# Assurance Paramétrique : Les hôpitaux face aux risques Cyber

Joséphine Valentin
Daniel Lyons
Sabri Boudrama

FORSIDES DESCARTES

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut.

## Ce que nous allons voir

1. Cyber : les menaces spécifiques pour le secteur hospitalier et les limites de l'approche traditionnelle
2. Assurance Paramétrique : dépasser les limites des approches traditionnelles
3. La couverture cyber pour les hôpitaux : le modèle de Descartes Underwriting

# 1. Cyber : les menaces spécifiques au secteur hospitalier

& les limites de l'approche traditionnelle

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## Menaces : vue d'ensemble

- **Infrastructures** complexes et obsolètes
- **Objets connectés** médicaux et **Interconnexion avec des tiers** (prestataires, cloud, télémédecine)
- **Données** sensibles à forte valeur
- **Personnel** insuffisamment formé à la cybersécurité
- **Budget** sécurité souvent limité

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## Menaces : conséquences d'une cyberattaque

- **Financières** : coûts de reprise, rançon, perte d'exploitation
- **Opérationnelles** : interruptions de soins, reports, saturation
- **Cliniques** : risque vital pour certains patients
- **Réputation** : perte de confiance, impact médiatique
- **Systémiques** : effet domino sur tout un territoire

FORSIDES DESCARTES

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut A

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## Quelques statistiques aux USA

Table. Trends in Hacking or IT Incidents and Ransomware Data Breaches in Health Care, 2010-2024[a]

| | Breaches | | | Records affected[b] | | |
|---|---|---|---|---|---|---|
| Year | Total No.[c] | Hacking or IT, No. (%)[d] | Ransomware, No. (%)[e] | Total No. | Hacking or IT, No. (%) | Ransomware, No. (%) |
| 2010 | 216 | 8 (4) | 0 | 6066 | 92 (2) | 0 |
| 2011 | 200 | 17 (9) | 1 (1) | 13 162 | 298 (2) | 3 (0.02) |
| 2012 | 218 | 17 (8) | 2 (1) | 2855 | 908 (32) | 35 (1) |
| 2013 | 276 | 29 (11) | 2 (1) | 7019 | 298 (4) | 11 (0.2) |
| 2014 | 314 | 39 (12) | 1 (0.3) | 19 074 | 7991 (42) | 4 (0.02) |
| 2015 | 269 | 55 (20) | 3 (1) | 112 466 | 110 971 (99) | 16 (0.01) |
| 2016 | 328 | 114 (35) | 30 (9) | 16 711 | 13 482 (81) | 324 (2) |
| 2017 | 358 | 149 (42) | 58 (16) | 5315 | 3697 (70) | 1887 (36) |
| 2018 | 369 | 165 (45) | 37 (10) | 15 236 | 11 267 (74) | 2800 (18) |
| 2019 | 511 | 314 (61) | 72 (14) | 44 970 | 40 992 (91) | 4739 (11) |
| 2020 | 663 | 457 (69) | 203 (31) | 35 310 | 32 628 (92) | 18 176 (51) |
| 2021 | 715 | 547 (77) | 222 (31) | 60 193 | 58 045 (96) | 26 754 (44) |
| 2022 | 720 | 570 (79) | 204 (28) | 57 665 | 49 807 (86) | 29 246 (51) |
| 2023 | 745 | 602 (81) | 165 (22) | 166 504 | 158 009 (95) | 84 491 (51) |
| 2024 | 566 | 457 (81) | 61 (11) | 170 001 | 154 616 (91) | 116 946 (69) |
| Total, No. | 6468 | 3540 | 1090 | 732 546 | 643 100 | 285 431 |

[a] Data for 2024 are incomplete because the sample period ended on October 31, 2024, and should be interpreted with caution because they do not represent complete annual trends.

[b] Represents the number of records affected by all data breaches, hacking, or information technology (IT) incidents and ransomware attacks, respectively.

[c] The total number of data breaches reported to the Office for Civil Rights that affected 500 or more individuals' electronic protected health information as required under the Health Insurance Portability and Accountability Act, as amended by the Health Information Technology for Economic and Clinical Health Act.

