

LUNDI DE LA CYBERSÉCURITÉ

18 OCTOBRE 2021

CYBER RISK INDEX ET CYBER NOTATIONS



ARCSI

Association des Réservistes du Chiffre
et de la Sécurité de l'Information



Université
de Paris

PIERRE-LUC REFALO

VICE PRÉSIDENT – CAPGEMINI GROUP CYBERSECURITY



Avertissement

CETTE PRÉSENTATION PROPOSE UN
ÉTAT DE L'ART DES TENDANCES OU DES
POINTS DE DISCUSSION BASES SUR
L'EXPERIENCE DE L'INTERVENANT,
EN AUCUN CAS DES POSITIONS DE SON
ENTREPRISE (CAPGEMINI).





Plus de 30 ans d'engagement dans
La sécurité numérique
et la protection des données.



1997 - 2002

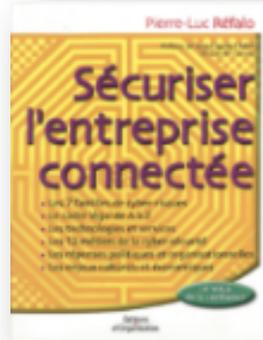


Depuis 2013

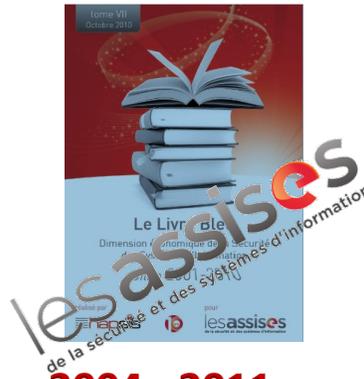


2018

Auteur



2002



2004 - 2011



2012



Prix du Livre

Enseignant

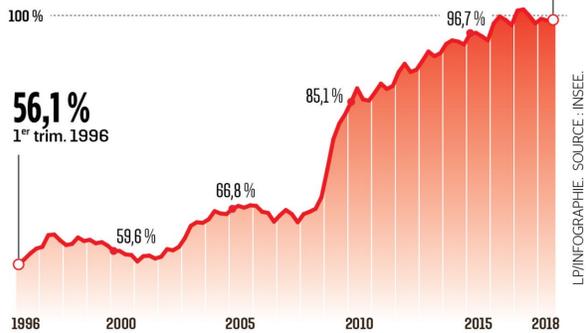


Conférencier



Evolution de la dette publique française

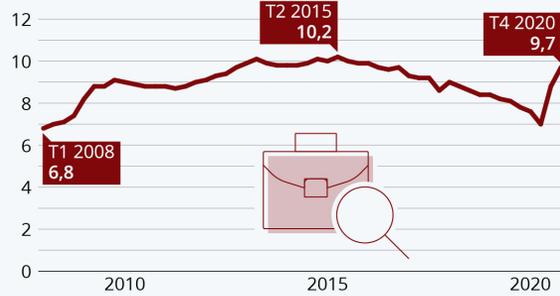
En pourcentage du PIB



LP/INFORMAPHIE - SOURCE : INSEE

Chômage : la crise annihile 5 ans de baisse

Évolution trimestrielle du taux de chômage en France métropolitaine (%) *



* Chômage au sens du Bureau International du Travail (BIT). Dernière prévision en date d'octobre pour le T4 2020. Source : INSEE



statista

Les hauts et les bas du CAC 40

Évolution du CAC 40 et principales phases baissières depuis janvier 2000 (jusqu'au 12 août 2021) *



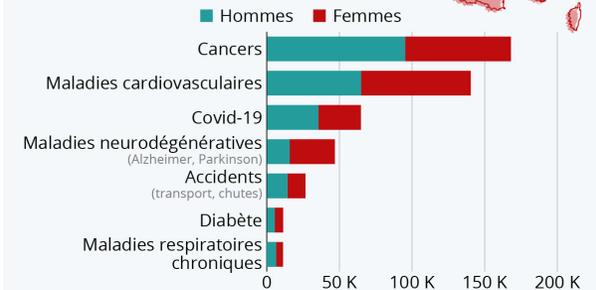
* Les % représentent la variation entre le point le plus haut et le plus bas au cours des phases baissières indiquées. Source : investing.com



statista

Le Covid-19, troisième cause de mortalité

Nombre annuel de décès en France attribués aux causes sélectionnées *



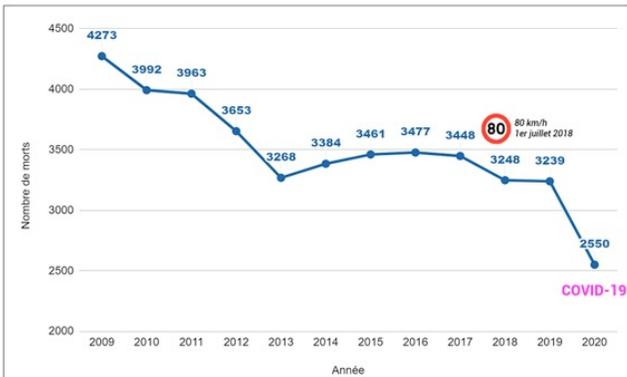
* Covid-19 : décès enregistrés en 2020. Autres causes de mortalité : dernières données disponibles de 2016. Sources : Santé publique France, Our World in Data



