Sécurité des Systèmes

La « cyber vigilance » dans les conseils scolaires de l'Ontario : *création d'une culture*

Août 2025

Chris Dale,
Directeur des solutions de sécurité
dss@ecno.org

Téléchargez ce manuel
ou écoutez le podcast
qui l'accompagne :
ECNO.org/CyberCulture

L'autorité en technologie des conseils scolaires de l'Ontario

La « cyber vigilance » dans les conseils scolaires de l'Ontario : création d'une culture

Les menaces en ligne ne sont plus uniquement l'affaire des équipes techniques des conseils scolaires. Plusieurs incidents récents à travers le Canada ont souligné cette réalité. Dans un conseil scolaire de l'Ontario, les élèves sont revenus de vacances d'hiver pour découvrir qu'ils n'avaient plus accès à Internet et que les communications étaient perturbées en raison d'une cyber-attaque[1]. Dans un autre cas, un enseignant a découvert que 17 membres du personnel avaient involontairement révélé leur mot de passe dans le cadre d'une escroquerie par hameçonnage[2]. Ces exemples envoient un message clair: **il est désormais essentiel de créer une culture de cyber vigilance** afin de protéger nos élèves, notre personnel et nos communautés scolaires. Ce texte explique ce que signifie une culture de la cyber vigilance dans le contexte scolaire au primaire et au secondaire, pourquoi elle est essentielle, ses bénéfices, les risques liés à son ignorance et comment les responsables des Conseils peuvent mettre en œuvre et maintenir une telle culture.

82%

Violation des accès aux données des écoles

En 2024, une enquête a révélé que 82% des institutions scolaires ont été victimes de violation des accès à leurs données.

575%

Augmentation des attaques

Le secteur de l'éducation est la cible la plus importante des cyber attaques avec une augmentation de 575% par an.

70%

Taux des erreurs humaines

Plus de 70 % des violations des accès aux données impliquent des erreurs humaines ou des méthodes de manipulation sociale des individus.

Ces chiffres mettent en évidence **l'ampleur de la menace** et le potentiel des **opportunités**. Si le facteur humain fait partie de la plupart des incidents alors l'accroissement du niveau de conscientisation et du niveau de connaissance du phénomène pourra réduire les risques de façon significative. Comme le mentionnait un expert en cybersécurité, *« la cybersécurité est un sport d'équipe »*; Chacun a un rôle à jouer en défense. La culture d'une cyber vigilance rendra cela possible.

Qu'est-ce qu'une culture de cyber vigilance dans les classes de M-12?

Une culture de cyber vigilance veut dire que chaque membre de la communauté du conseil scolaire est conscient des concepts de cybersécurité et joue un rôle actif dans la protection des informations. Dans un conseil scolaire M-12, cette culture commence dans les bureaux du conseil jusqu'à la salle de classe; Les conseillers scolaires, les directions, les surintendances, le personnel informatique, les enseignants, les élèves et même les parents partagent une compréhension commune des principes fondamentaux et des meilleures pratiques en matière de cybersécurité. Il s'agit d'un environnement où **les personnes sont formées pour reconnaître, signaler et déjouer les menaces de cybersécurité**, plutôt que de tout laisser sous la responsabilité du service informatique[1].

Les éléments clés d'une culture de cyber vigilance sont :

- Une r**esponsabilité partagée :** la sécurité est *« la responsabilité de tous »*, même si elle est dirigée et soutenue par l'administration[3]. **Des bureaux administratifs aux élèves, tous et chacun sont impliqués.** En fait, les programmes-cadres en Ontario mettent l'accent sur la création d'une culture de sensibilisation à la cybersécurité et à la protection de la vie privée *« dans toutes les écoles, au sein du conseil scolaire et à tous les niveaux de l'organisation »* afin de réduire considérablement les risques de violations des accès aux données[1].
- **Leadership et responsabilité : le leadership donne le ton.** L'engagement du plus haut niveau de l'administration est essentiel à la réussite[3]. Les dirigeants des conseils scolaires doivent promouvoir la cybersécurité dans les plans stratégiques, allouer des ressources et l'intégrer dans leurs politiques. Ils veillent également au respect des exigences réglementaires et des politiques internes en matière de protection de la vie privée, une obligation fondamentale en matière de leadership[2]. Lorsque les plus hauts dirigeants accordent visiblement une priorité à la cybersécurité (par exemple, en en faisant référence de façon régulière lors des réunions et des communications), cela souligne son importance pour toute l'organisation.
- **Formation continue : les activités de formation et de sensibilisation** continues sont le pilier de la culture. Le personnel et les élèves reçoivent régulièrement une formation sur la manière de détecter les courriels qui contienne de l'hameçonnage, d'utiliser des mots de passe forts, de protéger les données et d'adopter un comportement sûr en ligne. L'objectif est de développer des habitudes saines et sécuritaires afin que des comportements prudents et soucieux de la sécurité, deviennent une seconde nature dans le travail et l'apprentissage quotidien. Tout le monde doit savoir « s'arrêter et réfléchir » avant de cliquer sur des liens suspects ou de partager des informations sensibles. Par exemple, Timothy King, un enseignant, conseille au personnel *« de s'arrêter et de se méfier »* lorsqu'un événement impromptu se produit, renforçant ainsi un état d'esprit prudent[2].
- **Communication ouverte :** dans une culture cyber vigilance, les communications relatives aux menaces et au sujet des incidents sont **transparentes et non punitives**; Les personnes sont encouragées à signaler immédiatement leurs préoccupations ou leurs erreurs en matière de cybersécurité (comme cliquer sur un lien malveillant), cela sans crainte d'être blâmé, et de façon qu'une réponse rapide puisse y être apporté. Les conséquences tirées des incidents sont partagées afin qu'ils ne se reproduisent. Cette ouverture d'esprit contribue à éliminer la stigmatisation liée à la cybersécurité et contribue plutôt à la considérer comme une opportunité d'apprentissage pour tous.

- **Intégration dans nos activités quotidiennes :** la cyber vigilance/conscientisation ne se limite pas à des modules de formation annuels. Elle s'intègre à la vie scolaire quotidienne. Les enseignants insèrent le thème de la sécurité numérique dans leurs cours; les équipes informatiques partagent régulièrement leurs « Conseils de sécurité de la semaine » et les directions discutent de sécurité en ligne lors des rencontres scolaires. Les pratiques de sécurité (telles que la vérification d'identité pour les demandes à caractère sensible ou la double vérification des courriels suspects ou inhabituels) sont intégrées dans les procédures opérationnelles standard. Au fil du temps, ces pratiques deviennent aussi courantes que le verrouillage des portes de l'école le soir.

La cybersécurité est un sport d'équipe
Construire une culture de cyber vigilance veut dire que chacun, du conseil scolaire à la salle de classe, travaille ensemble pour la protection de l'école. Ce n'est pas seulement le problème des équipes techniques mais une mission partagée.

Les leaders donnent la note
L'administration défie la cyber sécurité, y alloue des ressources et donne l'exemple. Une culture de la sécurité débute au plus haut avec un appui sans équivoque et avec redevabilité.

Une conscience journalière
Dans un conseil cyber vigilant, les habitudes numériques sûres font parties des routines quotidiennes. Formation continue et communication ouverte font que la vigilance numérique est une deuxième nature pour les élèves et le personnel.

En pratique, une culture de cyber vigilance au primaire et secondaire crée un environnement scolaire plus sûr et plus résilient. Les gens comprennent pourquoi la cybersécurité est importante pour l'éducation, connaissent leur rôle dans la protection des données et des systèmes, et se sentent habilités à agir en toute sécurité. Il en résulte non seulement une défense plus solide contre les menaces cybernétiques, mais aussi la création d'une communauté qui valorise et protège la vie privée, la sécurité et un continuum dans l'apprentissage.

Les avantages pour les conseils scolaires

Investir dans une culture de la cyber vigilance apporte des avantages significatifs pour l'organisation du conseil dans sa globalité en particulier au niveau de sa direction et au niveau opérationnel.

- **Réduction du risque de violations des accès et interférences :** le principal avantage est la diminution du risque d'incidents cybernétiques coûteux. Lorsque le personnel et les élèves sont vigilants (par exemple, en sachant repérer les tentatives d'hameçonnage et en adoptant des pratiques sûres), le facteur humain dans les violations des accès aux données diminue considérablement. Cela peut *« réduire considérablement le risque de cybersécurité et de violations des accès aux données »* à tous les niveaux[4]. Moins d'incidents signifie moins de temps d'arrêt pour les systèmes informatiques et une perturbation minimale de l'enseignement en classe. Il est essentiel de maintenir les réseaux des écoles en état de fonctionnement, car une cyber-attaque réussie peut

« faire dérailler les activités quotidiennes des écoles » en paralysant leurs réseaux et l'accès aux données[1]. Une culture de cyber vigilance contribue ainsi à prévenir ces scénarios catastrophe.