[d] The number of breaches attributed to hacking or IT incidents.

[e] The number of ransomware attacks, representing a subset of hacking or IT incidents.

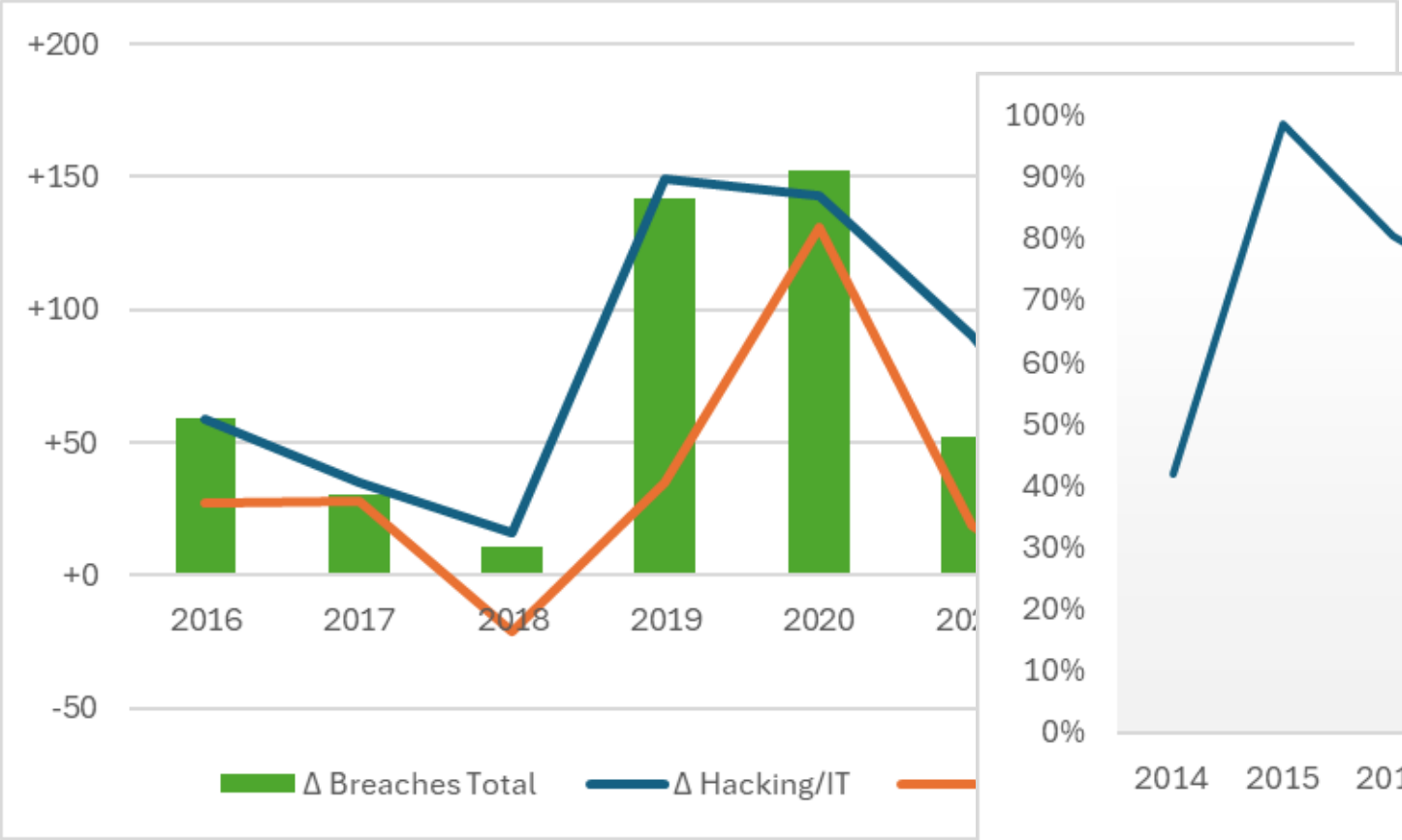
From: **Ransomware Attacks and Data Breaches in US Health Care Systems,** JAMA

