Atelier sur l'EMR - Évaluation des risques et des menaces

29 avril 2022

Colloque annuel 2022

Forum étudiant d'échange et d'information en cybercriminologie

Plan de l'atelier

- Introduction
- Partie I: Phase d'identification et d'évaluation des biens
- Partie II: Phase d'évaluation des menaces
- Partie III: Phase d'évaluation des vulnérabilités
- Partie IV: Phase d'évaluation des risques
- Conclusion

Sources pertinentes

- *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33). Extrait de https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie
- *Méthodologie harmonisée d'EMR (TRA-1).* Extrait de https://cyber.gc.ca/fr/orientation/methodologie-harmonisee-demr-tra-1
- *NIST SP 800-60 Vol. 1 Guide for Mapping Types of Information and Information Systems to Security Categories.* Extrait de https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final
- *NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments*. Extrait de https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- *NIST SP 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management.* Extrait de https://pages.nist.gov/800-63-3/sp800-63b.html

ITSG-33 & Méthodologie harmonisée de l'EMR

ITSG-33

- Publié par le CST
- Axé sur la sécurité des TI
- Pas une méthodologie de EMR en soi, et non liée à une méthodologie spécifique
- But: aider les ministères à envisager dès le début les enjeux liés à la sécurité
- Catalogue de contrôles de sécurité
  - Technologie
  - Opérationnels
  - Gestion
- Approche axée sur le cycle de vie

EMRH

- Publié par le CST & la GRC
- Application générale:
  - Biens matériels
  - Biens TI
  - Protection des employés
  - Prestation de services
- Méthodologie de l'évaluation des menaces et des risques
- Approche statique

Introduction

- **Qu**'est-ce que le risque?
- **Pourquoi** évaluons-nous le risque?
- **Quand** devrions-nous évaluer le risque?
- **Comment** le risque est-il généralement formulé?

Qu’est-ce que le risque?

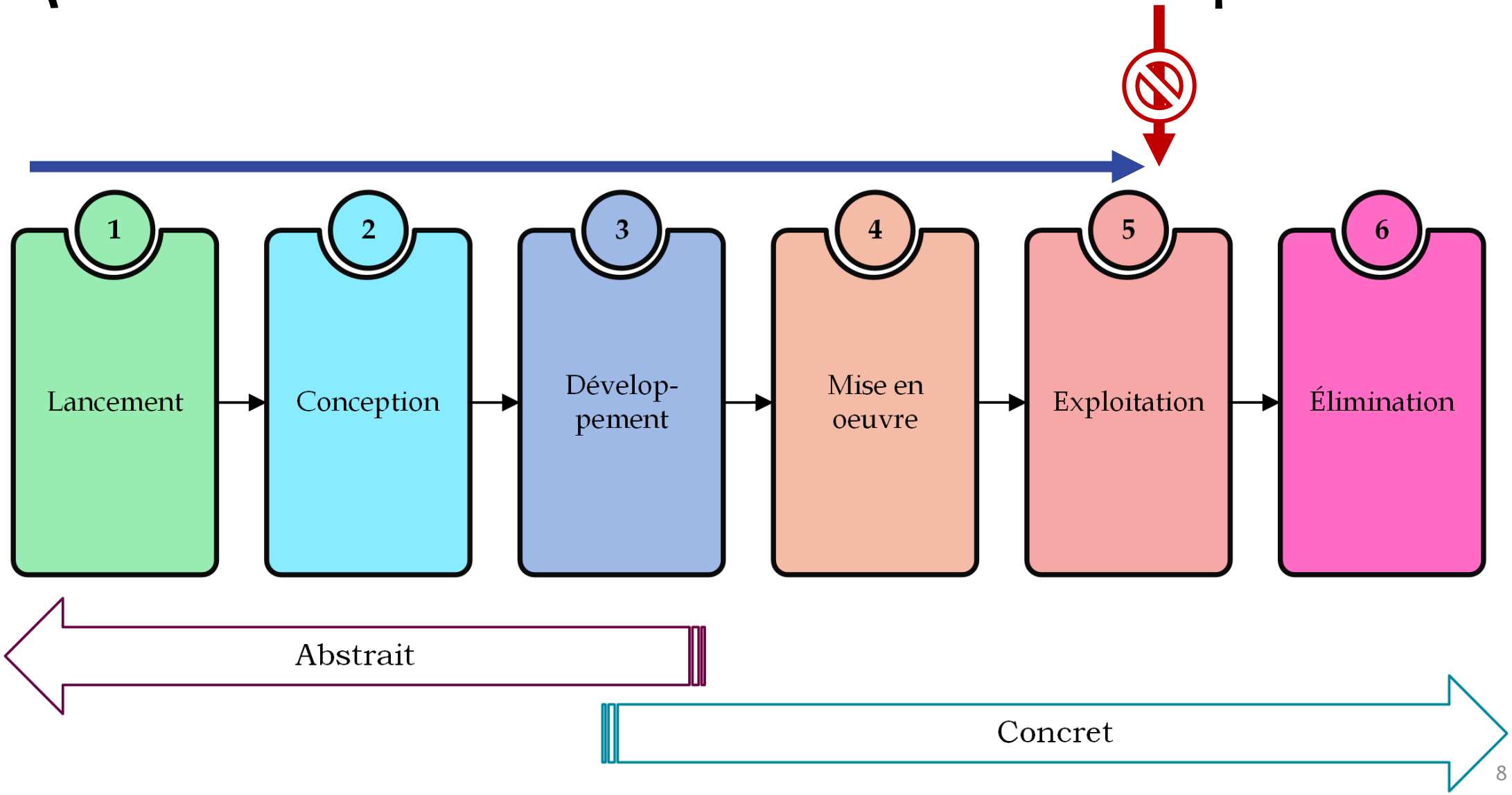
Sans contexte, le risque est un concept difficile à définir

- Larousse: possibilité, probabilité d’un fait, d’un événement considéré comme mal ou un dommage – danger, inconvénient plus ou moins probable auquel on est exposé
- Finance: le degré d’incertitude (et/ou de perte potentielle) inhérent à une décision d’investissement
- SST: probabilité qu'une personne subisse un préjudice ou des effets nocifs pour sa santé en cas d'exposition à un danger
- TI: possibilité qu’une *menace* donnée *compromette des biens de TI* et cause un *préjudice* (ITSG-33)

Pourquoi évaluons-nous le risque?

- Nous évaluons le risque dans le but de prendre des décisions
  - Le point de vue du *business owner*
- L'évaluation du risque fournit des informations supplémentaires pour appuyer une décision lorsque les objectifs sont concurrents et que les ressources sont limitées

Quand devrions-nous évaluer le risque?

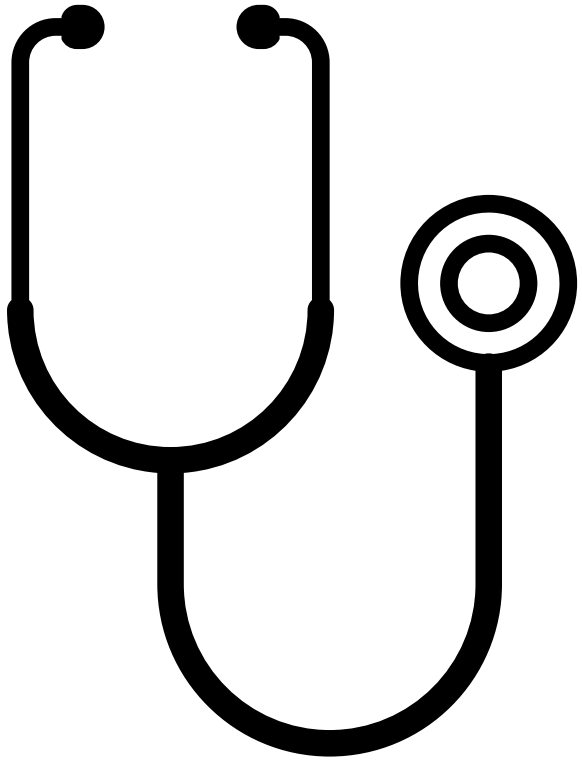


Comment le risque est-il généralement formulé?

