⚠ INTRUSION EN COURS

« Je suis dans votre réseau.
L'hôpital de Pontarlier ne le sait pas encore… »

1

LUNDI 15 JUIN 2026

Les Lundi de la Cybersécurité
De la thèse à la crise…

Ce n'est pas une panne…
C'est un système hospitalier qui lutte pour rester debout qui perd sa mémoire numérique, sa voix, puis réinvente ses gestes pour continuer à soigner.

Thomas Vadot
RSSI — CHI de Haute-Comté

Judith Nicogossian
Docteur en Anthropologie

2

Le Récit

Une crise en six mouvements

01

Avant l'attaque

Une exposition silencieuse, déjà visible.

02

La nuit du 18 au 19 octobre

Moment de bascule. La crise devient réelle et irréversible.

03

Premières heures

Contenir avant de comprendre. Sauver avant de réparer.

04

Mode dégradé

Réinventer les gestes. Maintenir le soin sans le numérique.

05

Reconstruction

Rebâtir sans se réinfecter. La prudence comme seule boussole.

06

Transformation

La crise comme catalyseur d'une résilience institutionnelle durable.

Une cybercrise hospitalière déroule une dramaturgie du doute, de la décision et de la solidarité.

3

CADRE INTELLECTUEL

Ce que disait ma Thèse

La thèse mobilise une lecture croisée des sciences de gestion, de la résilience et du **bricolage organisationnel**. La réponse à une attaque ne relève pas d'un protocole technique seul — elle combine ajustements humains, coordination interprofessionnelle et leadership sous incertitude.

Une crise à quatre visages

- Socio-technique
- Du soin
- Du sens
- De l'organisation

La cyberattaque du CHIHC ne contredit pas la thèse : elle la **valide, acte par acte**. La théorie n'est pas abstraite — elle est opératoire.

Conduite du changement

Naviguer sous contrainte

Bricolage organisationnel

Faire autrement qu'avant

Dynamiques de résilience

Absorber, adapter, rebondir

4

L'Hôpital avant l'Impact

Une exposition déjà visible

Le CHIHC, établissement multi-sites à hébergement mutualisé, affichait avant l'incident des **vulnérabilités structurelles** — non par négligence, mais par une transformation en cours au moment précis où l'attaquant a frappé.

Accès distants exposés

Connexions à distance nécessaires mais dont la sécurisation n'avait pas encore atteint le niveau requis face aux nouvelles menaces.

Authentification classique

Le MFA n'était pas encore universellement déployé, laissant des points d'entrée accessibles à des attaquants déterminés.

Segmentation incomplète

La segmentation réseau était engagée mais pas totalement déployée — rendant possible une propagation latérale en cas de compromission.

Supervision cyber immature

L'absence d'un SOC pleinement opérationnel limitait la détection précoce et l'alerte en temps réel sur les comportements anormaux.

La fragilité n'est pas toujours l'absence de projet — elle peut être le temps d'avance qu'a l'attaquant sur le déploiement des protections.

5

2 h du matin

Le moment de bascule

🔒 Chiffrement massif

Fichiers, dossiers, partages réseau verrouillés un à un dans un silence algorithmique.

🚫 Applications hors ligne

DPI, prescriptions, planification — inaccessibles. L'hôpital devient aveugle.

📞 Téléphonie perturbée

La coordination interne se fracture. On ne peut plus se parler. On ne peut plus synchroniser.

💀 Message de rançon

Sur les écrans encore allumés : l'injonction des attaquants. Ce n'est plus une alerte — c'est une déclaration de guerre.

En deux heures, l'hôpital perd sa mémoire numérique, sa voix et sa capacité à synchroniser ses métiers. Personne ne possède encore la totalité du tableau.