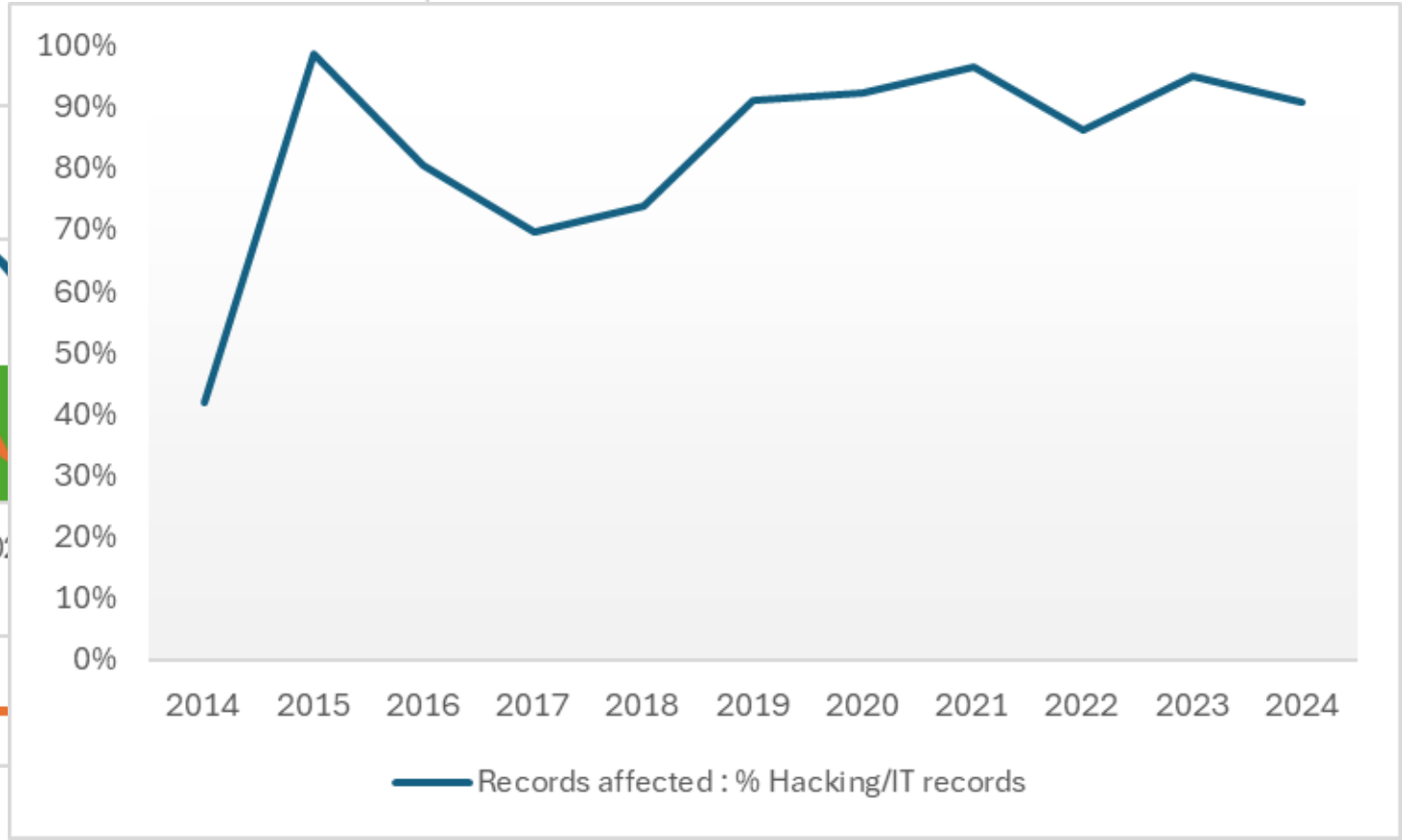
FORSIDES DESCARTES

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut A

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## Quelques statistiques aux USA




