Fiche de cours

S-10 Sécurité informationnelle

Contenus

La sécurité de l'information est un domaine hautement spécialisé en soi, mais les gestionnaires de documents et les archivistes doivent connaître certaines des bases. Dans cette classe, nous explorerons quelques concepts fondamentaux de la sécurité de l'information, tant physique que numérique.

Le contenu devrait introduire la sécurité informationnelle, ses enjeux, ses défis et surtout les aspects qui concernent la gouvernance informationnelle.

Les approches, les normes et les dispositifs devraient être traités. Le niveau de détail dépendra du public et du programme dans lequel le cours est donné.

Typologies de RI basée sur **…**

- Les métiers et secteurs d'activités des institutions (Smallwood, 2014)
  - Administration publique, hôpitaux, banques, universités, …
- Type de données/informations (Vallès, 2015)
  - Technique, scientifique, stratégique, opérationnel, …
- Type de supports et formats
  - Données web, données électroniques, documents papiers, …
- Niveaux de confidentialité
  - Données ouvertes, confidentielles, …
- Nature des dommages (Léger 2015)
  - Dommage matériel (accidents, vandalisme) et immatériel (erreur, fraude, cyber crime)
- Type d'évènements imprévus (Vermeys 2009) :
  - Dommage physique : feu, inondation, vandalisme, panne de courant, catastrophes naturelles, etc.
  - Interaction humaine : action ou inaction accidentelle ou intentionnelle qui peut interrompre la productivité
  - Défaillance technique : échec des systèmes informatiques et périphériques
  - Attaques internes et externes : pirates informatiques (crackers), bidouilleurs (hackers), etc.
  - Abus de données : partage de secrets commerciaux, fraude, espionnage, vol, etc.
  - Perte de données : destruction intentionnelle ou non intentionnelle d'information

- Erreurs logicielles : erreurs informatiques, erreurs de saisie, dépassement de mémoire tampon, etc.

L'urbanisation du système d'information comme pour se prémunir des menaces

- ❑ Cartographie du SI, par exemple d'un point de vue fonctionnel
- ❑ Permet de faire évoluer le SI en fonction des changements stratégiques
- ❑ Permet d'être réactif
- ❑ Facilite la transformation continue
- ❑ Ne fait pas table rase de l'existant, mais l'intègre
- ❑ Objectif : avoir un SII structuré pour améliorer ses performances et son évolutivité

Sécurité informationnelle

La sécurité informationnelle devrait être basée sur l'identification précise et documentée des actifs informationnels.

Actif informationnel = Information Assets

L'actif est un élément représentant une valeur pour l'organisme (ISO 13335-1:2004; ISO 27001:2005).

« Les actifs informationnels, en effet, touchent tous les éléments rentrant dans le processus de mise en place et d'exploitation des systèmes d'information de l'entreprise. Cela prend en compte le matériel informatique, les processus, les données, de même que l'information conservée sur support papier ou sur tout autre type de support » (Vallès, 2015)

Information Assets

"(…) An asset is any data, device, or other component of the environment that supports information-related activities. (…) Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization" (InterPARES, 2017)

Deux cas pertinents à explorer à cet égard :

- ❑ Canada, Guide de catégorisation de l'information (2016)

  SECRÉTARIAT DU CONSEIL DU TRÉSOR QUÉBEC, 2016. *Guide de catégorisation de l'information* [en ligne]. Juillet 2016. [Consulté le 18 octobre 2019]. Disponible à l'adresse : https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/categorisation_information.pdf

- ❑ Royaume-Uni, Registre des actifs informationnels (2017)

  THE NATIONAL ARCHIVES, 2017. *What is an Information Asset Register?* [en ligne]. Février 2017. [Consulté le 18 octobre 2019]. Disponible à l'adresse : https://www.nationalarchives.gov.uk/documents/information-management/info-asset-register-factsheet.pdf

Remarque : Il est fortement suggéré d'inviter un intervenant externe, pour un témoignage professionnel ou/pour un éclairage et complément d'information technique

La gouvernance informationnelle

"IG is a subset of corporate governance, and includes key concepts from records management, content management, IT and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, long-term digital preservation, and even business intelligence." (Smallwood 2014, p. 5)

Types d'évaluation

Un travail de groupe sur une étude de cas : analyse et présentation

Ressources bibliographies

Blogs

CLULEY, Graham, 2019. *Graham Cluley: Computer security news, advice and opinion* [en ligne]. 2001-2019. [Consulté le 18 octobre 2019]. Disponible à l'adresse : https://www.grahamcluley.com

