Les chantiers de la cybersécurité : le train passe, qui embarque ?

JACINTHE COULOMBE, B.A., ARCHIVISTE
Responsable en sécurité de l'information, UQAT
Étudiante à la maîtrise en gestion de l'information (MIM), Université Dalhousie

51e CONGRÈS DE L'AAQ

« Nous, les professionnels de l'information, sommes constamment incités à élargir le spectre de nos compétences. Nous devrions être proactifs à rechercher de nouveaux rôles et de nouvelles façons de découvrir, d'analyser et de présenter l'information afin de demeurer des acteurs essentiels pour notre organisation et de maintenir notre place sur la scène. »

(Affelt, 2014, p.11 [traduction libre])

Contenu de la présentation

1. La sécurité de l'information : une fonction archivistique
2. Sensibiliser les acteurs organisationnels à la sécurité de l'information : les meilleures pratiques
3. La gouvernance SI : besoins et opportunités

Sondage de démarrage !

Au sein de mon milieu de pratique, je me considère comme :

- A) Pas du tout impliquée ou impliqué en SI
- B) Peu impliquée ou impliqué en SI
- C) Relativement impliquée ou impliqué en SI
- D) Très impliquée ou impliqué en SI

1. La sécurité de l'information : une fonction archivistique

1. La sécurité de l'information, une fonction archivistique

4 postulats :

A) La SI est inhérente à la réalisation des mandats de l'archiviste

B) La cybersécurité dépasse la sécurité des systèmes

C) La valeur de l'information dicte les couches de sécurité requises

D) Le calendrier de conservation est le précurseur du registre de catégorisation des actifs informationnels