$$R = f(B_{val}, M, V)$$

Scénario

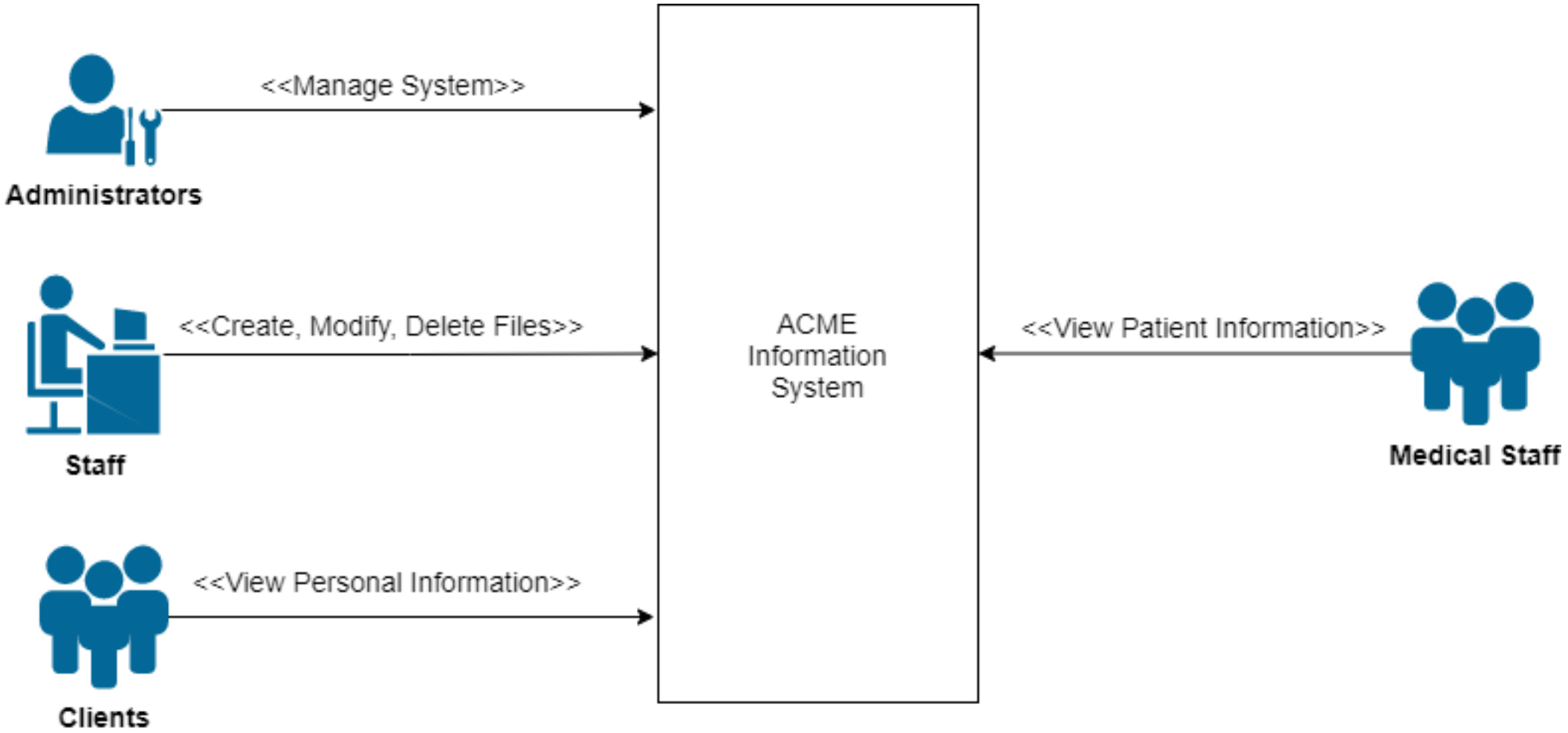
EMR d’ACME Services médicaux



Société ACME Services médicaux

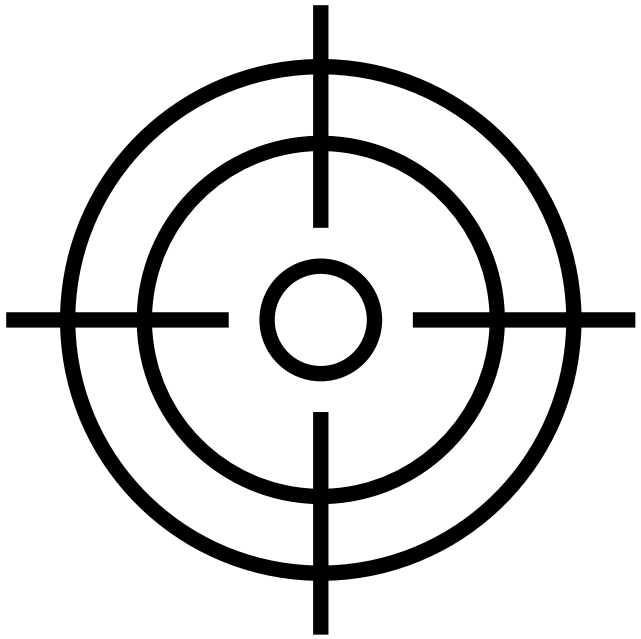
- ACME est une nouvelle société qui compte offrir des services de diagnostic et d'imagerie médicale et de prélèvements.
- Les services d'ACME seront soutenus par un système *cloud*
  - Les employés du laboratoire pourront inscrire les résultats des examens diagnostiques et les rendre disponibles au personnel médical dans diverses cliniques et hôpitaux.
  - S'ils le souhaitent, les individus (clients) pourront se connecter à la plateforme et être en mesure de consulter et de télécharger leur dossier médical.

Société ACME Services médicaux



Scénario – Société ACME Services médicaux

- Objectif de l'EMR :
  - Le C.A. veut s'assurer que les données personnelles sont protégées.
  - L'équipe de la sécurité a recommandé la mise en place d'un système d'authentification, pour tous les utilisateurs.
  - L'équipe de gestion souhaite connaître les alternatives ainsi que les risques associés avant d'engager les fonds.



Partie I: Identification et évaluation des biens

1. Quels sont les biens d'ACME?
2. Quelle est leur « valeur »?

$$R = f(B_{Val}, M, V)$$

Quelle est la valeur des biens?

