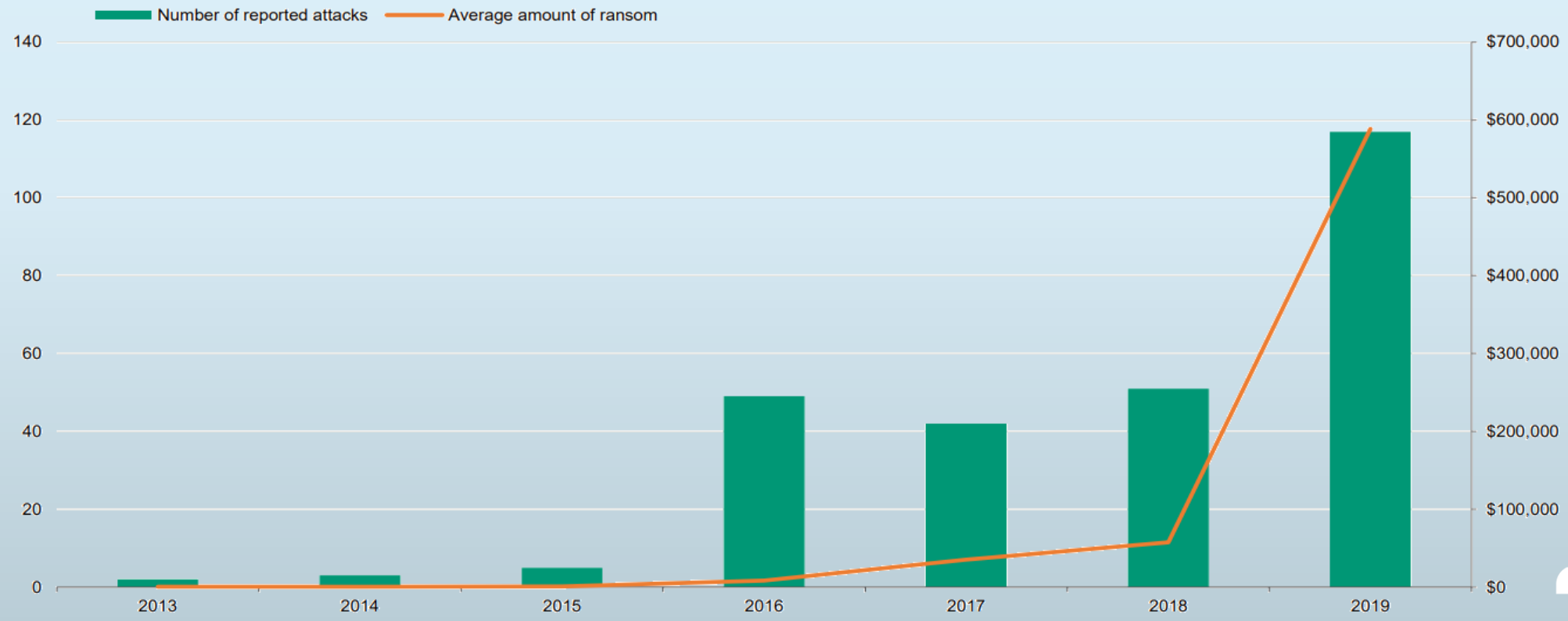
	Risk Discussion		Risk Oversight			Risk Management			
Sector	Total # of Issuers	Management Discussion & Analysis	Board Committee	Director Qualifications	CISO interaction with Board	Cyber Insurance	Detailed Risk Mitigation Strategy	Global Cyber Strategy	# of Above Average Subcategories
Banks	10	10	7	5	5	3	5	5	7
Telecommunications & Media	10	10	4	3	3	5	5	2	6
Securities Firms and Market Infrastructure Providers	18	17	9	7	2	8	9	4	5
Electric Utilities	10	8	3	6	2	4	3	3	5
Lodging, Gaming & Cruise	10	10	7	2	0	7	1	0	3
Retail	10	7	7	3	2	1	0	0	3
Technology	10	8	6	3	2	1	2	0	3
Health Insurance	7	7	6	2	0	0	0	0	2
Medical Devices	10	9	5	1	2	1	1	1	2
Hospitals and Healthcare Providers	10	10	4	1	0	2	1	1	1
Manufacturing & Auto	10	7	3	2	0	1	3	0	1
Transportation Services	10	8	6	2	0	1	2	1	1