statista

Evolution de la mortalité routière sur 11 ans

2009 à 2020

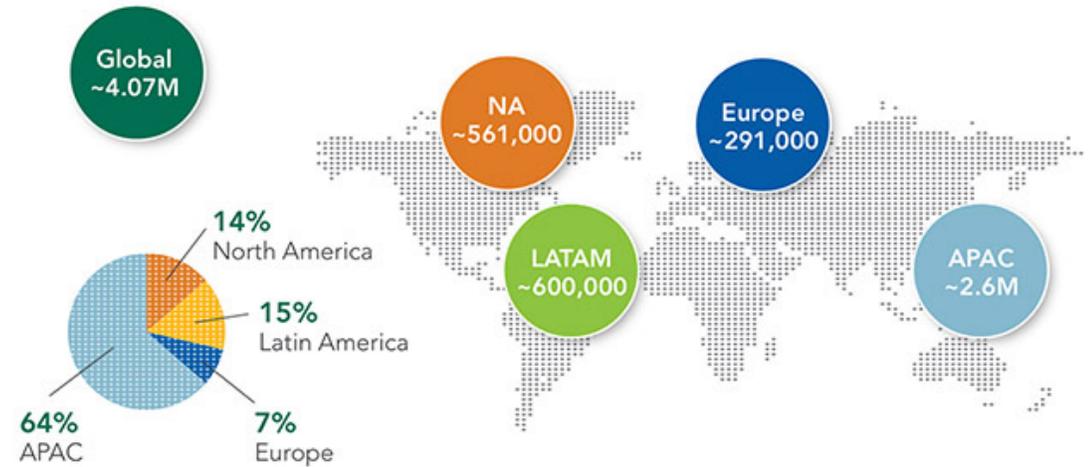


Source des données ONISR - en France métropolitaine

2021 This Is What Happens In An Internet Minute



The Cybersecurity Workforce Gap by Region

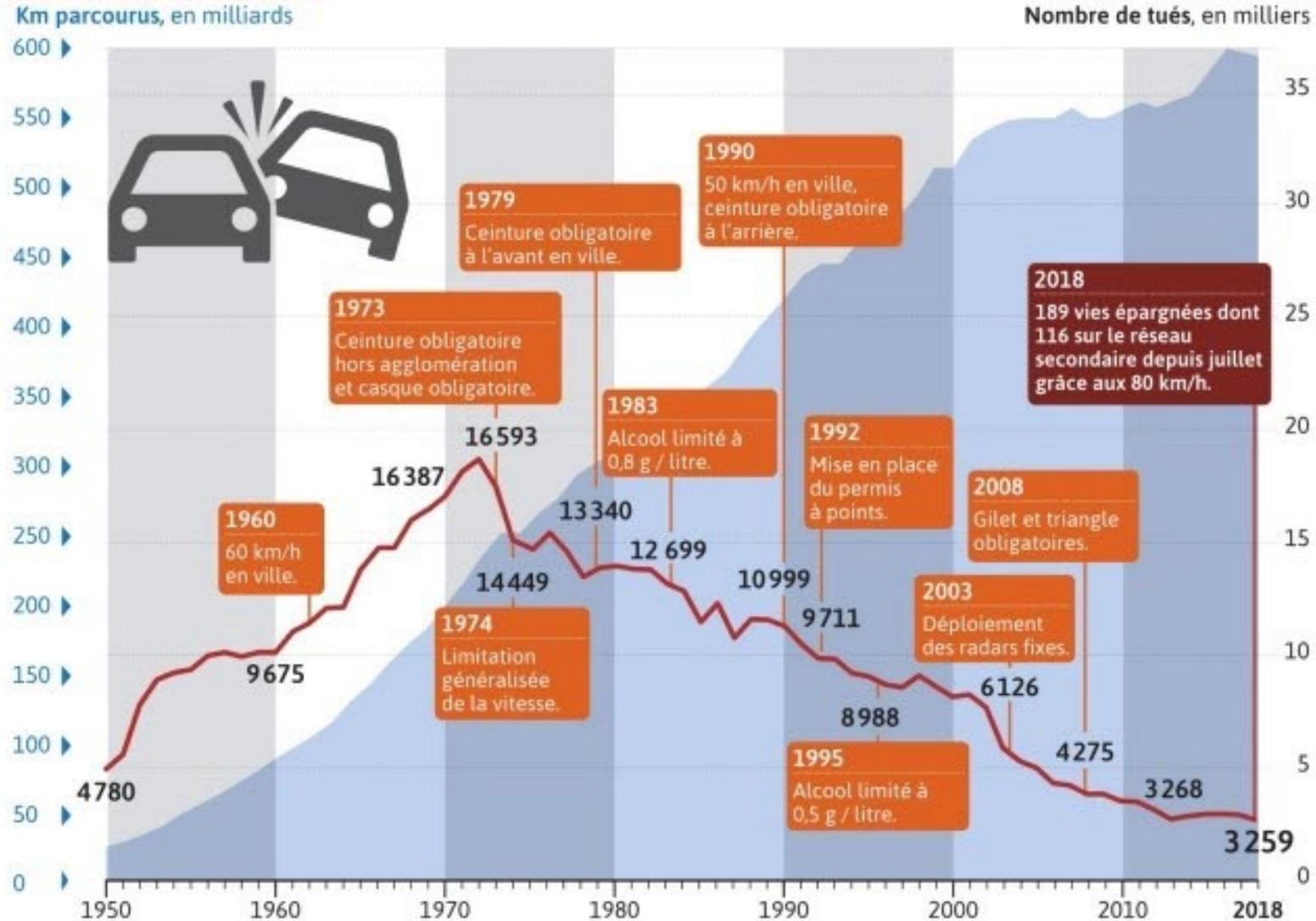


Le poids des nombres au quotidien ...

INDICATEURS DE LA SECURITE ROUTIERE

SÉCURITÉ ROUTIÈRE

LES TUÉS SUR LES ROUTES EN FRANCE MÉTROPOLITAINE



Sources : Sécurité routière (janvier 2019).

VISACTU

« J'ai appris qu'une vie ne vaut rien mais rien ne vaut une vie. »

