Deloitte.

Cybersécurité et protection de la vie privée : répercussions sur l'enseignement supérieur au Canada

Comment votre établissement vivra-t-il la reprise et la prospérité?

Table des matières

L'enseignement supérieur en temps de pandémie mondiale

La COVID-19 a semé une incertitude généralisée qui est appelée à persister dans le secteur de l'enseignement supérieur où les défis sont pressants et complexes. Les collèges et les universités ont dû réagir rapidement pour résoudre un certain nombre de problèmes pédagogiques pressants, dont l'augmentation de l'enseignement à distance (c'est-à-dire l'adaptation de l'enseignement en classe à l'univers virtuel) et de la formation en ligne, l'élaboration de stratégies de correction et de diplomation, et l'offre d'un soutien supplémentaire aux étudiants sous la forme de programmes de mieux-être. Toutes ces nouveautés sont rapidement devenues la nouvelle normalité à l'ère de la COVID-19.

Dans le cadre de notre engagement envers le secteur de l'enseignement, Deloitte a publié un rapport intitulé Planification des répercussions de la COVID-19 sur l'enseignement supérieur au Canada qui s'appuie sur le cadre « **Réaction, reprise et prospérité** » de Deloitte, qui offre une vision tridimensionnelle de la gestion de crise. Compte tenu de la fluidité de la situation et de nos engagements antérieurs, nous nous concentrons dans le présent document sur les préoccupations relatives à la cybersécurité et à la protection de la vie privée en nous attardant à une série de considérations que nous jugeons cruciales.

Même si ces **préoccupations relatives à la cybersécurité et à la protection de la vie privée** ne figuraient pas auparavant au sommet de nos priorités, certaines raisons nous incitent maintenant à nous y consacrer :

- **Certains auteurs de menaces abusent actuellement** de l'environnement créé par la COVID-19 en multipliant les attaques contre les employés et les étudiants forcés de fonctionner dans l'univers du télétravail et du télé-enseignement.

- La pandémie a entraîné une **augmentation imprévue, et néanmoins substantielle, du recours au télétravail**. Une multitude d'étudiants et d'employés se branchent désormais à distance au moyen d'ordinateurs personnels et à partir de réseaux non sécurisés.

- **Les chercheurs demeurent des cibles attrayantes**. Dans certains établissements d'enseignement[1], les chercheurs qui s'intéressent à la COVID-19 sont ciblés par des courriels d'hameçonnage très perfectionnés capables d'installer des logiciels de rançon et de perturber les activités de recherche.

- Il est possible que dans certains établissements, la protection des **actifs les plus précieux** (c. à d. les systèmes et les données clés) soit insuffisante.

- Afin de faciliter le télétravail, **de nouvelles applications** sont constamment installées, mais sans être systématiquement soumises aux tests rigoureux de protection de la vie privée qui auraient été exigés avant la pandémie.

Compte tenu de la sensibilité des données dans le contexte de l'enseignement supérieur, et maintenant que nous pouvons commencer à entrevoir la forme que prendra le retour du personnel sur les lieux de travail, il faut accorder une attention particulière aux considérations relatives à la cybersécurité et à la protection de la vie privée afin que tous les intéressés puissent évoluer dans cet univers en toute sécurité. Lorsque nous réintégrerons finalement nos lieux de travail, ce retour sera vraisemblablement progressif. Certains employés et étudiants recommenceront à travailler sur place tandis que d'autres continueront de le faire à distance, ce qui donnera aux établissements d'enseignement supérieur la possibilité de mettre en place des contrôles additionnels tout en continuant de surveiller l'application de la réglementation actuelle.

[1]. « Caution : Cyber security campaign targeting COVID-19 researchers », Research Alerts, University of Guelph, https://www.uoguelph.ca/research/alerts/content/caution-cyber-security-campaign-targeting-covid-19-researchers.

Cadre de gestion de crise

Appelé « Réaction – Reprise – Prospérité », notre cadre s'appuie sur une vision tridimensionnelle de la gestion de crise au fil du temps. Les établissements d'enseignement se situent actuellement à la phase « réaction » et ont déployé beaucoup d'efforts pour parer aux problèmes immédiats. Les établissements se préparent maintenant à s'engager dans la phase de « reprise » et il sera important qu'ils se concentrent sur les conséquences à plus long terme de la crise et, à cette fin, qu'ils planifient soigneusement chacune de leurs actions pour être bien positionnés en prévision de la réintégration des lieux de travail.