- Sécurité de l'information - cybersécurité

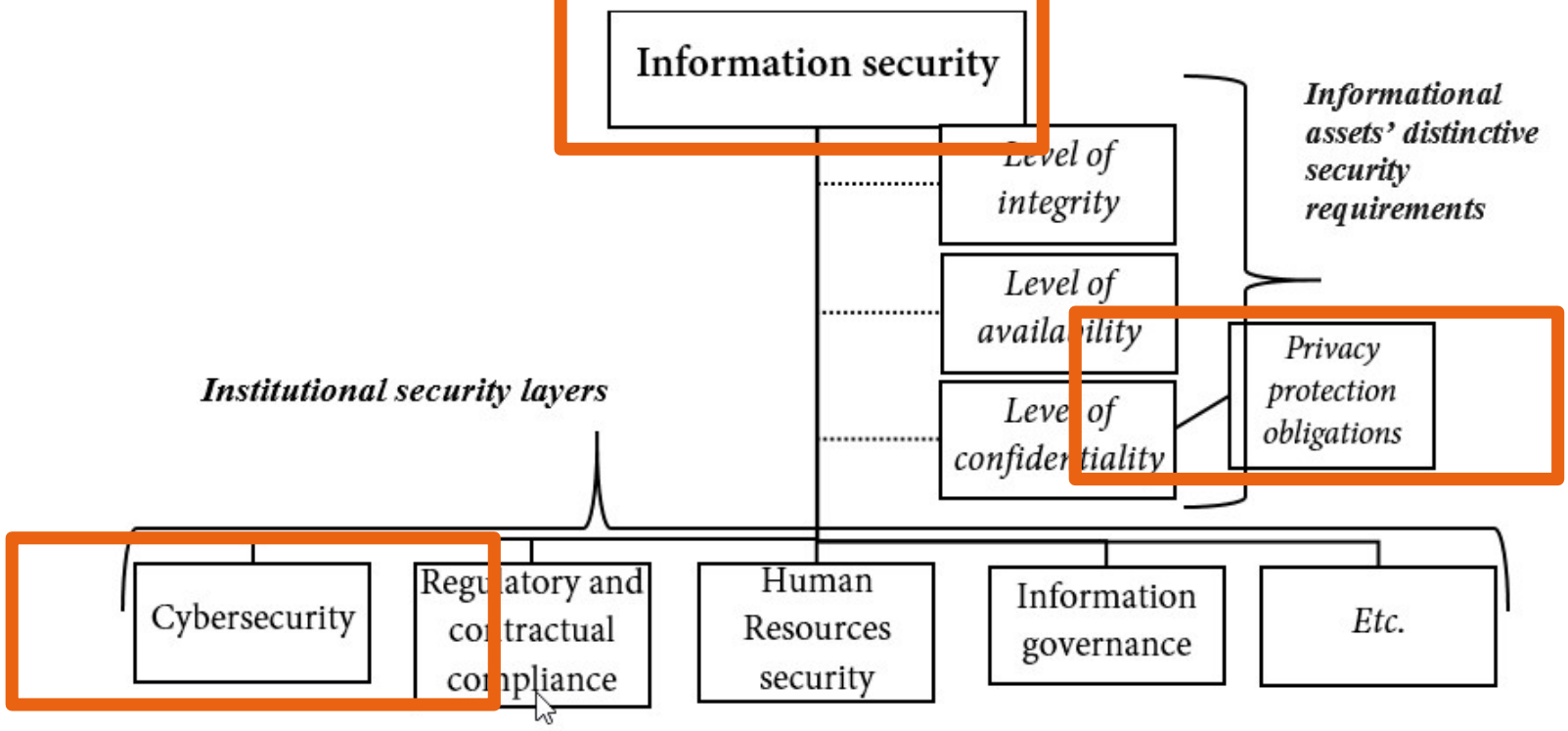


Figure 1 - A schematization of concepts related to information security. Though non-exhaustive, this schema offers a hierarchical view of information security concepts at an organization's level.

Registre de catégorisation des actifs informationnels

« Le registre de catégorisation permet une description détaillée des objets de catégorisation. On y retrouve leurs principaux attributs tels que le libellé, l'unité administrative responsable, le processus utilisateur, le détenteur, la localisation, le niveau d'impact sur le plan de la DIC, la date de catégorisation, les références aux justificatifs d'attribution de niveaux d'impact, etc. ».

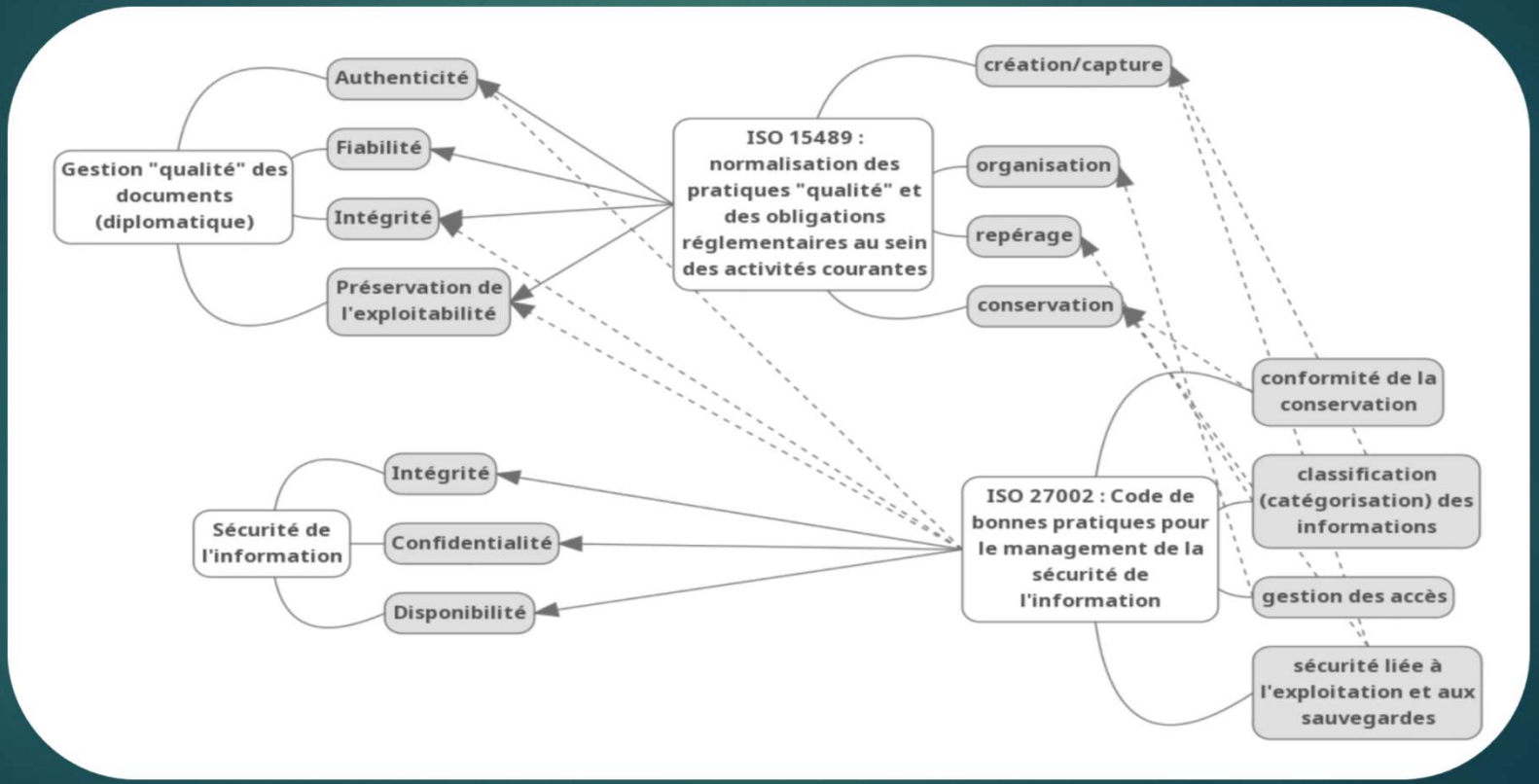
Secrétariat du Conseil du trésor (2016)