GHERNAOUTI, Solange, 2019. *Cybersécurité | Le blog de Solange Ghernaouti* [en ligne]. 2018-2019. [Consulté le 18 octobre 2019]. Disponible à l'adresse : https://blogs.letemps.ch/solange-ghernaouti/

KERBS, Brian, 2019. *KrebsonSecurity: In depth security news and investigation* [en ligne]. 2010-2019. [Consulté le 18 octobre 2019]. Disponible à l'adresse : https://krebsonsecurity.com

SCHNEIER, Bruce, 2019. Schneier on Security [en ligne]. 2004-2019. [Consulté le 18 octobre 2019]. Disponible à l'adresse: https://www.schneier.com

HUNT, Troy, 2019. *Troy Hunt* [en ligne]. 2009-2019. [Consulté le 18 octobre 2019]. Disponible à l'adresse : https://www.troyhunt.com

Lectures

UNITED KINGDOM GOVERNMENT - NATIONAL CYBER SECURITY CENTRE, 2018a. *Mitigating Malware: How organisations and home users can reduce the likelihood of malware infection* [en ligne]. 8 février 2018. [Consulté le 18 octobre 2019]. Disponible à l'adresse : https://www.ncsc.gov.uk/guidance/mitigating-malware

UNITED KINGDOM GOVERNMENT - NATIONAL CYBER SECURITY CENTRE, 2018b. *Risk management guidance: Guidance to help organisations make decisions about cyber security risk* [en ligne]. 8 août 2016. Mis à jour le 16 novembre 2018. [Consulté le 18 octobre 2019]. Disponible à l'adresse : https://www.ncsc.gov.uk/collection/risk-management-collection

UNITED KINGDOM GOVERNMENT - NATIONAL CYBER SECURITY CENTRE, 2018c. Step 3 - Keeping your smartphones (and tablets) safe. *Small Business Guide: Cyber Security* [en ligne]. 15 novembre 2018. [Consulté le 18 octobre 2019]. Disponible à l'adresse : https://www.ncsc.gov.uk/collection/small-business-guide/keeping-your-smartphones-and-tablets-safe

UNITED KINGDOM GOVERNMENT - NATIONAL CYBER SECURITY CENTRE, 2019. *Phishing attacks: defending your organisation* [en ligne]. 5 février 2018. Mis à jour le 8 août 2019. [Consulté le 18 octobre 2019]. Disponible à l'adresse : https://www.ncsc.gov.uk/guidance/phishing

Références

Asset (computer security). *Wikipedia The Free Encyclopedia* [en ligne]. Dernière modification de la page le 10 juillet 2017 à 20:58. [Consulté le 22 septembre 2017]. Disponible à l'adresse : https://en.wikipedia.org/w/index.php?title=Asset_(computer_security)&oldid=789980839

CARIOU, Marjorie, 2016. *Criticité des documents : Ecart entre perception et évaluation. Apport de la norme ISO 18128:2014 Cas du Crips Ile-de-France* [en ligne]. Paris : Conservatoire national des arts et métiers (Cnam). Rapport pour l'obtention du Certificat de spécialisation « Maîtrise de l'archivage à l'ère numérique ». [Consulté le 12 septembre 2017]. Disponible à l'adresse : http://www.marjorie-cariou.info/cv/portfolios/criticite-des-documents-ecarts-entre-perception-et-evaluation-apport-de-la-norme-iso-18128-2014-cas-du-crips-ile-de-france-1

CENTRE NATIONAL DE RESSOURCES TEXTUELLES ET LEXICALES (CNRTL), 2012. RISQUE : Définition de RISQUE. *Cnrtl.fr* [en ligne]. [Consulté le 28 septembre 2017]. Disponible à l'adresse : http://www.cnrtl.fr/definition/risque

CLEMENT, J., 2019. Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions). *Statista* [en ligne]. 5 août 2019. [Consulté le 26 septembre 2019]. Disponible à l'adresse : https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), [s. d.]. *Le management des risques de l'entreprise - Cadre de Référence* [en ligne]. [Consulté le 16 août 2017]. Disponible à l'adresse : https://www.coso.org/Documents/COSO-ERM-Executive-Summary-French.pdf

CONFÉDÉRATION SUISSE, 2010. *Directives sur la politique de gestion des risques menée par la Confédération* [en ligne]. 24 septembre 2010. [Consulté le 28 septembre 2017]. Disponible à l'adresse : https://www.efv.admin.ch/dam/efv/fr/dokumente/finanzpolitik_grundl/risiko_versicherungspolitik/Weisungen_Risikopolitik_f.pdf.download.pdf/Weisungen_Risikopolitik_f.pdf