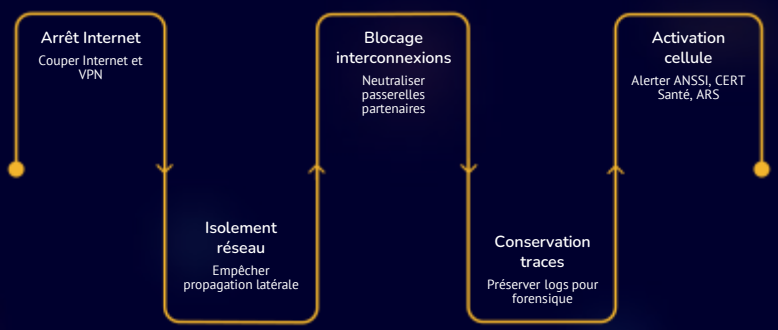
6

RÉPONSE IMMÉDIATE

Les Premiers Gestes

Contenir avant tout

La première réponse ne consiste pas à réparer — elle consiste à **isoler, couper, préserver et signaler**. L'objectif : empêcher l'extension du dommage et protéger les preuves numériques indispensables à l'investigation.



La bonne réponse n'est pas "remettre en route" — c'est "empêcher la propagation et garder la main". Le courage organisationnel tient dans la discipline du geste juste.

7

Chronologie J0

Une journée sous tension

~2h00 — 1
Premiers signaux. Alerte astreinte. Constat du chiffrement. Isolements réseau activés.

2 — **~4h00**
Confirmation ransomware. Notification RSSI et direction. Investigation et cartographie des systèmes touchés.

~6h00 — 3
Cellule de crise opérationnelle. Bilans par pôles. Premiers renforts humains mobilisés.

4 — **~8h00**
Appui SAMU, ARS, CHU activé. Téléphones et ordinateurs prêtés. Numéro vert d'urgence ouvert.

~10h00 — 5
Bascule en mode dégradé officialisée. Circuits reconstitués. Équipes soignantes et patients informés.

6 — **~12h–18h**
Notification ANSSI et CERT Santé. Coordination inter-établissements. Gouvernance de crise stabilisée.

La crise se gère parce qu'elle se structure — pas parce qu'elle devient silencieuse. L'organisation est le premier outil de survie.

8

GOUVERNANCE DE CRISE

La Cellule de Crise

Une architecture de décision

1

Niveau terrain

Urgences, bloc, maternité, imagerie, laboratoire — adaptation clinique immédiate et protocoles dégradés.

2

Niveau opérationnel

DSI, équipes techniques, référents pôles, pharmacie, logistique — coordination et remontée terrain en temps réel.

3

Niveau stratégique

Direction générale, direction médicale, RSSI — arbitrages de fond, communication externe, décisions engageantes.

ⓘ Les partenaires externes — ANSSI, CERT Santé, ARS, CHU — complètent ce dispositif en apportant expertise, ressources et légitimité institutionnelle.

MODE DÉGRADÉ

Retour au Papier

Le soin réinventé

Ce qui disparaît

- Dossier patient informatisé (DPI)
- Prescriptions électroniques
- Résultats de biologie en ligne
- Plannings et agendas numériques
- Messagerie sécurisée de santé
- Imagerie accessible en réseau

Ce qui prend le relais

- Formulaires papier d'admission et de prescription
- Dossiers physiques reconstitués manuellement
- Étiquettes identité réimprimées hors réseau
- Numéros de fax recensés et testés en urgence
- Listings de contacts physiques distribués
- GSM comme seul canal de coordination

La panne numérique ne suspend pas le soin — elle oblige à retrouver ses gestes élémentaires. C'est aussi le moment où la dépendance au numérique devient soudainement, douloureusement visible.

Le PCA en Vrai

La mémoire organisationnelle

Le Plan de Continuité d'Activité a tenu parce qu'il n'était pas un classeur dormant. Il était **vivant, incarné, entraîné et distribué dans les métiers**.

Fiches réflexes opérationnelles

Procédures courtes, claires, accessibles sans réseau. Plastifiées, actualisées, affichées — prêtes à être saisies à 2h du matin.

Exercices antérieurs

Les simulations avaient créé des automatismes partagés. Les équipes n'improvisaient pas depuis zéro — elles activaient une mémoire collective.

Supports papier préparés

Listings de contacts, circuits dégradés par pôle, procédures pharmaceutiques manuelles — disponibles sans dépendre d'un SI compromis.

Un langage commun pour agir

Sous stress, ce vocabulaire d'action partagé remplace les instructions qui ne parviennent plus. Il s'apprend avant la scène.