- # Registre de catégorisation des actifs informationnels (exemple)

Classification et conservation prévues					Propriété, localisation et entreposage								Catégorisation des actifs					
Série	Sous-série	Activité	Processus	No Règle	Détenteur	Description et utilisation	Type d'objets/Supports		Systèmes d'information	Localisation	Émetteur (intrant)	Partenaires au processus	Destinataire (extrant)	Seuils d'impact			Processus critique	Date	Référence
							Numérique	Papier						D	I	C	O/N		
7000 -	EFFECTIF ÉTUDIANT																		
	7100-00 - Gestion du cheminement académique																		
	7101-00	Recrutement		7101-00	Service des communications et du recrutement														
	7102-00	Prévisions et confirmation des inscriptions																	
		7102-10	Prévisions	7102-00	Décanat à la gestion académique et aux études	Documents relatifs à la prévision, à l'étude et à l'analyse de l'évolution de la clientèle étudiante de l'établissement	x	x											
		7102-20	Transmission des inscriptions	7102-00	Bureau du registraire														
	7103-00	Exigences et normes d'admission		7103-00	Bureau du registraire														
					Décanat à la gestion académique et aux études														
					UER														
	7104-00	Gestion de l'admission																	
		7104-10	Étudiants canadiens	7104-00	Bureau du registraire														
		7104-20	Étudiants étrangers	7104-00	Bureau du registraire														
	7105-00	Gestion de l'inscription																	
		7105-10	Liste des étudiants inscrits	7105-00	Bureau du registraire														

Pour en savoir plus, voir Diane Baillargeon (2017), La catégorisation des actifs informationnels : l'expérience de l'Université de Montréal.

A) La SI est inhérente à la réalisation des mandats de l'archiviste



B) La cybersécurité dépasse la sécurité des systèmes

- La LGGRI paraît éluder le rôle de l'archiviste, malgré l'objectif :

« 1° d'instaurer une gouvernance intégrée et concertée, fondée sur la préoccupation d'assurer des services de qualité aux citoyens et aux entreprises de même que la pérennité du patrimoine numérique gouvernemental » (Chap. G-1.03)

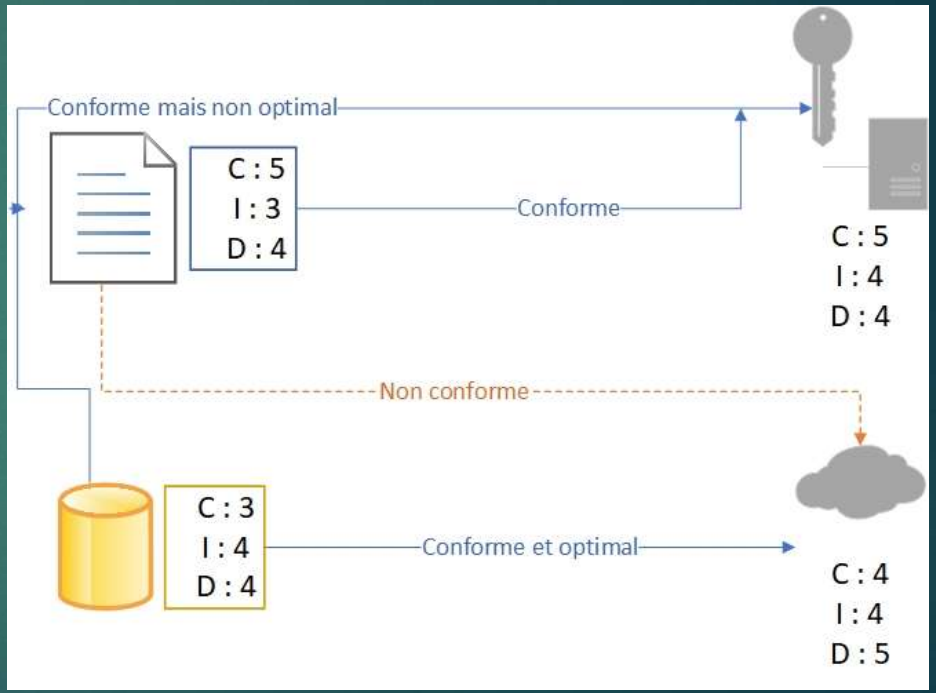
- Les tâches que la LGGRI vise à encadrer apparaissent à première vue davantage orientées systèmes que données : pourtant, le concept d'actif informationnel couvre toutes ces réalités (données + systèmes + infrastructure)

