Transformation numérique et sécurité (en santé)

Philippe TOURRON

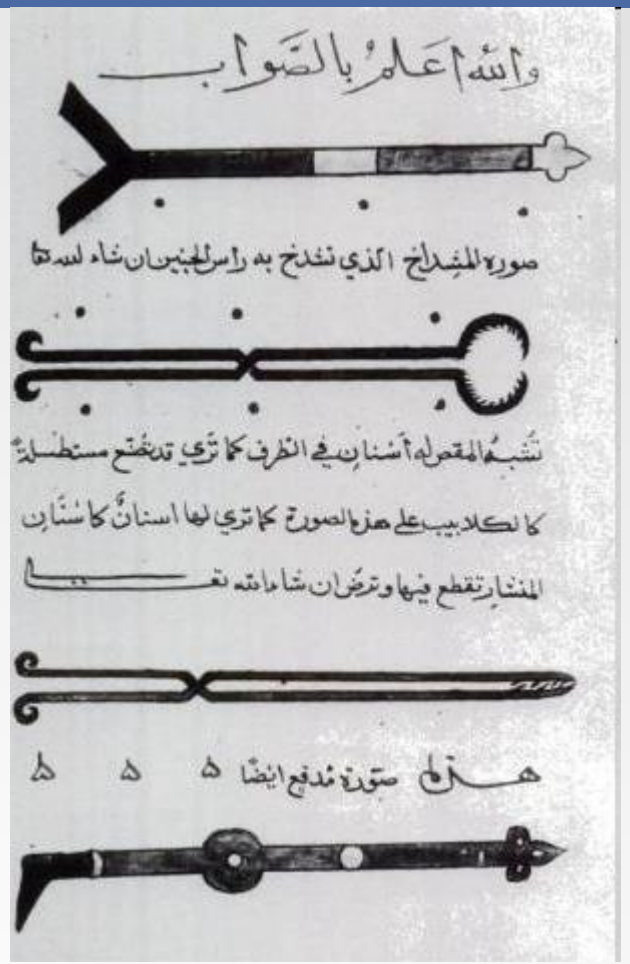
RSSI-APHM

PLAN

1. Permettre les **usages numériques** ou comment l'hôpital peut-il devenir numérique ? les nouveaux usages sont déjà là nous devons les accompagner voire les précéder.
2. Les **technologies** apportent des solutions, les règlementations des contraintes, comment trouver le bon équilibre ?
3. Mais le numérique c'est aussi de nouveaux dangers : Protéger les données des patients semble une évidence, analyser les **risques**, mettre en place des protections pour limiter les menaces (anciennes et nouvelles)
4. La sécurité : **une valeur ajoutée**