11

MISSION CENTRALE

Continuité des Soins

Tenir la mission

Urgences maintenues
Aucun patient refusé. Fonctionnement continu avec coordination renforcée SAMU et structures régionales.

Bloc & maternité
Actes urgents maintenus. Coordination orale renforcée entre chirurgiens et anesthésistes, supports papier.

Imagerie & laboratoire
Priorisation des examens critiques. Résultats transmis par fax et téléphone. Aucun résultat vital en suspens.

Pharmacie
Ordonnances manuscrites, circuits papier validés, registres physiques avec double vérification systématique.

La continuité des soins se mesure en actes concrets : prises en charge maintenues, examens réalisés, patients orientés avec soin selon les capacités réelles du moment.

12

INTELLIGENCE DE TERRAIN

Le Bricolage Organisationnel

Faire avec, faire sans, faire autrement

Ce n'est pas de l'improvisation désordonnée — c'est une **compétence collective de survie** quand le cadre standard s'effondre. Une vertu discrète, noble et professionnelle.

Étiquettes reconstituées manuellement

Identification des patients par étiquettes manuscrites, tampons et doubles vérifications orales. La traçabilité devient affaire d'attention humaine.

Radios et GSM 4G réinstallés

Communications reprises sur des canaux hors réseau IP : talkie-walkies, téléphones personnels et GSM mis à disposition par les partenaires régionaux.

Fax recensés et testés en urgence

Une infrastructure oubliée — biologie, imagerie, pharmacie, médecins traitants — retrouvée, testée et distribuée sur papier. Soudainement vitale.

Secrétariats repositionnés

Les secrétaires médicales deviennent des relais de coordination clinique : saisie manuelle, acheminement de résultats, communication inter-services.

Ce qui a Coûté Humainement

L'envers de la performance

Charge mentale et fatigue prolongée

Vigilance constante, mémoire de travail surchargée, attention qui ne peut se relâcher. La fatigue s'accumule de façon invisible — et érode progressivement la qualité des décisions.

Peur diffuse de l'erreur

Sans vue consolidée sur les dossiers, la tension entre vitesse et sécurité est permanente. Chaque soignant porte une responsabilité décuplée en environnement dégradé.

Saturation informationnelle

Flux proliférant par canaux non habituels — appels, messages oraux, papiers manuscrits. Le tri et la vérification deviennent eux-mêmes sources d'épuisement.

Dépendance révélée au numérique

Beaucoup attendaient que l'informatique leur dise comment travailler sans informatique. La **perte des réflexes pré-numériques** est l'un des apprentissages les plus profonds.

⚠ Ce n'est pas seulement le système qui souffre — ce sont les équipes qui portent la continuité dans une fatigue prolongée. La dimension humaine est une composante à part entière de la gestion de l'incident.

ACTE III

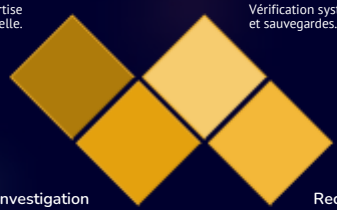
La Remédiation

Rebâtir sans réintroduire la menace

La remédiation ne consiste pas à *réparer vite*. Elle consiste à **reconstruire juste**. Chaque étape est pensée comme un filtrage rigoureux pour éviter toute réinfection.

Coordination
ANSSI et CERT Santé : expertise institutionnelle.

Cartographie
Vérification systèmes, comptes et sauvegardes.



Investigation
Traces, vecteur d'entrée, périmètre compromis.

Reconstruction
Réintroduction par paliers en environnement isolé.

La remédiation est une reconstruction disciplinée, contrôlée, traçable — le prix que l'on accepte de payer pour ne pas recommencer.