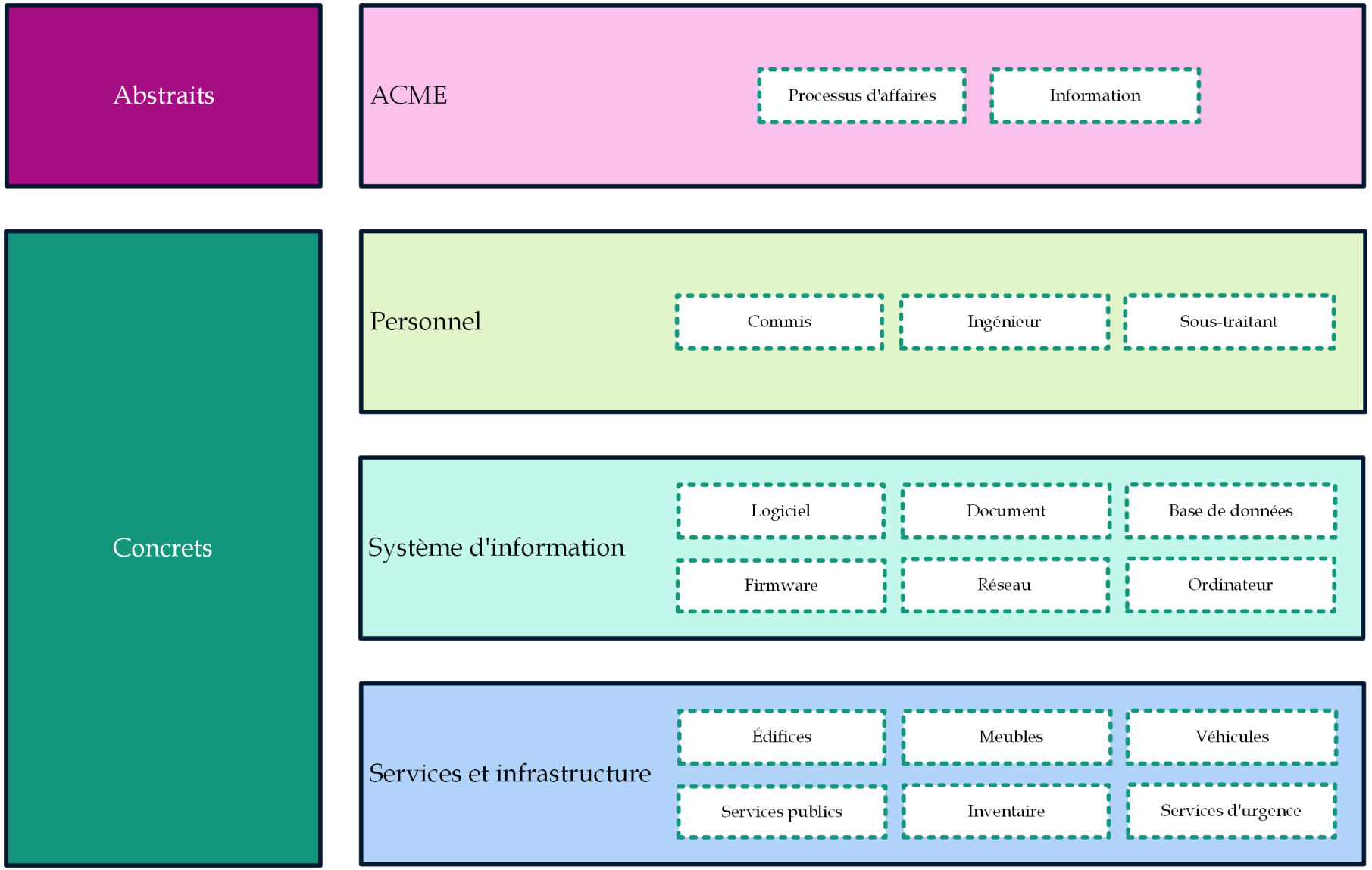
- Pourquoi est-ce que l'on se questionne sur la "valeur" des biens?
- Nous devrions nous poser cette question pour quelle classe de biens? Pourquoi ?
- Qui est la personne tout indiquée pour comprendre les impacts ou les conséquences d'un événement de menace contre une entreprise?
- Comment est-ce que la valeur peut être établie?

Quelle est la valeur des biens?

- L'approche adoptée pour déterminer l'impact d'une compromission des biens dépend de la méthodologie.
- Dans la méthodologie FAIR, tous les impacts sont déterminés en termes de valeur monétaire.
- Dans le EMRH du Gouvernement du Canada et dans le NIST 800-30, la valeur d'un bien est attribuée en fonction des préjudices qui pourraient vraisemblablement découler d'une compromission.
- Les préjudices sont évalués par rapport à la nation, aux individus, aux opérations, à d'autres organisations et aux biens tangibles.

Quelle est la valeur des biens?

- Le processus utilisé dans la version ITSG-33 de l'EMRH est la « catégorisation » et se base sur:
  - FIPS-199
  - NIST SP 800-60 Vol 1
- Dans ce processus, les préjudices sont évalués selon trois paramètres:
  - Confidentialité
  - Intégrité
  - Disponibilité
- Et selon cinq niveaux:
  - Très faible, Faible, Moyen, Élevé, Très élevé


Abstraits
ACME
Processus d'affaires
Information
Concrets
Personnel
Commis
Ingénieur
Sous-traitant
Système d'information
Logiciel
Document
Base de données
Firmware
Réseau
Ordinateur
Services et infrastructure
Édifices
Meubles
Véhicules
Services publics
Inventaire
Services d'urgence

Scénario ACME – Biens

- Vous êtes des parties prenantes d'ACME.
- L'analyste EMR vous a convoqué dans le but de l'aider à identifier les biens importants et de déterminer leur valeur.
- Au besoin, un analyste d'affaires est disponible pour apporter son soutien en identifiant les activités organisationnelles de haut niveau.

Scénario ACME – Biens

Bien	Description
Examens diagnostiques (Processus)	Le processus de réalisation des examens. Le système ACME reçoit les informations concernant les tests ainsi que les rapports.
Résultats diagnostiques (Information)	Information connexe: radiographies numériques, rapports d'échographies, etc.
Inscription de nouveaux clients (Processus)	Le processus d'enregistrement de nouveaux clients dans le système ACME.
Informations personnelles et bancaires des clients (Information)	Information connexe: Les informations personnelles du patient (client), incluant les coordonnées, les informations de paiement telles que les cartes de crédit et informations bancaires

Scénario ACME – Valeur des biens

- Par exemple, ITSG-33 utilise ce *cadre* de catégorisation pour évaluer la "valeur" des biens, en termes de préjudice organisationnel
- Nous devons créer un tableau qui identifiera les "préjudices" causés à ACME, ainsi que la signification du niveau de ces préjudices

Type de préjudice	Description et niveau				
	Très faible	Faible	Moyen	Élevé	Très élevé
Agitation ou désordre civil	Préjudice négligeable ou aucun préjudice raisonnable prévu	Désobéissance civile, entraves publiques	Émeute	Actes de sabotage à l'égard de biens essentiels (p. ex. infrastructure essentielle)	Émeute générale ou actes de sabotage nécessitant l'imposition de la loi martiale
Préjudice physique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort physique	Douleurs physiques, blessures, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
Préjudice psychologique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress	Détresse, traumatisme psychologique	Maladie mentale ou physique	Traumatisme psychologique généralisé
Perte financière pour des particuliers	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress ou inconfort	Incidence sur la qualité de vie	Sécurité financière compromise	
Perte financière pour des entreprises canadiennes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement	Réduction de la compétitivité	Viabilité compromise	
Perte financière pour le gouvernement du Canada	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement des programmes	Incidence sur les résultats des programmes	Viabilité des programmes compromise	Viabilité des programmes essentiels compromise
Préjudice causé à l'économie canadienne			Incidence sur le rendement	Perte de compétitivité à l'échelle internationale	Secteurs économiques clés compromis
Préjudice causé à la réputation du Canada	Préjudice négligeable ou aucun préjudice raisonnable prévu	Perte de la confiance du public	Embarras (au Canada ou à l'étranger)	Relations fédérales-provinciales compromises	Relations diplomatiques et internationales compromises
Perte de la souveraineté canadienne			Entrave à l'établissement de politiques gouvernementales importantes	Entraves à l'application efficace de la loi Cessation des activités du gouvernement	Perte de la souveraineté territoriale

Scénario ACME – Valeur des biens

Type de préjudice	Description et niveau				
	Très faible	**Faible**	**Moyen**	**Élevé**	**Très élevé**
Préjudice physique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort physique	Douleurs physiques, blessures, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
Préjudice psychologique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress	Détresse, traumatisme psychologique	Maladie mentale ou physique	Traumatisme psychologique généralisé
Perte financière pour des particuliers	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress ou inconfort	Incidence sur la qualité de vie	Sécurité financière compromise	
Perte financière pour ACME	Préjudice négligeable ou aucun préjudice raisonnable prévu	??	??	??	??
Préjudice causé à la réputation de l'entreprise	Préjudice négligeable ou aucun préjudice raisonnable prévu	??	??	??	??