Guide de catégorisation de l'information (SCT, 2016)
Méthodologie du portrait des actifs informatiques (SCT, 2018)

C) La valeur de l'information dicte les couches de sécurité requises

- la protection maximale de l'ensemble des actifs informationnels est extrêmement coûteuse – voire inatteignable – d'où la nécessité d'une démarche rationnelle basée sur la valeur de l'information

- qui d'autre que l'archiviste peut aider les acteurs organisationnels à établir la valeur de l'information ?



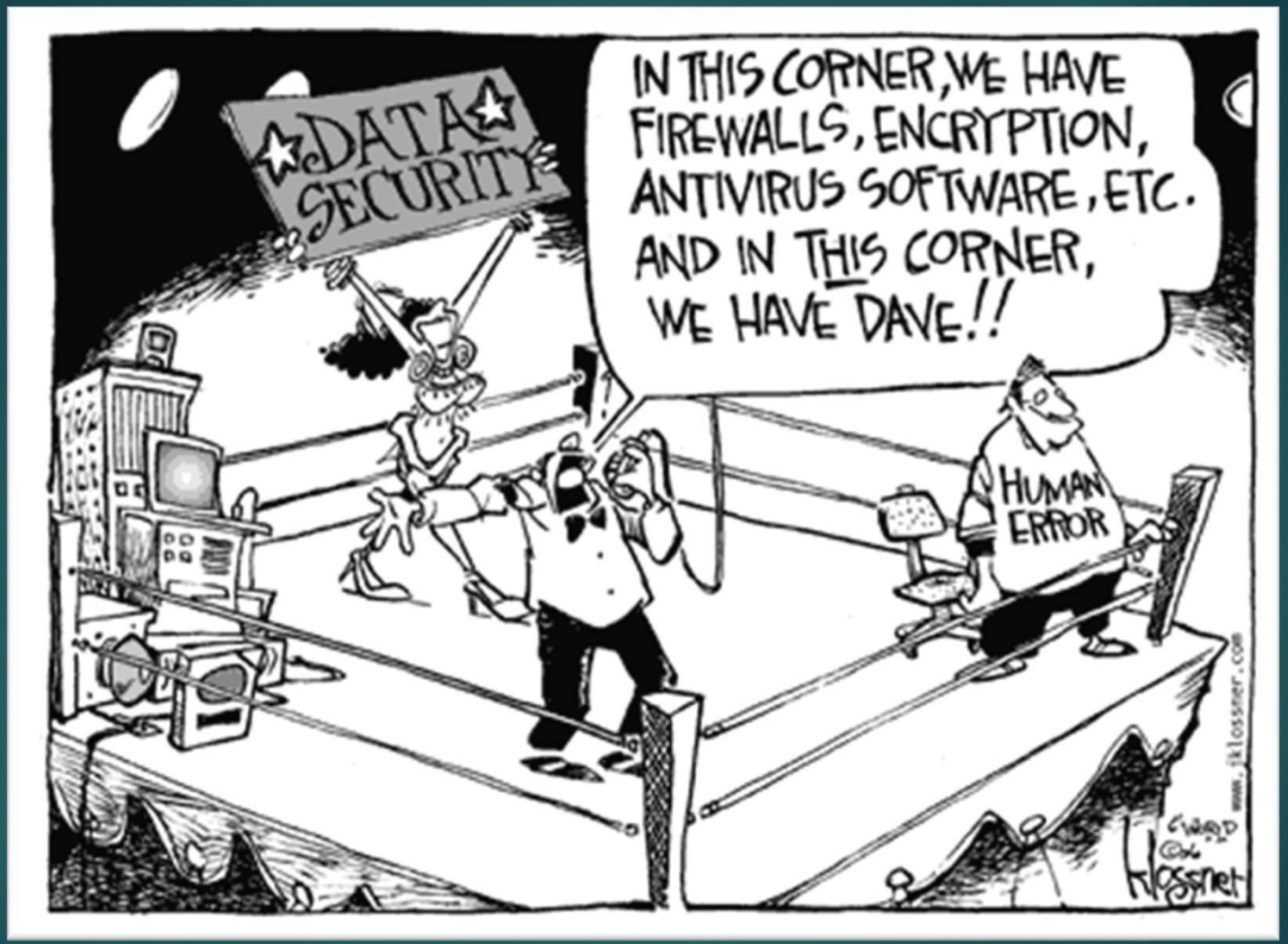
D) Le calendrier de conservation est le précurseur du registre de catégorisation des actifs informationnels