- **Protection des données sensibles et respect de la vie privée :** les conseils scolaires détiennent une **vaste quantité de renseignements personnels** sur les élèves, leurs familles et sur le personnel, ce qui fait de la protection de la vie privée une préoccupation majeure. Une culture de la sécurité solide contribue à protéger les données contre tout accès non autorisé ou toute fuite d'informations. Cette culture n'est pas seulement le vecteur de bonnes pratiques, mais aussi d'une obligation légale et éthique. Les lois ontariennes sur la protection de la vie privée (MFIPPA) exigent que les conseils protègent les renseignements personnels qu'ils détiennent, et les nouvelles normes provinciales placent la barre encore plus haut. En 2025, l'Ontario a introduit l'exigence explicite pour les institutions publiques de « prendre des mesures raisonnables pour protéger les renseignements personnels… contre le vol, la perte et l'utilisation ou divulgation non autorisée »[1]. **La cyber vigilance garantit que tout le monde respecte les protocoles qui assurent la sécurité des dossiers scolaires des élèves et des renseignements personnels**. Ceci permet au Conseil de se conformer aux exigences réglementaires et de maintenir la confiance du public[6]. De plus, éviter les atteintes à la protection de la vie privée signifie également éviter les pénalités potentielles et les problèmes de non-conformité aux règlements.
- **Protection financière et réduction des coûts : les violations peuvent être extrêmement coûteuses :** la restauration des systèmes, le paiement des frais liés à la réponse aux incidents cybernétiques, les éventuels paiements de rançons, la notification des personnes concernées et le traitement des conséquences légales impliquent des coûts importants. Une culture proactive en matière de cybersécurité est bien moins coûteuse que la réaction à un incident majeur. En prévenant les incidents (ou en minimisant leur impact), les conseils évitent les **lourdes pertes financières** associées aux cyber-attaques. De plus, la cyber vigilance peut entraîner une réduction des primes d'assurance ou de meilleures conditions de couverture, car les assureurs reconnaissent que le risque est moindre lorsqu'une stratégie est en place.
- **Continuité opérationnelle et résilience :** le renforcement de la cyber vigilance améliore la résilience du Conseil. Son personnel est prêt à réagir calmement et de façon appropriée en cas d'événement suspect, en suivant des procédures déjà établies. Les services importants tels que les plateformes d'apprentissage en ligne, les services de messagerie et les systèmes de suivi de l'assiduité et de l'absentéisme du personnel sont moins susceptibles d'être interrompus pendant de longues périodes. Cela garantit que l'enseignement et l'apprentissage peuvent se poursuivre avec un minimum d'interruption, même en cas de menaces. Par exemple, disposer d'un plan d'intervention en cas d'incident et d'une équipe informée, signifie que même si une attaque se produit, elle sera contenue et la situation résolue plus rapidement[1]. En bref, un conseil scolaire cyber vigilant peut « encaisser les coups » et se remettre rapidement sur pied, ce qui est essentiel pour dispenser un enseignement sans interruption prolongée.
- **Réputation et confiance de la communauté :** Les parents et la communauté au sens large, attendent de leur conseil scolaire qu'il protège les informations des élèves et offre un environnement d'apprentissage sûr. La mise en place de pratiques solides en matière de cybersécurité renforce la confiance de la communauté. À l'inverse, une violation grave des accès aux données peut **éroder la confiance du public** : les familles peuvent s'inquiéter des vols d'identité ou remettre en question la compétence du Conseil. Les hauts dirigeants, en particulier les directions de l'éducation et les surintendances, sont pleinement conscients de leur devoir en tant que protecteurs des données des élèves. En investissant dans une culture de la cybersécurité, les conseils font preuve de

responsabilité et d'attention, renforçant ainsi leur réputation de gardiens responsables du bien-être des élèves. Maintenir cette confiance est primordial dans le secteur de l'éducation[6].

- **Innovation stimulée :** lorsqu'un conseil intègre des mesures de sécurité appropriées dans sa culture scolaire, il **libère l'organisation et lui permet d'innover en toute confiance**. Ses dirigeants peuvent rechercher de nouveaux outils d'apprentissage numériques et des services nuagiques en sachant que les risques seront gérés. Par exemple, le leadership solide d'un conseil de l'Ontario en matière de technologies de l'information et de sécurité lui a permis de devenir un conseil leader dans l'adoption de technologies nuagiques en toute sécurité[5]. Les membres de son personnel, cyber-vigilants, ont pu adopter des technologies telles que des plateformes de collaboration en ligne ou des applications d'apprentissage en ligne, avec un minimum de craintes, car ils savaient comment les utiliser en toute sécurité. En conséquence, une culture de cyber-vigilance peut être un catalyseur d'innovation pédagogique plutôt qu'un obstacle.

En résumé, une culture de cyber-vigilance agit comme une **police d'assurance et un stimulant de performance** pour le conseil scolaire : elle protège contre les catastrophes tout en renforçant la fiabilité des systèmes au quotidien et la confiance des parties prenantes. Cette culture aligne la cybersécurité dans l'axe de la mission du conseil, qui est de garantir un enseignement sûr et dépourvu d'interruptions.

Avantages pour le personnel, les élèves et pour la communauté

Une culture de la cybersécurité ne profite pas seulement à l'organisation; elle apporte des avantages concrets à toutes les intervenants concernés, les membres de son personnel, ses élèves, les parents et la communauté au sens large. Voici comment :

Le personnel et les enseignants : Les enseignants, les directions et le personnel de soutien acquièrent une tranquillité d'esprit et de précieuses compétences. Dans un environnement cyber vigilant, le personnel est moins susceptible d'être victime d'escroqueries qui pourraient compromettre les renseignements personnels et les systèmes informatiques de l'école. La culture permet d'apprendre à **identifier les menaces telles que l'hameçonnage dans les courriels et à les gérer les situations en toute confiance** (par exemple, en vérifiant toute demande inhabituelle qui pourrait se révéler être une escroquerie). Cela réduit le stress des individus: en effet, personne ne veut être celui qui a accidentellement ouvert la porte à intrus. Cela crée un environnement de travail plus positif et plus responsabilisant. De plus, la formation à la cybersécurité contribue au développement professionnel. Le personnel améliore ses compétences numériques et se tient au courant des dernières technologies. Étant donné que « l'informatique est à la base de tout » dans l'éducation moderne[2], la maîtrise de la cybersécurité est désormais une compétence essentielle pour les enseignants. Le personnel se sent également soutenu en sachant que le Conseil le soutient avec des procédures claires en cas de problème (par exemple, elles indiquent qui contacter en cas de suspicion de violation des accès). Dans l'ensemble, les employés se sentent plus en sécurité et plus confiants dans l'utilisation des technologies pour l'enseignement et dans l'administration.

Pour les élèves : une culture de cyber vigilance se traduit directement par un **environnement d'apprentissage plus sûr et des leçons de vie essentielles** pour les élèves. Les élèves d'aujourd'hui grandissent immergés dans la technologie. En intégrant la une cyber vigilance dans la culture scolaire,

nous les aidons à développer des habitudes en ligne saines et des compétences de réflexion critique. Ils apprennent à protéger leur vie privée, à gérer le harcèlement numérique en ligne, détecter les messages suspicieux, et à devenir des citoyens numériques responsables. Ces leçons vont au-delà des cours d'informatique : elles sont renforcées par des campagnes, des assemblées et l'intégration dans les programmes-cadres. Le système scolaire de l'Ontario, par exemple, fournit des ressources telles que la « Zone » *Cyber Security Ontario K-12*, qui propose des jeux et des vidéos *« conçus pour aider les générations futures à rester protégées alors qu'elles grandissent dans notre monde numérique en constante évolution »*[2]. Les élèves auront également moins de perturbations: lorsque les écoles évitent les pannes informatiques majeures dues à des rançongiciels ou à d'autres attaques de logiciels malveillants, les élèves ne perdent pas de temps précieux en classe ni de temps pour leur accès aux supports pédagogiques. De plus, impliquer les élèves dans la cybersécurité (par le biais de clubs, de concours ...) peut susciter leur intérêt pour des carrières dans les STEM et la cybersécurité, un domaine très en demande. En bref, les élèves bénéficient non seulement d'une protection, mais aussi d'une éducation : **ils acquièrent des connaissances et des compétences qui leur serviront toute leur vie** dans notre monde numérique.

Pour les parents et les familles : les parents confient aux conseils scolaires leurs informations personnelles et la sécurité de leurs enfants. Une culture solide en matière de cybersécurité **rassure les familles** sur le fait que cette confiance est méritée. Cela signifie que le conseil prend des mesures concrètes pour protéger les informations des parents et des élèves (adresses, informations sur la santé, bulletins scolaires, etc.) contre les usurpateurs d'identité ou les pirates informatiques. Cela réduit l'anxiété liée à la réception de ces « avis redoutés » concernant les violations des accès aux données dans le système scolaire[1]. Les parents peuvent être garantis que leur vie privée est respectée et protégée. Aussi, une culture de cyber vigilance passe souvent par la **sensibilisation et la formation des parents**. Les conseils peuvent partager avec ceux-ci des conseils sur les pratiques en ligne sûres pour les enfants à la maison et alerter rapidement les familles au sujet de toute nouvelle menace visant les élèves. Ce partenariat parents-Conseil aide à renforcer les habitudes de sécurité à la maison, créant ainsi un message cohérent pour les enfants. Par exemple, si une escroquerie par hameçonnage usurpe l'identité de l'école, un parent cyber-vigilant qui a été formé par les communications de l'école, saura comment vérifier l'origine de la communication et ne se laissera pas duper. Au bout du compte, les familles feront preuve d'une *plus grande confiance et satisfaction* envers le conseil scolaire lorsqu'elles savent que la cybersécurité est une priorité.