DESROCHES, Chantal, 2013. *La gestion des risques informationnels dans l'entreprise privée : perspective des gestionnaires de la sécurité* [en ligne]. Montréal : Université de Montréal. Mémoire. [Consulté le 16 août 2017]. Disponible à l'adresse : https://papyrus.bib.umontreal.ca/xmlui/handle/1866/11469

Directive 2012/18/UE du Parlement européen et du Conseil du 4 juillet 2012 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses, modifiant puis abrogeant la directive 96/82/CE du Conseil. *EUR-Lex* [en ligne]. 4 juillet 2012. [Consulté le 14 août 2017]. Disponible à l'adresse : http://eur-lex.europa.eu/eli/dir/2012/18/oj

HARBULOT, Christian, 2005. *La manipulation de l'information. Symposium sur la Sécurité des Technologies de l'Information et des Communications* [en ligne]. Rennes: 1 au 3 juin 2005. [Consulté le 22 août 2017]. Disponible à l'adresse : http://piloupilou.sstic.org/SSTIC05/Entreprise_face_au_risque_informationnel/SSTIC05-Harbulot-Entreprise_face_au_risque_informationnel.pdf

LACROIX, Jérémie, 2007. *Analyse et gestion des risques dans les grandes entreprises : Impacts et rôle pour la DSI* [en ligne] Institut d'Etudes et de Recherche pour la Sécurité des Entreprises (IERSE) et Club Informatique des Grandes Entreprises Françaises (CIGREF), 2007. [Consulté le 16 août 2017]. Disponible à l'adresse : http://cigref.typepad.fr/cigref_publications/RapportsContainer/Parus2007/gestion_des_risques/Analyse_et_gestion_des_risques_dans_les_grandes_entreprises_-_impacts_pour_la_DSI-rapport_2007_web.pdf

LÉGER, Marc-André, 2013. *Introduction à la gestion de risque informationnel* [en ligne]. Montréal : Centre de recherche Hochelaga-Maisonneuve, 1er mars 2013 [Consulté le 16 août 2017]. Disponible à l'adresse : http://www.leger.ca/wp-content/uploads/2015/09/Introduction-%C3%A0-la-gestion-de-risque.pdf

LÉGER, Marc-André, 2015. Typologie des risques informationnels. *Le site de Marc-André Léger* [en ligne]. 23 octobre 2015. [Consulté le 16 août 2017]. Disponible à l'adresse : http://www.leger.ca/2015/10/23/typologie-des-risques-informationnels/

MOORE, Susan, KEEN, Emma, 2018. Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. *Gartner* [en ligne]. 15 août 2018. [Consulté le 26 septembre 2019]. Disponible à l'adresse : https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

ORGANISATION INTERNATIONALE DE NORMALISATION, 2011. *Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information*. 2e éd. Genève : ISO, 6 janvier 2011. ISO/IEC 27005

ORGANISATION INTERNATIONALE DE NORMALISATION, 2014. *Information et documentation - Évaluation du risque pour les processus et systèmes d'enregistrement*. Genève : ISO, 15 mars 2014. ISO/IEC 18128

SMALLWOOD, Robert F., 2014. *Information governance: concepts, strategies and best practices*. Hoboken : Wiley. Wiley CIO series. ISBN 9781118218303.

TRAVAUX PUBLICS ET SERVICES GOUVERNEMENTAUX CANADA, 2019. INFOSEC. *TERMIUM Plus®, la banque de données terminologiques et linguistiques du gouvernement du Canada* [en ligne]. [Consulté le 18 octobre 2019]. Disponible à l'adresse : http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&srchtxt=INFOSEC&i=1&index=frr&codom2nd_wet=1#resultrecs

VALLÈS, Lyonel, 2015. Le risque informationnel et l'urgence de le gérer de façon adéquate. *Lyonel Vallès, CISA, CRISC* [en ligne]. 20 décembre 2015. [Consulté le 22 août 2017]. Disponible à l'adresse : http://lyonelvalles.com/2015/12/20/le-risque-informationnel-et-lurgence-de-le-gerer-de-facon-adequate/

VERMEYS, Nicolas, 2009. *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile* [en ligne]. Montréal: Université de Montréal. Thèse. [Consulté le 22 août 2017]. Disponible à l'adresse : https://papyrus.bib.umontreal.ca/xmlui/handle/1866/3663