Cybersécurité, à qui la faute ?

Journée APSSIS, Paris

28 septembre 2023

relyens

GROUPE MUTUALISTE EUROPÉEN
ASSURANCE ET MANAGEMENT DES RISQUES

Enjeux

Regard juridique sur la notion de faute en cas de cyberattaque

En lien avec la personne morale

- Le paiement d'une rançon

A l'initiative de patients

- La fuite des données imputable à l'établissement ?

A l'initiative du personnel

- Impacts individuels par la cyberattaque ?

Stratégie de défense pour un établissement mis en cause

Régime juridique de **faute présumée**

Constitution du dossier de défense (1) :

- En amont de l'incident : preuve de l'adéquation des mesures de sécurité dans le traitement des données

- Au moment de l'incident :
  - Détection rapide
  - Mise en œuvre sans tarder des mesures permettant de limiter la propagation et les impacts

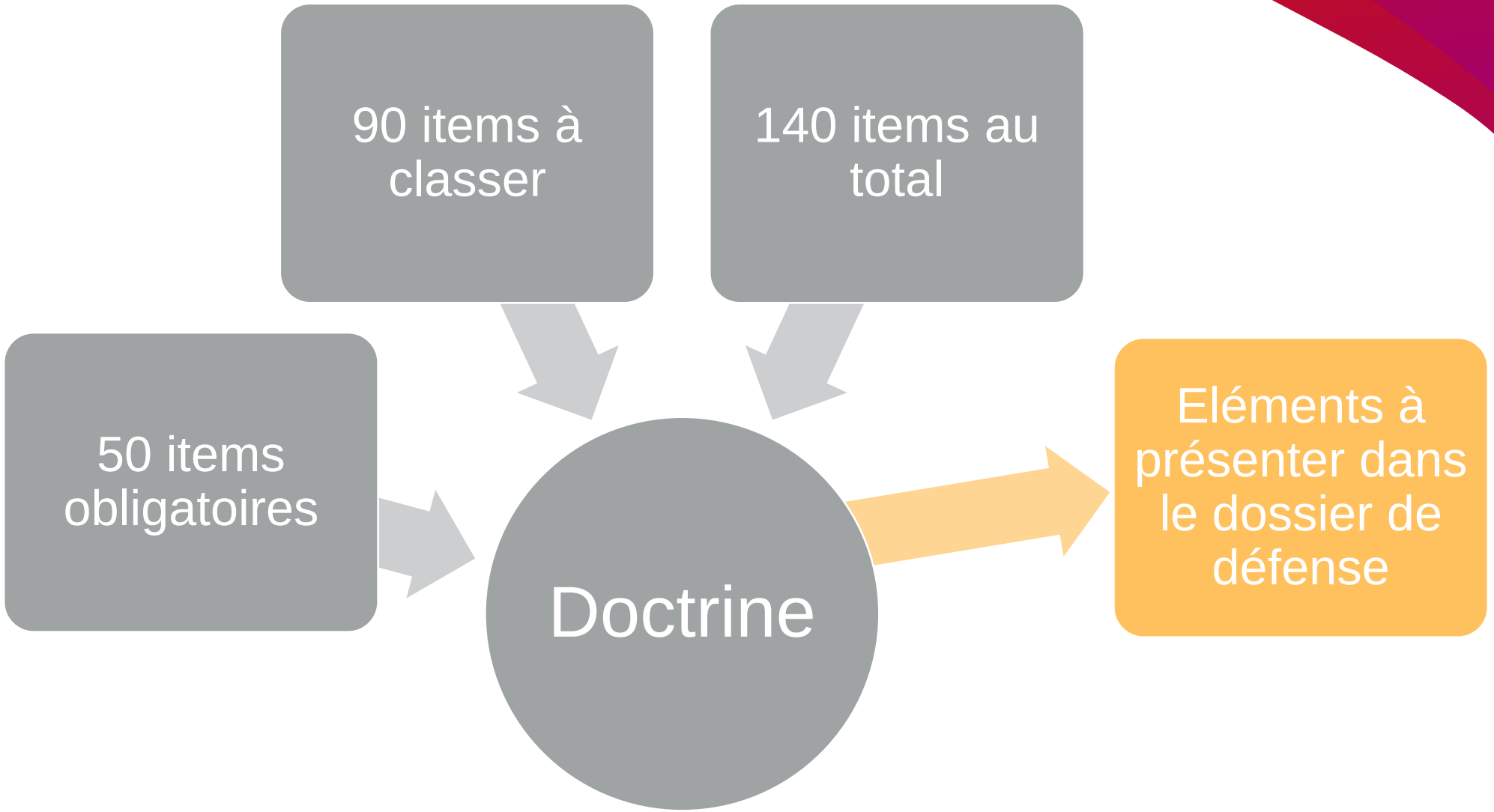
(1) sans certitude, à date, quant à l'appréciation que pourra faire un juge de ces éléments