Scénario ACME – Évaluation des biens

ID	Bien	Classe	Niveau de préjudice maximal		
			C	I	D
A1a	Examens diagnostiques	Processus	N/A		
A1b	Radiographies, échographies, rapports	Information			
A2a	Inscription de nouveaux clients	Processus	N/A		
A2b	Informations personnelles et bancaires des clients	Information			

Scénario ACME – Évaluation des biens

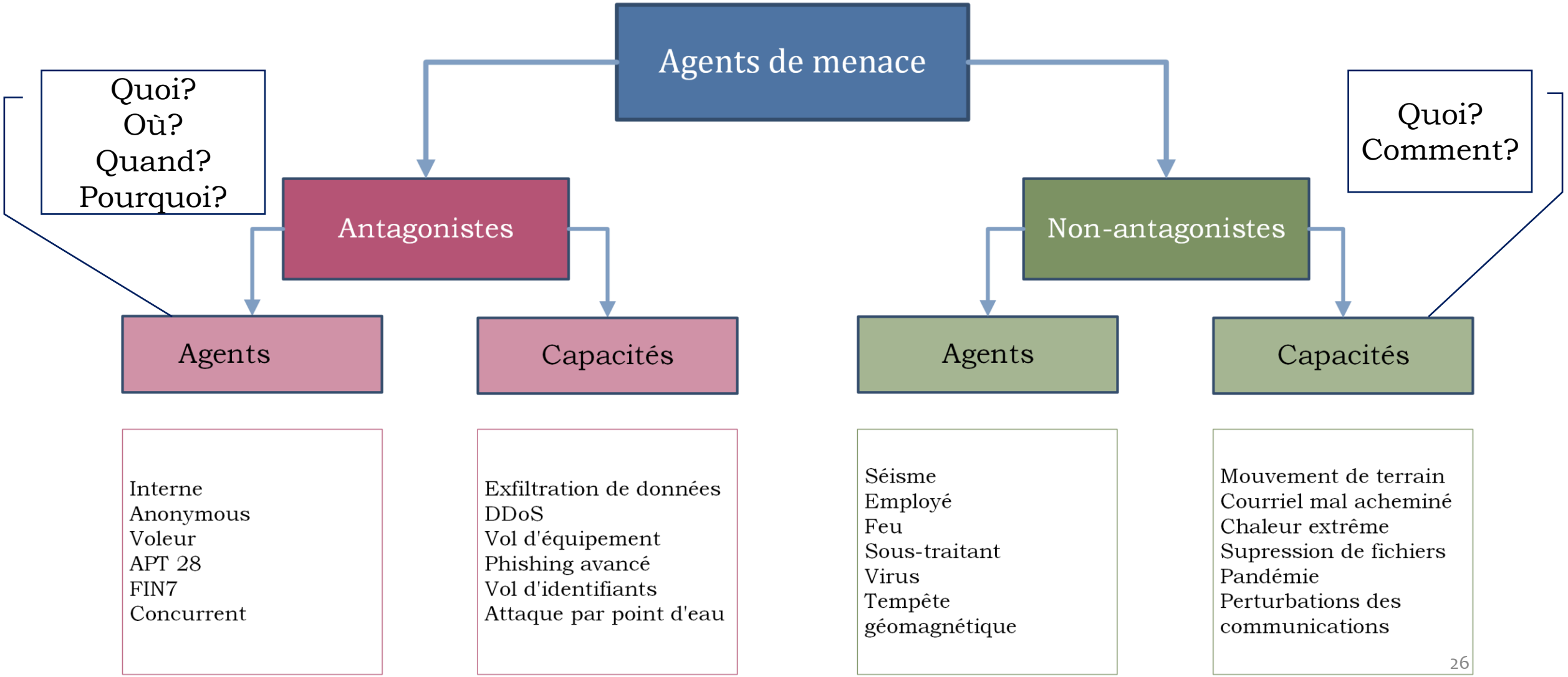
ID	Bien	Classe	Niveau de préjudice maximal		
			C	I	D
A1a	Examens diagnostiques	Processus	N/A	Moyen Délais supplémentaires parce que des étapes sont à recommencer,	Faible 1-5 jours Moyen 5-10 jours Élevé >10-20 jours Très élevé > 20 jours
A1b	Radiographies, échographies, rapports	Information	Moyen (peu) Élevé (plusieurs)	Élevé Si le rapport est modifié accidentellement ou malicieusement, peut changer le traitement, peut affecter la santé + la vie	Faible 1-5 jours Moyen 5-10 jours Élevé >10-20 jours Très élevé > 20 jours
A2a	Inscription de nouveaux clients	Processus	N/A	Faible	Faible 1-3 jours Moyen 4-8 jours Élevé >9-15 jours Très élevé > 15 jours
A2b	Informations personnelles et bancaires des clients	Information	Moyen (peu) Élevé (plusieurs)	Faible	Faible

Partie II: Phase d'évaluation des menaces

- Identifier les menaces dans le contexte de votre organisation
- Évaluer la catégorie (gravité) des menaces
- Évaluer la probabilité

$$R = f\,(B_{Val}, M, V)$$

Identification des menaces



Identification des menaces

- Les informations concernant les agents de menaces et leurs capacités sont disponibles via:
  - Nouvelles
  - Rapports d'incidents (externe et interne)
  - Documents internes (expérience, EMR précédents)
  - Répertoires - bases de données - de tierces parties (collections d'incidents, de nouvelles, etc.)
    - VERIS, Canadian Disaster Database, Hackmaggedon, etc.
  - Statistiques
    - Statistique Canada, Comptes publics du Canada
  - Cadres analytiques
    - MITRE CAPEC, ATT&CK
  - Évaluations des menaces de tierces parties
    - Évaluation des cybermenaces nationales du Gouvernement du Canada
    - ODNI National Threat Assessment, États-Unis
    - Évaluations des menaces réalisées par des entreprises privées

Évaluation de la catégorie (gravité) des menaces

- Selon la méthodologie EMR choisie, l'évaluation des menaces peut inclure une échelle qui assignera une valeur représentant la « force » de la menace
- Dans la méthodologie harmonisée de l'EMR du GC, on parle de *gravité*
- Dans la version ITSG-33 de l'EMR, on parle de *catégorie*
- Ce concept n'est pas inclus dans toutes les méthodologies d'EMR, mais il est très utile aux fins d'analyse
  - Souvent, les sources de renseignements sur les menaces vont mentionner les agents par groupe plutôt qu'individuellement (ex: *Cyber-espionnage* au lieu de *APT28*)

Évaluation de la catégorie (gravité) des menaces

- Une catégorie peut représenter des agents de menaces (antagonistes) qui ont des similarités au niveau de:
  - Connaissances
  - Compétences
  - Accès
  - Tolérance au risque
  - Intentions
  - Etc.

Évaluation de la catégorie (gravité) des menaces

Catégorie	Description		
	Caractéristiques	**Exemples d'agents**	**Exemples de capacités**
Md1	Attaquant non malveillant	Utilisateurs du système, Invités, Visiteurs	Connexion d'appareils non-autorisés
Md2	Attaquant occasionnel et passif possédant un minimum de ressources et disposé à prendre de petits risques.	Employés, Délinquants	Vol de petits items attrayants
Md3	Attaquant possédant un minimum de ressources et disposé à prendre des risques importants.	Employés contrariés, activistes	Installation de *keyloggers*, vol de documents à l'imprimante
Md4	Attaquant sophistiqué possédant des ressources moyennes et disposé à prendre de petits risques.	Chercheurs, *hacktivistes*	Lancer un DDoS, interception illicite de communications
Md5	Attaquant sophistiqué possédant des ressources moyennes et disposé à prendre de grands risques	Cybercriminels, crime organisé	Corruption d'employés internes clés pour obtenir de l'information, installation de *botnets*
Md6	Attaquant extrêmement sophistiqué possédant des ressources abondantes et disposé à prendre de petits risques	Parrainé par un État, États-nations	Interception et modification de matériel *hardware*, installation de maliciels adaptés (sur mesure)
Md7	Attaquant extrêmement sophistiqué possédant des ressources abondantes et disposé à prendre des risques extrêmes	États-nations en temps de crise (guerre)	Destruction d'installations, élimination (meurtre) du personnel clé