Au-delà d'un outil de gestion de l'espace, un outil de gestion des risques liés:

- à la non-disponibilité de l'information institutionnelle (mention de « documents essentiels »)

- à la conservation indue de renseignements personnels

2. Sensibiliser les acteurs organisationnels à la sécurité de l'information : les meilleures pratiques



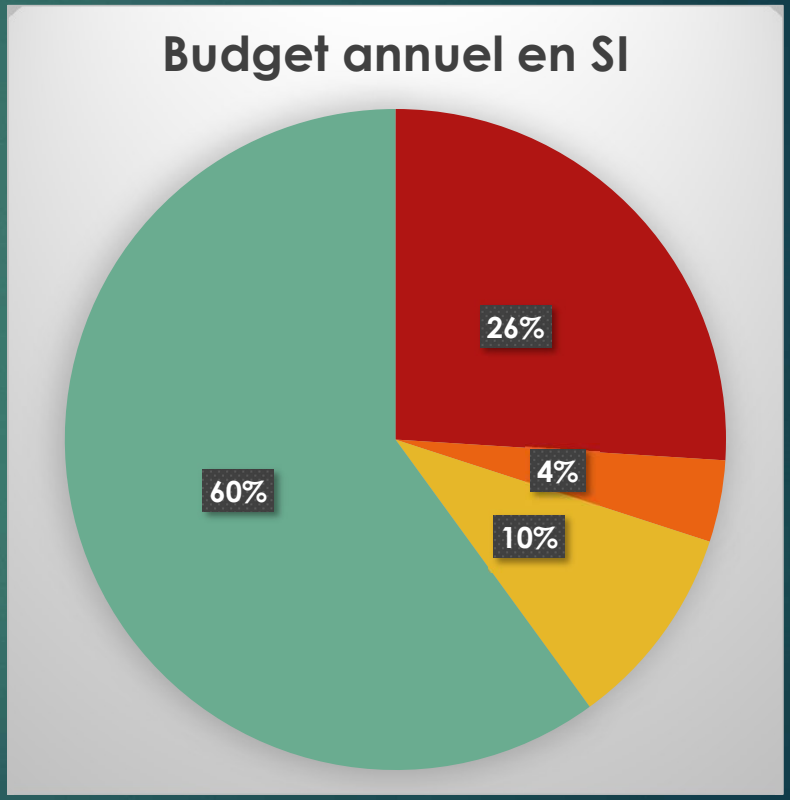
« To embed cybersecurity into the fabric of the organization and be effective against any insider threats, organizations must bring together human resources, learning and development, legal and IT teams to work closely with the security office and business units. »

(Bissell et Ponemon, 2019, p.9)

Un portfolio équilibré d'investissements en SI

- 26 % : architecture et outils TI
- 4% : sensibilisation
- 10% : politiques
- 60% : coordination des activités