Document de référence

Guide d'aide à la préparation numérique du Plan blanc
DGOS/PF/2023/94 du 15 juin 2023

- Opposable
- Applicable immédiatement
- France métropolitaine et certains territoires Outre-Mer
- Diffusion par les ARS auprès des Directeurs d'établissements de santé
- Ne concerne pas les ESMS (constitution d'un « Plan bleu » en cours)

Introduction



01

En amont : mon organisation est-elle bien préparée ?

Partie 1 : Prévenir le risque numérique
Chapitre 1 : Maîtriser son système d'information

Disposer des ressources humaines pour sécuriser le système d'information	Désignation d'un responsable de la sécurité du système d'information	OBLIGATOIRE	
	Sensibilisation forte lors de l'accueil des nouveaux arrivants	OBLIGATOIRE	
	Affichage permanent des principales recommandations en matière de « prise en compte des éléments de sécurité » dans les services	OBLIGATOIRE	
	Ensemble des actifs matériels, logiciels métiers, prestataires et services, ainsi que ceux en lien avec la chaine d'approvisionnement numérique	OBLIGATOIRE	
L'analyse de risques	Associer un facteur de criticité aux applications métier et définir une durée maximale d'interruption admissible	OBLIGATOIRE	
	Prendre en compte les droits spécifiques pour les fournisseurs, pour anticiper la compromission de la chaine d'approvisionnement	OBLIGATOIRE	
	Accorder son attention aux opérateurs de télémaintenance ayant accès par des réseaux publics	OBLIGATOIRE	
	Etablir une politique de sauvegarde particulière pour l'annuaire	OBLIGATOIRE	

Partie 1 : Prévenir le risque numérique
Chapitre 2 : Formaliser un plan de mise en conformité adapté

Les directives NIS	La directive NIS a été transcrite en droit national, et est applicable aux 135 établissements supports de GHT depuis mai 2018	OBLIGATOIRE	
La PSSI	Rédaction d'un document de PSSI, celle-ci étant opposable	OBLIGATOIRE	
	Prise en compte de l'instruction « 309 » pour la rédaction de la PSSI	OBLIGATOIRE	
	Prise en compte du document ANS « PGSSI-S » pour la rédaction de la PSSI	OBLIGATOIRE	
23 règles de sécurité spécifiques aux OSE	Application de 23 règles ANSSI au système d'information essentiel (arrêté du 14 septembre 2018)	OBLIGATOIRE	
	Désigner un point de contact avec l'ANSSI	OBLIGATOIRE	
	Déclarer les systèmes essentiels à l'ANSSI (décret du 23 mai 2018)	OBLIGATOIRE	
	Notifier à l'ANSSI les incidents cyber apparus sur le système d'information essentiel	OBLIGATOIRE	
Maîtrise des accès et mots de passe	Renouvellement des mots de passe utilisateurs et administrateurs tous les 6 mois	OBLIGATOIRE	
Protéger la messagerie pro	Sensibilisation à l'usage de la messagerie	OBLIGATOIRE	

Partie 2 : Elaborer le volet numérique
Chapitre 1 : Les modalités de mise en œuvre