CONTEXTE

L'évolution des pratiques du monde santé / social



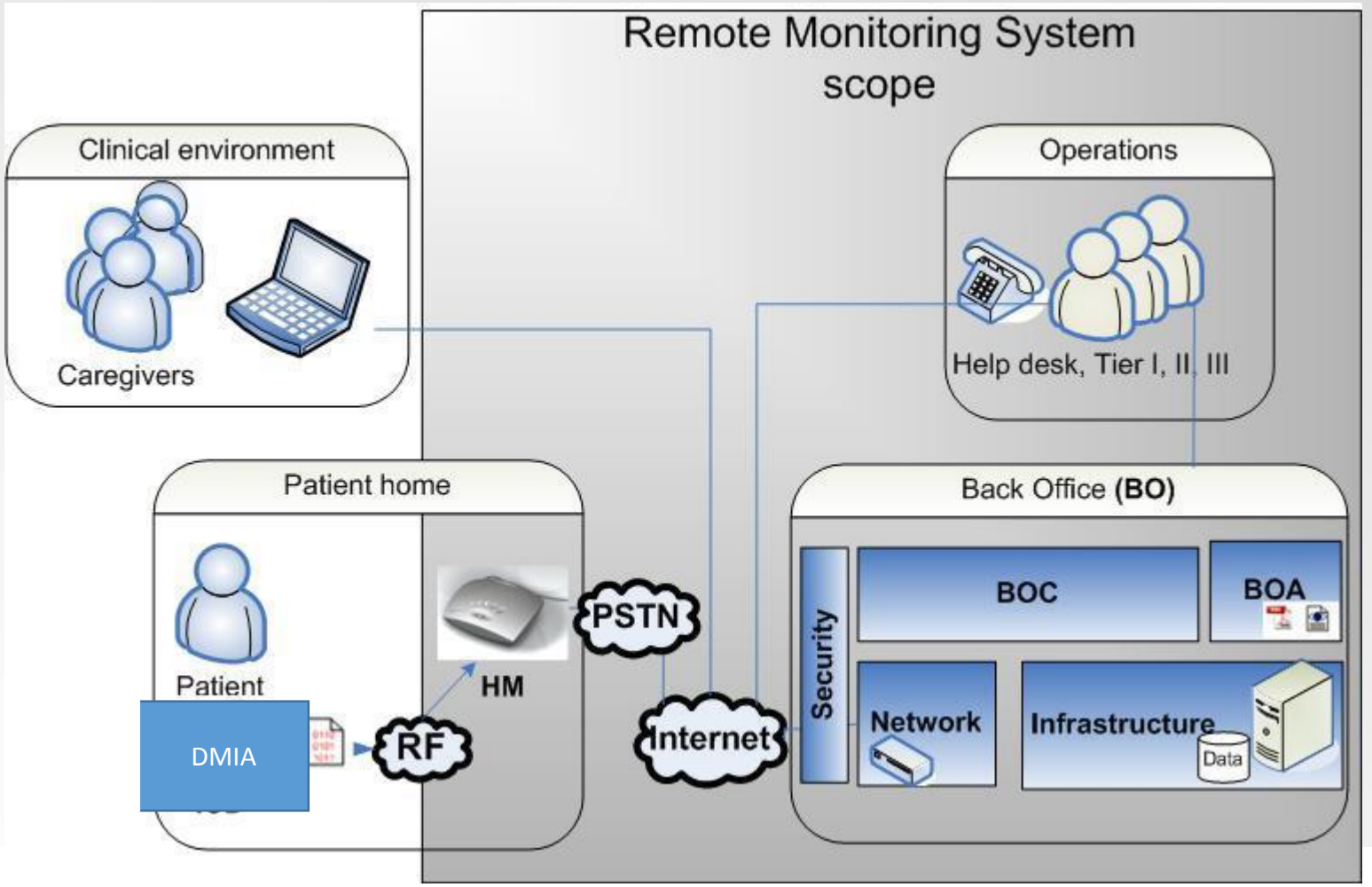
Instruments chirurgicaux dans l'encyclopédie médicale du XIe siècle du médecin musulman médiéval Abulcasis : *Kitab al-Tasrif*

DPI

Commençons par un exemple du numérique de santé réparti

Le patient connecté Exemple simplifié

Le patient connecté Exemple d'architecture



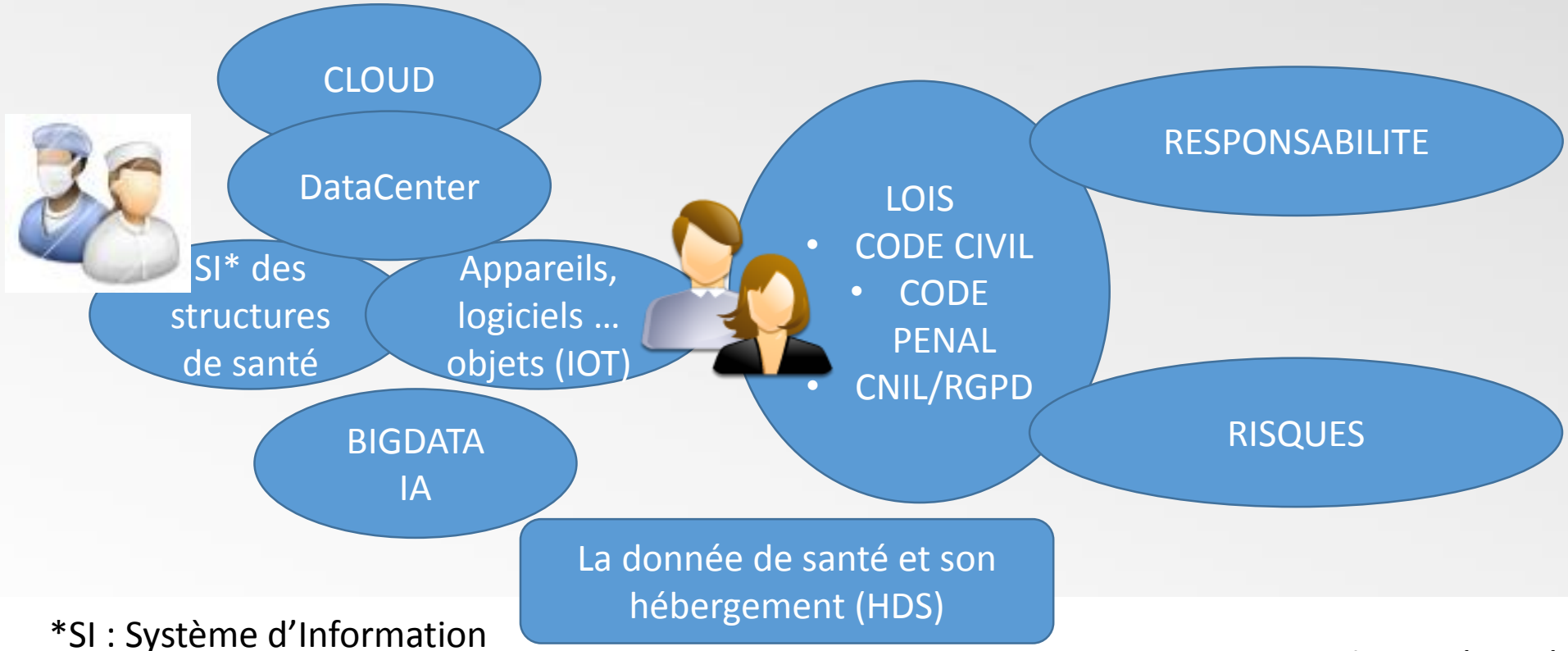
Une tendance de société : les objets connectés … de santé