Pour la communauté et la société : Au-delà de la communauté scolaire immédiate, il existe des avantages sociétaux plus larges. Les écoles primaires et secondaires font partie de nos infrastructures essentielles : les sécuriser contribue à protéger nos communautés locales contre les menaces. Une attaque par rançongiciel contre un conseil scolaire peut avoir des répercussions telles que la fermeture des écoles ou la perte de renseignements personnels à des fins de fraude. En renforçant la résilience face à de telles attaques, les conseils contribuent à la stabilité de la communauté. De plus, **la cyber conscientisation des jeunes présente des avantages sociaux à long terme :** les élèves mettent leurs connaissances en pratique dans l'enseignement supérieur et sur le marché du travail, ce qui signifie que les citoyens et les employés de demain seront plus compétents en matière de cybersécurité. Cela contribue à améliorer le niveau de cybersécurité global de notre société au fil du temps. Les conseils scolaires qui font la promotion de la cybersécurité partagent souvent leurs connaissances avec d'autres institutions locales (bibliothèques, centres communautaires) et montrent l'exemple dans le secteur

public. Tout cela renforce la défense globale de la communauté contre les cybermenaces. Comme l'a souligné le ministre des Services publics et du développement des entreprises de l'Ontario, nous devons enseigner la cybersécurité aux jeunes, car la province est de plus en plus numérique et nous avons besoin que tout le monde mette en place des mesures de sécurité rigoureuses pour protéger les données et les services[2]. Un conseil scolaire cyber conscient est un leader communautaire dans cet effort.

En résumé, **toutes les parties prenantes ont à gagner lorsqu'une culture de cyber-vigilance est en place**. Le personnel et les élèves se sentent plus en sécurité et mieux informés. Les parents ont l'esprit plus tranquille. La communauté bénéficie de services éducatifs plus fiables et d'une génération mieux préparée au monde numérique. Ces avantages centrés sur la personne s'ajoutent aux avantages organisationnels. Ensemble, ils démontrent que la culture de la cybersécurité n'est pas seulement une initiative informatique, mais une amélioration globale de l'ensemble de l'écosystème scolaire.

Les risques de ne pas créer de culture de cyber vigilance

Que se passe-t-il lorsqu'un conseil scolaire ne favorise pas l'établissement d'une culture de cyber conscientisation? Les risques sont sérieux et mènent progressivement à une situation insupportable dans notre environnement où les menaces sont partout. Sans culture de cyber vigilance un conseil scolaire est essentiellement en train de **laisser les clés sur la porte** et inviter les cambrioleurs à entrer. Les risques principaux sont les suivants :

- **Risque élevé d'incidents cybernétiques :** en l'absence de cyber vigilance, la question n'est pas de savoir si un incident cybernétique se produira, mais quand. Les pirates informatiques ciblent activement le secteur de l'enseignement, attirés par les bases de données riches en information et par les systèmes de protection parfois dépassés. Les écoles sont devenues des « cibles attrayantes » pour les cybercriminels[1]. Si le personnel et les élèves ne sont pas sensibilisés aux menaces, le conseil scolaire est beaucoup plus vulnérable aux attaques communes telles que l'hameçonnage, les virus des logiciels malveillants ou les rançongiciels. Un simple clic involontaire sur un courriel malveillant peut compromettre l'ensemble du réseau des écoles. Prenons l'exemple de ce scénario d'hameçonnage impliquant un enseignant : 17 employés ont révélé leur code d'accès avant qu'un enseignant expérimenté en technologie n'intervienne[2]. Sans cette intervention ou sans formation préalable, cet incident aurait pu dégénérer en une violation totale des accès aux données du système du conseil scolaire. Le manque de cyber vigilance augmente considérablement la probabilité de réussite des attaques, car les pirates exploitent le facteur humain. Étant donné que plus de 70 % des violations impliquent une erreur humaine ou une manipulation psychologique de quelque façon[4], ne pas prendre en compte le facteur humain, c'est courir au désastre.
- **Grave perturbation de l'enseignement :** un cyber incident majeur peut paralyser le fonctionnement des écoles si un conseil scolaire ne s'est pas préparé. Par exemple, une attaque par rançongiciel peut mener à l'encodage de données critiques et mettre hors service les systèmes nécessaires à toutes les tâches, de la prise des présences à la communication avec les parents. Nous avons vu des cas où toute une partie d'un conseil scolaire a vu « pratiquement tout ce qu'elle utilise » s'arrêter : ordinateurs, systèmes de sonorisation, Internet et cela pendant des semaines[1]. Sans mesures

préalables de préparation (où chacun sait quoi faire et comment empêcher la propagation des incidents), la reprise peut être lente et chaotique. Cela peut se traduire par des jours d'enseignement perdus, des cours annulés, l'impossibilité d'accéder aux ressources pédagogiques et une agitation générale. Des fonctions de sécurité importantes (telles que les systèmes de communication pour des services d'urgence) pourraient ne pas fonctionner en cas de besoin[1]. Ne pas être cyber vigilant revient essentiellement à mettre en péril la capacité du conseil scolaire à remplir sa mission.

- **Des données sensibles exposées :** les conseils scolaires détiennent des décennies de données sensibles : dossiers scolaires, renseignements personnels, voire informations sur la santé et l'enfance en difficulté. Une faille dans le système de protection peut entraîner des violations d'accès massives aux données. Récemment, la violation d'un système d'information scolaire couramment utilisée a révélé des données sur les élèves et sur le personnel remontant à plusieurs décennies, y compris, dans certains cas, des renseignements telles que des numéros d'assurance sociale[1]. Sans une culture de la sécurité solide, de telles violations peuvent passer inaperçues et finir par prendre une ampleur plus importante avec le temps. Les conséquences peuvent être graves : les personnes exposées doivent faire face à des risques d'usurpation d'identité (les criminels peuvent s'emparer de l'identité d'élèves pour ouvrir des comptes frauduleux[1]), et le conseil scolaire est confronté à des responsabilités légales et aux coûts qui s'en suivent. Le commissaire à la protection de la vie privée mènerait alors une enquête et le conseil pourrait être jugé négligent si des mesures de protection et de sensibilisation de base n'avaient pas été mises en place. Ne pas cultiver la cyber-vigilance crée un risque pour la vie privée de ses élèves et celle de ses employés, ce qui peut faire perdre la confiance pendant longtemps voir plusieurs années.
- **Conséquences financières et légales :** Le coût d'un cyber incident peut être énorme, surtout si le conseil doit réagir à partir de rien. Les pirates qui verrouillent les données peuvent exiger le paiement d'une rançon ; même si celle-ci n'est pas versée, la restauration des services techniques peut coûter des centaines de milliers de dollars en heures supplémentaires, en équipement et en services d'expertises externes. Sans sensibilisation aux risques, le personnel pourrait également être plus enclin à enfreindre les réglementations telle que le traitement de manière incorrecte des données des élèves ou en ne rapportant pas un incident dans les délais impartis, ce qui peut avoir des conséquences légales. Avec l'émergence de nouvelles législations, les conseils qui ne suivent pas les meilleures pratiques en matière de cybersécurité pourraient faire l'objet d'un contrôle plus strict. Par exemple, alors que le nouveau projet de loi **194** en Ontario impose le signalement des violations des accès aux données et des mesures de protection des agences provinciales[6], les conseils scolaires sont tenus d'adopter des pratiques exemplaires similaires afin de « réduire les risques… et maintenir la confiance du public »[6]. Un conseil scolaire qui aura négligé la mise en place d'une culture de cyber vigilance pourrait se retrouver en situation de non-conformité si (ou lorsque) ces attentes rentrent en application. Même en l'absence de pénalités, il faudra également tenir compte de l'impact financier associée à la perte de confiance des donateurs ou du gouvernement après une brèche majeure. Les assureurs pourraient également augmenter leurs primes ou même refuser de couvrir les conseils scolaires dont la culture de sécurité est médiocre, ce qui se traduit par des coûts supplémentaires.
- **Érosion de la confiance des groupes concernés :** Le préjudice le plus irréparable causé par l'absence d'une culture de cyber vigilance est peut-être la perte de confiance des élèves, des parents et du personnel. Les familles modernes sont très conscientes des questions qui relèvent de la cybersécurité : elles lisent les titres des articles sur les violations des accès aux données dans les écoles et attendent de la transparence et des compétences. Si un conseil est victime d'un incident

évitable, par suite de négligence ou par manque de formation de ses employés, la confiance du public peut s'effondrer. Les parents peuvent hésiter à partager des informations ou à utiliser les services en ligne fournis par le conseil. Le moral du personnel peut également en souffrir. En effet, les employés ne veulent pas avoir l'impression de travailler dans un environnement numérique peu sûr ou, à l'inverse, ils peuvent redouter l'idée d'être désignés comme boucs émissaires-responsables si quelque chose tourne mal. La nouvelle d'un conseil scolaire qui a « échoué » dans la protection de ses données peut ternir sa réputation pendant des années. Il est plus difficile de rétablir la confiance après une violation des données que de la maintenir par des mesures proactives. Dans le domaine de l'éducation, la confiance et la crédibilité sont primordiales. Elles sont gravement menacées sans une culture solide en matière de cybersécurité.