Réaction	Reprise	Prospérité
• Atténuer les problèmes immédiats : p. ex., effectuer la transition vers les cours en ligne, élaborer un plan pour les examens et les évaluations finales, déplacer les étudiants à l'extérieur du campus. • Gérer les prévisions financières et la planification de scénarios : surveiller les tendances et répertorier toutes les considérations liées à la COVID-19, puis évaluer leurs répercussions financières possibles dans différentes situations. • Investir dans les tâches et les systèmes clés : p. ex., acquérir et fournir les technologies nécessaires à l'apprentissage à distance et au télétravail, à la cybersécurité et à l'aide financière aux étudiants. • Mettre en œuvre des protocoles de gestion de trésorerie et de réduction des coûts : ces protocoles peuvent inclure des mesures pour limiter les déplacements non essentiels, et la consommation d'électricité et de gaz, et pour réduire les heures de travail.	• Planifier la viabilité financière : permet la transition du mode de simple survie à la stabilité. • Atténuer les problèmes à plus long terme : peut comprendre les problèmes de cybersécurité et le nombre incertain d'inscriptions. • Effectuer des investissements stratégiques : p. ex., au moyen d'une aide supplémentaire aux étudiants et du développement plus poussé des systèmes et programmes d'apprentissage à distance.	• Se concentrer sur la solvabilité et la santé financière à long terme : l'objectif est d'assurer la viabilité et d'atteindre les objectifs financiers. • Viser des programmes d'apprentissage numérique et des expériences en ligne pour les étudiants de niveau supérieur : avec ces mises à niveau, on s'attend à ce que les étudiants bénéficient de nouveaux atouts sur le plan éducatif et de l'apprentissage. • S'adapter à la nouvelle normalité : établir de nouveaux modes de fonctionnement dans le monde de l'après-COVID-19 et y adhérer.

Le présent document a pour objet d'aider les établissements dans la phase de reprise pendant laquelle il leur faudra **atténuer les problèmes à plus long terme et plus précisément les problèmes de cybersécurité et de protection de la vie privée** (voir l'étape pertinente entourée d'un rectangle rouge ci-dessus).

Principaux facteurs et incertitudes à considérer

Au cours de cette période imprévisible, il sera essentiel pour les établissements de faire preuve de **rapidité** et d'**agilité** plutôt que de chercher la perfection à tout prix et de s'attarder de manière excessive aux détails et au temps global consacré à l'effort. Dans l'environnement typique de l'enseignement supérieur, voici quelques exemples de facteurs clés porteurs de changement qui seront nécessaires pendant la phase de reprise :

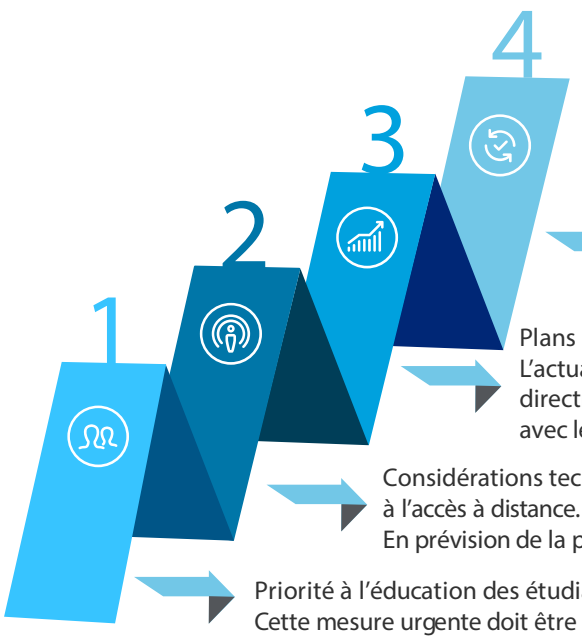
1. **Actifs les plus précieux** : Il importe de déterminer quels actifs les plus précieux (ceux qui sont essentiels à la mission de l'établissement) sont le plus touchés par la pandémie et de trouver le moyen de rapidement adresser tout problème de cybersécurité ou de protection de la vie privée susceptible de se présenter. Ainsi, si des étudiants étrangers bénéficient d'un accès à distance à leur faculté et à leurs cours, quels sont les risques dont il faut tenir compte? Les mesures de sécurité empêcheront-elles l'application d'un filtre d'accès fondé sur la géolocalisation?
2. **Décentralisation des activités :** Comment les établissements gèrent-ils la nature fortement décentralisée des différentes facultés et de la propriété des données?