Institut A

FORSIDES DESCARTES

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## Quelques statistiques en Europe

| | ENISA Threat Landscape : Health Sector 2021 - mars 2023 |
|---|---|
| **Part des ransomwares** | 54 % |
| **Durée d'interruption** | Peu mesurée (~18 jours aux USA) |
| **Cibles** | Hôpitaux : 42%<br>Prestataires de soins : 53% |
| **impacts** | Fuite/Vol de données : 43% des incidents<br>Perturbation des services de santé : 26% des incidents |
| **Coût médian d'un incident significatif dans le secteur santé** | ~300 000 € |

En France :

- 581 incidents en établissements de santé en 2023 vs 592 en 2022, 733 en 2021 (*rapport national "Cyberattaques sur les secteurs santé et médico-social" - 2023*)
- 86 % des incidents signalés à l'ANSSI concernent les établissements de santé en 2022 et 2023

Institut

FORSIDES DESCARTES

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## Quelques cas emblématiques

- Centre Hospitalier Sud Francilien (2022)
- DDoS pro-russes (2023) : attaques sur plusieurs hôpitaux européens
- UnitedHealth (2024)

FORSIDES DESCARTES

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut.

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## Quelques cas emblématiques

- **Centre Hospitalier Sud Francilien (2022)**

- Le groupe LockBit 3.0 revendique une attaque massive par rançongiciel
- Rançon exigée : ~10 millions $
- Cette cyberattaque a paralysé près de 80 % de son système d'information : déclenchement d'un « plan blanc », certains patients ont été réorientés et l'hôpital a dû basculer en mode « papier-stylo »
- À l'issue d'un ultimatum, les cybercriminels ont commencé à diffuser des données sensibles, ce qui a entraîné l'envoi d'environ 700 000 notifications aux usagers et aux membres du personnel potentiellement concernés par la violation de données (RGPD)

FORSIDES DESCARTES

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## Quelques cas emblématiques

- Centre Hospitalier Sud Francilien (2022)
- **DDoS pro-russes (2023) : attaques sur plusieurs hôpitaux européens**

- En 2023, des attaques DDoS de groupes pro-russes ont visé des hôpitaux et autorités sanitaires en Europe, représentant ~ 9 % des incidents signalés dans le secteur santé selon ENISA

FORSIDES DESCARTES

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## Quelques cas emblématiques

- Centre Hospitalier Sud Francilien (2022)
- DDoS pro-russes (2023) : attaques sur plusieurs hôpitaux européens
- **UnitedHealth (2024)**

- En 2024, une attaque par ransomware du groupe ALPHV/BlackCat contre Change Healthcare (filiale de UnitedHealth) a compromis les systèmes de facturation et de remboursement de nombreux hôpitaux, pharmacies et prestataires de soins
- Les données personnelles de ~190 millions de patients ont été touchées (soit plus de la moitié de la population américaine)
- UnitedHealth a payé ~ 22 millions USD pour contenir l'incident

FORSIDES DESCARTES

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## La question assurantielle

- Limites et défis (1)
  - Le marché de l'assurance cyber est en forte croissance, mais c'est un marché « jeune », avec des données historiques limitées et hétérogènes
  - Sévérité élevée : certains incidents entraînent des pertes très importantes
  - Évolution rapide du risque, des techniques, des régulations : les tendances d'hier ne sont pas celles de demain

  - Tensions entre cyber et RC pro / responsabilité médicale
  - Délais et conditions de réaction parfois incompatibles avec l'urgence médicale

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## La question assurantielle

- Limites et défis (2)

Incertitudes sur les couts :

- Complexité de la chaîne causale / difficulté à évaluer les pertes réelles : coûts IT, pertes d'exploitation, réputation, …
- Temps et coûts de règlement élevés : les sinistres cyber nécessitent des enquêtes longues, complexes, et le recours à des experts variés

- Risque d'accumulation systémique : un seul événement (ex. attaque cloud ou ransomware massif) peut affecter plusieurs assurés à la fois
- Pour les risques systématiques ou systémiques, l'approche ***fréquence × sévérité*** ne suffit pas, car l'agrégation est critique et difficile à modéliser : effets réseau, dépendances, concentration