En bref, ignorer l'établissement d'une culture de la cybersécurité est un pari risqué dont les résultats négatifs sont presque garantis. **Le climat cybernétique pour les écoles s'aggrave :** les attaques sont plus fréquentes (+575 % ces dernières années) et les menaces sont de plus en plus sophistiquées[4]. Sans une culture de vigilance numérique, un conseil scolaire est susceptible d'être confronté à des incidents fréquents et à être mal préparé pour y faire face. Les conséquences vont de la paralysie opérationnelle immédiate à des dommages financiers et réputationnels à long terme. Comme le souligne Patricia Kosseim, Commissaire à la protection de la vie privée de l'Ontario, « les cyber-attaques sont très répandues… mais les écoles et les conseils scolaires peuvent faire beaucoup pour réduire les risques et les impacts »[1]. À l'inverse, si ces mesures ne sont pas prises, les risques et les répercussions ne feront qu'accroître. Le message est clair : **le coût de ne pas favoriser une culture de cyber vigilance dépasse de loin les efforts nécessaires pour en instaurer une.**

Comment mettre en œuvre une culture de cyber vigilance

Développer une culture de cyber vigilance dans un environnement M-12 requière l'emploi d'une stratégie à plusieurs facettes. Cela ne viendra pas par magie, mais requerra un effort constant avec l'appui de leaders. Même les conseils scolaires qui partent de zéro verrons une amélioration significative. Ci-dessous, voici les étapes à suivre par les leaders pour la mise en œuvre d'une culture de cyber vigilance :

1. **Faire un état des lieux :** commencez par évaluer en toute franchise le niveau de connaissance de votre conseil scolaire en matière de cybersécurité. Vous ne pouvez pas améliorer ce que vous ne pouvez pas mesurer. Évaluez le niveau de sensibilisation du personnel et des élèves et identifiez les principales lacunes. Cela peut inclure la réalisation de sondages ou de questionnaires pour évaluer les connaissances (par exemple, les employés et les élèves savent-ils repérer un courriel qui contient des hameçons?), l'examen de rapports d'incidents passés pour identifier les causes courantes, et même la réalisation de tests d'hameçonnage simulés pour voir combien d'utilisateurs se font piéger. Envisagez de faire appel à une équipe externe spécialisée dans la cybersécurité ou d'utiliser les services d'ECNO pour un examen de la gouvernance en matière de sécurité afin d'identifier les faiblesses[8]. L'objectif de cette étape est de recenser les domaines à risque critique, qu'il s'agisse d'une faible connaissance des meilleures pratiques en matière de mots de passe, d'un manque de

planification des réponses aux incidents, de politiques obsolètes ou de vulnérabilités techniques. En établissant une base de référence, vous créez la référence de base pour mesurer les améliorations et cibler vos efforts là où ils sont le plus nécessaires.

2. **Obtenir l'engagement de la direction et définir des objectifs :** le ton donné par la direction du conseil est crucial. Les hauts responsables du conseil scolaire (direction de l'éducation, surintendances, direction informatique, etc.) doivent soutenir ouvertement l'initiative en matière de cybersécurité. Commencez par définir ce qu'est « une culture de la cyber vigilance » pour votre conseil scolaire et obtenez l'adhésion à des objectifs clairs (par exemple : 100 % du personnel doit suivre une formation sur la cybersécurité cette année ; ou réduire le nombre de personnes qui cliquent sur les courriels d'hameçonnage par un certain pourcentage). Attribuez la responsabilité de l'initiative à un cadre. Souvent, c'est le directeur informatique ou un responsable dédié à la sécurité (comme un responsable de la sécurité des systèmes d'information ou un responsable des services de sécurité) qui dirigera le programme. Tous les autres cadres doivent être tenus de le soutenir. Les dirigeants doivent également accepter d'allouer les ressources nécessaires, qu'il s'agisse du budget pour les outils de formation ou du temps consacré par le personnel aux activités de sensibilisation[3]. **Mettez en place et/ou actualisez la structure de gouvernance du conseil:** cela peut impliquer la création d'un comité directeur ou d'un groupe de travail sur la cybersécurité comprenant des représentants des services informatiques, du monde universitaire, des ressources humaines et de l'administration scolaire. Dès le début, intégrez des objectifs de cybersécurité dans les plans stratégiques et les politiques du conseil scolaire, en montrant qu'il s'agit d'une priorité au même titre que les résultats scolaires. L'engagement de la direction implique également de donner l'exemple; Par exemple en suivant des formations, en appliquant rigoureusement les politiques de sécurité et en abordant la cybersécurité lors des réunions et dans les communications. Lorsque le personnel voit les dirigeants défendre cette cause, cela renforce l'idée qu'il s'agit d'un effort sérieux et à long terme, et non d'un projet ponctuel
3. **Mettre à jour les politiques et procédures :** un changement de culture nécessite un encadrement avec des politiques pour le soutenir. Revoir et mettre à jour les politiques, procédures et directives du conseil scolaire en matière de cybersécurité afin de s'assurer qu'elles définissent des attentes claires. Cela peut inclure des politiques d'utilisation acceptable (pour le personnel et les élèves), des règles de gestion des mots de passe, des directives de sécurité pour le travail/l'apprentissage à distance, des politiques de traitement des données et de confidentialité, des plans d'intervention en cas d'incident et des exigences en matière de sécurité pour le choix des fournisseurs. Veillez à ce que les **rôles et les responsabilités soient** clairement définis. Par exemple, les politiques doivent préciser que tout le monde (employés, élèves, voire sous-traitants ou bénévoles) a un rôle à jouer dans la protection des données[4]. Intégrez des références à ces politiques dans les supports de formation, afin que les participants puissent faire le lien entre la formation et les la mise en oeuvre[4]. Il est important que les politiques ne restent pas simplement des documents rangés dans une bibliothèque. Il faut les diffusez et les rendre visibles dans les ateliers ou sur fiches récapitulatives afin qu'elles deviennent des lignes directrices vivantes. **Alignez les politiques sur les normes réglementaires et les meilleures pratiques**. Par exemple, assurez-vous que vos pratiques en matière de protection des données soient conformes aux lois sur la protection de la vie privée et aux normes émergentes (telles que celles recommandées par le projet de loi 194 pour la protection des informations[6]). Élaborez une **procédure claire de signalement des incidents** (qui appeler, mesures immédiates à prendre) et communiquez-la à l'ensemble du personnel, afin d'encourager le comportement souhaité, à savoir, un signalement rapide des menaces. En établissant des politiques

solides, vous créez la base d'une culture de cyber vigilance, et donnez à chacun des points de repère sur ce qui est attendu.

4. **Formation continue :** La formation est au cœur de la création d'une culture de cyber vigilance. Lancez un programme de formation complet à la cyber vigilance pour l'ensemble du personnel et étendez-le aux élèves, parents, administrateurs, le cas échéant. Les éléments clés sont les suivants :
   - **Formation du personnel :** proposez une formation à la cybersécurité obligatoire pour les ligne, de webinaires ou d'ateliers en présentiel. Couvrez des sujets pratiques tels que la détection de l'hameçonnage, la navigation en toute sécurité sur Internet, le stockage approprié des données, l'utilisation de l'authentification multifactorielle, etc. Utilisez des exemples pertinents tirés du contexte scolaire (par exemple, « Que faire si vous recevez un courriel qui semble provenir de la directrice, mais qui ne l'est pas »). Encouragez une participation active avec : des quiz, du contenu interactif et des sessions de questions-réponses pour maintenir l'intérêt. Heureusement, il existe des ressources gratuites ou à bas prix à la disposition des conseils scolaires canadiens. Par exemple, Fortinet propose un service de formation sur la sensibilisation à la sécurité dans le contexte scolaire, offert gratuitement à tous les conseils scolaires pour le primaire et le secondaire au Canada[9]. Ce service fournit des modules actualisés et permet même de suivre les progrès des participants, ce qui facilite la mise en place d'un programme de formation régulier. De nombreux conseils scolaires profitent de ces offres pour préparer une main-d'œuvre « cyber-formée»[9].
   - **Sensibilisation des élèves et en classe :** Intégrez les thèmes liés à la cybersécurité dans l'expérience scolaire des élèves. Cela peut commencer par des leçons de base sur la citoyenneté numérique dans les classes du niveau élémentaire (par exemple, la confidentialité des renseignements personnels, ce qu'est un mot de passe fort) et progresser vers des thèmes plus avancés au secondaire (comme la compréhension de l'ingénierie sociale des individus, ou même des cours/clubs d'introduction à la cybersécurité pour les élèves intéressés). Le ministère de l'éducation, ECNO avec ses partenaires ont créé des contenus adaptés à l'âge des élèves pour les aider dans cette démarche. Par exemple, la campagne annuelle du Mois de la cyber conscientisation dans les écoles primaires et secondaires, qui a lieu chaque année en octobre, propose des vidéos, des jeux et des plans de cours adaptés aux élèves de la maternelle à la 12e année en Ontario[10]. Les enseignants peuvent utiliser ces ressources pour animer des conversations et des activités sur la cybersécurité en classe. D'autres initiatives, telles que les thèmes « Cyber Heroes United » d'ECNO sont pour différents niveaux scolaires, rendent ludiques les thèmes liés à la sécurité pour les enfants[11]. En tirant parti de ces ressources, les conseils scolaires n'ont pas à réinventer la roue : ils peuvent intégrer des ressources existantes dans les programmes cadres et les événements scolaires.
   - **Sensibilisation des parents et de la communauté :** impliquez les parents et tuteurs dans vos efforts de sensibilisation. Cela peut se traduire par l'envoi de conseils sur la cybersécurité dans les communications aux parents, l'organisation d'une soirée d'information sur la sécurité en ligne pour les enfants ou le partage de courts tutoriels sur la manière de sécuriser son Wi-Fi à domicile ou encore d'apprendre à reconnaître les escroqueries qui ciblent les parents (par exemple, les faux courriels concernant de soi-disant frais de scolarité). Lorsque les parents adoptent de bonnes pratiques en matière de cybersécurité et les mettent en œuvre à la maison, cela renforce ce que les élèves apprennent à l'école. Certains conseils scolaires partagent les ressources du gouvernement du Canada, telles que le guide « Get Cyber Safe » destiné aux

familles[12], afin de sensibiliser l'ensemble de la communauté. Il peut également être utile de créer une page sur le site web du conseil scolaire avec des mises à jour et des ressources relatives à la cybersécurité.