- La Cnil distingue les objets de « confort » des objets de santé

- Les DMIA : besoin de surveillance
- Passer de rdv tous les 6 mois à un suivi … Temps réel
- La technologie apporte des réponses
- Connectivité sans fil, 3G-4G, Box internet, …

Contexte numérique en santé

Capter, stocker, traiter, communiquer des données



*SI : Système d'Information

Nouveaux usages

Pour les professionnels de santé :

- Dématérialisation interne et dans la communication externe
- Mobilité dans l'hôpital
- Mobilité hors hôpital

Et pour les patients :

- Accès des patients au SI : Portail
- Prise de rdv
- Rappel rdv par sms
- Services numériques dans l'hôpital

➢ **Augmentation de la valeur de la donnée de santé**

➢ **La transformation numérique augmente aussi la surface de vulnérabilité**

Nouvelles technologies

- Virtualisation
  - Serveurs
  - postes
- Cloud privé, public, hybride
- Identité numérique
- Authentification forte
- Intelligence Artificielle
- Objets connectés
- Big data

Facteur d'évolution : GHT et CONVERGENCE

- Pour les architectures (réseaux, datacenter, postes, …)
- Les applications, les services
- Les équipes

- Facteurs de réussite
  - L'entraide, le partage, la cohérence
  - Les standards (ITIL, ISO27001, ISO9001, HDS)
  - L'EAI (IHE) interopérabilité

- … Manager les systèmes et leur transformation numérique

POURQUOI
PROTEGER LES DONNEES DE SANTE ?