2. 2020 Scenario

Ransomware

Ransomware attacks picked up speed in 2019 and will continue to gain pace in 2020

Ransomware attacks against US regional and local governments, 2013 to 2019



Data privacy regulations

The introduction of data privacy laws in a number of large jurisdictions raises the likelihood of more frequent and higher fines in 2020

Top 10 data breach fines and settlements globally

National security

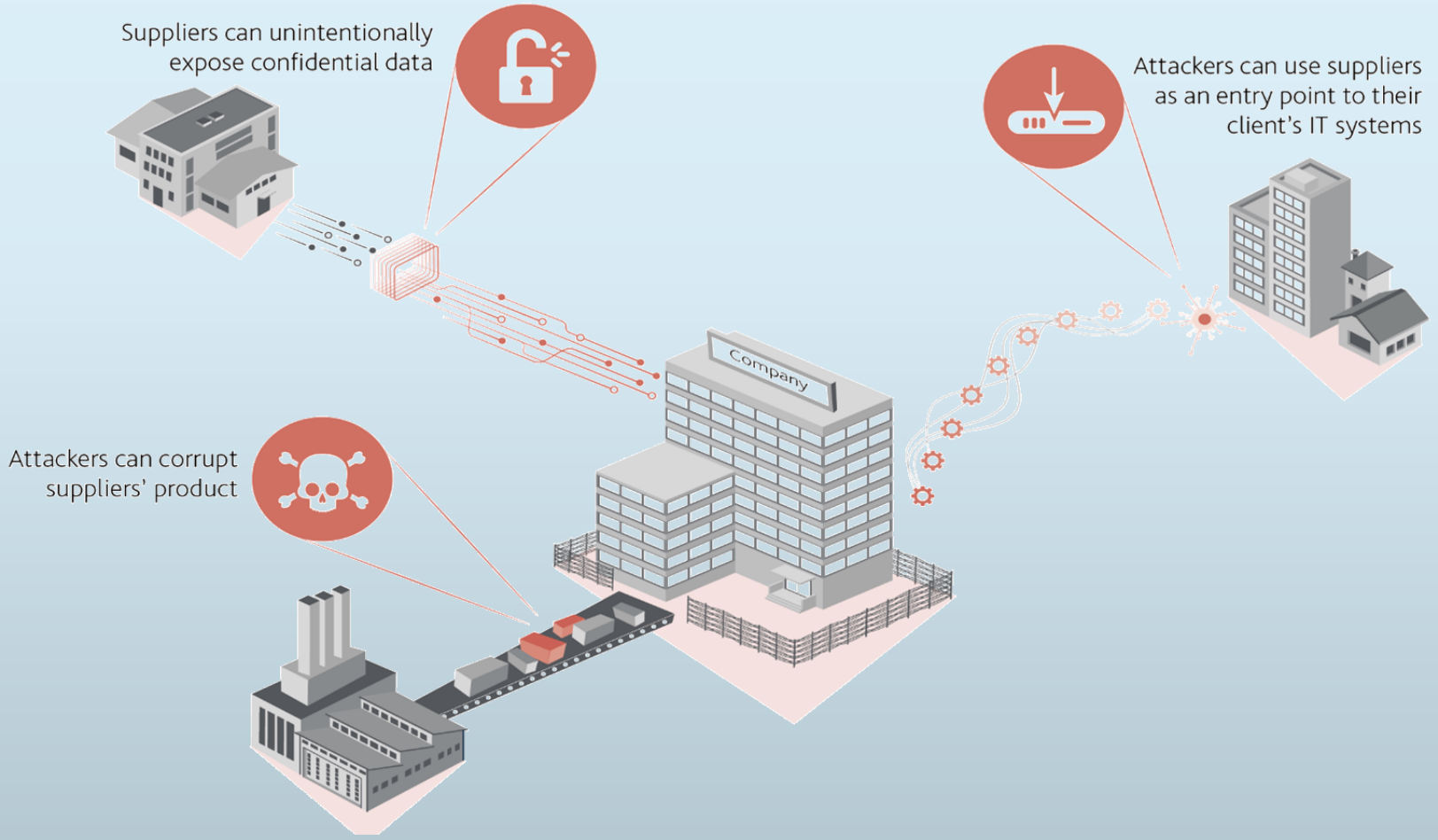
Government punitive actions against foreign firms will pressure revenue