15

LE PRIX DE LA CONFIANCE

Pourquoi c'est Long

La lenteur comme discipline

Ce qu'il faut vérifier

- Chaque serveur physique et virtuel
- Chaque sauvegarde — intégrité et absence de contamination
- Chaque compte utilisateur — compromission, élévation de privilèges
- Chaque machine virtuelle dans l'infrastructure
- Chaque interconnexion avec des partenaires externes
- Chaque application métier avant réintroduction

Les contraintes invisibles

Matérielles
Équipements, délais d'approvisionnement, hébergement temporaire

Logistiques
Coordination entre équipes internes, prestataires et autorités

Administratives
Recertification, obligations réglementaires, traçabilité

Humaines
Disponibilité des experts, fatigue des équipes, maintien de la vigilance

La rapidité rassure dans le discours — mais **seule la prudence protège durablement**. Chaque test évité est une réinfection potentielle. Chaque validation bâclée est une bombe à retardement.

16

Le PRA et la Bulle de Confiance

Reprendre sans se réinfecter

La reprise s'appuie sur un **cœur de confiance isolé** — un environnement de redémarrage minimal, sûr et auditable — qui protège les outils, les données et la confiance des métiers.

1

Bulle de confiance

Environnement réseau isolé, nettoyé, surveillé. Aucun système y accède sans validation préalable.

2

Test des sauvegardes

Sauvegardes secondaires et tertiaires vérifiées, testées en restauration. Seules les sauvegardes certifiées propres entrent dans la bulle.

3

Priorisation clinique

DPI, pharmacie, urgences, biologie — premiers réintroduits. La priorisation clinique guide l'ordre de reprise technique.

4

Remise en service par paliers

Chaque service reprend après validation. Montée en charge progressive, surveillée, réversible.

Sans la bulle de confiance, le risque de réinfection transformerait la reprise en rechute.

17

ARCHITECTURE DE RÉSILIENCE

PCA versus PRA

Deux rôles complémentaires, deux temps de crise

PCA — Plan de Continuité d'Activité

Temps : Pendant la crise, dès les premières heures.
Objectif : Maintenir la mission de soin avec des moyens dégradés.
Nature : Organisationnel, humain, procédural.
Question clé : *"Comment continuer à soigner sans le SI ?"*
Ce qu'il protège : La mission. Les patients. La continuité des actes.

PRA — Plan de Reprise d'Activité

Temps : Après la stabilisation, en phase de remédiation.
Objectif : Reconstruire un SI sain, sans réintroduire la menace.
Nature : Technique, séquentiel, auditable.
Question clé : *"Comment reconstruire l'outil sans se réinfecter ?"*
Ce qu'il protège : L'intégrité du SI. La sécurité de la reprise. La confiance des utilisateurs.

Le PCA protège la mission. Le PRA reconstruit l'outil. Les confondre coûte cher.

18

FACTEUR AGGRAVANT

Les Facteurs Aggravants

L'effet domino de la mutualisation

Hébergement mutualisé

Un seul environnement pour plusieurs établissements — une compromission initiale se propage sans traverser de frontière technique signifiante.

Approbations de domaine partagées

Un Active Directory commun permet à l'attaquant ayant compromis un compte de se mouvoir librement dans l'ensemble du périmètre.

Sauvegardes centralisées et accessibles

Des sauvegardes accessibles depuis le réseau compromis sans isolation ni immuabilité deviennent elles-mêmes des cibles à chiffrer ou détruire.

Un espace de confiance trop large devient une autoroute pour la propagation. **Mutualiser sans isoler, c'est fabriquer un effet domino** et offrir à l'attaquant le rayon d'action maximal au coût d'effort minimal.

19

Les Facteurs de Résilience

Ce qui a permis de tenir

La résilience ne s'improvise pas le jour J — elle s'entraîne avant. Ce qui a permis de faire face est le résultat d'une **préparation patiente** et d'investissements antérieurs.

Sauvegardes immuables

Hors ligne, non altérables, régulièrement testées. La ligne de défense la plus décisive lors de l'attaque.

Documentation à jour

Procédures actualisées, schémas réseau, fiches de contact — un actif stratégique, pas une formalité.

Expertise interne

Double culture technique et clinique — déterminante. Elle ne s'acquiert pas dans l'urgence, elle se construit dans la durée.

Appui institutionnel

ANSSI et CERT Santé — cadre d'action clair, ressources et légitimité. Ces partenariats se nouent avant la crise.

Partenaires de confiance

Prestataires identifiés, contrats actifs, relations préétablies — mobilisation rapide sans les délais d'une mise en relation dans l'urgence.