CONTEXTE

LES CYBER-ATTAQUES EN RECRUDESCENCE EN 2016

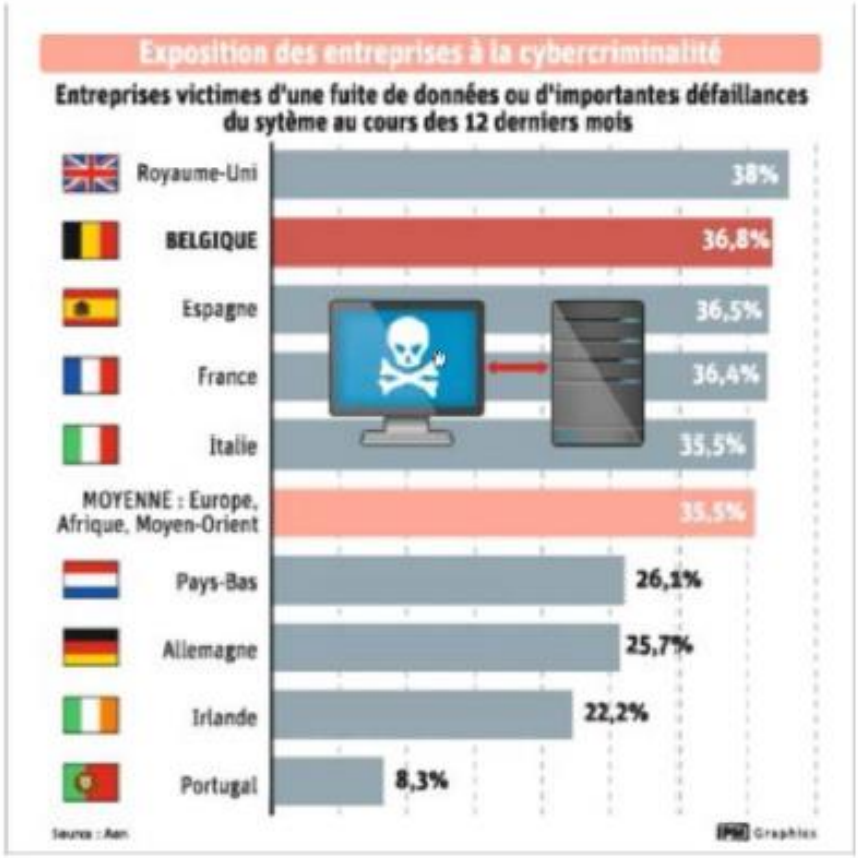
80%*

Des entreprises ont constaté au moins une cyber-attaque sur les 12 derniers mois

DDoS x 2
(vs. 2015)