Foreign technology companies are increasingly coming under scrutiny from government authorities

Supply chain

Risks from vendors and software supply chain exposure will continue

Compromised suppliers can affect customers in many ways



3. Some examples

Travelex

Cyberattack disrupts online business, forces manual operations, a credit negative

- Travelex was hit by the ransomware Sodinokibi in January 2020. As a result, it chose to shut down its the website and apps. A large share of its operations had to operate manually.

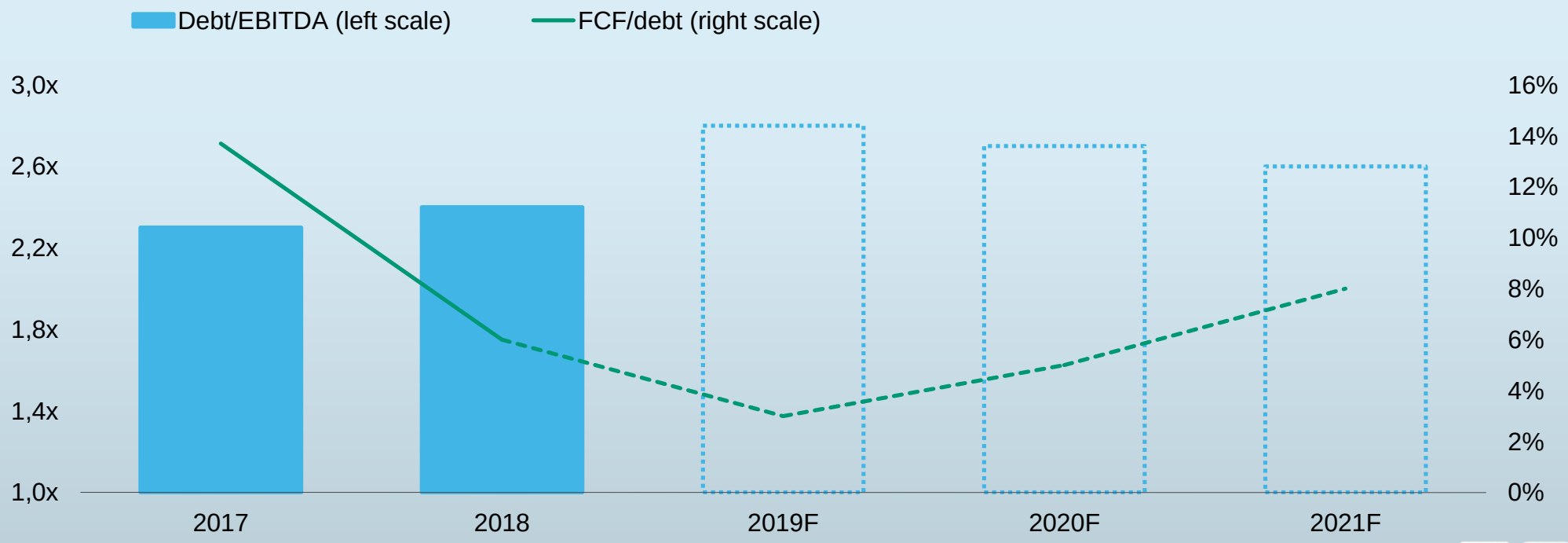
- The attack will reduce revenue and margins, a credit negative. Assessing the ultimate credit impact will depend on total remediation costs, insurance benefits and effects on consumers' confidence.