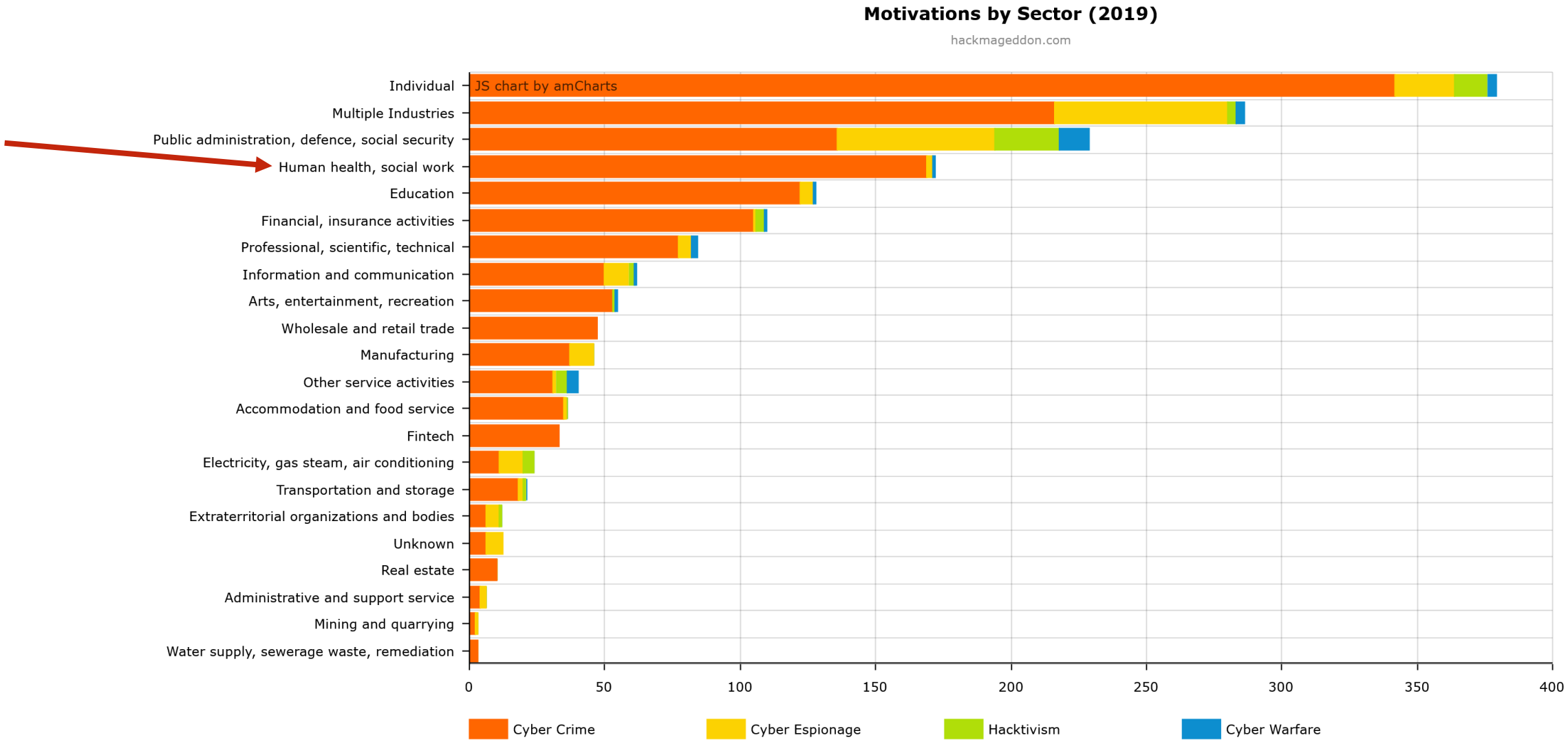
Évaluation de la probabilité des menaces

- Aspect de l'EMR pouvant être le plus difficile et le plus subjectif
- L'évaluation de la probabilité influence le calcul du risque
  - Une mauvaise évaluation peut mener à de piètres décisions
- L'évaluation de la probabilité se fait à l'aide de:
  - Collectes de données d'incidents
  - Évaluations de menaces de tierces parties
  - On peut se fier à des industries/secteurs similaires
- S'il y a un manque d'information, devrait-on assumer que la menace est plus importante ou moins importante?

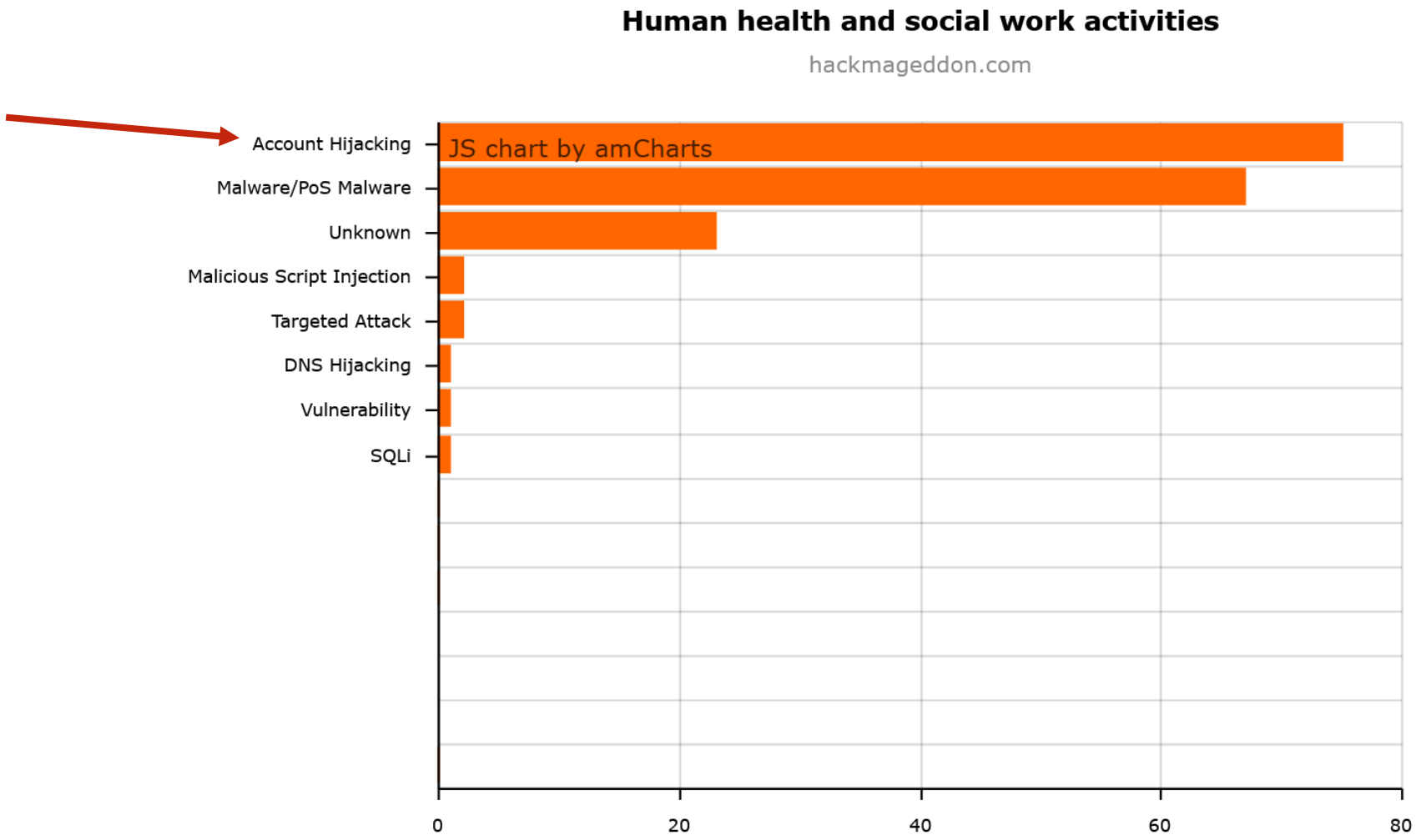
Évaluation de la probabilité des menaces

- Les collectes de données événementielles peuvent servir de “base statistique”
- Lorsque l’on collecte des données sur les événements dans diverses sources, il est normalement possible d’attribuer les incidents à des agents de menaces spécifiques, ou à des *catégories d’agents de menaces*
- La probabilité peut être déterminée par la collecte de certains attributs d’incidents pour chaque agent de menaces, tels que:
    - Localisation géographique de l’incident
    - Cible (e.g., infrastructure essentielle, commerce)
    - Objectifs (ex: gain financier, espionnage)
    - Fréquence des événements sur une période donnée

Évaluation de la probabilité des menaces



Évaluation de la probabilité des menaces



Évaluation de la probabilité des menaces

- Les évaluations des menaces de tierces parties permettent de “déléguer” une partie du travail à faire pour déterminer les probabilités
- Habituellement, ces évaluations comprennent des “avis d’experts” à propos des agents de menaces et des probabilités
- Ces jugements d’experts sont faits par des analystes formés spécifiquement dans l’évaluation des menaces et ils utilisent un large éventail de sources de données
- Les évaluations des menaces de tierces parties ne sont pas toujours disponibles, ou ne considèrent pas nécessairement le contexte souhaité