Selon les données présentées par L'ACPAU, 2019

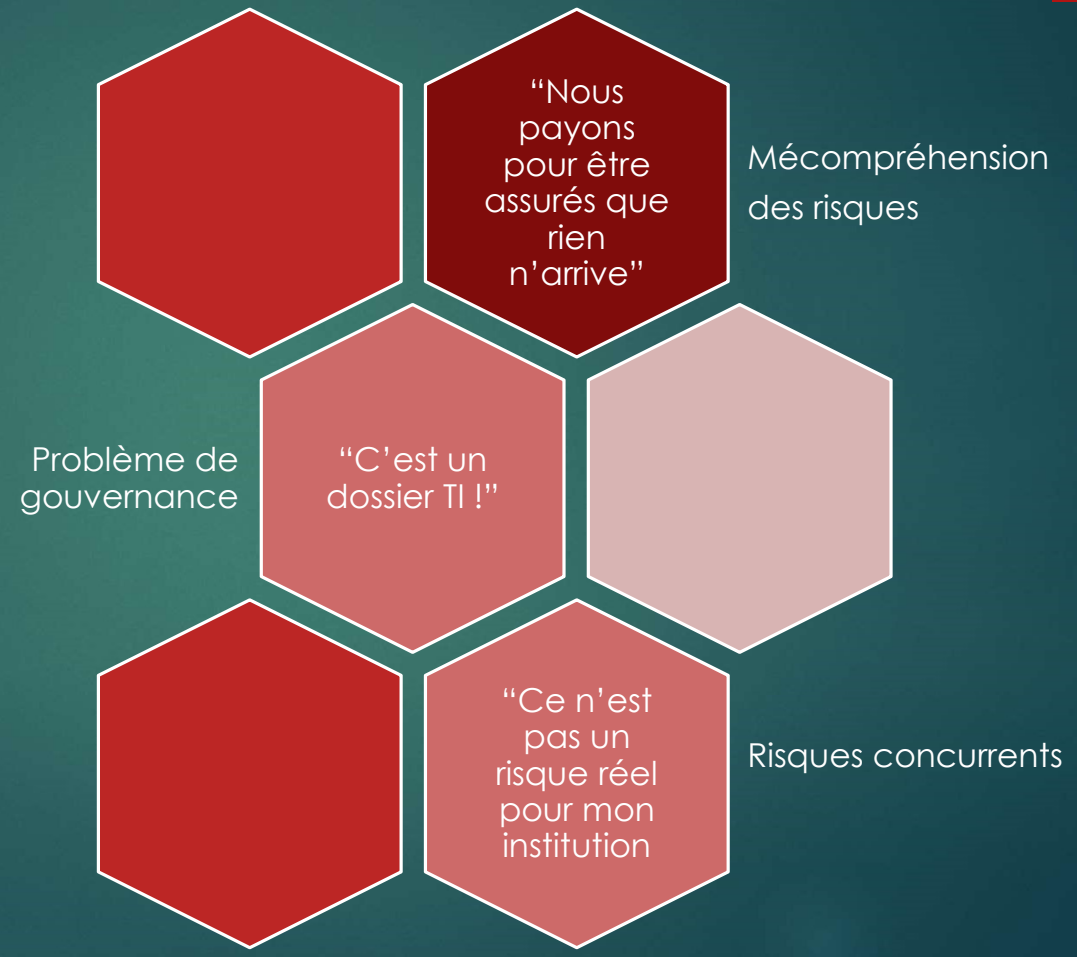


« La sensibilisation à la SI réfère à la connaissance individuelle qu'ont les individus des politiques et procédures qu'ils doivent suivre, leur compréhension des motifs pour lesquels ils doivent y adhérer (leur attitude) et de leurs actions concrètes (leur comportement). »

(McCormac et al., 2017, p. 151 [Traduction libre]).

Vers une sensibilisation accrue à la SI : quelques défis!

Perceptions fréquentes des décideurs



Employés

Facteurs externes

Facteurs internes

- Pression à accomplir les tâches
- Concentration & vigilance
- Motivation différentielle
- Tendance à prendre des risques
- Abus volontaire

20 mesures recommandées en sensibilisation à la sécurité de l'information

A twenty measures' checklist towards ISA – Section 1
1.0 Board of directors' awareness-leveraging plan
1.[illegible] managers considering IS as a business threat to engage their managerial responsibility
1.[illegible] Present the organization's strategic position in regards to IS through benchmarking
1.3 Encourage managers' engagement in IS governance formation programs focusing on IS as a business strategy
1.4 Provide board with evidence-based statistics that IS investments constitute mid/long-term savings
1.5 Demonstrate the managerial responsibility towards securing informational assets
1.6 Get the approval of the awareness and training program guidelines, ensuring they are in phase with business needs
1.7 Engage managers to promote IS compliance and participation in training programs
1.8 Engage managers to allow all compliance conditions required by the employees (e.g.,

20 mesures recommandées en sensibilisation SI – volet Gestionnaires

https://www.gartner.com/en/conferences/calendar

- 1.1 Communiquer le dossier SI comme une préoccupation organisationnelle touchant tous les secteurs d'activité et les processus de l'organisation (alliance avec STI !)
- 1.2 Communiquer le positionnement organisationnel (benchmarking)
- 1.3 Encourager les cadres à prendre part à des webinaires traitant des aspects stratégiques de la SI
- 1.4 Documenter l'économie potentielle que représentent les investissements en SI