André Malraux

INDICATEURS DE LA DIGITALISATION DE LA SOCIÉTÉ

2020 *This Is What Happens In An Internet Minute*



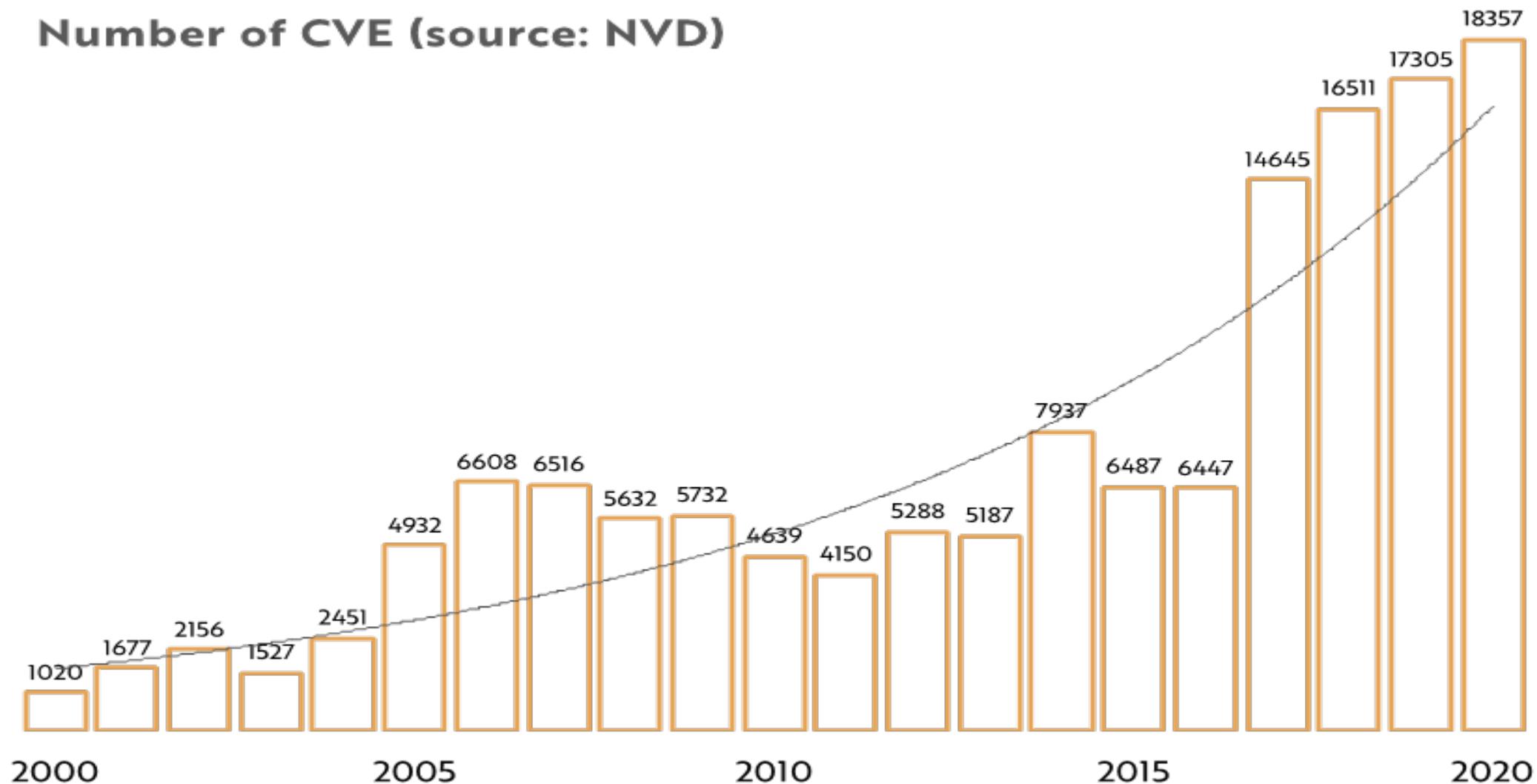
2021 *This Is What Happens In An Internet Minute*



« Our goal is to organize the world's information and to make it universally accessible and usefull. »

Larry Page

Number of CVE (source: NVD)

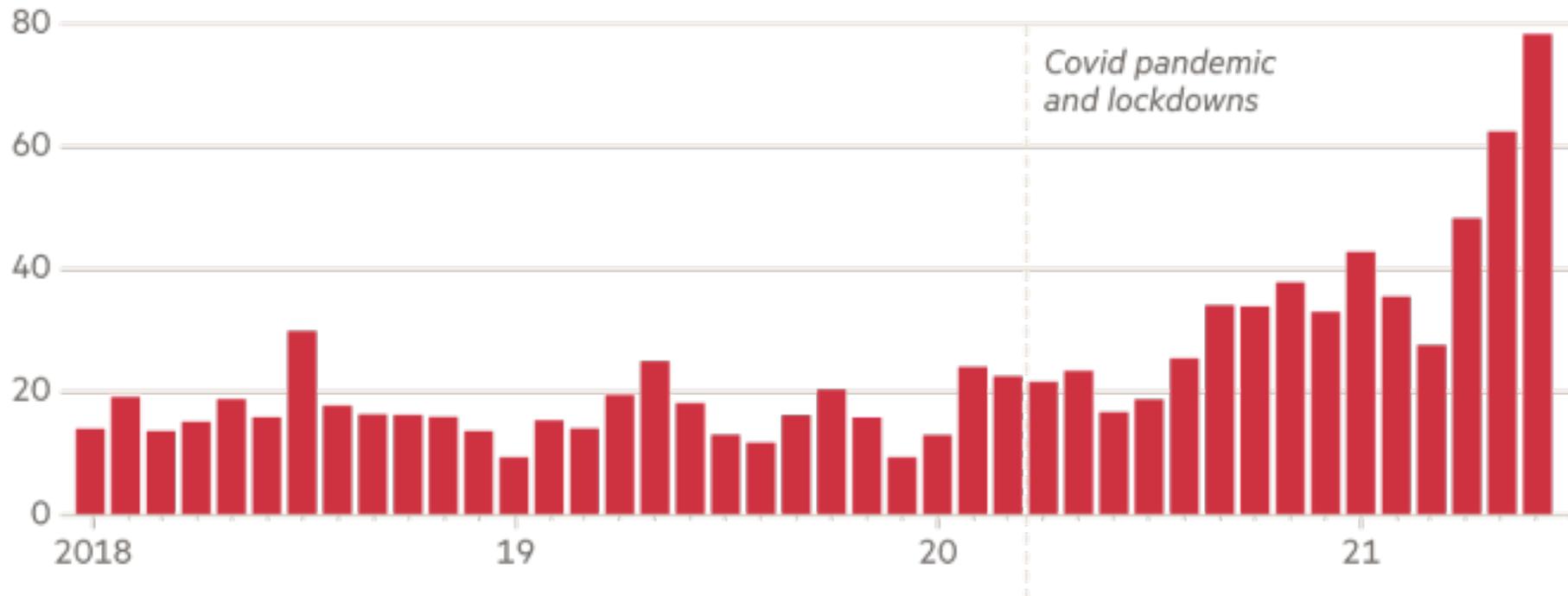


Nos faiblesses: Plus de 100 000 vulnérabilités en 20 ans !