Évaluation de la probabilité des menaces

GC National Cyber Threat Assessment 2021

«Les auteurs de cybermenace [parrainés par des États] continueront probablement de mener des activités d'espionnage industriel contre les entreprises, le milieu universitaire et les gouvernements du Canada afin de voler la propriété intellectuelle et des renseignements canadiens de nature exclusive.»

https://cyber.gc.ca/en/reports-assessments

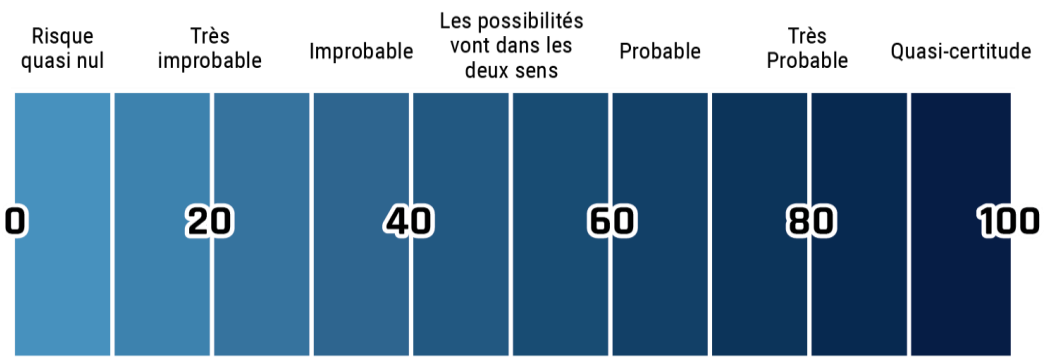
- Qui sont les agents de menaces?
- Qui est la cible?
- Quelle est la catégorie?
- Quelle est la probabilité?

Évaluation de la probabilité des menaces

- L'échelle utilisée pour évaluer la probabilité dépend de la méthodologie d'EMR
  - Valeurs numériques entre 0 et 1 (méthodes purement quantitatives)
  - Valeurs numériques entre 0 et 100
  - Niveaux distincts (variables discrètes)

Échelle ITSG-33 EMRH
Très Improbable
Improbable
Possible
Probable
Très Probable

Échelle d'évaluation du CCCS



https://cyber.gc.ca/fr/orientation/propos-du-present-document-2

Scénario ACME – Identification des menaces

Portée des menaces				
Classe	**Agent de menaces**	**Catégorie**	**Capacités**	**Probabilité**
Délibérée	Cyber-guerre	Md7	Toutes les capacités	
Délibérée	États-nations, parrainé par un État	Md6	La majorité des capacités	
Délibérée	Crime organisé, cybercriminels	Md5	Prise de contrôle de comptes (vol d'identité), DDoS, injection SQL	
Délibérée	Hacktivistes / *Hacker for hire*	Md4	DDoS, prise de contrôle de comptes (vol d'identité)	

Scénario ACME – Évaluation des menaces

Niveau de menace		Probabilité de la menace				
Gravité de la menace	Gravité de la menace	Très improbable	Improbable	Possible	Probable	Très probable
Md6/7	Ma5	Faible	Moyen	Élevé	Très élevé	Très élevé
Md5	Ma4	Très faible	Faible	Moyen	Élevé	Élevé
Md4	Ma3	Très faible	Faible	Moyen	Moyen	Élevé
Md3	Ma2	Très faible	Très faible	Faible	Faible	Faible
Md1/2	Ma1	Très faible	Très faible	Très faible	Faible	Faible

Partie III: Phase d'évaluation des vulnérabilités

- Recensement des mesures de protection
- Identifier les vulnérabilités
- Analyser les incidences des vulnérabilités
- Attribuer les niveaux de vulnérabilités

$$R = f\,(B_{Val}, M, V)$$

Qu’est-ce qu’une vulnérabilité?

- Une exposition exploitée par un agent de menace, pouvant ainsi causer des impacts négatifs contre l’organisation
- Exemples:
  - Vulnérabilités logicielles – peuvent être exploitées, permettant aux agents de menace de poser des actions illicites
  - Connectivité sans fil – n’importe qui peut se connecter et observer le trafic réseau
  - Utilisation d’ordinateurs portables et de téléphones intelligents – ces appareils sont mobiles et ont une probabilité accrue d’être perdus ou volés
  - Accès à des comptes – n’importe qui peut avoir accès à n’importe quoi

Qu’est-ce qu’une mesure de protection?

Mesures de protection:

Mécanismes mis en place pour prévenir et/ou détecter les méthodes utilisées par les agents de menace pour compromettre les systèmes d'information.

- **Vulnérabilités logicielles** – processus d’assurance-qualité des logiciels, gestion des patches, processus et systèmes de détection des intrusions et des anomalies
- **Vulnérabilités de la connectivité sans fil** – chiffrement et contrôle d’accès
- **Vulnérabilités des appareils portatifs** – serrures physiques, formations et sensibilisation, l’effacement (*wipe*) et la désactivation à distance
- **Vulnérabilités des accès aux comptes** – mécanismes et processus d’identification et d’authentification, gestion des comptes, autorisations

Identification des vulnérabilités

- Une vulnérabilité existe quand:
  - Il y a une exposition…
  - Qu'un agent de menace est capable d'exploiter…
  - Qui n'a pas été résolue efficacement.
  - Mesures de sécurité inefficaces ou absentes.
- L'évaluation des vulnérabilités est le processus:
  - D'identification de toutes les expositions ou conditions qui pourraient être exploitées par des agents de menaces pertinents au contexte et…
  - D'évaluation de l'efficacité des mécanismes de protection qui sont (ou peut-être qui ne sont pas) en place pour adresser ces vulnérabilités.

ACME - Identification des vulnérabilités

- Les vulnérabilités qui nous intéressent dans le cadre de ce projet sont celles en lien avec le contrôle d'accès.
- Le système permettra l'accès à partir d'internet (exposition), mais les utilisateurs pourraient ne pas être qui ils prétendent être (vulnérabilité d'authentification)
- Trois mécanismes d'authentification sont proposés:
  - Nom d'utilisateur et mot de passe
  - Nom d'utilisateur, mot de passe et TOTP logiciel
  - Carte à puce cryptographique (*smart card/USB crypto token*)

Évaluation de l'efficacité des mesures de protection

Classe de menace	Description
Vol	L'authentificateur est volé par l'agent
Duplication	L'authentificateur est dupliqué sans permission et à l'insu du propriétaire
Analyse (*cracking*) hors ligne	L'authentificateur est exposé à l'aide de méthodes analytiques en dehors du mécanisme d'authentification
Hameçonnage	L'*output* de l'authentificateur est récolté en faisant croire à l'abonné que l'agent est un vérificateur
Écoute clandestine	L'authentificateur est révélé à l'agent alors que l'utilisateur est en train de s'authentifier
Ingénierie sociale	L'agent convainc une personne de lui donner ses secrets d'authentification
Attaques *brute-force* en ligne	L'agent tente de deviner un authentificateur valide en ligne
Appareil compromis	L'appareil est compromis par un malware
Gestion des authentificateurs	L'agent abuse le système de gestion d'authentification - obtention d'un nouvel authentificateur par la récupération d'un facteur/information d'identification

Évaluation de l’efficacité des mesures de protection

Classe de menaces	Mot de passe	Logiciel TOTP	Carte à puce cryptographique
Vol et/ou duplication			
Usurpation d’identité, Hameçonnage, Ingénierie sociale			
Attaques *brute-force* en ligne			
Appareil compromis			
Gestion des authentificateurs			
Évaluation de l’efficacité			