- Par exemple, dans bien des cas, les droits sur la recherche appartiennent aux chercheurs ou sont contrôlés par ceux-ci. Les données sont-elles stockées sur un serveur sécurisé géré lui-même par un groupe centralisé de TI? Ou sont-elles plutôt stockées sur les ordinateurs des chercheurs?

- Au début de la pandémie, plusieurs changements ont été adoptés rapidement afin de faciliter l'apprentissage virtuel et l'accomplissement à distance d'autres tâches. Ces changements ont-ils été depuis approuvés par les syndicats et les groupes de relations de travail pertinents?

3. **Retombées sur les politiques, les procédures et les contrats :** Depuis un an, les établissements d'enseignement supérieur ont rapidement mis en place des systèmes de télétravail. Le temps est-il maintenant venu d'analyser les retombées de ce nouveau mode de travail sur les politiques et les procédures ainsi que sur les plans de continuité des activités? Des mesures appropriées de gestion des parties prenantes ont-elles été mises en place (p. ex., groupes de relations de travail, groupes de négociation des conventions collectives)?

Vous trouverez ci-dessous un sommaire des **quatre considérations tactiques** et recommandations qui, à notre avis, devraient être analysées avec les préoccupations susmentionnées. Vous trouverez par ailleurs plus de détails relatifs à celles-ci aux pages 5 à 9 du présent document.



Priorité à l'éducation des étudiants et des employés
Cette mesure urgente doit être prise avant même d'apporter des changements techniques.

Considérations techniques relatives à la protection de l'identité et à l'accès à distance.
En prévision de la phase de prospérité, quelles mesures doivent être adoptées?

Plans de continuité des activités (PCA)
L'actualisation des PCA et des politiques, procédures et lignes directrices pertinentes facilitera la reprise des établissements avec le moins d'effets nuisibles possible.

Surveillance continue à long terme
Il est important de se concentrer sur la nécessité de constamment s'ajuster à la nouvelle normalité.

1. Priorité à l'éducation des étudiants et des employés

Avec un effectif nombreux et une population étudiante non moins nombreuse travaillant à distance, les vecteurs possibles de menaces contre la cybersécurité se multiplient. L'accès à distance généralisé a pour principale conséquence que les employés aussi bien que les étudiants mènent maintenant leurs activités depuis des réseaux Wi-Fi domestiques non sécurisés et non surveillés. Le risque que représentent les éventuelles attaques d'hameçonnage et autres s'en trouve amplifié. Voici les principales mesures immédiates qu'il est recommandé de mettre en œuvre :

- Aider les utilisateurs à mettre en place chez eux les **mesures fondamentales « d'hygiène réseau »** en leur communiquant les pratiques exemplaires consistant à segmenter leur réseau domestique en créant une zone privée et une zone professionnelle, et à s'abstenir autant que possible d'utiliser les réseaux Wi-Fi publics ou non sécurisés sans recourir à des logiciels de chiffrement appropriés.

- S'assurer que les utilisateurs ont bien modifié le **mot de passe par défaut du routeur** de leur réseau Wi Fi domestique et que le nouveau mot de passe est fort.

- Éduquer les utilisateurs sur la manière d'éviter les **mots de passe souvent utilisés ou figurant dans le dictionnaire**.

- Communiquer aux utilisateurs de l'information sur les fraudes d'ingénierie sociale et les campagnes d'hameçonnage propres à la pandémie de COVID-19 et leur enseigner comment les détecter et éviter de tomber dans le piège. Pour les étudiants, il serait peut-être approprié d'intégrer au début de chaque cours une séance d'information ou de formation **de cinq minutes**. On peut à cette fin utiliser des trousses d'outils comme celle offerte par le SANS Institute, une organisation de recherche et d'éducation en cybersécurité (voir la liste à puces ci-dessous), qui recommande de **se fier davantage aux personnes qu'à la technologie pour** prévenir les fraudes d'ingénierie sociale, d'utiliser un gestionnaire de mots de passe et, pour les employés, de réserver certains appareils aux usages professionnels, et d'autres aux usages personnels.
  - Trousse de sensibilisation à la sécurité SANS pour le télétravail : (en anglais seulement)
  - Plateforme de gestion de l'apprentissage SANS et hameçonnage : (en anglais seulement)

- Former les utilisateurs à la **sécurisation de l'accès physique** à leurs appareils afin d'en prévenir le vol et, par conséquent, de prévenir le vol de données appartenant à l'université.