# MENACES SPECIFIQUES AU SECTEUR HOSPITALIER

## La question assurantielle

- Pour les actuaires : une modélisation de référence encore à construire
  - Données incomplètes (sous-déclaration, opacité), hétérogénéité des couvertures
  - Queue de distribution : sinistres majeurs, volatilité et incertitude élevées → les distributions de pertes sont lourdes et instables
  - Risque systémique : multi-sinistres corrélés, risque élevé d'accumulation et dépendances difficiles à modéliser → modèles de contagion, copules…
  - Intégration de données externes (cyber-incidents, vulnérabilités, fournisseurs tiers) et de posture de sécurité
  - Evolution rapide du risque (nouveaux vecteurs, IA, cloud) : la modélisation doit être dynamique

Modèles et paramétrages sont basés sur de nombreuses hypothèses complexes à estimer/justifier

→ **faible crédibilité d'expérience, volatilité extrême, charges de capital élevées**

Enjeu du partage entre assureurs / entre assurés pour améliorer la base statistique

# 2. Assurance paramétrique

Dépasser les limites des approches traditionnelles

# ASSURANCE PARAMETRIQUE

## Dépasser les limites des approches traditionnelles

Il s'agit dans cette partie de donner un aperçu général de l'assurance paramétrique par rapport à l'assurance traditionnelle dans le contexte de la problématique que nous présentons.

Ne sont pas abordés :

- Les techniques mathématiques de tarification
- Les avantages et inconvénients opérationnels (gain de gestion…)
- Les aspects juridiques liés au principe indemnitaire
- Les impacts du risque de base

# ASSURANCE PARAMETRIQUE

## Les principes du produit

### Assurance traditionnelle

- **Evénement garanti** : Survenance d'un fait provoquant un dommage matériel, corporel ou financier (ex. incendie, inondation, vol, accident)
- **Montant de l'indemnisation** : dépend de l'évaluation du dommage subi
- **Processus d'indemnisation** : déclaration de sinistres, expertise, évaluation des dommages et vérification des sinistres
- **Finalité** : Réparer un dommage

### Assurance paramétrique

- **Evénement garanti** : Survenue d'un phénomène mesurable dont les caractéristiques dépassent un certain seuil prédéfini (ex. : pluviométrie < xx mm, vitesse vent > xxx km/h…)
- **Montant de l'indemnisation** : Forfaitaire en fonction de la valeur du paramètre et non pas du montant exact des dommages
- **Processus d'indemnisation** : versement automatique dès confirmation du déclenchement de l'indice
- **Finalité** : Favoriser le redémarrage après un choc

FORSIDES DESCARTES

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut

# ASSURANCE PARAMETRIQUE

## Les bases de la tarification

### Assurance traditionnelle

- Estimation de la fréquence, basée sur des observations passées du nombre de sinistres déclarés au sein d'un groupe assuré
- Estimation du coût moyen des sinistres à partir d'un historique des coûts de sinistres déclarés

### Assurance paramétrique

- Définition d'un phénomène déclencheur
- Estimation de la probabilité de survenance du phénomène déclencheur, calculée à partir d'indicateurs contextuels prédéfinis
- Montant du préjudice déterminé à la souscription avec le contractant

FORSIDES DESCARTES

# ASSURANCE PARAMETRIQUE

## Illustration : assurance sécheresse pour des exploitations agricoles

### Assurance traditionnelle

- **Evénement garanti** : perte d'exploitation due à la sécheresse
- **Montant de l'indemnisation** : montant des pertes constatées par l'exploitant
- **Bases de tarification** :
  - Estimation de la fréquence de sinistres à partir de l'historique des exploitations sinistrées dans le passé
  - Estimation du coût moyen des sinistres à partir des sinistres enregistrés précédemment