Les menaces: Plus de 100 millions de tentatives d'attaque par ransomware en 3 ans!

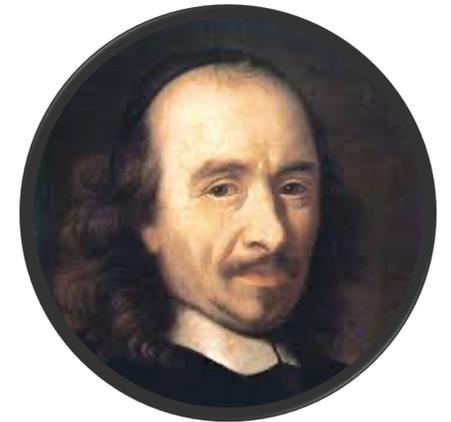
Ransomware attempts reached an unprecedented level in 2021...

Global ransomware attempts (m)



« He who fears not death fears not a threat. »

Pierre Corneille



4^e édition

Guide 2020-2021 CYBERSÉCURITÉ

French Directory

La sécurité du travail à distance

Ransomware : fléau des années 2020

Les solutions, les services, la distribution
Les ACTEURS du MARCHÉ

www.solutions-numeriques.com/security
Prix : 30€ - ISBN : 2806-2890
Paris-Saclay SOLUTIONS
En partenariat avec

400

MEMBERS AND GROWING!



INDICATEURS DE L'INNOVATION EN CYBERSECURITE

INDICATEURS DE LA CROISSANCE DU MARCHE DE LA CYBERSECURITE

Market Segment	2017	2018	2019	2020	2021	Growth%
Application Security	2 434	2 742	3 003	3 333	3 738	12.2
Cloud Security	185	304	459	595	841	41.2
Data Security	2 563	3 063	3 524	2 981	3 505	17.5
Identity Access Management	8 823	9 768	10 578	12 036	13 917	15.6
Infrastructure Protection	12 583	14 106	15 337	20 462	23 903	16.8
Integrated Risk Management	3 949	4 347	4 712	4 859	5 473	12.6
Other Information Security Software	1 832	2 079	2 285	2 306	2 527	9.6
Security Services	52 315	58 920	64 237	65 070	72 497	11.4
Consumer Security Software	5 948	6 395	6 661	6 507	6 990	7.4
Total	101 544	114 152	124 116	133 776	150 409	12.4%

WORLDWIDE SECURITY SPENDINGS BY SEGMENT, 2017-2021 (MILLIONS OF U.S DOLLARS)**

Les agences de notation ... Note de la France

STANDARD & POORS		MOODY'S		FITCH RATINGS		Sécurité optimale
LONG TERME	COURT TERME	LONG TERME	COURT TERME	LONG TERME	COURT TERME	
AAA	A-1+	AAA	P-1	AAA	F1+	De bonne qualité à qualité moyenne inférieure
AA+		AA1		AA+		
AA		AA2		AA		
AA-	A-1	AA3		AA-	F1	
A+		A1		A+		
A	A-2	A2	P-2	A	F2	Spéculatif
A-		A3		A-		
BBB+	A-3	BAA1	P-3	BBB+	F3	
BBB		BAA2		BBB		
BBB-		BAA3		BBB-		
BB+	B	BA1	NOT PRIME	BB+	B	Extrêmement spéculatif
BB		BA2		BB		
BB-		BA3		BB-		
B+		B1		B+		
B		B2		B		
B-		B3		B-		En défaut
CCC+	C	CAA		CCC	C	
CCC		CA				
CCC-		C				
SD	/	/		DDD	/	
D		/		DD		
		/		D		

La note correspond aux perspectives de remboursement de ses engagements envers ses créanciers



MOODY'S

Fitch Ratings

S&P Global Ratings

LA NOTATION DES ENTREPRISES : Une santé financière sous surveillance

LA CYBERSECURITE S'INVITE DANS LA RESPONSABILITE SOCIALE ET ENVIRONNEMENTALE

**UNE
ORGANISATION
RESPONSABLE
...**

EST INNOVANTE



EST ATTRACTIVE



**DÉVELOPPE LES CIRCUITS
COURTS ET LES ACHATS
RESPONSABLES**



**FAVORISE L'EMPLOI
SUR LE TERRITOIRE**



**DÉVELOPPE SA
COMPÉTITIVITÉ**



**RESPECTE
L'ENVIRONNEMENT
ET LA BIODIVERSITÉ**



**FAVORISE L'ÉGALITÉ
ET LA DIVERSITÉ**



**FAVORISE LA SÉCURITÉ
ET LE BIEN-ÊTRE
AU TRAVAIL**



**CONTRIBUE À
LA TRANSITION
ÉNERGÉTIQUE**



**FAVORISE LE
DÉVELOPPEMENT DE
L'ÉCONOMIE CIRCULAIRE**



**LUTTE CONTRE
LA CORRUPTION**



**EST OUVERTE
AU DIALOGUE
ET COLLABORATIVE**



**DÉVELOPPE CULTURE ET
MAÎTRISE DES RISQUES**



AGENCES DE NOTATION

Vue interne – RSE & Cybersecurity / Data Protection

Deux approches: RSE et Evaluation des fournisseurs

Plate-forme en ligne avec questionnaires thématiques (déclaratif) avec ou sans fourniture de preuves (analyse par consultant)

Scoring valable un an accessible à tous clients de la plateforme

Des questionnaires parfois très volumineux et évolutifs

Une mise en valeur de la cybersécurité auprès des dirigeants

Un usage important en termes de réputation et de maîtrise des risques intégrant les « fournisseurs »



Dow Jones
Sustainability Indexes

ecovadis

ecodesk

cybervadis



CyberGRX



CESIN

Almond

Examply Ltd.

France | Telecommunications

Share my performance

Resume reassessment

Assessment date

Mar 11, 2021

Current 

Performance

Improvement Plan

Documents

OVERALL SCORE



MODERATE



— Average score

FOCUS AREA SCORES



Data Privacy / GDPR



MODERATE



Data Protection



MODERATE



Third-Party Management



MODERATE



Business Continuity



MODERATE



Examply Ltd.