12 mai 2017
27 juin 2017
CYBERATTAQUES MONDIALES

150 pays touchés
200 000 victimes



RÉGLEMENTATION DÉDIÉE EN HAUSSE

ANSSI

PROJET DE LOI DE PROGRAMMATION MILITAIRE 2014 / 2019

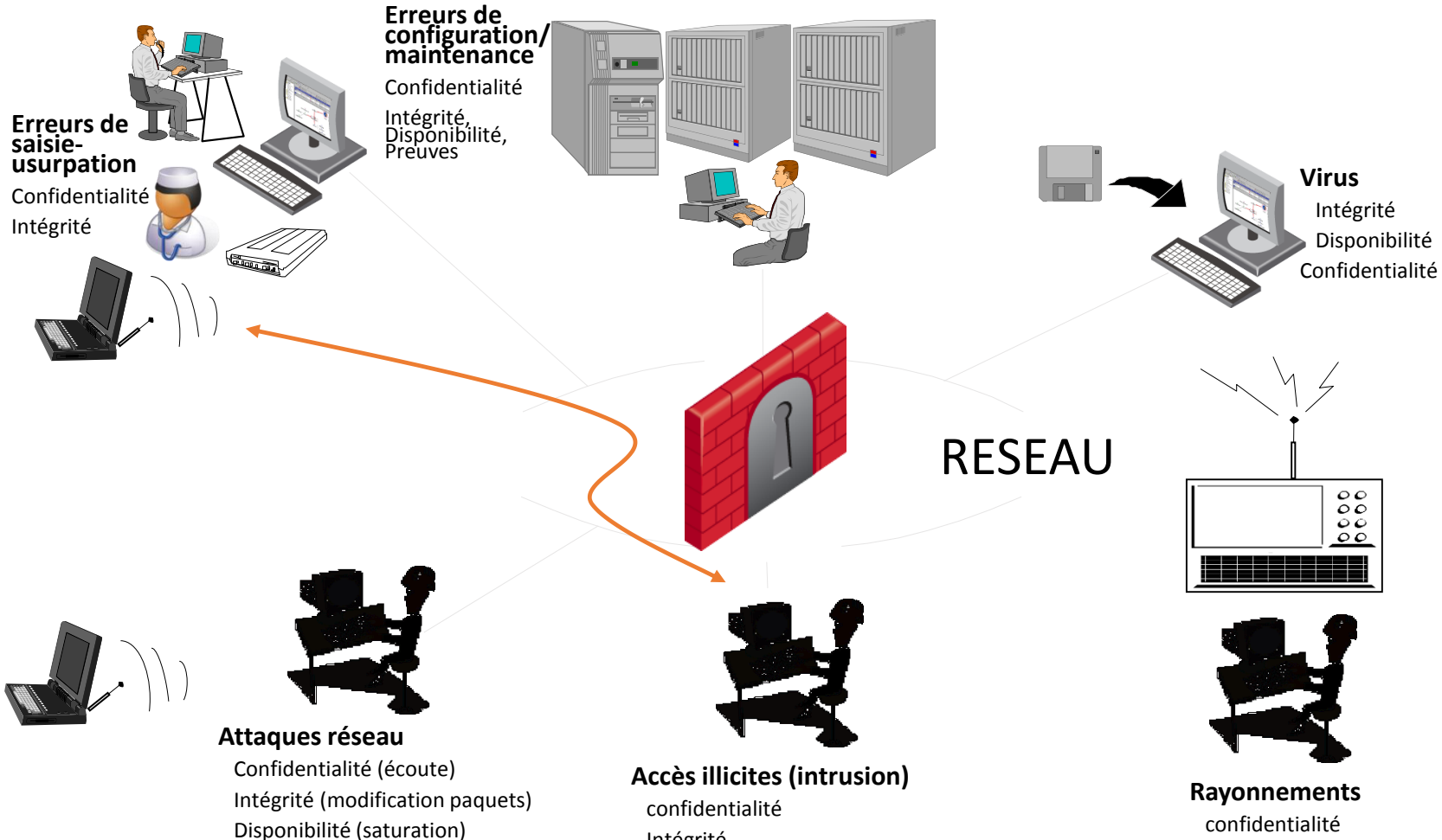
General Data Protection Regulation

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

* source baromètre CESIN de janvier 2017
** source étude Kaspersky 2016

Atteintes au SI : Comment ?

La sécurité des systèmes informatiques



Les avantages et/mais risques des Nouvelles technologies

Nouvelle techno	Avantages	Risques
Virtualisation	scalabilité, rapidité de mise en oeuvre	complexité/compétences
Cloud	OPEX, débordement vers cloud externe à la demande, indépendance/matériel	Réversibilité, dépendance fns et internet (ext), ne pas choisir le bon niveau de sécurité
Authentification forte	Sécurité des accès	Difficulté d'usage
Intelligence Artificielle	Produire de nouvelles données : générer de la valeur, aide à la décision	Perte du contrôle, de la conformité par croisement de données
Objets connectés	Nouvelles informations, nouveaux services services, accessibilité	Failles accès et données

Contexte : Sécurité numérique

Enjeux majeurs : protéger les patients

- Leurs soins, leur « santé »
- Leurs données
  - **Disponibles**
  - **Intègres**
  - **Confidentielles**
  - **Auditables**
- **Freins à la sécurisation : 30% budget, 30% absence de prise de conscience des risques, 40% (divers : applications, hétérogénéité, …)**

Le périmètre ?

- Les logiciels (du DPI au portail patient)
- Les infrastructures (des serveurs au pilotages de l'électricité), cloud …
- Les moyens médicaux techniques (de l'ECG à la l'IOT de santé)

-> dans l'établissement/l'entreprise

-> Et au-delà

Pourquoi protéger : la confiance

Garantir la confiance dans le SI pour les patients et pour les professionnels

Quels événements redouter ?

- Pour le patient (RGPD)
  - Ne pas être «connu»
  - Etre « reconnu », vie privée
  - Perte de chance au soin
  - Ne pas disposer de ses informations
- Pour l'établissement ou l'entreprise
  - perdre toutes les données,
  - perdre l'intégrité des données patients,
  - bloquer l'activité pendant plusieurs jours /heures
  - diffuser anormalement les données patients (sur internet, …)
  - Ne pas être conforme (HAS, certification des comptes, CNIL/RGPD, instruction DSIS 309,… PSSI-MCAS, RGS, …)

Comment protéger : Sécurité numérique

Et si finalement tout convergeait vers …? une vision de la cible à atteindre, un cadre prêt et « relativement constant », une légitimité : la gestion par les risques

Un système de management de la sécurité du SI : conformité/certification ISO27001

Pourquoi protéger : aspect Sécurité numérique

Un système d'information pour l'ouverture et la mobilité : L'attractivité pour les patients, les professionnels de santé, le lien ville-hôpital, l'intégration du numérique au quotidien

- Le mariage difficile de la disponibilité et de la confidentialité devient ainsi un enjeu stratégique.
- **Un contexte de cybermenaces en hausse (rançon, revente, …)**

- **Minimiser les causes et les impacts des risques SI : manager le sécurité**

La logique de Système de Management

SECURISER

C'est

MANAGER

donc

GOUVERNER

Et au final

DECIDER LA PRISE DE RISQUE au bon niveau de responsabilité

Manager : revue régulière SSI et SDSI, sanctuariser des budgets

Les propriétaires de risques sont ceux qui peuvent les traiter

(prendre, éviter, réduire, transférer) cf ISO 27001:2013

COMMENT
PROTEGER LES DONNEES DE SANTE ?