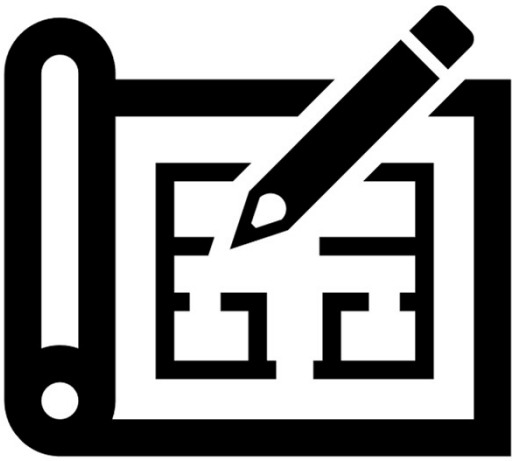
- 1.5 Démontrer la responsabilité managériale inhérente à la protection adéquate des actifs informationnels (nos « détenteurs d'actifs informationnels ! »)
- 1.6 Faire approuver les programmes de formation et de sensibilisation, et s'assurer que ceux-ci sont ajustés à la réalité organisationnelle
- 1.7 Engager les gestionnaires à faire la promotion des programmes SI et à participer eux-mêmes aux formations
- 1.8 Demander l'engagement des gestionnaires à offrir à leurs employés les conditions adéquates pour adopter une attitude conforme
- 1.9 Engager les gestionnaires à montrer l'exemple par leur pratique

20 mesures recommandées en sensibilisation SI – volet Employés

- 2.1 Ajuster le matériel à la réalité des différents services
- 2.2 Offrir une variété de formations incluant toutes les dimensions SI
- 2.3 Ajuster le contenu au public-cible (niveau de compétences, corps d'emploi)
- 2.4 Développer une approche d'apprentissage en groupe
- 2.5 Adopter une approche normative et persuasive

- 2.6 Offrir des « exemples parlants » aux participants
- 2.7 Insister sur le rôle positif joué par les employés
- 2.8 Humaniser les exigences
- 2.9 Adopter une approche d'amélioration continue du matériel
- 2.10 Planifier une offre de soutien au personnel entre les formations et des outils disponibles en tout temps
- 2.11 Souligner les efforts et les bons coups

3. La gouvernance SI : besoins et opportunités



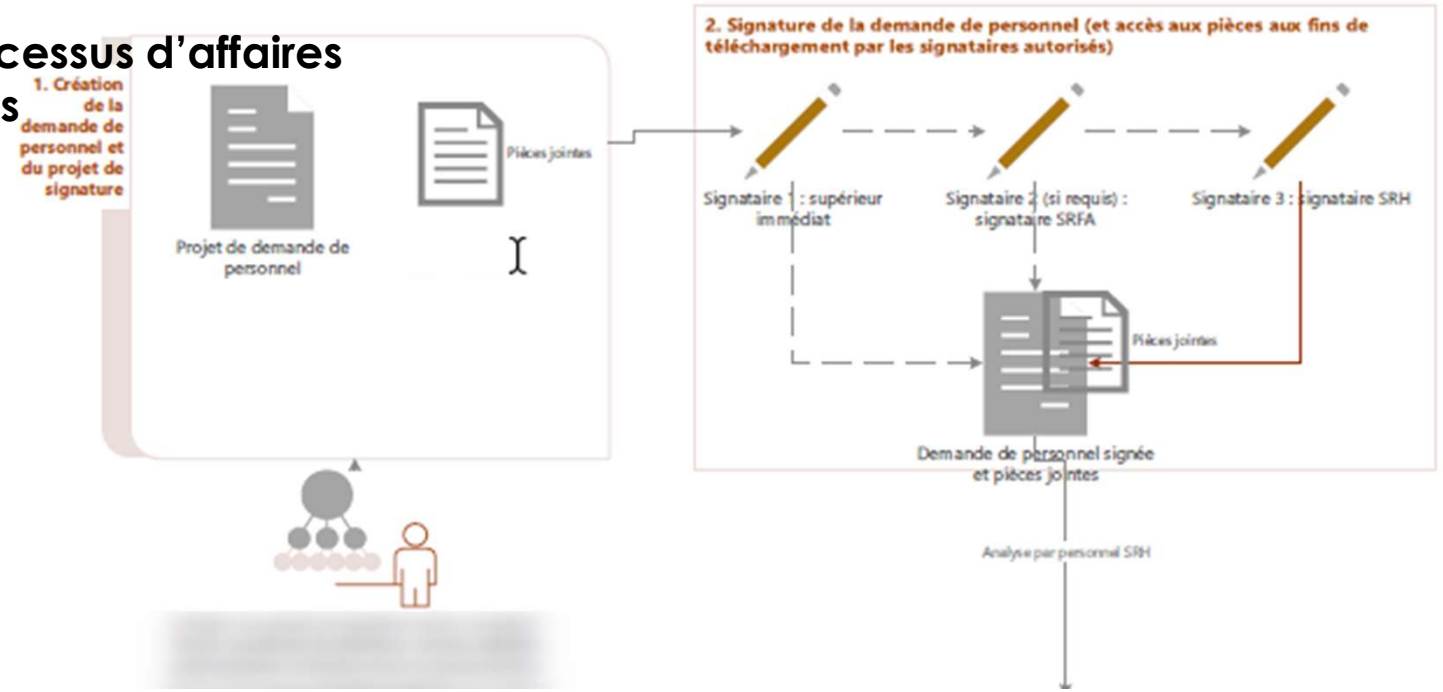
Opportunité 1 :