France | Telecommunications

Share my performance

Resume reassessment

Assessment date
Mar 11, 2021

Current

Performance

Improvement Plan

Documents

Identify

33 To do **2** In progress **3** Completed

Protect

100 To do **0** In progress **0** Completed

Detect

13 To do **0** In progress **0** Completed

React

4 To do **0** In progress **1** Completed

Criterion ▼ Priority ▼ Show only requested

To do (33)

In progress (2)

Completed (3)

Data privacy

Ensure that systems can accommodate withdrawal of consent

▲ High priority

Move to In progress

Data privacy

Formalize a process to handle personal data (PII) transfer to third-parties

▲ High priority

Move to Completed

Compliance

Insufficient evidence or only statement provided - Identify the impacts of potential legal or regulatory non-compliance affecting your organization's data privacy

AGENCES DE NOTATION

Vue externe – External Risk Rating

Un « scanning » des noms de domaines et IP avec de grands différences entre plateformes (scope, périodicité, qualification et faux positifs, suivi des remédiations).

Des algorithmes peu transparent et évolutifs.

Des méthodes de scoring non homogènes.

Des plateformes de management très complètes (monitoring permanent ou ponctuel, benchmark, etc.)

Une maturité naissante pour un marché en forte croissance.

Des usages variables : risques « fournisseurs » pour démarrer mais aussi risques / vulnérabilités et incidents en lien avec le SOC

Des scores minimum requis lors d'appels d'offres

Fort utile lors d'acquisitions



BIT SIGHT

riskrecon™



BITSIGHT: PILOTAGE DES SECURITY RATINGS DANS UNE ORGANIZATION DECENTRALISÉE

Compromised Systems

Botnet Infections	A
Spam Propagation	A
Malware Servers	A
Unsolicited Communications	A
Potentially Exploited	C

User Behavior

File Sharing	A
Exposed Credentials**	N/A

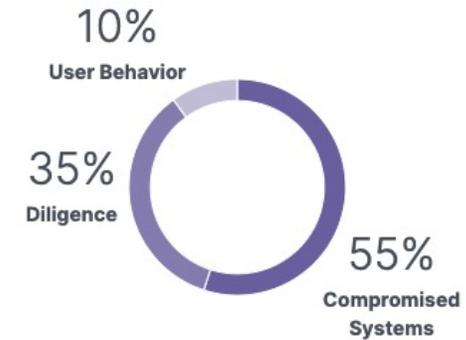
Public Disclosures

Security Incidents/Breaches	A
Other Disclosures*	N/A

Diligence

SPF Domains	A
DKIM Records	A
TLS/SSL Certificates	C
TLS/SSL Configurations	C
Open Ports	C
Web Application Headers	D
Patching Cadence	C
Insecure Systems	B
Server Software	B
Desktop Software	B
Mobile Software	B
DNSSEC*	B
Mobile ^	B

What Makes A Security Rating?

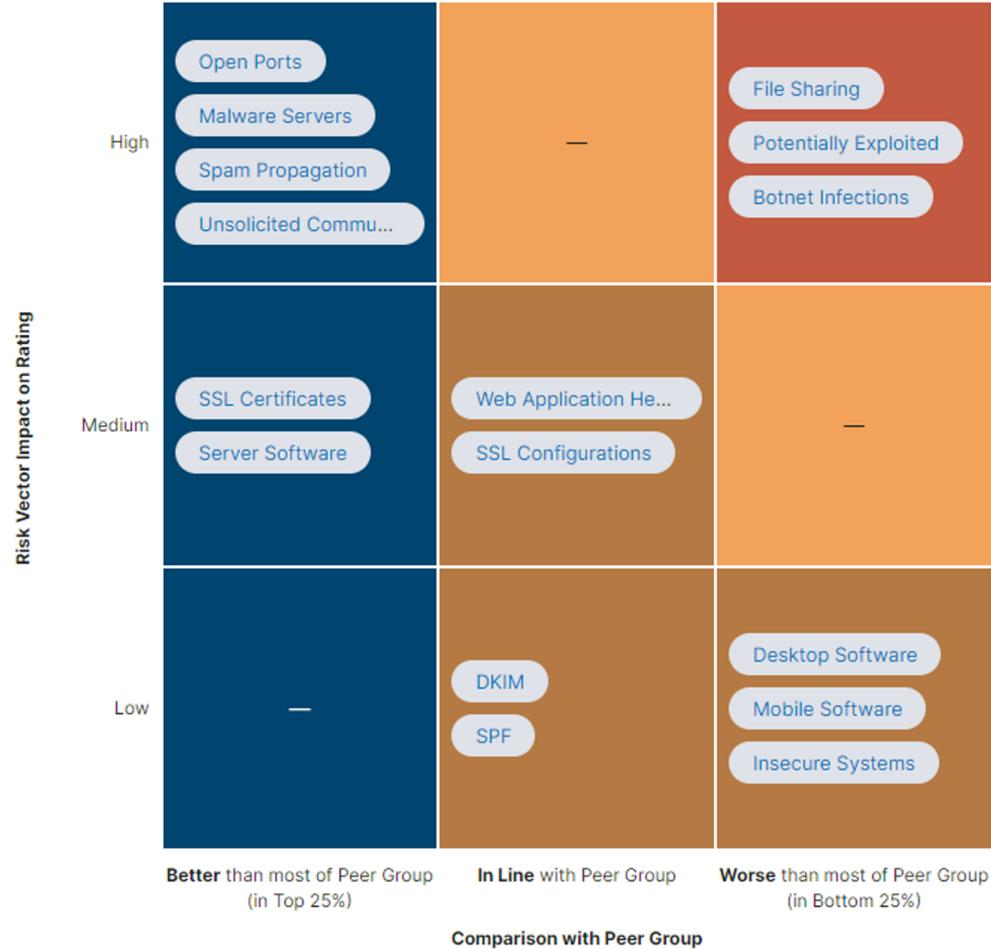


	Oct 2021	Sep 2021	Aug 2021	Jul 2021	Jun 2021	May 2021
	530	580	570	570	560	580
	630	630	630	630	630	630
	670	670	670	670	670	660
	710	710	710	710	720	720
	720	720	720	720	720	720
	720	720	720	720	720	720
	720	720	720	720	690	700
	730	730	730	730	730	730
	750	750	750	750	750	750
	760	760	760	760	760	760