- Informer les utilisateurs au sujet des **politiques de cybersécurité** à distance de leur établissement ainsi que des meilleures pratiques en la matière et plus particulièrement celles portant sur les protocoles d'accès à distance, l'utilisation des appareils personnels, les lignes directrices sur la gestion des mots de passe et les mesures d'authentification et de contrôle des accès privilégiés.

2. Centrer l'action sur le reprise fonctionnel dans le sillage des conséquences techniques de la COVID-19

Comme les établissements d'enseignement ont dû opérer un virage rapide vers la nouvelle normalité, certaines des décisions prises l'ont peut-être été avant tout dans un souci de rapidité et de simplicité. Afin de répertorier ces décisions, il est recommandé de procéder à une **analyse rapide des risques liés aux configurations informatiques d'apprentissage à distance** et notamment d'étudier comment les utilisateurs se branchent aux portails de l'établissement et avec quels appareils (étudiants et employés). Il est de plus conseillé que **l'acceptation de ces risques** et d'autres risques soit formellement consignée par écrit.

Lorsque des utilisateurs passent massivement à **l'accès à distance**, il arrive que les équipes de TI éprouvent des difficultés **à appliquer et à maintenir des contrôles de sécurité rigoureux**. Comme la surveillance du trafic est généralement indispensable sur les réseaux d'entreprise gérés centralement auxquels se branchent à distance les utilisateurs, les politiques de sécurité et de surveillance devraient se concentrer sur les éléments de base décrits ci-dessous, ce qui contribuera à protéger les actifs les plus précieux. Veuillez prendre note que ces dispositions doivent être suffisamment souples pour s'adapter à la nature fortement décentralisée de nombreux établissements d'enseignement supérieur.

- **Protection de l'identité** : S'assurer que les utilisateurs à distance des portails d'apprentissage en ligne se soumettent à des procédures de vérification et de validation multifactorielles. Voici quelques exemples :
  - **Politiques de mots de passe forts.** Les mots de passe devraient être suffisamment complexes et comporter des échéances comme ceux de l'établissement.
  - Nombre **limité** d'échecs de connexion. Un nombre précis de tentatives devrait être fixé, et une fois ce nombre franchi, l'utilisateur devrait être temporairement bloqué.
  - **Authentification à deux facteurs (A2F) ou authentification multifactorielle (AMF).** Envisager de rendre obligatoire une solution A2F ou AMF pour les étudiants, si possible, sans négliger d'évaluer les conséquences de ce choix sur le personnel en télétravail. Faudra-t-il accroître l'effectif des services d'assistance technique virtuels pour aider les étudiants à s'inscrire à ce nouveau mode d'authentification?
  - **Filtre d'accès fondé sur la géolocalisation.** Veuillez prendre note que cette option peut ne pas être disponible.
- **Options d'accès à distance** : **Utiliser des réseaux sécuritaires.** Envisager le recours à un réseau privé virtuel (RPV) ou à une passerelle d'accès à distance (en sus du vulnérable protocole « *hypertext transfer protocol secure* » ou HTTPS) au réseau universitaire. La sécurisation des réseaux est plus importante que jamais dans un contexte de multiplication des dispositifs actuellement utilisés pour se brancher et travailler ou étudier à distance.
  - Dans la mesure du possible, s'assurer que les utilisateurs sont tenus d'ouvrir une session sur le RPV pour accéder au portail de l'université. On ajoute ainsi une couche de protection entre le réseau de l'université et les réseaux domestiques non sécurisés souvent utilisés par les utilisateurs.
  - Diffuser des directives détaillées afin que les étudiants téléchargent un RPV à partir d'un site web approuvé de l'établissement afin d'éviter la propagation des virus et des logiciels malveillants et les pannes généralisées parfois causées par des applications obtenues sur des sites non autorisés.
  - Analyser les retombées de ces nouvelles méthodes de travail auprès des groupes pertinents de relations de travail.
- Procéder à des **évaluations des risques liés aux tiers**. Communiquer avec les fournisseurs de logiciels-services (SaaS) et s'informer de leurs plans de continuité des activités.
- Confirmer les exigences relatives aux licences d'utilisation de technologies. Étudier les coûts des nouveaux services de voix par protocole Internet (VoIP), d'obtention de licences additionnelles pour les services de webconférences ou d'ajout de capacité au RPV pour tenir compte de l'augmentation du nombre d'utilisateurs en télétravail.