Comment protéger : aspect Sécurité numérique

Les Freins :

- Manque de conscience des risques
- Changer
- Coûts
- prioriser

Les leviers :

- La règlementation/lois : HDS évolution vers une certification ; RGPD
- Les incidents (l'actualité) et La prise de conscience de la criticité du SI de santé sous tous ses angles (DI**C** … A)
- Les soutiens des structures nationales (HFDS/FSSI, ASIP, ANSSI, …) et des autres
- La prise de conscience de la criticité/valeur du SI et de la donnée personnelle
- Des label, normes (ISO 27001)

Les basics :

- Sauvegarde, chiffrement, protection/privacy by design
- Authentification renforcées, cloisonnement et filtrage des réseaux internes ET externes
- Sécurité physique
- La gestion de l'obsolescence/maintenance
- Charte utilisateur, mainteneur, PSSI, sensibilisation/formation …

- MAIS AUSSI SE PREPARER AU PIRE

La pédagogie de la CRISE

Gérer les crises = **Gérer les risques à grande vitesse**

- Identifier les scénarios de risques
- Améliorer-tester les PRA, les PCA
- Se préparer à l'imprévu
- S'organiser pour décider
- S'organiser pour (ré)agir … vite

Des rôles, un entrainement, des reflexes, des procédures

10 conseils de survie pour le SI

1. **Sauvegardes:** Vérifiez vos rétentions votre capacité et délai à les restaurer (existence de sauvegarde hors ligne) mais aussi … la sauvegarde des composants techniques critiques (AD, DNS, configurations, …)
2. **Gestion de crise :** entrainez les acteurs aux rôles et reflexes
3. **Data center :** vérifiez/testez courant secouru, climatisation, accès, matériels inflammables, système d'extinction incendie, conformité électrique
4. **Cloisonnement :** soyez prêts à isoler des parties de votre réseau et internet
5. **Accès internet :** surveillez les contournements de proxy
6. **Accès maintenance :** cloisonnez/tracez, séparez les remontées de monitoring de la prise de main à distance, surveillez les VPN
7. **Anti-menaces et mises à jour sécurité :** sortez du cercle de la qualification des applications, ajoutez des défenses périmétriques (matériels ou logiciels) notamment pour le périmètre médicotechnique
8. **Modes dégradés :** vérifiez leurs fonctionnements EN PRATIQUE et … la confidentialité
9. **Acquisition :** mettez vos conditions (exigences et recommandations pour tous les SI, référentiels ASIP, …)
10. **Comptes d'administration :** vérifiez régulièrement (leur nombre, individualisés, authentification renforcée, cloisonnement pour mel et web, traces d'accès et d'actions, alertes sur usages anormaux).

ENJEUX A VENIR

ENJEUX à venir : Sécurité du numérique de santé, des opportunités et une valeur ajoutée