Les plans régionaux	Répondre aux sollicitations de l'ARS dans le cadre du plan ORSAN régional, y compris suite à des évènements de cybersécurité	OBLIGATOIRE	
	Intégrer le cyber dans le plan de gestion des tensions hospitalières niveau 1 (mobilisation interne)	OBLIGATOIRE	
	Intégrer le cyber dans le plan de gestion des tensions hospitalières niveau 2 (plan blanc)	OBLIGATOIRE	
La gestion des tensions hospitalières	Décrire les étapes à suivre en cas d'activation du PCA	OBLIGATOIRE	
	Décrire les étapes à suivre en cas d'activation du PRA	OBLIGATOIRE	
	Prévoir des critères de déclenchement du plan blanc numérique	OBLIGATOIRE	
Confidentialité du volet numérique	Limiter la diffusion des éléments du plan blanc en interne et en externe, en particulier pour les OSE	OBLIGATOIRE	
La cellule de crise : action et opérations	Création d'un niveau décisionnel impliquant la Direction Générale, le RSSI, le président de CME, le directeur médical de crise	OBLIGATOIRE	
	Création d'un mode de communication pour l'échange des informations en temps réel pour les acteurs de la cellule de crise	OBLIGATOIRE	
	Création d'un niveau opérationnel impliquant les biomed, services généraux, services informatiques	OBLIGATOIRE	
	Tenue d'un journal de crise horodaté et signé	OBLIGATOIRE	

Partie 2 : Elaborer le volet numérique
Chapitre 1 : Les modalités de mise en œuvre

	Communiquer en permanence avec le SAMU-Centre 15 et l'ARS	OBLIGATOIRE	
La logistique en situation de crise	Prévoir des moyens réservés à la cellule de crise (lien internet, postes de travail, édition papier de l'annuaire tél)	OBLIGATOIRE	
	Rappel de l'interdiction de communiquer des informations médicales ou secret professionnel via des canaux non sécurisés	OBLIGATOIRE	
Stockage stratégique mutualisé	Disposer de matériels facilement accessibles et mobilisables 24/7	OBLIGATOIRE	
	Gestion de crise, renvoi vers le guide ANSSI et kits d'exercices	OBLIGATOIRE	
Préparer la communication	Se préparer à communiquer avec les média et réseaux sociaux, organes de tutelle, et grand public	OBLIGATOIRE	
Mobilisation des ressources techniques expertes	Disposer d'une équipe technique mobilisable dès les premières heures des incidents	« IL S'AGIT DE »	
Signalement interne d'une anomalie	Mettre en place une procédure de signalement	NÉCESSAIRE	

Partie 3 : L'organisation des soins
Chapitre 1 : L'impact sur l'organisation des soins

Procédures documentées hors du système d'information	Préciser les niveaux de ressource et services minimum indispensables	OBLIGATOIRE	
	Cahiers de mesures opérationnelles imprimés et distribués dans les services	OBLIGATOIRE	
Le DPI	Solution dégradée via un ordinateur de secours, synchronisé périodiquement, et muni d'une imprimante locale	OBLIGATOIRE	
Le « PC de sauvegarde »	Poste de travail dédié, autonome, et immédiatement accessible aux soignants	OBLIGATOIRE	
Sécurisation des communications des SAS et SAMU-Centre 15	Etablir une solution téléphonique de secours entre le centre 15 et certains « grands » services de soins	OBLIGATOIRE	
Soins critiques : réa, soins intensifs, soins continus	Permettre une restauration rapide en cas d'avarie, concernant les plans de soins, dossier patient	OBLIGATOIRE	
La pharmacie à usage intérieur	Disposer de sauvegardes déconnectées du réseau	RECOMMANDÉ	
	Disposer d'accès Internet de secours et messagerie	« IDEALEMENT »	

02

Au moment de l’incident : mon organisation sait elle faire face ?