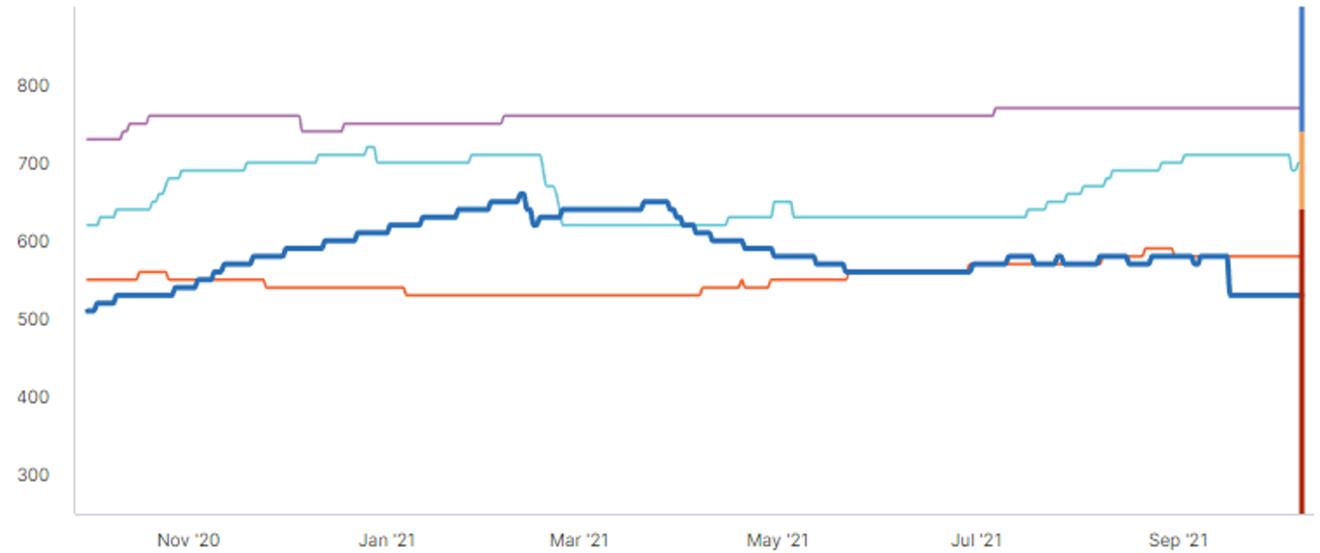
BITSIGHT: BENCHMARKING

Risk Vector Gap Analysis

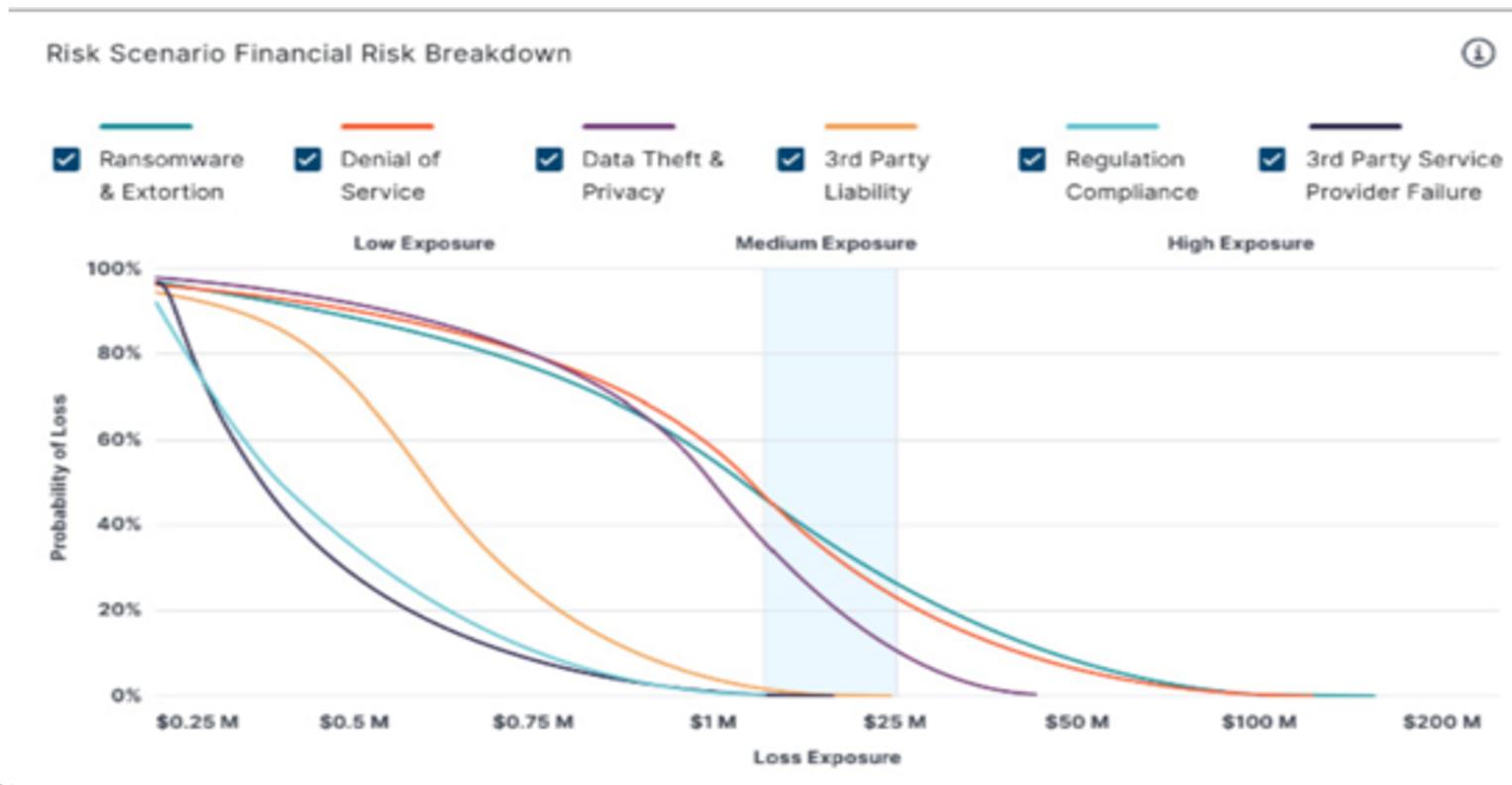
Priority: ■ Low ■ Medium ■ High ■ Very High



Security Rating



BITSIGHT: QUANTIFICATION FINANCIÈRE DES CYBER-RISQUES



CYBER ASSURANCE

Cyber rating pour la cyber-assurance

Au delà des questionnaires, qui se multiplient et se complexifient, les assureurs ont besoin de mieux qualifier le risqué cyber de leurs clients.