### Assurance paramétrique

- **Phénomène déclencheur** : sécheresse définie à partir de **l'indice d'aridité (IA)** qui est fonction des précipitations annuelles, de l'évapotranspiration annuelle, et éventuellement de la capacité de rétention du sol
- **Evénement garanti** : IA < seuil contractuel
- **Montant du capital garanti** : forfaitaire
- **Bases de tarification** :
  - Historique des taux de précipitation, évapotranspiration, et capacité de rétention du sol de la zone à couvrir
  - Caractéristiques des exploitations à couvrir pour un choix pertinent du capital forfaitaire garanti

# ASSURANCE PARAMETRIQUE

## Les principaux enjeux

Fondée sur un phénomène extérieur et indépendant du bénéficiaire, l'assurance paramétrique constitue une alternative à l'assurance traditionnelle, offrant une protection même en l'absence d'un historique de sinistres.

Plusieurs enjeux demeurent quant à l'élaboration d'une tarification réellement équitable et adaptée au risque :

- Identification du phénomène sous-jacent et sélection des indices les plus pertinents pour le caractériser
- Corrélation entre les indices et les pertes constatées
- Disponibilité et fiabilité des données

Un travail préparatoire avec des experts du domaine est indispensable pour identifier des indicateurs pertinents.

Si les indicateurs apparaissent évidents pour certains risques, leur identification s'avère beaucoup plus complexe pour d'autres. C'est le cas des risques cyber.

Illustration des travaux préparatoires pour le risque sécheresse :

*« Renforcement De La Résilience Financière Face À La Sécheresse: Une Étude De Faisabilité - Pour Une Solution Indicielle De Financement Des Risques De Sécheresse Pour Les Éleveurs Pastoraux (Etude De Cas Au Sénégal) » - Institut International de Recherche sur l'élevage et la World Bank Group*

# 3. La couverture cyber pour les hôpitaux

DESCARTES

Descartes protects **corporate clients** against **climate and emerging risks** with parametric insurance

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut.

**We leverage vast amounts of data to improve:**

Pricing

Loss adjustment

In addition to a team of insurance natives, more than half of our employees are data scientists, meteorologists and software engineers coming from the most prestigious institutions.

**Our value proposition relies on 3 key differentiators:**

1. **Simplicity** of indemnity payments through automation (within weeks instead of months)
2. **Fairness** of pricing through quality risk assessment and bespoke quotes to reward good risk management
3. **Transparency** of policy coverage for both the insurer and the insured

**€200+M**
GWPs generated in 2024
in 70+ countries at Descartes

**150+**
PhDs, data scientists &
software engineers

**A-**
Minimum rating of reinsurers
backing Descartes*

**S&P or AM Best rating on 16/01/2025*

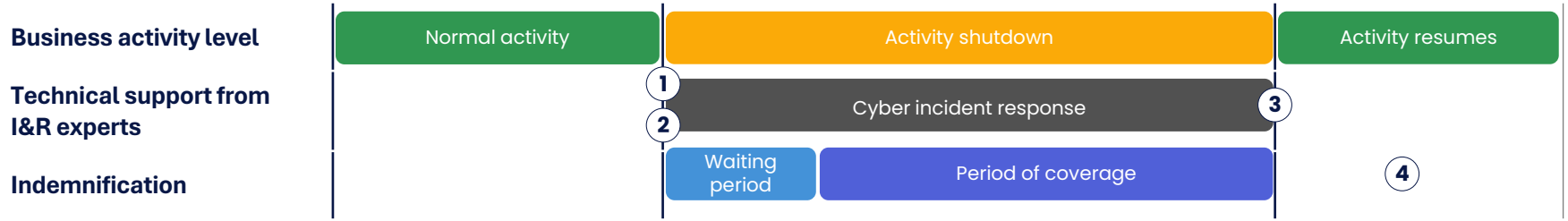
# Descartes’ Cyber Shutdown Cover

FORSIDES DESCARTES

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut A

## In case of a cyberattack

Descartes brings fully integrated technical support and swift parametric indemnification for financial relief




| | | |
|---|---|---|
| 1 | **Initial contact with I&R experts** | The insured notices malicious activity in the IT system and calls I&R experts through the dedicated hotline available 24/7. |
| 2 | **Event certification** | I&R experts set up an incident resolution strategy and certify that the insured event has happened. **The insured knows in real-time if coverage may apply.** |
| 3 | **End of shutdown certification** | Once the incident is resolved and the company is ready to resume activity, experts certify that IT systems are online.<br><br>**Example hospital:** new patients can be entered into the system, appointments can be made, lab results can be generated and sent patients |
| 4 | **Parametric indemnification** | Descartes calculates the parametric indemnity and **sends payment within days.** |