- **Autres considérations techniques :**
  - Demander aux équipes de sécurité de passer en revue les **règles relatives aux parefeu** ou d'en établir à l'intention de ceux qui accèdent à vos systèmes à distance, d'analyser l'utilisation et les comportements des utilisateurs (UEBA), de surveiller l'intégrité des fichiers et de mettre en place des mesures de lutte contre les logiciels malveillants et les intrusions. Toute lacune de sécurité devrait être évaluée et des contre-mesures être mises en place le plus rapidement possible.
  - **Examiner** tous les services et dispositifs d'accès à distance afin de s'assurer que les microprogrammes et les rustines de sécurité sont à jour. Fermer tous les ports ouverts sans raison et établir la nature du trafic sur les ports non standard.
  - S'assurer que **tous les correctifs requis** ont été installés sur les outils et applications ou systèmes utilisés dans votre univers informatique (c.-à-d. que toutes les vulnérabilités ont été éliminées et que les systèmes sont à jour).
  - **Revoir le processus d'autorisation ou de refus de l'accès aux utilisateurs** fondé sur les raisons d'accès et sur la durée et la fréquence des demandes d'accès.
  - Appliquer **de manière constante et stricte le respect de toutes les exigences d'audit et de conformité** pendant la période d'accès à distance d'un utilisateur. Les organisations devraient porter une attention particulière à la surveillance des activités pendant les sessions à distance et les documenter, et à l'utilisation des identifiants afin de s'assurer que les exigences de conformité sont respectées et de faciliter toute analyse judiciaire future.

3. Passer en revue les plans de continuité des affaires (PCA) et les politiques, procédures et lignes directrices de sécurité et de protection de la vie privée pertinentes

Compte tenu de la nature changeante de l'environnement dans lequel les collèges et universités exercent actuellement leurs activités étant donné le niveau d'agilité qu'exige l'accomplissement de chaque tâche clé, il est important de revoir les conseils stratégiques typiques suivants qui ont pour but de guider les organisations en ces périodes troubles. N'oubliez pas que dans le contexte actuel, il est impossible d'étaler ces tâches sur plusieurs mois; elles doivent être exécutées rapidement

- **Revoir et actualiser les protocoles existants :**
  - **Passer en revue et hiérarchiser les politiques, procédures et lignes directrices de sécurité actuelles** afin de s'assurer qu'elles sont suffisamment résilientes pour accommoder l'augmentation du nombre d'étudiants en apprentissage à distance. Ces protocoles devraient porter sur certains facteurs comme la gestion des accès à distance, l'utilisation des appareils personnels, la mise à jour des considérations relatives à la protection de la vie privée pour l'accès à des documents et d'autres données et l'utilisation accrue de technologies parallèles (c.-à-d., des programmes qui ne sont ni gérés ni supervisés par les services de TI de l'établissement) et de l'infonuagique.
  - S'assurer que les politiques, les procédures et les lignes directrices de sécurité et de protection de la vie privée de l'établissement **donnent de la visibilité à** des logiciels-services (SaaS) de collaboration et à des services de clavardage comme Zoom (utilisé souvent pour l'apprentissage virtuel), Google Meet, Cisco Webex, Google Classroom, Slack et Microsoft Teams auxquels les utilisateurs (étudiants ainsi que professeurs et instructeurs) se sont adaptés dans la nouvelle réalité. Ce principe s'applique également à la propriété des données et aux outils utilisés pour la faciliter (voir **Décentralisation des activités** à la page 4 du présent document).
  - Définir et continuer d'évaluer les systèmes et les stratégies qui respectent **les lignes directrices sur la protection de la vie privée, la sécurité et l'éthique** applicables aux utilisateurs des services d'apprentissage à distance.
  - **Entretenir un dialogue constant** avec les administrateurs, instructeurs et groupes d'étudiants et les consulter au sujet des répercussions de l'apprentissage virtuel sur la sécurité et la protection de la vie privée à mesure que l'information devient disponible. Voici quelques exemples de questions qui peuvent être posées pendant ces rencontres :
  - Des renseignements permettant d'identifier une personne et des renseignements protégés sur la santé sont-ils collectés lorsqu'un étudiant utilise ces produits/plateformes? Dans l'affirmative, il pourrait s'agir d'une infraction

aux lois canadiennes sur la protection des renseignements personnels dont la Loi sur l'accès à l'information et la protection de la vie privée et la Loi sur la protection des renseignements personnels sur la santé et pourrait conduire à la marchandisation ou à la revente des renseignements personnels.