Les assureurs s'appuient sur les agences de notation afin de déterminer l'assurabilité et évaluer les primes dans le cas de nouveaux contrats ou de renouvellements.

AIG Partners with BitSight To Provide Cyber Insurance Diligence

DEBBIE UMBACH | APRIL 28, 2015 | TAG: CYBER INSURANCE



AXA turns to SecurityScorecard to boost cyber underwriting

by Gabriel Olano
07 Jun 2018

SHARE



AXA has selected leading security ratings firm SecurityScorecard to provide input for its cyber insurance underwriting process.



BHSI is here for you.

We combine the strength of a top-rated balance sheet with a worldwide team of professionals who have excellent credentials, capabilities and character. So you can count on us for stable



Agences de notation Cyber Rating

BENEFICES

OUTIL DE DECISION ET PRESSION POUR AGIR
COMPLEMENTARITÉ INTERNE / EXTERNE
EDUQUER (AU DELA DU SCORE)
VISIBILITE SUR LES ASSETS
AUTOMATISATION / API (EN COURS)

LIMITES

ABSENCE DE MODELE
FAUX POSITIFS (ASSETS, NIVEAU DE RISQUE)
CHANGEMENT DE L'ALGORITHME
PAS DE PATEFORME UNIFIEE
ENVIRONNEMENTS « CLOUD »

CONFIDENTIALITE / SECURITE DES PATEFORMES

CHARGE DE TRAVAIL IMPORTANTE DANS LES
ENVIRONNEMENTS COMPLEXES ET ÉVOLUTIFS

CYBER RISK INDEX

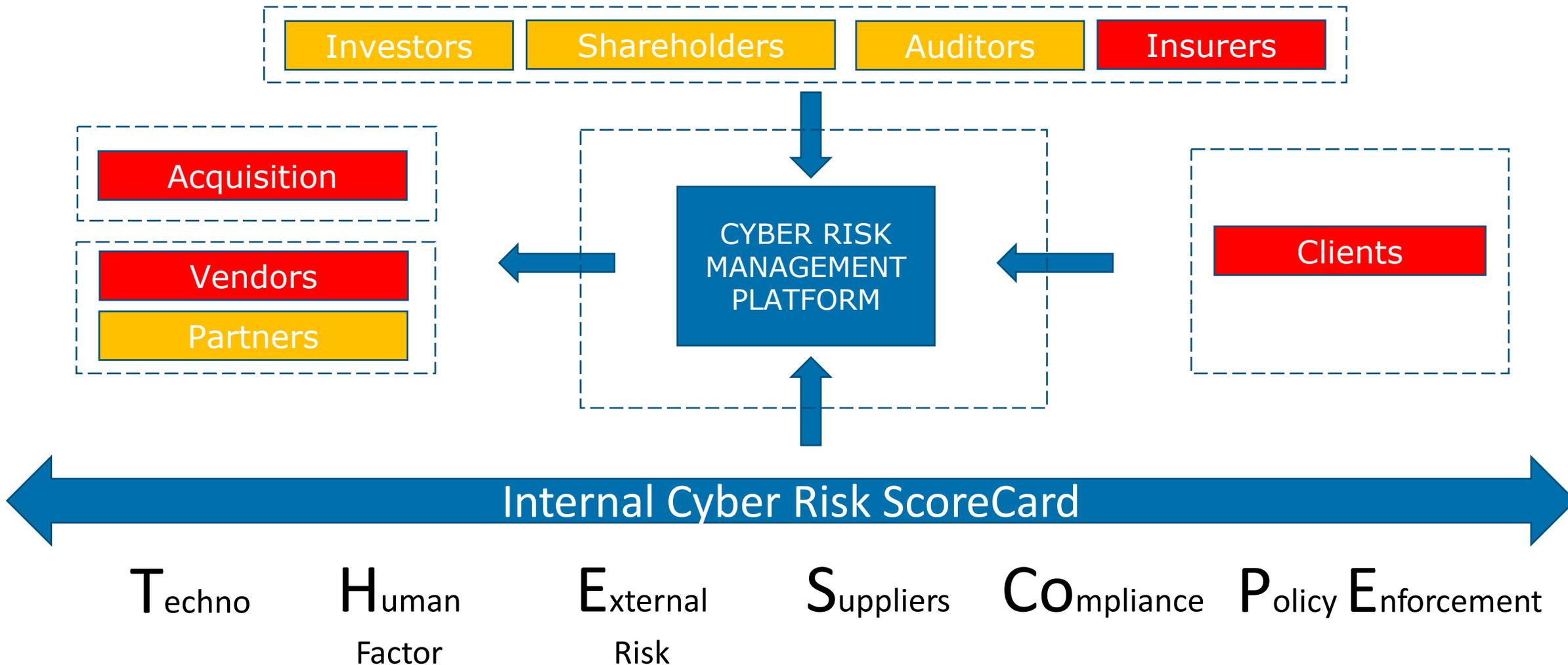
VALORISER DES INDICATEURS DE RISQUE

Face à la complexité du domaine, comment consolider des indicateurs de natures et sources variées pour caractériser un “niveau” de risqué “cyber”?