Exercices antérieurs

Les simulations ont forgé des réflexes collectifs. Le sang-froid le jour J est la mémoire musculaire d'une organisation entraînée.

Chaque investissement consenti avant la crise multiplie la capacité de réponse le jour où elle survient.

20

TRANSFORMATION DURABLE

Ce que la Crise a Transformé

La cyber devient gouvernance

Authentification forte (MFA)

Déploiement systématique sur l'ensemble des accès critiques. Mesure à fort impact, faible coût, immédiatement généralisable.

Segmentation réseau

Cloisonnement des zones critiques — blocs, laboratoires, pharmacie — avec des règles de flux strictes et auditées.

EDR, SOC et SIEM

Visibilité en temps réel sur les endpoints et les événements de sécurité — un prérequis opérationnel, non une option.

Refonte PCA / PRA

Plans révisés à la lumière de l'expérience vécue. Scénarios réalistes, rôles clarifiés, exercices réguliers intégrés.

Message fort : La cybersécurité n'est plus une ligne de support technique — elle devient un sujet de **direction générale**, avec les arbitrages budgétaires, les responsabilités et la visibilité que cela implique.

21

ENSEIGNEMENTS

Quatre vérités de terrain

Une cyberattaque hospitalière est une crise du soin autant qu'une crise informatique. Ces vérités, forgées dans l'épreuve, ne s'apprennent pas dans les manuels.

01 — Une crise du soin

Chaque minute d'indisponibilité se traduit par des décisions cliniques prises dans l'incertitude. L'enjeu : la continuité du soin et la dignité des patients.

02 — Le mode dégradé, un art collectif

Ce n'est pas une procédure dans un classeur. C'est une culture qui s'apprend ensemble. Les équipes qui tiennent sont celles qui se connaissent avant la crise.

03 — PCA & PRA : d'abord humains

Un plan parfait sur papier ne vaut rien si les équipes ne l'ont jamais exercé. La dimension humaine est le facteur critique de succès.

04 — Protéger le SI, c'est soigner

La sécurité du système d'information n'est pas une contrainte bureaucratique — c'est une condition de la mission de soin.

22

CLÔTURE

Une crise devenue apprentissage

« J'avais écrit une thèse sur la continuité des soins sous cyberattaque ; un mois plus tard, l'hôpital m'a demandé de la vivre. »

Ce que nous avons traversé doit devenir transmissible — documenté, analysé, partagé sans filtre avec la communauté hospitalière.

Résilience
Se construit **avant** la crise, pas pendant

Collectif
Première ligne de défense

Gouvernance
La cybersécurité est une responsabilité de direction

Mémoire
Chaque incident est un héritage à transmettre

23

✓ ATTAQUE DÉJOUÉE

« Opération échouée !
Aucune rançon versée !
Face à la crise, la solidarité et la résilience des équipes ont permis de poursuivre la mission première : soigner. »

24

L'Éclairage Anthropologique

Judith Nicogossian

Docteur en Anthropologie — Spécialiste des dynamiques collectives en situation de crise

Elle observe ce que les tableaux de bord ne montrent pas : les micro-réglages, les solidarités informelles, les rites de stabilisation.

Une grille de lecture inédite

La crise n'est pas seulement une chaîne de décisions rationnelles. C'est une **expérience humaine partagée**, traversée par des peurs, des alliances et des gestes de soutien.

Dans une crise cyber hospitalière, l'humain n'est pas un facteur périphérique — il est le cœur battant de la remédiation.

- Coordinations hors protocole
- Rites de passage informels
- Figures de référence spontanées
- Construction collective du sens

ANTHROPOLOGIE DE LA CRISE

Voir les gestes et les liens

Là où le regard gestionnaire cherche des indicateurs, l'anthropologie observe des **pratiques**. Ce sont les pratiques informelles, situées, relationnelles qui font tenir l'organisation.

Coordinations informelles

Routines improvisées

Formes d'entraide

Construction du sens

La résilience n'est pas seulement une question de sauvegardes ou de pare-feux — elle est une affaire d'alliances concrètes autour du patient.