La signature numérique, le chiffrement, l'authentification forte

La sécurité numérique : valeur ajoutée pour la confiance numérique

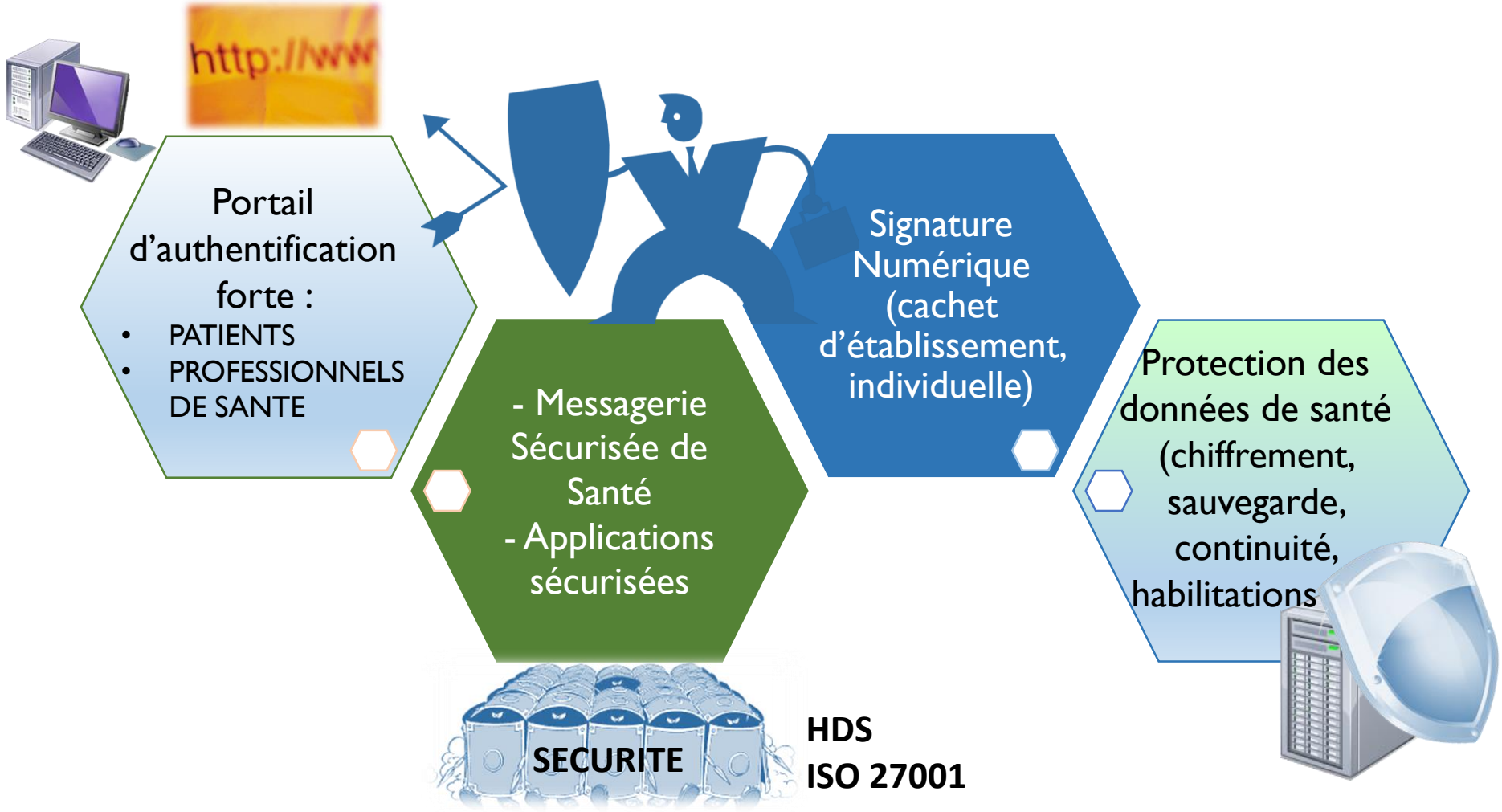
Rends possible (conformité/fiabilité) :

- **L'identité numérique** (pour l'accès aux données et aux dispositifs) pour les personnes, pour les logiciels, pour les appareils médicaux
- La dématérialisation : la preuve numérique
- La communication sécurisée (IOT, cloud, …)
- Les soins/télémédecine à distance