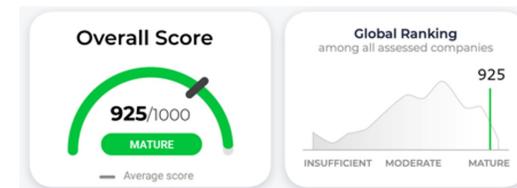
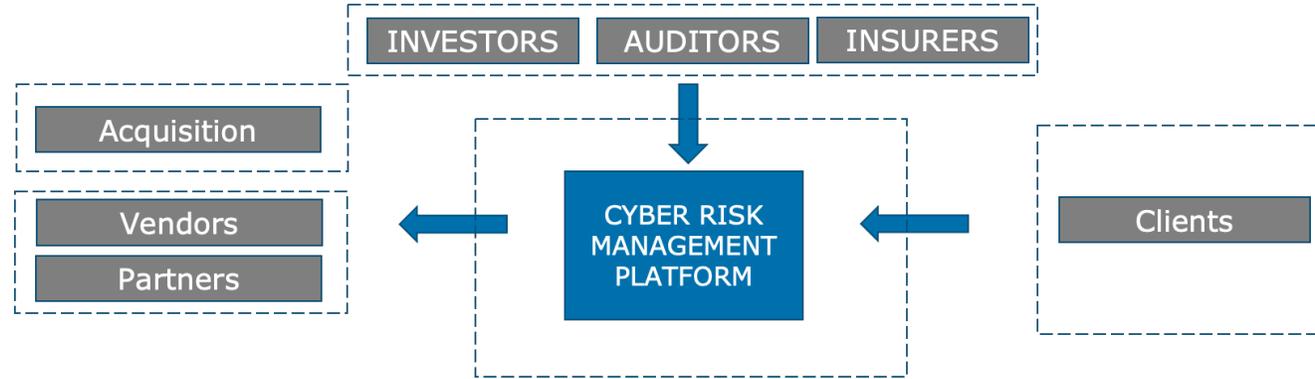
Peut-on créer un modèle qui nécessite des éléments externes et indépendants comme des éléments internes sous le contrôle de l’organisation (plus détaillés et moins transparents...) ?



UN CYBER RISK INDEX « COMPOSITE » QUI TRADUIT LA SECURITE DE L'ECOSYSTEME



CAS 1 : FOCUS SUR LES SCORING EXTERNES (EXEMPLE)



Créer son propre algorithme avec pondérations
Associer son évaluation et celle de ses fournisseurs / partenaires / acquisitions

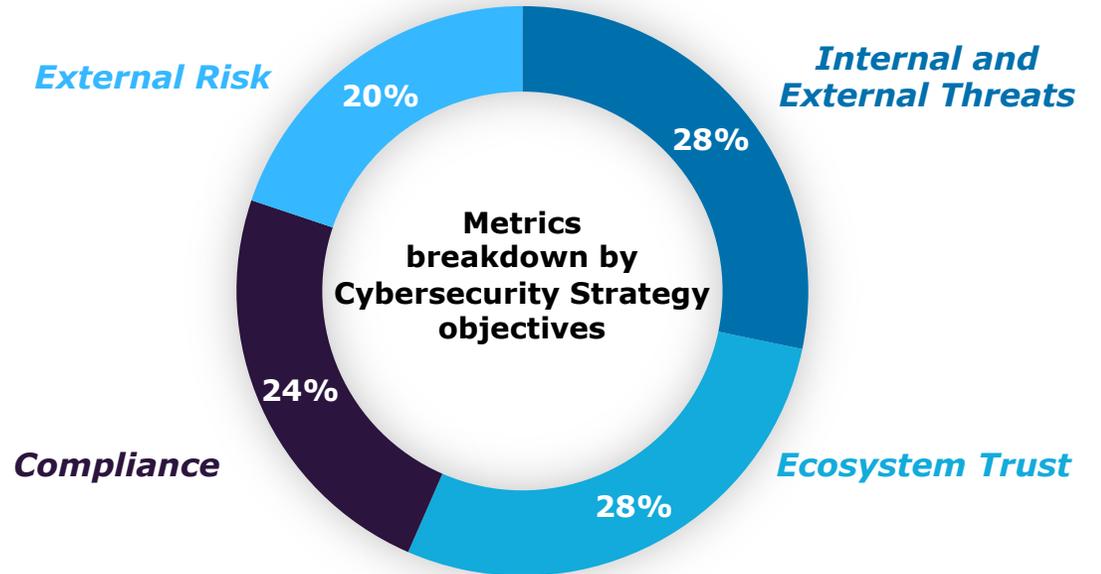
CAS 2 : CONSOLIDER DES METRIQUES DE « RISQUE » POUR REPORTING INTERNE



T_{echno} H_{uman}
Factor E_{xternal}
Risk S_{uppliers} C_{ompliance} P_{olicy} E_{nforcement}

TECHNOLOGY	HUMAN FACTOR	EXTERNAL RISK	SUPPLIERS	COMPLIANCE	POLICY ENFORCEMENT
T1 Technical Debt (W2003) T2 Technical Debt (W2008) T3 Technical Debt (Linux)	H1 New Joiners Awareness H2 Phishing test (click rate) H3 Phishing test (shared data) H4 Local Awareness Campaigns	E1 Platform 1 Score E2 Platform 2 Score E3 # of Critical issues	S1 Third Party Security Plan S2 # of T1 vendors at risk	C1 Baseline score C2 Baseline Findings C3 Findings Duration C4 CIS Benchmark score	P1 Policy adoption P2 Sites to be ISO27001 certified P3 Contract management P4 Projects Risk assessment

Group Risk & Audit Committee
 Group Executive Board
 Group Executive Committee



CYBER RISK INDEX INTERNE – REPORT (EXEMPLE)

Metric	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Technical Debt W2003	4	4	1	4	4
Technical Debt W2008	4	4	4	4	4
New Joiners Awareness	4	1	1	0	2
Phishing test (click rate)	2	0	0	2	2
Phishing test (shared data)	2	1	0	2	2
Awareness campaigns	4	2	0	4	1
RiskRecon P1/P2	1	2	2	0	1
RiskRecon P1-P4	2	4	2	4	0
Bitsight P1-P2	1	0	0	1	0
Bitsight score	4	2	2	0	0
Third-Party Security Plan	4	4	2	0	0
Baseline Policy compliance score	4	2	1	0	0
Baseline Policy compliance findings	4	2	0	0	0
Days to remediate findings	4	1	1	1	2
Policy Adoption	4	1	4	4	0
Sites to be ISO 27001 certified	4	4	4	4	0
Total points	52	34	24	40	30
Score (%)	81,3	53,1	37,5	62,5	46,9

FAKE



Réflexions pour
2022-2025



UN MODELE COMPOSITE
DES ACTEURS CLES
DE L'AUTOMATISATION
UN LIEN AVEC FINANCE
UN LEADER EUROPEEN ?

MERCI



prefalo



@plrefalo