- No rating action taken yet in light of Travelex's low rating (B3 negative) and history of shareholder support. Also, the financial cost of the attack is still unknown.

Equifax

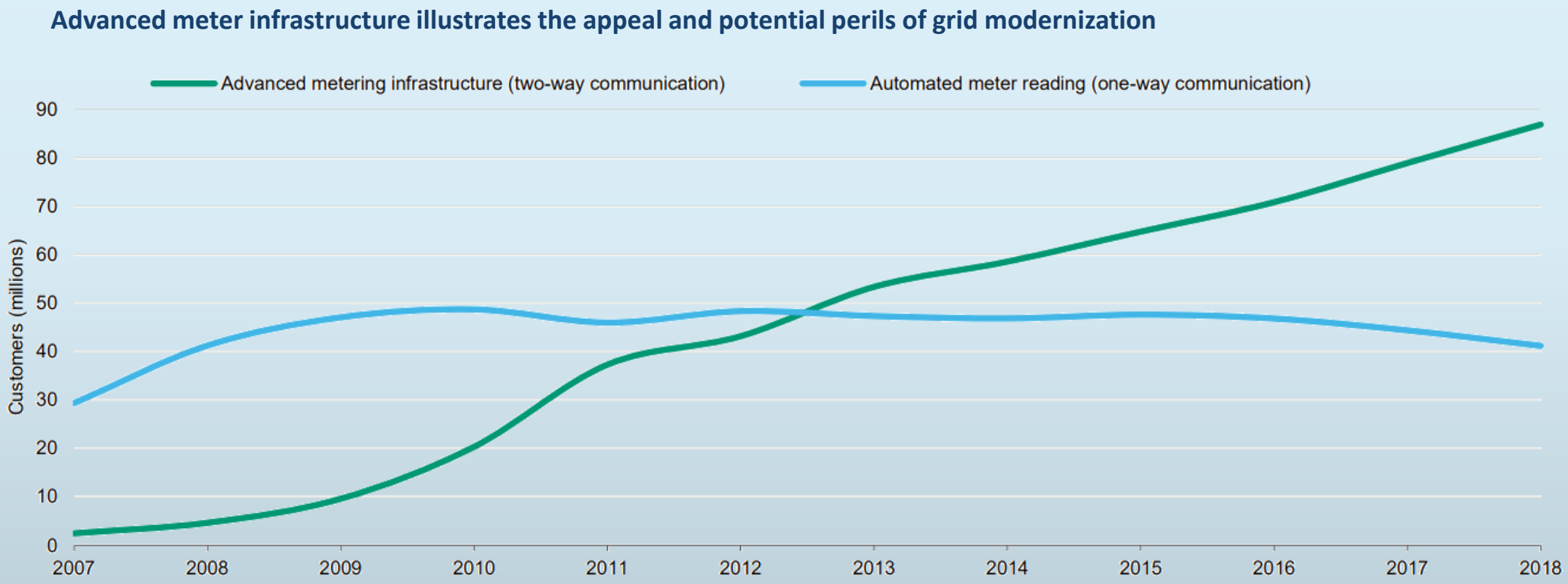
Cybersecurity investments, lagging operating performance and debt-funded M&A to weigh on metrics

Equifax's Moody's-adjusted credit ratios



Utilities

Grid modernization heightens vulnerability of US utilities to cyberattacks



Hospitals & health service providers

Cyberattacks pose growing operational and financial risks for hospitals

Hospitals are exposed to various types of cybersecurity threats

Threat	Potential impact of attack
E-mail phishing attack	Malware delivery or credential attacks. Both attacks further compromise the organization.
Ransomware attack	Assets locked and held for monetary ransom (extortion). May result in the permanent loss of patient records.
Loss or theft of equipment or data	Breach of sensitive information. May lead to patient identity theft.
Accidental or intentional data loss	Removal of data from the organization (intentionally or unintentionally). May lead to a breach of sensitive information.
Attacks against connected medical devices that may affect patient safety	Undermined patient safety, treatment, and well-being.