- **Formations spécialisées pour certains postes clés :** offrez une formation supplémentaire au personnel occupant des postes particulièrement sensibles, comme ceux du personnel financier (prévention des escroqueries par usurpation d'identité), du personnel des ressources humaines (protection des renseignements personnels), les gestionnaires informatiques (sur les expertises en matière de sécurité) et les administrateurs des bureaux scolaires (qui gèrent souvent dossiers des élèves / DSO). En adaptant le contenu pour ces groupes, vous vous assurez qu'ils disposent des connaissances approfondies et adaptées à leur fonction.
- **Mises à jour fréquentes et remise en mémoire :** ne vous contentez pas d'une formation unique. **Faites de la sensibilisation aux menaces une campagne permanente**. Utilisez des bulletins d'information mensuels sur la sécurité ou envoyez régulièrement des courriels qui contiennent des conseils. Préparez des affiches pour être sur les murs du salon du personnel; Présentez de courtes vidéos lors des réunions du personnel et des cours de remise à niveau annuels pour que la cybersécurité reste une priorité. Les utilisateurs ont tendance à oublier avec le temps, il est donc essentiel de renforcer régulièrement les connaissances acquises. Vous pouvez par exemple introduire «La menace du mois » (par exemple, en janvier : l'hameçonnage, en février l'utilisation sécurisée des applications nuagiques, etc.) tout cela en vous alignant sur le calendrier M-12 de Cyber Conscientisation qui propose des thèmes tout au long de l'année[12]. Actualisez régulièrement le contenu et mettez-le à jour pour y inclure les nouveaux types de menaces comme les Infox qui sont les nouvelles arnaques en IA.
- **Un engagement positif dans la création de la culture :** dans la mesure du possible, rendez l'expérience amusante et attrayante. Certains conseils ont mis en place des concours d'hameçonnage amicaux et des quiz ludiques avec des prix pour les meilleures écoles. ECNO, en partenariat avec Fair Chance Learning, a récemment organisé **le Cyber Champion Challenge**, qui invitait les élèves à créer des œuvres d'art et des projets sur la cybersécurité, rendant l'apprentissage « sérieusement amusant »[13]. Vous pouvez adapter cette idée en interne, par exemple en organisant un concours pour les classes qui consiste à créer une affiche sur la cybersécurité, ou en demandant aux élèves de produire un petit sketch ou une vidéo sur la sécurité en ligne. Célébrer le mois de la cyber conscientisation en octobre avec des activités à l'échelle de l'école est un autre moyen de susciter l'enthousiasme. L'objectif est d'intégrer la sécurité de manière positive, et non pas seulement sous forme d'une suite d'avertissements et de contraintes.

Ne pas oublier de faire un suivi de l'engagement des participants: assurez-vous que tout le personnel suit la formation requise et notez les personnes qui pourraient avoir besoin d'un suivi supplémentaire. Le conseil pourrait établir une politique stipulant, par exemple, que tous les employés doivent suivre une formation annuelle sur la cybersécurité, et lier la conformité de cette mesure à des évaluations ou à tout autre mesure de redevabilité. Selon une étude, 97 % des décideurs dans le secteur de l'éducation estiment que davantage de formation et de sensibilisation contribuent à réduire les attaques cybernétiques[9], ce qui souligne à quel point cette initiative est cruciale.

1. **Impliquer et responsabiliser tous les groupes concernés** : en s'appuyant sur la formation, s'efforcer d'impliquer activement tous les groupes dans la culture de la cyber-vigilance. Formez des champions de la cybersécurité à différents niveaux : il peut s'agir d'enseignants intéressés par la technologie ou d'un « responsable du numérique » dans chaque école, qui peut aider ses collègues à répondre à leurs questions et maintenir le sujet vivant au niveau local. Encouragez les clubs d'élèves ou trouvez des « cyber ambassadeurs » (par exemple, parmi les élèves qui participent à des clubs TIC ou STEM) pour promouvoir des pratiques en ligne sûres auprès de leurs pairs. Certaines écoles organisent des assemblées dirigées par des élèves sur des sujets tels que le harcèlement en ligne et la sécurité, qui peuvent être très efficaces en raison de leur capacité d'influence sur les élèves. Pour le personnel, envisagez de créer des forums ou des groupes de travail dans lesquels des représentants de différents départements discutent de préoccupations en matière de cybersécurité et partagent des idées d'amélioration (par exemple, une réunion mensuelle des représentants techniques de l'école ou un canal Microsoft-Teams dédié aux conseils en matière de cybersécurité).

Il est également important de **donner aux gens les moyens d'agir**. Faites clairement comprendre que la vigilance de chacun est importante. Par exemple, si un assistant pédagogique remarque la circulation d'un courriel suspect, cette personne doit se sentir en droit de le signaler. Une façon de renforcer ce comportement consiste à reconnaître de manière positive ceux qui signalent des incidents ou suggèrent des améliorations. Une simple mention dans une note de service du personnel du type « Merci à l'enseignant qui a alerté le service informatique au sujet d'un courriel infecté ou contenant de l'hameçonnage la semaine dernière. Grâce à son signalement rapide, nous avons pu bloquer la menace à l'échelle du conseil scolaire », peut stimuler les comportements recherchés.

Étendez également les efforts d'engagement aux parents et à la communauté. Vous pouvez par exemple organiser un séminaire de sensibilisation à la cybersécurité en partenariat avec les conseils de parents ou dans les bibliothèques publiques locales. Collaborez avec votre équipe de communication pour diffuser des messages de cyber vigilance sur les réseaux sociaux ou dans les bulletins d'information du conseil scolaire afin de rejoindre un plus grand public. En faisant de la cybersécurité un sujet de conversation communautaire, vous l'encadrez dans la vie scolaire. Comme le faisait remarquer un expert, « la cybersécurité était autrefois un sujet de conversation dans les salles de réunion. Aujourd'hui, c'est un sujet de conversation pendant les repas »[1] – en d'autres termes, le sujet devrait être abordé ouvertement en famille, et non pas seulement entre les membres des services informatiques.

1. **Mettre en œuvre des mesures techniques et se préparer (en même temps) pour les incidents :** bien que la culture concerne des personnes et des procédures, il ne faut pas négliger les mesures de protection technologiques qui garantissent la sécurité de l'environnement numérique. Bien veillez à ce que l'équipe informatique du Conseil applique des mesures de sécurité à jour : pare-feu et protections des réseaux, filtres de messagerie puissants, authentification multifactorielle pour les connexions du personnel, mises à jour/correctifs logiciels réguliers, sauvegardes sécurisées, etc. De nombreux conseils scolaires en Ontario ont recours à des services collectifs à cette fin. Par exemple, 66 des 72 conseils scolaires de la province participent au programme « Security Operations » d'ECNO afin d'accéder à des expertises et à des outils de cybersécurité[8]. Une base technique solide offre aux utilisateurs un filet de sécurité : même si quelqu'un commet une erreur, les contrôles en place permettent de détecter ou de limiter les dommages.

En même temps, il faut élaborer **un plan de réponse aux cyber incidents** clair en veillant à ce qu'il soit connu des membres de la communauté et mis en pratique. Ce plan doit décrire la manière dont le Conseil réagit à une variété d'incidents tels que les violations des accès aux données, la lutte contre la propagation de logiciels malveillants, etc... Il faut notamment préciser quels sont les membres de l'équipe d'intervention, comment isoler les systèmes contaminés, les protocoles de communication internes et externes avec le public et comment restaurer les services. Il faut distribuer aux écoles un organigramme facile à suivre pour signaler les incidents, afin que tous les membres du personnel sachent quoi faire et qui contacter lorsqu'ils soupçonnent un problème cybernétique. On peut organiser des exercices **comme des simulations** pour passer en revue les étapes de réponse à une attaque hypothétique[8]. La direction de l'école doit faire partie de ces exercices qui sont un excellent moyen de renforcer la mémoire et même la mémoire musculaire. La mise en pratique des mesures de réponses aux incidents améliore non seulement une préparation actuelle, mais renforce également la culture en envoyant le message que la communauté scolaire « prend le sujet au sérieux et qu'elle est prête ». Comme l'a suggéré Patricia Kosseim, les équipes informatiques et la direction des Conseils devraient passer en revue les plans de réponses aux incidents cybernétiques à des fins de formation, de la même façon que les exercices d'évacuation incendie[1].

Bien que cette étape soit davantage opérationnelle, elle recoupe la culture : lorsque les gens constatent la mise en place de système de défense techniques solides avec un plan éprouvé, il y a un renforcement de la confiance ce qui les encourage à faire leur part du contrat (signaler les problèmes, suivre les protocoles) car ils savent que l'organisation réagira avec efficacité.

1. **Mesurer les progrès et s'adapter :** après avoir mis en place ces améliorations, **mesurez en permanence leur impact** et adaptez-les suivant les besoins. Utilisez des indicateurs (rappelez-vous que les indicateurs sont essentiels pour garantir la redevabilité[3]) afin de suivre l'évolution de votre changement de culture. Voici quelques indicateurs utiles :
    - Les résultats des simulations d'hameçonnage (par exemple, le taux d'ouverture de courriels de test qui contiennent des hameçons devrait diminuer au fil du temps, à mesure que la vigilance se développe).
    - Le nombre d'incidents de sécurité ou de quasi-incidents signalés par le personnel. Au début, vous constaterez peut-être une augmentation du nombre de signalements, ce qui est un bon signe qui montre que les gens s'impliquent; Cependant, à long terme, le nombre d'incidents devrait diminuer.
    - Le taux de réussite aux tests/quiz inclus dans les formations.
    - Les commentaires des employés et des élèves dans le cadre d'enquêtes sur leur confiance dans leurs connaissances de la cybersécurité, à savoir s'ils se sentent-ils plus à l'aise qu'auparavant ?
    - Les résultats des audits ou des contrôles de conformité visant à vérifier si les politiques sont respectées. Par exemple, y a-t-il moins de mots de passe faibles employés ou quel est la fréquence d'utilisation de clés USB non cryptées).