**I&R: Incident and response**, external IT provider, serves as the objective index for parametric insurance

Institut A

# Pricing model is fully tailored to an insured's evaluated level of risk and desired coverage

| | Frequency module | Severity module | Payable loss module |
|---|---|---|---|
| **Goal** | Provide the number of events per year | Provide the duration of total shutdown for each event | Provide the insurance cost of total shutdown for each event according to duration. |
| **Data Scope** | Cyber intrusions for French medium-sized to large companies and public entities since 2020. | Duration of total shutdown for French medium-sized to large companies and public entities since 2020. | Gross margin for French medium-sized to large companies and budget for public entities. |
| **Data Collection** | Collected from news using LLM and cleaned/validated by Descartes. A confidence level is associated with each data input. | Collected from news using LLM and cleaned/validated by Descartes. A confidence level is associated with each data input. | Collected from financial reports from publicly traded companies and budget information for public entities. |
| **Model assumptions** | • Event occurrence follows a Poisson law;<br>• Frequency is inflated to consider undisclosed attacks;<br>• Frequency is calculated based on the average in 2020 – 2025, not just on last year. | • Total shutdown duration is approximated by several different laws<br>• Duration is calculated based on the average in 2020 – 2025, not just on last year. | • Public entity budget is equivalent to gross revenue of companies |
| **Calibration** | Based on our data, fine tuned with historical data from the insured. | Based on our data, fine tuned with historical data from the insured. | Based on our data and the results of the insured's business impact study |
| **Validation** | • Data is updated every trimester;<br>• Validation of frequencies with expert feedback and publicly available surveys. | • Data is updated every trimester;<br>• Validation of durations with expert feedback and publicly available surveys. | Validation of data from:<br>• National statistics data (INSEE in France)<br>• Historical losses recorded by publicly available sources or loss adjusters |
| **Main Drivers** | • Company size;<br>• Industry;<br>• Internal cybersecurity level: employee training policy, patching policy, maturity of IT security tools, dedicated budget, …<br>• External cybersecurity level: provided by third-party providers<br>• IT Architecture: are there many independent IT subsystems? | • Company size;<br>• Industry;<br>• Cyber resilience level: backup policy, training frequency for the attack recovery plan, incident response time, …<br>• IT Architecture: how dependent are operations on the IT system? | Unlike with the frequency and severity modules, the parameters of the indemnification module may be tailored to the insured's needs:<br>• Waiting period duration;<br>• Limit per contract;<br>• Daily indemnification. |

# Pricing model is fully tailored to an insured's evaluated level of risk and desired coverage

Our pricing model has been designed to ensure full consistency with the contract terms.

Typically, prices will range from 0.5% to 3% RoL depending on the client and its desired coverage.

The adjacent table provides insight on how the price may vary according to company's characteristics and desired coverage.

| If the following changes... | ... what will be the impact on premium? |
|---|---|
| **Frequency module** | |
| Company/Entity size increases | **increase** |
| Internal cybersecurity level increases | **decrease** |
| External cybersecurity level increases | **slight decrease** |
| **Severity module** | |
| Company/Entity size increases | **slight increase** |
| Cyber resilience level increases | **decrease** |
| **Payable loss module** – *these parameters can be tailored to the client's needs* | |
| Waiting period duration increases | **strong decrease** |
| Daily indemnification increases | **strong increase** |
| Limit per contract increases | **slight increase** |

FORSIDES DESCARTES

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut.

# Q&A

FORSIDES DESCARTES

100% ACTUAIRES DATA SCIENCE DURABILITÉ BY Institut.

# Evaluez cet atelier

Institut