Banks

Global investment banks heighten readiness against constant cyber threat

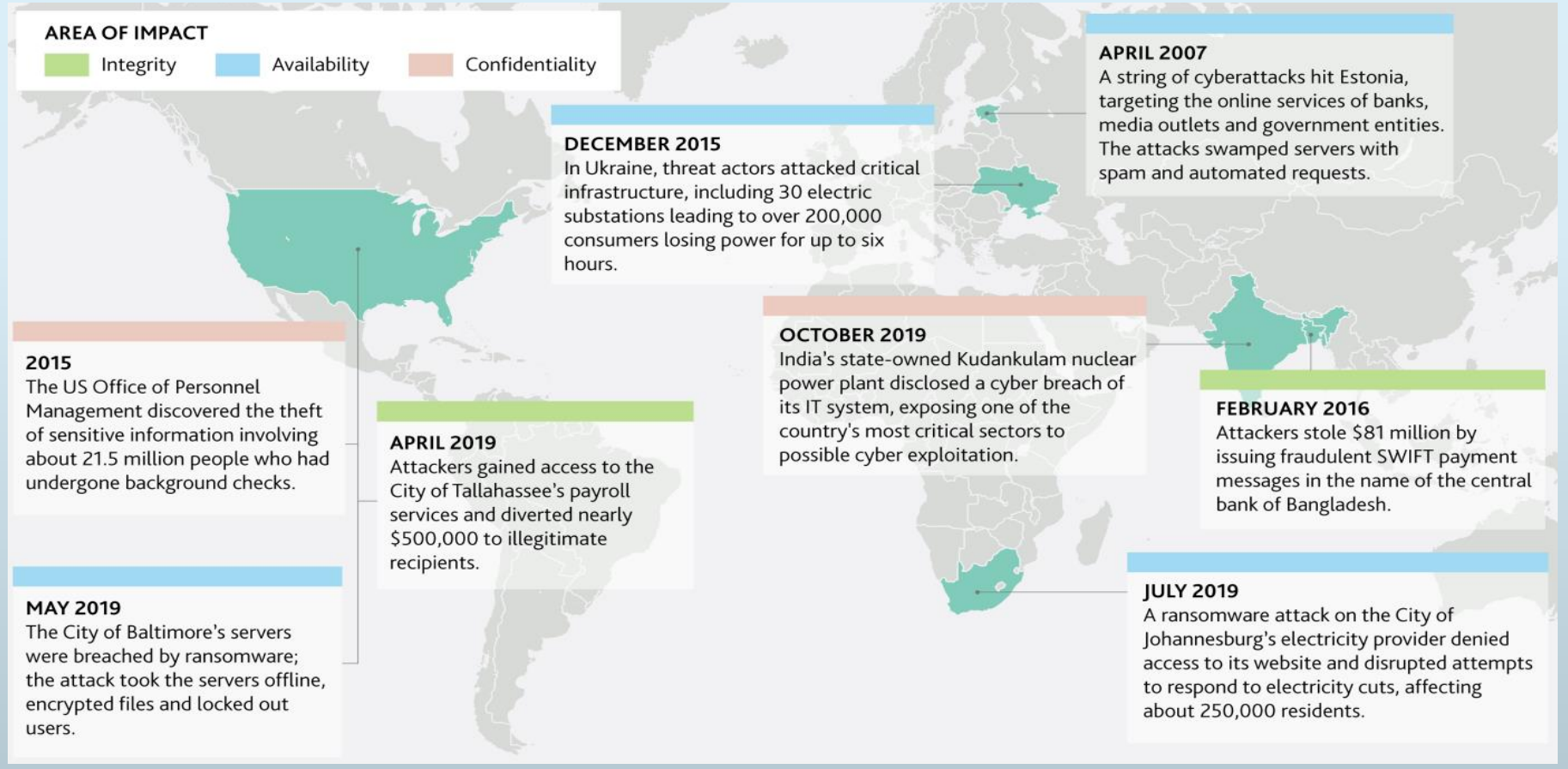
Assessment of cyber risk impact: an example for a global investment bank