L'examen régulier de ces indicateurs au niveau de la direction. Cela permet de célébrer les succès, comme une école qui a atteint un taux de réussite de 100 % à la formation ou un incident qui a été rapidement maîtrisé grâce à l'action rapide d'un employé. Il faut intervenir dans les domaines qui sont

à la traîne. Par exemple, si un service de l'organisation particulier ne cesse de se faire piéger par des tests d'hameçonnage, il sera peut-être nécessaire d'y donner une attention particulière ou d'utiliser une méthode de formation différente.

Il faut adaptez ses stratégies en fonction de ce que l'on a appris. Les menaces cybernétiques évoluent également et le programme culturel doit donc évoluer lui aussi. Cette année, l'accent sera peut-être mis sur l'hameçonnage, mais l'année suivante, vous constaterez peut-être que les gens ont du mal à partager des documents en toute sécurité dans le nuage et vous devrez donc ajouter une formation dans ce domaine. Sollicitez toujours des commentaires : créez un canal de communication qui permet au personnel de suggérer des idées ou d'exprimer ses préoccupations vis-à-vis des processus de cybersécurité. Les enseignants sont peut-être submergés par un trop grand nombre de courriels sur la sécurité et vous pourriez ainsi regrouper les communications; Ou encore, les élèves pourraient trouver que le contenu est ennuyeux : impliquez-les alors dans la création de nouveaux supports qui seront mieux reçus par les jeunes. En conservant un dynamisme dans l'initiative culturelle, vous éviterez qu'elle ne devienne obsolète ou qu'elle soit considérée comme une simple formalité.

1. **Institutionnaliser et pérenniser :** Finalement, visez à **intégrer la cybersécurité dans le fonctionnement du Conseil à long terme**. Le protocole d'intégration des nouveaux employés devrait inclure une orientation sur la cybersécurité (et même dans celui pour l'orientation des nouveaux élèves avec une approche adaptée à leur âge). Intégrez la considération de la cybersécurité dans tous les projets et toutes les décisions. Par exemple, tout nouveau logiciel adopté par le conseil doit faire l'objet d'un examen de sécurité/confidentialité au préalable, et toute nouvelle initiative comme l'utilisation d'appareils 1:1 pour les élèves, doit s'accompagner d'un plan de sensibilisation aux risques. Faire du mois de la sensibilisation à la cybersécurité une tradition annuelle et envisagez de l'aligner sur les révisions et mises à jour périodiques des politiques. En institutionnalisant les pratiques, la culture se perpétuera indépendamment du roulement du personnel et de ses nouveaux leaders.

Il est également judicieux de rester en contact avec vos contacts externes : **collaborez et partagez vos meilleures pratiques avec d'autres conseils scolaires et organisations.** De nombreux conseils scolaires partagent des informations sur les menaces qu'ils ont dû traiter et partagent des conseils via le forum d'ECNO et d'autres forums[1]. Une telle collaboration peut inspirer de nouvelles idées pour renouveler votre programme. Le paysage continuera d'évoluer (pensez à l'essor de l'apprentissage à distance pendant la pandémie, qui a introduit de nouveaux défis en matière de cyber sécurité du jour au lendemain. Il faut donc maintenir une culture de cyber vigilance, ce qui signifie l'engagement à apprendre et à améliorer de façon continue. Au fil des années, efforcez-vous de faire de la cyber vigilance une priorité permanente, au même titre que la sécurité des élèves, c'est-à-dire une partie intégrante de « notre façon d'enseigner ».

Tout au long de ce processus de mise en œuvre, le soutien et l'appui observable de la part des dirigeants du conseil sont essentiels. Lorsque les employés et la communauté voient que les dirigeants accordent systématiquement une priorité à la cybersécurité, dans les communications, les ressources et leurs actions, le changement culturel se produit.

Surmonter les défis les plus communs

La mise en place d'une culture de sensibilisation à la cybersécurité n'est pas sans défis. Les environnements scolaires ont des contraintes particulières et il est normal de rencontrer une certaine résistance ou quelques difficultés en cours de route. Voici quelques défis communs auxquels les conseils scolaires sont confrontés dans cette démarche, **ainsi que des stratégies pour les relever :**

- **Défi : « La technologie intimide »**. De nombreux enseignants et membres du personnel qui ne travaillent pas dans le domaine des technologies de l'information peuvent trouver que la cybersécurité est trop technique ou effrayante. Comme l'observe un enseignant de l'Ontario, les gens « cessent souvent d'écouter parce qu'ils sont confus » lorsque l'on utilise du jargon technique[2].
  Solution : Démystifier le sujet. Commencez par les notions de base en matière de culture numérique et les concepts faciles à comprendre. Évitez le jargon dans vos formations; utilisez plutôt un langage simple avec des scénarios concrets et dans le contexte scolaire. Insistez sur le fait qu'il n'est pas nécessaire d'être un expert en technologie pour suivre les pratiques de base. Proposer des formations pratique, sous forme d'atelier, pour aider à réduire l'anxiété. Par exemple, une session où le personnel s'entraîne à vérifier si un courriel contient de l'hameçonnage ou à configurer les paramètres de confidentialité sur un appareil. Renforcez progressivement la confiance des apprenants. Favorisez également un état d'esprit orienté vers le développement personnel : rappelez à tout le monde que la cybersécurité fait appel à des compétences qui s'acquièrent, et qui ne sont pas innées. En présentant la cybersécurité comme une extension des pratiques de sécurité existantes (comme la vigilance vis-à-vis des inconnus », mais en ligne, ou encore, comme la fermeture de l'école à la fin de la journée, mais pour un ordinateur), elle devient moins intimidante. L'apprentissage entre pairs peut également aider : demandez aux membres du personnel les plus à l'aise avec la technologie d'appuyer leurs collègues de façon amicale et sans jugement.
- **Défi : Ressources et temps limités**. Les écoles ont un budget et un temps de travail limités pour le développement professionnel. Il peut être difficile de justifier le détournement de ressources vers la sensibilisation à la sécurité en ligne alors que les besoins pédagogiques sont pressants.
  Solution : tirez parti des ressources gratuites, telles que les plateformes de formation gratuite proposées aux écoles canadiennes[9] ou les supports fournis par le gouvernement, afin de réduire la charge financière. Intégrez la cyber vigilance dans les journées de développement professionnel ou dans les réunions du personnel existantes plutôt que d'ajouter des sessions spécifiques pour ce thème : profitez des rassemblements déjà prévus. Insistez sur le coût de l'inaction : partagez des données sur le coût d'une violation des accès aux données ou sur la manière dont elle pourrait perturber l'apprentissage, afin de démontrer qu'il vaut mieux prévenir que guérir. Commencez également à petite échelle et augmentez progressivement – vous n'avez pas besoin de tout faire en même temps. Si le temps est un problème majeur, commencez par le micro-apprentissage : de courtes formations de 5 à 10 minutes ou des conseils qui peuvent être présentés sans investir trop de temps. Donnez la priorité aux sujets à fort impact comme l'hameçonnage. En montrant des résultats rapides (par exemple, une amélioration des résultats aux tests d'hameçonnage après une formation rapide), vous développez l'argument d'y consacrer plus de temps et de ressources.
- **Défi : Complaisance ou croyance que le risque est faible**. Dans certains endroits, on observe une attitude du type « nous ne sommes qu'un conseil scolaire; Qui voudrait nous prendre pour cible? » Ou « nous n'avons pas encore connu d'incident majeur, donc tout va probablement bien se passer ».
  Solution : lutter contre la complaisance en sensibilisant votre communauté à la réalité. Utilisez des

exemples concrets, en particulier canadiens, pour montrer que les conseils scolaires sont vraiment pris pour cible. Partagez les articles qui ont été publiés sur les violations des accès aux données dans d'autres conseils scolaires (il y en a eu beaucoup à travers le Canada[7]) ou des statistiques comme l'augmentation de 575 % des attaques cybernétiques dans le secteur de l'éducation[4]. Lorsque les gens s'aperçoivent que leurs collègues dans les conseils scolaires voisins ont été touchés, ils comprennent que cela pourrait leur arriver. Envisagez également d'inviter un conférencier, peut-être quelqu'un d'un conseil scolaire qui a été victime d'une attaque, pour parler des conséquences que cela a eu. Il faut parfois entendre un témoignage de première main pour faire sortir les gens du déni. Une autre tactique consiste à organiser une simulation surprise (avec l'accord de la direction): par exemple, envoyer un faux courriel d'hameçonnage très convaincant, puis partager les résultats : Vous pourriez dire : « x % d'entre nous ont cliqué sur ce lien – c'est exactement ainsi qu'un pirate pourrait s'introduire dans le système ». Cela permet de tirer la sonnette d'alarme et de définir une base de référence à partir de laquelle s'améliorer. La clé est de rendre la menace tangible et de personnaliser le risque afin que les groupes d'utilisateurs comprennent l'urgence de la situation.