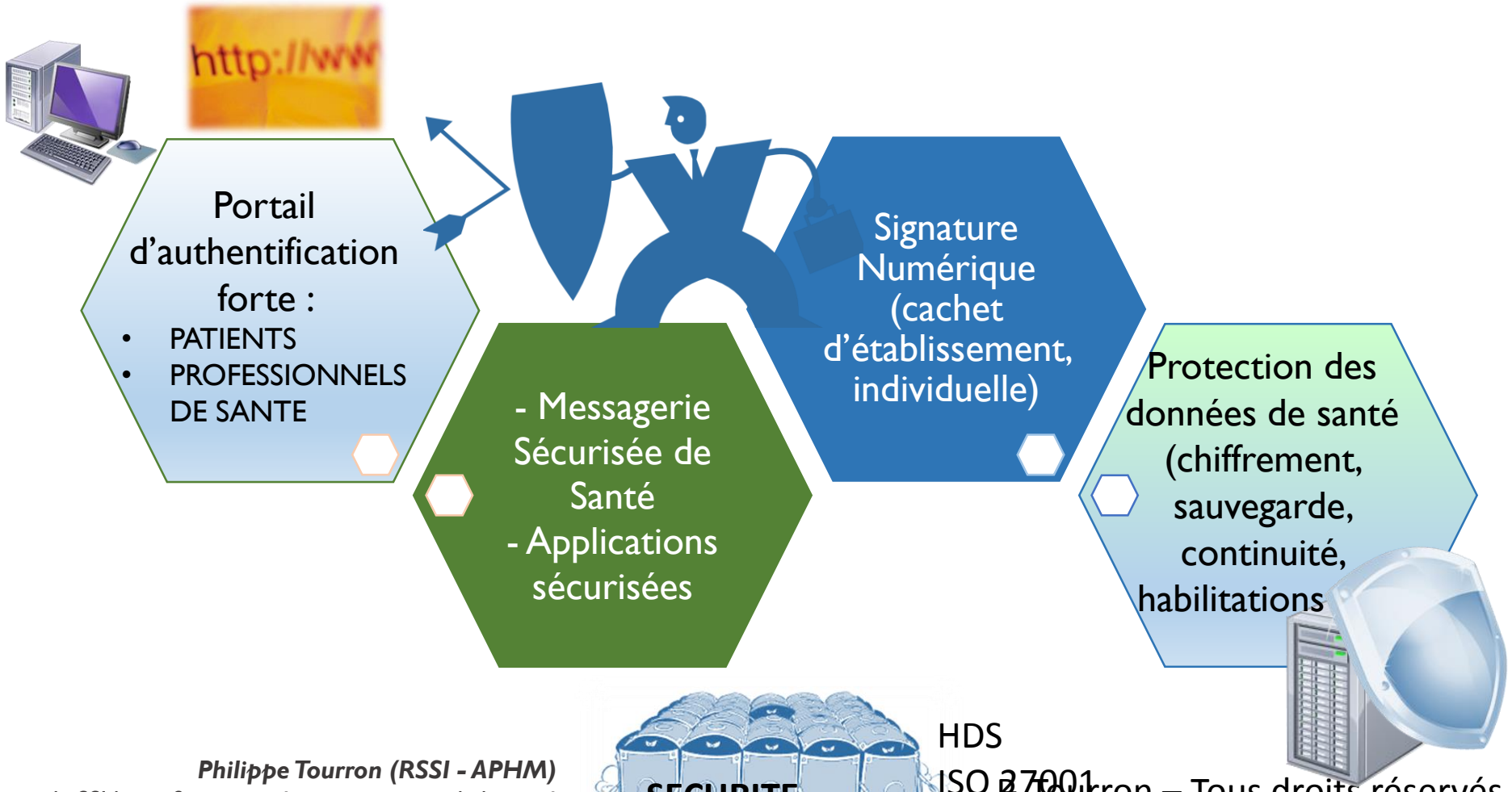
Enjeux pour l'avenir :

- Garantie du soin numérique
- Hébergements des données de santé communiquants
- Télémédecine
- Bigdata/opendata

Des opportunités de Sécurité du Système d'Information Pour La confiance numérique et la dématérialisation



Des opportunités de Sécurité du Système d'Information Pour La confiance numérique et la dématérialisation



MERCI DE VOTRE PARTICIPATION

DEBAT / QUESTIONS

PLAN INSTRUCTION DSSIS 309 : déclinaison

- Toutes les mesures organisationnelles : intégrées dans les démarches et certifications ISO 27001, 9001 (ITIL) et agréments HDS
- Passer en mode HDS pour les nouvelles applications
- Démarche d'homologation RGS
- Sensibiliser les utilisateurs : e-learning, formations aux nouveaux arrivants, au biomed, gestions des risques SI au plan de formation
- Charte utilisateurs au RI
- Inventaire (intégrant le biomed) et suivi des incidents et changements associés
- Augmenter le niveau et la finesse de filtrage avec les réseaux externes (ou interconnectés
- Protection des accès externes : mainteneur (bastion d'administration) et utilisateurs (portail d'authentification forte
- Segmentation réseaux et filtrage des réseaux internes : commencer par les zones sensibles (HDS, GTC, plateaux techniques biomed, composants non maintenus ou administrés par des tiers, …)
- Éliminer les systèmes obsolètes (ou les protéger)