- L'établissement d'enseignement supervise-t-il seul ou avec l'aide d'un consortium (p. ex., le système de recherche et d'éducation ORION d'Ontario, le réseau de services partagés d'enseignement supérieur de Colombie-Britannique, BCNET) l'application par le fournisseur de pratiques appropriées en matière de protection des renseignements personnels?
- Mettre à jour les protocoles afin de régler tout problème cerné pendant un des examens de système continus.

- **Mettre à jour les PCA et plans de reprise après sinistre (PRAS) :**
  - Mettre à jour le PCA de l'établissement en y intégrant l'apprentissage à distance. Utiliser des procédures de continuité **testées et éprouvées,** y compris un PRAS, afin d'éviter toute interruption du service et d'assurer la continuité des activités. Évaluer les besoins de l'établissement en cherchant à répondre aux questions suivantes, entre autres :
  - Les actifs les plus précieux sont-ils répertoriés de manière appropriée dans les plans et procédures de continuité des activités et de reprise après sinistre?
  - Les actifs les plus précieux ont-ils changé depuis le dernier examen ou la dernière mise à jour?
  - Examiner les PCA afin de vous assurer qu'ils permettront le maintien **en toute sécurité des cours donnés à distance**. Cette évaluation devrait établir notamment si les étudiants peuvent avoir accès en toute sécurité aux ressources réseau requises à partir de leur domicile et devrait prendre en compte les méthodes sécurisées de partage de fichiers entre étudiants et enseignants.
  - Élaborer un plan et un guide tactiques afin de pouvoir réagir rapidement aux intrusions informatiques (p. ex., gestion de crise et plans en cas d'atteinte aux données). Ce plan devrait dresser la liste de toutes les parties prenantes comme les professeurs et autres formateurs, et tenir compte des nouveaux **cas d'utilisation de l'apprentissage à distance**.
  - Procéder à un **exercice sur table du travail à distance** avec des administrateurs et des responsables du corps professoral. Dresser l'inventaire des applications commerciales actuellement utilisées par l'établissement et désigner les actifs les plus précieux (les systèmes essentiels à la mission).
  - Mettre à jour les politiques de sécurité afin de les harmoniser avec le **recours accru à la connectivité à distance**, en insistant sur le renforcement nécessaire de la protection de la vie privée et des données, et sur la détection des intrusions depuis un nombre de points d'accès augmenté.

4. Surveillance continue à long terme

Simultanément à leur adaptation à la nouvelle normalité, les établissements d'enseignement doivent encadrer les étudiants et les employés, et surveiller la manière dont ils continuent de collaborer à distance. En sus des recommandations qui précèdent, les initiatives décrites ci-après pourraient faciliter le retour à la normale au moment du retour sur les lieux de travail.

- **Surveiller et inspecter continuellement** les actifs informatiques internes tout en automatisant l'analyse des corrélations entre les registres afin de détecter d'éventuels comportements anormaux. Serait-il possible de détecter ces comportements à partir d'un centre des opérations de sécurité virtuel puisque l'accès physique aux immeubles demeure restreint?

- Surveiller et examiner les registres des applications critiques à la recherche d'activités inhabituelles et de fuites ou de vols possibles de données, y compris les sessions sur le RPV et sur certaines applications comme Office 365. Ces vérifications sont particulièrement importantes dans le cas des systèmes qui contiennent de l'information pouvant identifier une personne ou des renseignements personnels sur la santé, y compris les outils de vidéoconférence indispensables à l'apprentissage virtuel. Veuillez prendre note que les exigences réglementaires de protection de la vie privée et de protection des renseignements personnels, dont celles énoncées dans les lois mentionnées précédemment, continuent de s'appliquer dans le contexte créé par la pandémie.

- Surveiller les alertes de **prévention de perte de données** et de fuite de données, et effectuer les enquêtes requises.