Catégorisation des actifs informationnels “intégrée” incluant :

- Plan (code)
  - Calendrier (règle spécifique)
  - Valeur (CAI)
  - Plateformes/applications
  - Détenteurs
  - Intrants/extrants et partenaires
  - PI / renseignements personnels

Opportunité 2 :

Cartographie des processus d'affaires et des flux de données



Opportunité 3 : Participation au pilotage de la stratégie numérique de l'organisation

Contexte :

- Permanence envisagée du télétravail
- Offre accrue de services en ligne

Enjeux :

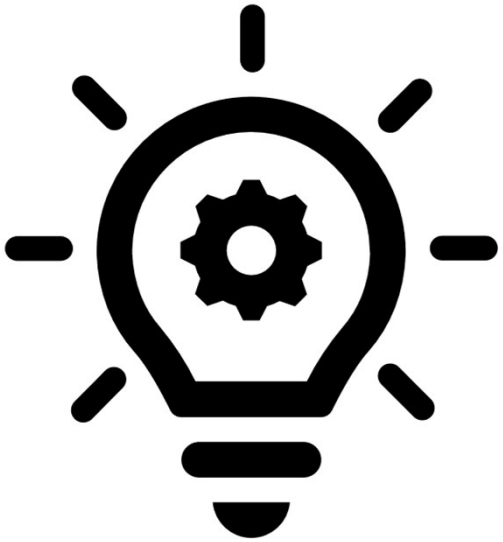
Démultiplication des outils technologiques

Analyses de risques sommaires (manque de temps)

Développement de pratiques de contournement

Recommandations de Amy Affelt (2014) :

- Voir les opportunités
- Se positioner pour y participer en faisant valoir ses habiletés
- Développer les aptitudes recherchées par le milieu de l'emploi
- Développer le langage des différents partenaires



Conclusion

Nous, professionnels de la gestion documentaire/gestion de l'information, sommes **directement concernés par les enjeux croissants liés à la sécurité de l'information**, et avons les **compétences requises pour participer à leur mitigation**

La **sensibilisation** de nos acteurs organisationnels constitue une **composante essentielle** de l'institution d'un programme de sécurité de l'information, et il existe des **stratégies optimales** et relativement simples pour y arriver

Les **opportunités** de développement de compétences et d'élargissement du spectre d'action des professionnels de la gestion documentaire/gestion de l'information sont **nombreuses** et peuvent permettre un **positionnement stratégique** de l'archiviste institutionnel au coeur du processus d'analyse et de prise de décisions liées aux risques SI

Le meilleur des succès dans votre propre démarche en gouvernance SI !

Période de questions

Références citées

ACPAU (CAUBO). (2019). Cyber-security in higher education: An overview. CAUBO/CUCCIO Workshop, Montreal.

Affelt, A. (2014). Acting on Big Data: A Data Scientist Role for Info Pros. Online Searcher. https://www.researchgate.net/publication/269698040_Acting_on_Big_Data_A_Data_Scientist_Role_for_Info_Pros/citation/download

Baillargeon, D. (2017). La catégorisation des actifs informationnels: L'expérience de l'Université de Montréal. 46e congrès annuel de l'Association des archivistes du Québec, Palais des congrès de Montréal. http://congres.archivistes.qc.ca/wp-content/uploads/2017/08/V10_Diane_Baillargeon.pdf

Bissell, K., & Ponemon, L. (2019). The cost of cybercrime: Ninth annual cost of cybercrime study. Unlocking the value of improved cybersecurity protection (No. 9; Accenture Security, p. 23). Ponemon Institute. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Couture, C. et Roy, J. (2006-2007). La norme ISO 15489 : principes et application, *Archives*, Vol. 38, no 2.

ISO. (2013). Norme internationale ISO/CEI 27002: Technologies de l'information—Techniques de sécurité—Code de bonne pratique pour le management de la sécurité de l'information.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. Computers in Human Behavior, 69, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Sous-secrétariat du dirigeant principal de l'information (2016). Guide de catégorisation de l'information. Gouvernement du Québec. https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/categorisation_information.pdf

Sous-secrétariat du dirigeant principal de l'information (2018). Méthodologie du portrait des actifs informatiques. Architecture d'entreprise gouvernementale 3.3.2. Gouvernement du Québec. https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/architecture_entreprise_gouvernementale/AEG_3_3/Portrait_actifs_informatiques.pdf