	Moderate	High	Very High
Disruption of critical processes			
- Systems interrupted	One system	Multiple systems	Numerous systems
- Length of interruption	Temporarily	Less than one day	More than one day
- Customer defections	None	Some franchise clients	Large franchise clients
- Monetary loss	$ ten millions	> $100 million	> $500 million / $1 billion
Client data			
- Data loss / corruption	None	Temporary	Sustained
- Data exposed to third party	None	Temporary	Sustained
Reputational effects			
- Negative media coverage	Local	National / International	Global and persistent
- Legal actions	Potential	Modest scale	Prolonged, large scale
- Regulatory response	Regulatory findings	Regulatory actions	Loss of licences

Governments

Cyberattacks on governments are rising but pose limited risks to credit quality

Overview of recent attacks



Governments

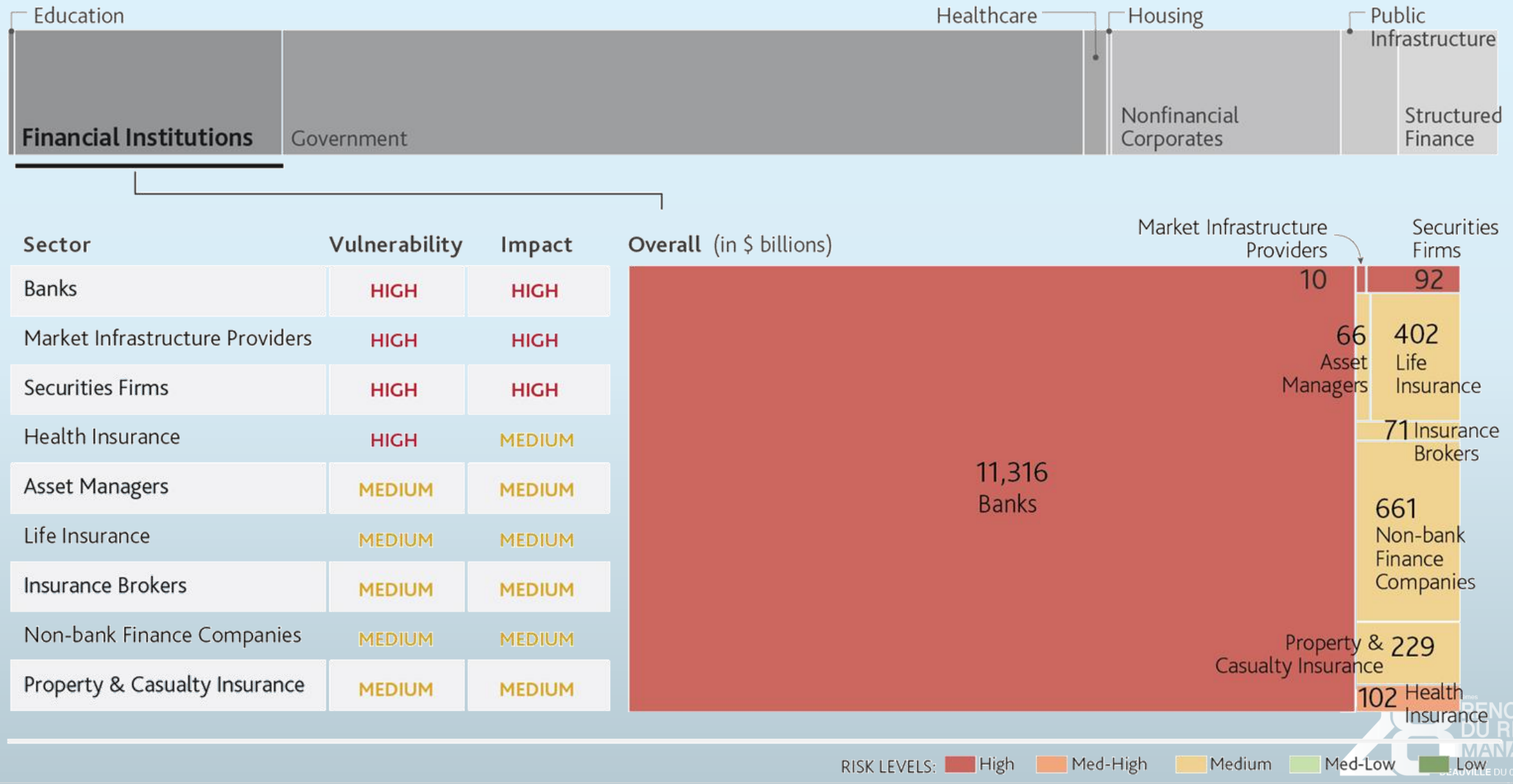
Cyberattacks on governments are rising but pose limited risks to credit quality