- **Défi : Un public divers (il n'existe pas de solution de formation pour répondre à tous les besoins)**. La communauté d'un conseil scolaire comprend des élèves, des enseignants chevronnés, des parents très occupés et des gestionnaires techniques. Il peut être difficile d'élaborer un programme de sensibilisation qui trouve écho auprès de tous les âges et tous les rôles. **Solution :** adaptez et différenciez votre approche. Segmentez votre public et utilisez différents canaux et styles de communication pour chaque groupe. Pour les élèves, utilisez un contenu attrayant et adapté à leur âge (dessins animés, jeux, activités interactives) – les programmes cadres de cyber vigilance de l'Ontario ont été conçus dans cette optique[11]. Pour les enseignants, concentrez-vous sur des scénarios d'utilisation des technologies en classe et à titre personnel. Pour les gestionnaires techniques, mettez l'accent sur les aspects liés aux politiques et à la conformité. Traduisez les documents dans les langues nécessaires à votre communauté afin de toucher les parents de tous bords. **Le conseil doit fournir des ressources accessibles que les enseignants peuvent adapter à leurs classes**[4], ce qui implique de leur donner la flexibilité nécessaire pour intégrer les thèmes liés à la cybersécurité d'une manière qui convienne à leurs élèves (un enseignant de 2e année abordera la sécurité en ligne autrement qu'enseignant de 10e année). Sollicitez des commentaires : demandez aux représentants de chaque groupe quel contenu ou format leur serait le plus utile. En personnalisant le message, vous vous assurez que chaque public le trouve pertinent et aura moins tendance à le rejeter.
- **Défi : maintenir l'effort.** Il est facile d'annoncer une nouvelle initiative, mais il est difficile de maintenir l'enthousiasme et la conformité à long terme. Le personnel peut participer activement pendant le mois de la cyber conscientisation, mais l'oublier par la suite. Les nouvelles initiatives peuvent s'estomper à mesure que d'autres priorités prennent le dessus. **Solution :** faites de la sécurité numérique un refrain régulier plutôt qu'une chanson ponctuelle. Intégrez-la dans le calendrier (thèmes mensuels, exercices trimestriels, rappels annuels en tant que politique). Renouvelez régulièrement le contenu : informez les gens des nouvelles menaces (par exemple, « Une nouvelle arnaque fait du bruit dans les réseaux sociaux : voici ce qu'il faut savoir cette semaine : … »). Utilisez différents supports : combinez les courriels avec des affiches, des bannières intranet, voire une vidéo humoristique de temps en temps. De plus, **les leaders devraient en parler régulièrement**. Si le directeur mentionne la cybersécurité à chaque réunion publique et que le sujet apparaît fréquemment dans les bulletins d'information internes, tout le monde y prêtera attention. Vous pouvez également maintenir la dynamique en rendant compte des progrès réalisés : par

exemple, rapporter l'augmentation des taux de détection de l'hameçonnage de 30 % ; bravo ! Voici notre prochain objectif ...». Lorsque les gens constatent que des progrès sont faits et que l'engagement est continu, alors ils sont plus enclins à rester mobilisés. Il est utile d'intégrer des responsabilités. Par exemple, inclure une obligation de sensibilisation à la sécurité dans les objectifs de performance des directions d'école ou dans les plans de développement professionnel des enseignants. Avec le temps, ces pratiques deviennent des routines.

- **Défi : la lassitude face aux incidents ou peur de signaler les menaces**. Parfois, si des incidents mineurs ou des activités suspectes se produisent fréquemment, le personnel peut soit devenir insensible (« encore un virus; peu importe, je continue...»), soit cacher les incidents par crainte d'être blâmé. **Solution :** créer une culture de signalement saine et positive. Veillez à ce que le signalement d'une erreur (comme le fait de cliquer sur un lien malveillant) soit accueilli avec reconnaissance et réactivité, et non avec des sanctions. Reconnaissez que les témoignages ou les signalements rapide ont permis d'éviter le pire, afin de renforcer les comportements positifs. Si les gens ne signalent pas les incidents, envisagez de mettre en place des moyens de signalement anonymes ou une politique de « non-responsabilité » pour favoriser l'auto-signalement des erreurs. Quant à la lassitude, soyez à l'écoute : ne surchargez pas tout le monde pour alerte de sécurité ; laissez le service informatique gérer le bruit de fond. Communiquez ce qui est nécessaire de manière concise. Alternez les domaines les sujets d'intérêt afin d'éviter de donner une impression de bombardement de la même information. Passer un mois sur la confidentialité, un autre sur l'hameçonnage, etc. En cultivant une atmosphère de soutien, vous vous assurez que les gens restent vigilants sans être anxieux, et qu'ils agissent lorsque cela est nécessaire.

Chaque organisation sera confrontée à un mélange de ces défis, et peut-être à d'autres, **mais grâce à des stratégies créatives et à un soutien continu de la direction, ils peuvent être surmontés**.
De nombreux conseils scolaires de l'Ontario ont déjà passé outre ces obstacles en partageant leurs ressources, en tirant parti des initiatives provinciales et en apprenant des expériences des uns et des autres. Il faut reconnaître que la création d'une culture de cyber vigilance est avant tout un effort de gestion du changement, qui implique de modifier des comportements et des mentalités. Cela demande du temps, de la patience et une capacité d'adaptation. Mais les défis sont surmontables et le résultat, à savoir un environnement scolaire sûr et prospère, en vaut largement la peine.

Les meilleures façons de maintenir une culture de cyber vigilance

Une fois que vous avez établi les bases d'une culture de cyber vigilance, le travail n'est pas terminé : il s'agit d'un engagement continu. **La cybersécurité est un domaine en constante évolution**.
C'est pourquoi une culture efficace doit également évoluer et se renforcer. Voici les meilleures pratiques pour maintenir l'élan et renforcer continuellement cette culture au fil du temps :

- **Maintenez la pertinence et les formations :** mettez régulièrement à jour le contenu de vos formations afin de refléter les nouveaux types de menaces et les technologies qui s'y associent. Les auteurs de menaces changent constamment de tactique, qu'il s'agisse de nouveaux thèmes d'hameçonnage (par exemple, les escroqueries liées à la COVID-19 une année, les escroqueries liées aux crypto-monnaies l'année suivante) ou de problèmes émergents comme les Infox. Veillez à ce que votre programme de sensibilisation reste à jour afin que le personnel et les élèves soient

préparés aux risques d'aujourd'hui, et non à ceux d'hier. Actualisez la formation **au moins une fois par an pour tout le personnel** – de nombreux conseils le font chaque année dans le cadre de la conformité. Les directives de l'Ontario suggèrent qu'avec l'évolution constante des menaces et des technologies, la formation devrait être actualisée régulièrement[4]. Envisagez également de brèves sessions de remise à niveau en milieu d'année, et non pas seulement une session globale annuelle. Veillez à ce que les nouveaux arrivants (nouveaux employés, nouveaux élèves inscrits) reçoivent une formation au plus tôt dans le cadre de leur intégration, afin qu'ils ne soient pas en retard dans le processus de sensibilisation. Une bonne pratique consiste à maintenir une bibliothèque de modules de micro-apprentissage ou de courtes vidéos qui peuvent être envoyés périodiquement (« Les mots de passe forts » ce mois-ci, « Comment détecter les liens d'hameçonnages » le mois prochain, etc.). Ce type de formation continue garantit que la cybersécurité reste une priorité et que le niveau de connaissance s'améliore progressivement.

- **Surveillance, audit et rétroaction :** établissez des procédures pour suivre en permanence l'efficacité de votre culture de vigilance mise en place. Cela comprend la surveillance technique (comme la détection du nombre de logiciels malveillants ou de tentatives d'hameçonnage bloqués et de celles qui ont réussi à passer) ainsi que la surveillance « culturelle » comme la vérification du respect des politiques sur le terrain. Effectuez des audits ou des contrôles périodiques : par exemple, effectuez des « contrôles ponctuels » aléatoires pour vérifier si les écoles gardent leurs entrepôts de stockage des données des élèves verrouillés et leurs ordinateurs déconnectés lorsqu'ils ne sont pas utilisés. Les réflexes de sécurité de base font également partie de la cyber vigilance. Utilisez des indicateurs que vous avez recueillis, tel que mentionné précédemment pour identifier les points de faiblesse. Si vous constatez, par exemple, une augmentation du nombre d'incidents ou une baisse du taux de succès des formations, cherchez à en comprendre la ou les raisons et adressez-les. **Sollicitez également les commentaires des utilisateurs :** peut-être que le personnel trouvera que les simulations d'hameçonnage sont désormais trop prévisibles et que les attaquants utiliseraient alors une méthode plus sophistiquée. C'est l'occasion d'améliorer votre stratégie. Peut-être encore, les enseignants trouveront que les modules de formation sont trop longs : ce retour d'information pourrait vous inciter à les diviser en segments plus courts. Donner et traiter les rétroactions montre que le Conseil ne se contente pas de prêcher, mais qu'il est à l'écoute et qu'il cherche l'amélioration, ce qui contribue au maintien l'engagement.
- **Identifier et récompenser les bonnes pratiques :** le renforcement positif contribue grandement à l'instauration d'une culture. Reconnaissez les écoles ou les personnes qui font preuve d'excellentes pratiques en matière de cybersécurité. Cela peut être un simple courriel de remerciement de la direction générale à une école qui n'a pas cliqué sur un hameçon au cours d'un trimestre, ou encore, une mention spéciale à l'équipe informatique pour avoir mis en œuvre avec succès une nouvelle procédure de sécurité. Certains conseils scolaires ont donné des titres amusants tels que « Cyber Champion du mois » aux membres du personnel qui font activement la promotion de la sécurité. Pour les élèves, vous pouvez organiser des concours ou attribuer des badges pour avoir participé à des activités de citoyenneté numérique. Faites connaître les réussites : « Cette semaine, un enseignant de l'école x a repéré et rapporté une tentative d'hameçonnage, empêchant ainsi la violation des accès aux données. Bravo ! ». Cela permet non seulement de récompenser les personnes vigilantes, mais aussi de montrer aux autres l'impact réel de la cyber vigilance. Cela renforce le sentiment de fierté de notre communauté qui devient de plus en plus cyber-intelligente. Au fil du temps, cette culture positive peut s'auto-renforcer, les gens prenant des initiatives puisqu'ils se sentent valorisées.