Évaluation de l'efficacité des mesures de protection

Classe de menaces	Mot de passe	Logiciel TOTP	Carte à puce cryptographique
Vol et/ou duplication	Duplication très facile à faire si les mots de passe sont écrits quelque part. • Piquage de mot de passe (*shoulder surfing*) • Fouille de poubelles • Bases de données sur le darkweb	Duplication difficile mais possible par un agent de menace de catégorie Md5. Vol et duplication possibles si l'appareil est compromis.	Relativement facile à voler mais très difficile à dupliquer. • Même si la carte est volée, le deuxième facteur est nécessaire pour compromettre le processus d'authentification. L'opportunité d'utiliser ou de dupliquer la carte est limitée par le temps nécessaire à un utilisateur de se rendre compte de la perte/vol de sa carte et de rapporter l'incident.
Usurpation d'identité, Hameçonnage, Ingénierie sociale	Facile à faire. Plusieurs exemples dans lesquels des utilisateurs sont incités à divulguer des données d'identification (mots de passe) via des sites web, des courriels ou des arnaques téléphoniques (individuellement ou toutes techniques combinées).	Difficile à faire, particulièrement pour les TOTP à courte durée. Toutefois, ces attaques ont été rapportées (voir attaque contre Twitter [1]).	Très difficile à faire. Le mécanisme de chiffrement (cryptographie) empêche l'usurpation d'identité, à moins que l'agent de menace ait réussi à voler ou à dupliquer la clé privée.
Attaques *brute-force* en ligne	Très facile, facile à faire • *Password spraying attack* • *Credential stuffing*		
Appareil compromis	Très facile, installation d'un *keylogger*	Moyen ou facile (s'ils ont un contrôle total de l'appareil, cela dépend de la façon dont ils l'ont compromis)	Difficile ou très difficile, si le deuxième facteur est un mot de passe, possible de l'obtenir. Mais si c'est un identifiant biométrique, très difficile.
Gestion des authentificateurs	Il est très facile de déjouer les systèmes de réinitialisation d'identifiants (mot de passe et nom d'utilisateur).	Parce que c'est basé sur le logiciel, l'accès au système de gestion des authentificateurs pourrait être fait à distance, donc les vecteurs d'attaques sont multiples. Compromission du *back-end*. Difficile.	Très difficile à faire. La réinitialisation du mot de passe peut être facile à faire (si le mot de passe est le deuxième facteur) mais la clé privée est nécessaire. L'obtention d'un renouvellement des identifiants signifie que l'agent de menace doit refaire le processus d'acquisition d'un identifiant en entier.
Évaluation de l'efficacité	**Très faible à faible**	**Moyen**	**Très élevé**

Évaluation de l'efficacité des mesures de protection

- À noter:
  - Pour un scénario donné, il n'est pas rare que le EMRH adresse l'efficacité *globale* de *toutes* les mesures de protection qui sont en place afin de remédier à une vulnérabilité donnée.
  - Ceci inclus:
    - Les mesures de protection préventives
    - Les mesures de protection utilisées afin de détecter les incidents, y réagir et revenir aux opérations normales (ex: cameras de surveillance, gardiens de sécurité, etc.)
  - Le scénario ACME ne considère que la valeur préventive des mécanismes de protection.

Évaluation de l'efficacité des mesures de protection

				HTRA Probability of Compromise (Prevention)				
				Very Low	Low(N/A)	Medium	High	Very High
				Prevent Safeguard Effectiveness				
				Very High	High	Medium	Low	Very Low
		Detect Safeguard Effectiveness		Very High	High	Medium	Low	Very Low
HTRA Outcome Severity	Very Low	Very High	Very High	Very Low	Very Low	Low	Medium	Medium
	Low(N/A)	High	High	Very Low	Very Low	Low	Medium	Medium
	Medium	Medium	Medium	Very Low	Low	Medium	Medium	High
	High	Low	Low	Very Low	Low	Medium	High	Very High
	Very High	Very Low	Very Low	Very Low	Low	High	High	Very High

Partie IV: Phase d'évaluation des risques

- Calcul et priorisation des risques résiduels
- Recommandations

$$R = f\,(B_{Val}, M, V)$$

Évaluation des risques

- Nous pouvons maintenant explorer l'ensemble des risques éventuels en:
  - Créant un scénario de menace qui combine chacun des éléments de risque
  - Utilisant la fonction du risque pour générer la valeur des risques.

Évaluation des risques

Variables	Description		
Description	Des cybercriminels compromettent les identifiants d'accès de l'admin et installent un rançongiciel		
Biens	Examens diagnostiques, inscription de nouveaux clients		
Catégorisation des biens	Catégorie la plus élevée		
Agent de menace	Crime organisé		
Catégorie - agent	Md5		
Probabilité - agent	Probable (selon notre recherche)		
Mesures de protection	Mot de passe	Logiciel TOTP	Carte à puce cryptographique
Efficacité	Faible	Moyen	Élevé/Très élevé
Risque			

Calcul des risques – valeur numérique

Niveau de la valeur du bien, des menaces et des vulnérabilités	Très faible	Faible	Moyen	Élevé	Très élevé
Cote de calcul du risque	1	2	3	4	5

Risque résiduel = Valeur du bien x Menace x Vulnérabilité

Calcul des risques

Scenarios	Scenario Description		Assets	Assets and Asset Value			Threats	Threats					Vulnerabili	Vulnerability					Risk		
	ID			Asset	Categorization	Notes		Threat Actor	Threat Category	Likelihood	Notes	Threat Level		Preventive Mechanism(s)	Prevent Effectiveness	Detect Mechanism(s)	Detect Effectiveness	Net Vulnerability		Risk Value	Risk Label
	S1	Cybercriminals compromise administrator credentials, install ransomware		Examens diagnostiques, Inscription de nouveaux clients Etc.	**High**	Process with the highest category		Organized Criminals	Td5	**Likely**	Organized crime targets administrators preferentially	**High**		Username/ Password	**Low**	None	**Very Low**	**High**		**64**	**High**
					High			Organized Criminals	Td5	**Likely**		**High**		TOTP	**Medium**	None	**Very Low**	**High**		**64**	**High**
					High			Organized Criminals	Td5	**Likely**		**High**		Crypto Token	**Very High**		**Very Low**	**Very Low**		**16**	**Low**

Évaluation des risques

Variables	Description		
Description	Des cybercriminels compromettent les identifiants d'accès de l'admin et installent un rançongiciel		
Biens	Examens diagnostiques, inscription de nouveaux clients		
Catégorisation des biens	Catégorie la plus élevée		
Agent de menace	Crime organisé		
Catégorie - agent	Md5		
Probabilité - agent	Probable (selon notre recherche)		
Mesures de protection	Mot de passe	Logiciel TOTP	Carte à puce cryptographique
Efficacité	Faible	Moyen	Élevé/Très élevé
Risque	**Élevé**	**Élevé**	**Moyen/Faible**

Évaluation des risques – autre scénario

Variables	Description		
Description			
Biens			
Catégorisation des biens			
Agent de menace			
Catégorie - agent			
Probabilité - agent			
Mesures de protection	Mot de passe	Logiciel TOTP	Carte à puce cryptographique
Efficacité			
Risque			

Recommandations - discussion

- Quels sont les risques résiduels inacceptables?
- Quelles mesures de protection pourraient atténuer les risques résiduels inacceptables?
- Quel serait le coût et la rentabilité?
- Quels sont les risques résiduels projetés?