Partie 2 : Elaborer le volet numérique
Chapitre 1 : Les modalités de mise en œuvre

Etapes à suivre lors d'un incident	Pouvoir mobiliser une expertise adaptée à l'ampleur de l'incident	OBLIGATOIRE	
Conservation des preuves, plainte, rançon	Collecter des preuves concernant les systèmes attaqués	NÉCESSAIRE	
	Valeur probante des éléments de journalisation collectés	POTENTIEL	

Partie 2 : Elaborer le volet numérique
Chapitre 2 : Les éléments généraux à préparer

Sécuriser le système d'information au plus tôt	Dès l'incident confirmé, confiner la partie saine du système d'information	NÉCESSAIRE	
Cadre réglementaire du signalement	Rappel des obligations de signalement aux différentes autorités (ARS, CERT-FR, CERT-SANTE, CNIL …)	OBLIGATOIRE	

Partie 2 : Elaborer le volet numérique
Chapitre 3 : Se préparer aux étapes à suivre

Qualification de l'incident	Savoir identifier les systèmes corrompus	OBLIGATOIRE	
	Rappel de l'obligation d'effectuer des exercices pour déterminer les systèmes corrompus	OBLIGATOIRE	
Détecter et reconnaître une perturbation informatique	Mettre en place un monitoring des usages « anormaux » des ressources techniques	RECOMMANDÉ	
Intégrité des sauvegardes	Vérifier l'atteinte aux sauvegardes (intégrité)	? S'ASSURER QUE ?	
	Vérifier sil y a eu exfiltration de données par atteinte aux sauvegardes	? S'ASSURER QUE ?	
	Rappel de l'obligation d'effectuer des exercices pour vérifier les sauvegardes	OBLIGATOIRE	
Confinement des zones affectées	Déconnexion « brutale » du réseau dans l'intérêt des patients	AUTORISÉ	

Partie 2 : Elaborer le volet numérique
Chapitre 3 : Se préparer aux étapes à suivre

Fonctionnement en mode dégradé	Mesures de contournement en mode temporairement dégradé	OBLIGATOIRE	
Eradication par correction des vulnérabilités	Les opérations d'éradication des codes malveillants sont effectuées sous validation du RSSI	NECESSAIRE	
	Etape de durcissement de la sécurité consécutive à l'étape d'éradication, voire remplacement si le système compromis est obsolète	NECESSAIRE	
Utilisation des sauvegardes en phase de restauration	Bonne pratique de déconnecter les sauvegardes du réseau (ou protection équivalente)	OBLIGATOIRE	
	Rappel de l'obligation d'exercices de restauration à partir de sauvegardes	OBLIGATOIRE	
Arbitrer la sortie de crise	Capacité à arbitrer	« IL S'AGIT DE »	
Effectuer un RETEX rapide	Dès la sortie de crise	OBLIGATOIRE	

03

Et après ?

Conclusion

C’est tout un programme fourni qui est présenté dans ce document

L’effort organisationnel et financier consécutif est considérable

Sa mise en œuvre doit se conduire sur plusieurs années

Nos recommandations

Implémentation en mode projet

- « Gap analysis »
- Priorisation des chantiers (« quick wins »)
- Planification et suivi des déploiements

Outillage adapté

- Traçabilité des déploiements des chantiers de prévention
- Traçabilité des actions effectuées en situation de crise
- Valeur probante et garantie de disponibilité

Relyens, Groupe mutualiste européen en Assurance et Management des risques, agit au quotidien auprès des acteurs de la Santé et des Territoires pour sécuriser leur activité et garantir la continuité et la qualité de leur mission d'intérêt général, au bénéfice des patients et des citoyens.

Depuis presque 100 ans, nous créons et tissons le lien qui nous unit avec nos parties prenantes pour avancer, ensemble, dans un monde où la confiance se nourrit, se partage, se transmet et se mutualise.

Maîtriser les risques, mutualiser la confiance.®

Siège social
20, rue Édouard Rochet
69372 Lyon Cedex 08 – France
Tél : +33 (0)4 72 75 50 25

relyens.eu

Christophe MILLET
Risk Manager Cyber
Christophe.millet@relyens.eu

relyens
GROUPE MUTUALISTE EUROPÉEN
ASSURANCE ET MANAGEMENT DES RISQUES