Channels through which a hypothetical cyber event could weaken government credit profiles

Ratings Methodology Factor Scores				
Sovereign	*Regional & Local Governments (RLGs)*		Hypothetical cyber event	Credit impact
Economic strength	*Economic fundamentals*		An attack on critical infrastructure could disrupt economic activity, or an attack could be perpetrated on a smaller, less diverse government that relies on a single industry as a source of growth.	Economic growth could slow significantly and economic strength could be impaired.
Institutions & governance strength	*Governance & management*		A cyberattack could expose sensitive information that reveals institutional arrangements that are weaker than previously thought.	Our assessment of institutional effectiveness and quality of governance could decline materially.
Fiscal strength	*Financial performance & debt portfolio*		While rare, fiscal costs associated with a cyberattack could be so large that they result in weaker overall fiscal strength for sovereigns, or weaker financial performance and debt profiles for RLGs.	Financial resources and fiscal strength could decline.
Susceptibility to event risk (Political risk)	*NA*		A cyberattack could attempt to disrupt domestic or geopolitics, including through direct or indirect election interference.	Political risk could rise.

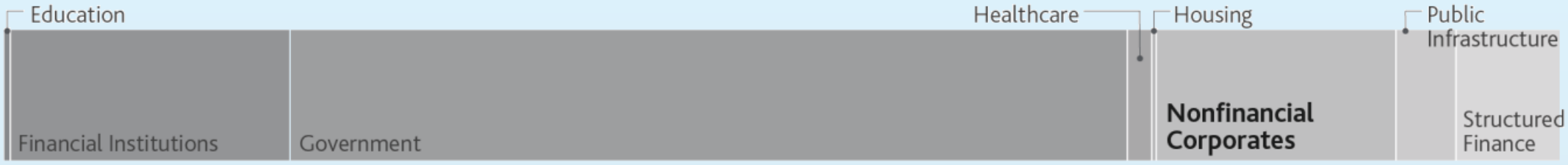
4. Appendices

Financial institutions are highly exposed to cyber risk



Sector	Vulnerability	Impact
Banks	HIGH	HIGH
Market Infrastructure Providers	HIGH	HIGH
Securities Firms	HIGH	HIGH
Health Insurance	HIGH	MEDIUM
Asset Managers	MEDIUM	MEDIUM
Life Insurance	MEDIUM	MEDIUM
Insurance Brokers	MEDIUM	MEDIUM
Non-bank Finance Companies	MEDIUM	MEDIUM
Property & Casualty Insurance	MEDIUM	MEDIUM

Corporates have a diverse risk exposure



Sector	Vulnerability	Impact
Basic Commodities	LOW	LOW
Consumer Products	MEDIUM	LOW
Lodging, Gaming and Cruise	HIGH	MEDIUM
Manufacturing & Autos	HIGH	MEDIUM
Oil & Gas	LOW	MEDIUM
Real Estate	LOW	LOW
Retail	HIGH	MEDIUM
Technology	HIGH	MEDIUM
Telecommunications & Media	HIGH	MEDIUM
Transportation Services	HIGH	MEDIUM