Conclusion

Type	Nom	Lien
Événements	Vocabulary for Event Recording and Incident Sharing (VERIS)	http://veriscommunity.net/vcdb.html
	Hackmaggedon	https://www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/
	Base de données canadienne sur les catastrophes	https://www.securitepublique.gc.ca/cnt/rsrcs/cndn-dsstr-dtbs/index-fr.aspx
	Statistique Canada	https://www.statcan.gc.ca/fr
	Comptes publics du Canada	https://www.tpsgc-pwgsc.gc.ca/recgen/cpc-pac/index-fra.html
Rapports	CCCS Évaluation des cybermenaces nationales 2020	https://cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020
	IBM Threat Intelligence Index 2022	https://www.ibm.com/downloads/cas/ADLMYLAZ
	ODNI National Threat Assessment (USA)	https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf
	FBI Internet Crime Report	https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
	Data Breach Investigation Report 2021 - Verizon	https://www.verizon.com/business/resources/reports/dbir/

Verizon report – 2021 Confidentiality violations

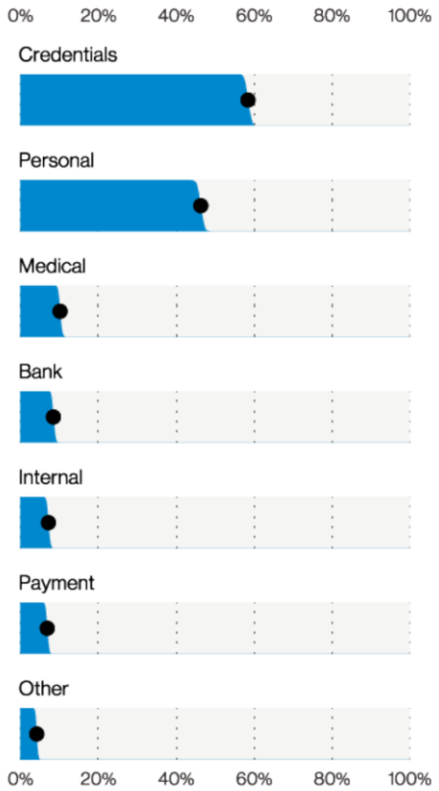
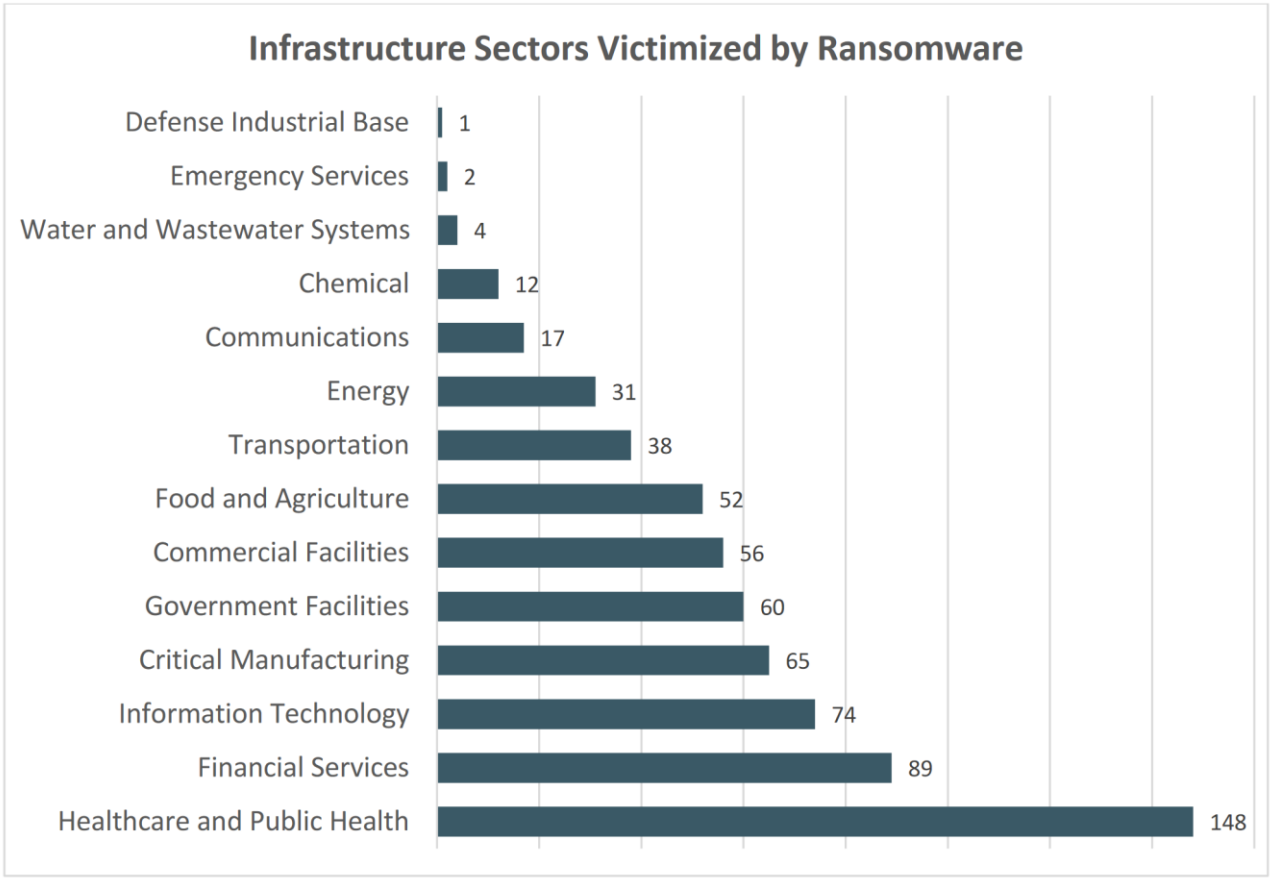


Figure 35. Top data varieties in breaches (n=4,552)

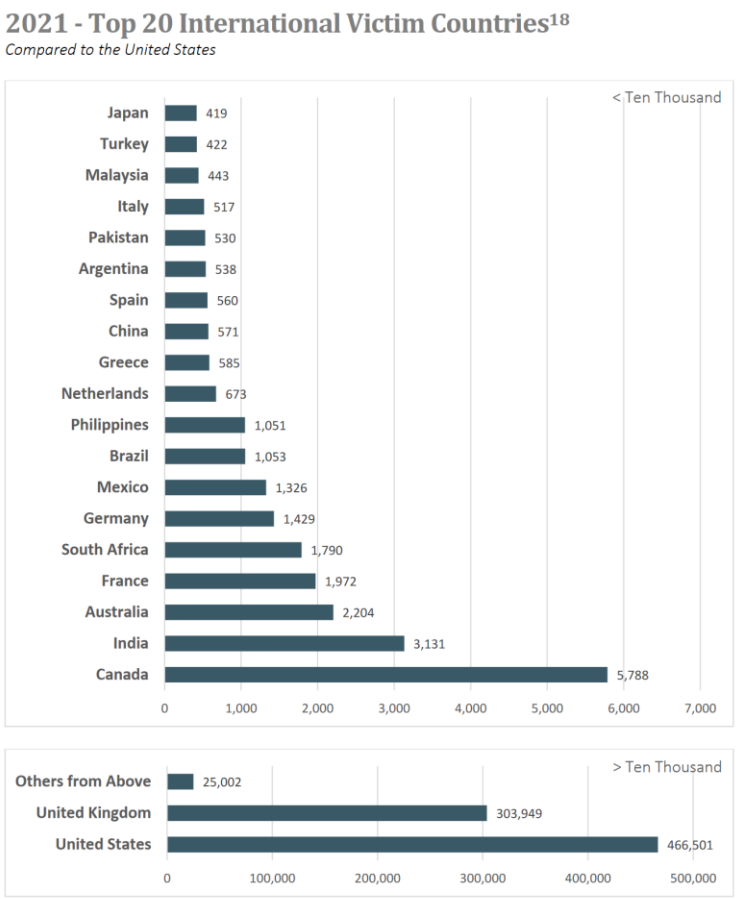
Figure 36. Top data varieties in Error breaches (n=839)

FBI IC3 Report, 2021

13



FBI IC3 Report, 2021



FBI IC3 Report 2021,

By Victim Loss			
Crime Type	*Loss*	*Crime Type*	*Loss*
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/Romance	$956,039,740	Ransomware	*$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$44,213,707
Tech Support	$347,657,432	Overpayment	$33,407,671
Non-Payment/Non-Delivery	$337,493,071	Computer Intrusion	$19,603,037
Identity Theft	$278,267,918	IPR/Copyright/Counterfeit	$16,365,011
Credit Card Fraud	$172,998,385	Health Care Related	$7,042,942
Corporate Data Breach	$151,568,225	Malware/Scareware/Virus	$5,596,889
Government Impersonation	$142,643,253	Terrorism/Threats of Violence	$4,390,720
Advanced Fee	$98,694,137	Gambling	$1,940,237
Civil Matter	$85,049,939	Re-shipping	$631,466
Spoofing	$82,169,806	Denial of Service/TDos	$217,981
Other	$75,837,524	Crimes Against Children	$198,950