- Établir et tester la capacité de **détection et la vitesse de réaction** des outils de sécurité et évaluer la capacité de ces programmes de réagir aux demandes d'accès à distance, sans égard au lieu où se trouve l'utilisateur.

- Fournir aux analystes de sécurité les outils et les autorisations nécessaires pour intervenir à distance en cas d'incident et mettre en place un service d'évaluation des menaces, c. à d., les doter de l'équipement nécessaire pour détecter, contenir et prévenir à distance toute atteinte à la cybersécurité. Voici quelques exemples d'outils et d'autorisations qui pourraient être nécessaires :
  - accès aux registres et aux données de sécurité du réseau central;
  - accès au réseau de l'établissement (p. ex., RPV, HTTPS ou système RDP);
  - accès aux ordinateurs portables et aux appareils personnels ainsi qu'aux logiciels qui y sont installés;
  - identifiants d'administrateur, comme ceux associés aux comptes de service (c. à d. les comptes assortis de privilèges spéciaux plus importants que ceux accordés aux autres utilisateurs), aux comptes Linux Sudo (c.-à-d. ceux qui donnent accès aux fichiers et aux opérations à accès restreint) et aux clés ssh (qui permettent d'accéder à un système sécurisé sans avoir besoin d'un mot de passe);
  - instructions aux logiciels antivirus de reconnaître les outils de juricomptabilité et de RI qui pourraient être utilisés (pour s'assurer que le programme antivirus considère les programmes d'évaluation de l'analyste en sécurité comme des programmes sécuritaires plutôt que comme une menace possible pour le système).

Principaux conseils pour se prémunir contre une cyberattaque lors de l'apprentissage en ligne

Les cyberattaques peuvent avoir de lourdes répercussions financières ou nuire à la réputation des établissements d'enseignement supérieur à un moment où, en raison de la COVID-19, ils sont particulièrement vulnérables à d'éventuelles pertes. Il s'ensuit que les utilisateurs (administrateurs, étudiants et employés) doivent agir sans tarder pour protéger les systèmes contre toute atteinte.

Même si le « cours normal des activités » ne fait plus vraiment partie de la réalité des établissements d'enseignement supérieur ni même de leurs aspirations légitimes en cette période trouble, une occasion s'offre en ce moment à l'ensemble du secteur d'évaluer les risques majeurs de perturbations pour la société que représentent les intrusions informatiques et la compromission des données personnelles pouvant découler de l'accès à distance massif aux systèmes à partir de systèmes informatiques non sécurisés ainsi que les retombées profondes que ces changements pourraient avoir. Le cadre **Réaction – Reprise – Prospérité** permet aux établissements d'évoluer au fil des changements jusqu'à ce qu'ils atteignent le plateau de la « nouvelle normalité ». Dans le cadre de notre engagement auprès de ces établissements, nous promettons de continuer à communiquer nos points de vue et de formuler des recommandations s'appuyant sur notre cadre de gestion de crise.

Personnes-ressources

Daisy Vora
Associée, Conseils en gestion des risques
dvora@deloitte.ca

Aneesa Ruffudeen
Directrice de service, Conseils en gestion des risques
aruffudeen@deloitte.ca

Remerciements

Mark DiNello
Associé, Consultation
Leader national, Enseignement supérieur

Bruce Adams
Directeur de service, Consultation

Craig Robinson
Directeur de service, Consultation

Jamie Lanoue
Associé, Cyberrisques et risques stratégiques

Noemi Chanda
Directrice principale, Cyberrisques et risques stratégiques

Trimaan Dang
Directrice, Cyberrisques et risques stratégiques

Surbhi Purwar
Directrice, Cyberrisques et risques stratégiques

Deloitte.

www.deloitte.ca

À propos de Deloitte

Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans différents secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500MD par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

Notre raison d'être mondiale est d'avoir une influence marquante. Chez Deloitte Canada, cela se traduit par la création d'un avenir meilleur en accélérant et en élargissant l'accès au savoir. Nous croyons que nous pouvons concrétiser cette raison d'être en incarnant nos valeurs communes qui sont d'ouvrir la voie, de servir avec intégrité, de prendre soin les uns des autres, de favoriser l'inclusion et de collaborer pour avoir une influence mesurable.

Pour en apprendre davantage sur les quelque 312 000 professionnels de Deloitte, dont plus de 12 000 font partie du cabinet canadien, veuillez nous suivre sur LinkedIn, Twitter, Instagram ou Facebook.