- **Restez informé et ouvert :** le domaine de la cybersécurité peut évoluer rapidement avec l'apparition de nouvelles menaces. Il suffit de voir à quelle vitesse les rançongiciels se sont développés ou comment les outils d'IA sont désormais utilisés dans les escroqueries. Veillez à ce qu'un membre ou une équipe du conseil soit chargé de se tenir au courant des dernières informations sur les menaces et des meilleures pratiques dans le domaine[5]. Il peut s'agir du directeur informatique, du responsable de la sécurité informatique ou d'une personne présente dans des groupes de partage d'informations tels que les forums pédagogiques de la division provinciale de la cybersécurité. Lorsque de nouveaux risques apparaissent, communiquez-les rapidement au personnel et adaptez vos directives en conséquence. Par exemple, si vous apprenez l'existence d'un nouveau logiciel malveillant ciblant les établissements d'enseignement, envoyez un avis à tout le personnel pour l'informer des précautions à prendre. En faisant preuve d'agilité et de proactivité, vous évitez que le développement de la culture ne stagne. Vous démontrez également l'engagement continu de la direction, en montrant qu'il ne s'agit pas d'un projet ponctuel, mais d'un programme vivant et en constante adaptation.
- **Renforcez la collaboration et le partage des connaissances :** encouragez un environnement dans lequel les écoles apprennent les unes des autres, mais aussi de sources externes. Le conseil scolaire peut organiser un sommet annuel sur la cybersécurité ou une journée d'atelier pour les représentants techniques des écoles afin qu'ils puissent échanger des idées et des exemples de réussite. Participez à des initiatives dans le domaine – l'Ontario a une forte approche collaborative qui permet d'une part aux conseils scolaires de partager leurs ressources via ECNO et d'autre part au ministère de coordonner des campagnes[10]. Tirez parti de ce réseau : participez à des webinaires, lisez les études de cas sur les mesures prises par les autres conseils scolaires après des incidents. Partagez les expériences de votre conseil scolaire. Cela contribue à l'amélioration de l'effort collectif. Comme le préconise Patricia Kosseim, l**es conseils scolaires devraient collaborer plus souvent pour partager les meilleures pratiques**[1]. Cela aide tout le monde à s'améliorer et évite que les conseils scolaires travaillent indépendamment sur les mêmes problèmes. Plus la cybersécurité est considérée comme un effort communautaire, mieux les écoles seront préparées.
- **Maintenez votre état de préparation aux incidents :** Raffinez continuellement votre capacité de répondre aux incidents. Organisez au moins une fois par an (voire chaque semestre) un exercice de simulation complet qui implique non seulement le service informatique, mais aussi les services de communication, la direction de l'école et même les plans de communication avec les élèves et parents. Chaque exercice révélera de nouveaux points à améliorer; Tirez-en avantage et mettez à jour vos manuels. Tenez à jour les listes de contacts (pour votre équipe d'intervention en cas d'incident, les fournisseurs contactés pour les urgences, les conseillers légaux, etc.). En effet, lorsqu'un incident se produit, une équipe bien préparée et entraînée est en mesure de le gérer beaucoup plus facilement et d'en atténuer l'impact. Une réponse rapide et efficace à l'incident renforce à son tour la culture de vigilance de l'école : « nous avons été touchés, mais nous avons bien géré la situation parce que nous étions préparés ». La réponse à l'incident fera la preuve de la valeur des efforts consacrés à la sensibilisation et à la préparation à sa réponse.
- **Intégrer la cybersécurité dans l'identité du Conseil :** enfin, visez à **intégrer la cybersécurité dans l'ADN de l'organisation**. Incluez une mesure de l'impact sur la sécurité/la confidentialité dans la planification de toute nouvelle initiative, tout comme on peut tenir compte de son budget ou de son impact sur les résultats scolaires. Dans les documents stratégiques ou les rapports annuels, mentionnez l'engagement du Conseil en faveur de la cybersécurité au même titre que les autres valeurs. Lorsque vous accueillez de nouvelles directions ou de nouveaux responsables de service,

informez-les de leur rôle dans la promotion de cette culture de vigilance. Il faut institutionnaliser la cybersécurité profondément de façon qu'elle survive aux changements de direction et devient une priorité permanente. Nous observons déjà cette tendance dans certaines orientations politiques. Par exemple, les lignes directrices et les notes politiques du ministère demandent explicitement aux conseils scolaires de créer une culture de vigilance et de cybersécurité pour la confidentialité à tous les niveaux[4]. À terme, le maintien d'une culture de cyber vigilance pourrait même devenir une exigence dans les évaluations des conseils scolaires et du Ministère.

En suivant ces bonnes pratiques, un conseil scolaire peut s'assurer que sa culture de cyber vigilance, non seulement prendra racine, mais continuera à se développer. Le paysage de la cybersécurité posera toujours des défis, mais une culture bien enracinée devient un mécanisme de défense puissant et adaptable. Elle transforme nos collaborateurs, de cibles potentielles en première ligne de défense. En donnant à nos enseignants et à nos élèves les connaissances et les outils nécessaires, nous créons un environnement scolaire numérique plus sûr.

Conclusion

À l'ère numérique, **la création d'une culture de cyber vigilance est aussi fondamentale pour le succès d'un conseil scolaire que la promotion d'une culture d'apprentissage positive**. La cybersécurité ne peut plus être cloisonnée ou laissée dans les mains de quelques spécialistes en informatique. Elle doit être une valeur partagée, ancrée dans le fonctionnement quotidien du conseil scolaire. Pour les conseils financés publiquement de l'Ontario, ce changement culturel n'est pas seulement idéal, il est impératif. Les menaces cybernétiques sont réelles et en nombre croissants dans le secteur de l'éducation. Mais en créant de manière proactive une culture de cyber vigilance et en accroissant la résilience des utilisateurs, nous pouvons transformer ces menaces en risques que l'on peut contenir.

La bonne nouvelle, c'est que la communauté scolaire de l'Ontario est en train de relever le défi. Grâce au soutien d'organisations telles qu'ECNO et aux initiatives du ministère de l'éducation[10], les conseils disposent, plus que jamais, de ressources pour former et protéger leurs communautés. De nombreux conseils ont déjà progressé. Soixante-six conseils se sont associés et collaborent aux services de sécurité d'ECNO[8]. Cet esprit de collaboration, associé à un leadership local fort, peut garantir que chaque conseil, qu'il soit grand ou petit, urbain ou rural, anglophone ou francophone, puisse renforcer sa position face aux cyber menaces.

Pour les responsables des conseils (directeurs, surintendants, directeurs informatiques), **l'appel à l'action est clair**. En défendant une culture de cyber vigilance :

- Vous donnez à votre personnel et à vos élèves les moyens de naviguer en toute sécurité dans le monde numérique;
- Vous protégez votre mission éducative contre des interruptions qui peuvent être évitées;
- Vous préservez la confiance de vos familles dans nos systèmes scolaires;
- Vous garantissez la conformité avec l'évolution des règlements;
- Vous exploitez le formidable potentiel de la technologie dans l'éducation tout en gérant ses risques de manière responsable.

Comme nous l'avons vu, l'instauration de cette culture nécessite des investissements et des efforts en matière de politiques, de formation et d'engagement communautaire. Cela peut sembler intimidant, mais étape par étape, le changement se réalise. De nombreux succès et bonnes pratiques sont disponibles pour vous guider. Le résultat est un conseil scolaire où la cybersécurité devient une seconde nature, tout comme le verrouillage des portes de l'école ou les exercices d'évacuation incendie. Dans un tel environnement, chacun peut se concentrer davantage sur l'enseignement et l'apprentissage, car les bases pour la confiance et de la sécurité dans nos systèmes informatiques sont posées.

En conclusion, **une culture de cyber-vigilance n'est pas seulement une initiative informatique, c'est un impératif éducatif et une opportunité de leadership.** En inculquant la cyber vigilance comme une valeur fondamentale, nous préparons nos écoles à exploiter en toute sécurité les avantages de la technologie tout en gardant les menaces à l'écart. Travaillons ensemble pour former une génération d'enseignants, d'élèves et de membres de nos communautés cyber vigilants, afin que l'enseignement au primaire et au secondaire en Ontario reste non seulement innovant et efficace, mais aussi sûr pour tous[4,1].

Références

[1] Cyberattacks can take entire school networks out. It's time to pay more ...
[2] National approach to cyber security education needed as attacks will ...
[3] Creating a culture of cybersecurity in your business
[4] Cyber Security and Privacy Awareness – cpco.on.ca
[5] ECNO Announces New Director of Security Services – ECNO
[6] Bill 194, the Strengthening Cyber Security and Building Trust in the ...
[7] Cyberattack affecting school boards across Canada may involve decades ...
[8] Security Solutions – ECNO
[9] Security Awareness and Training Service: Education Edition
[10] October is K-12 Cyber Awareness Month – Toronto District School Board
[11] Cyber Awareness Month – Grades K-8 – ECNO
[12] Cyber Security – Greater Essex County District School Board
[13] Cyber Champion Challenge