Le projet de loi 64 : des changements pour les entreprises québécoises?

Depuis quelques mois déjà, nous entendons parler du projet de loi 64. Ce projet de loi vise la sécurité des données personnelles que possèdent les entreprises, petites ou grandes. Les PME n'en sont pas exclues. Ce projet de loi aura des répercussions majeures sur le milieu entrepreneurial au Québec. Par exemple, vous devrez avoir un système fiable pour protéger les données de vos clients contre les pirates informatiques et contre le trafic de données. Ça signifie que vous devrez mettre en place des contrôles internes pour vos employés et collègues, de même que montrer clairement que vos systèmes informatiques protègent les données de vos clients. Ceci, que vous soyez dans une multinationale ou une très petite entreprise (TPE).

Non seulement devrez-vous mettre en place des mesures de contrôle internes, mais en plus, vous aurez à nommer un ou une responsable de la protection des renseignements personnels. Cette personne agira pour contrer la fuite des renseignements de votre entreprise et de vos clients, et au maximum de ce qui est possible de faire pour aider à protéger tous ces gens. Il y a alors une vérification des antécédents qui peut être faite pour vous assurer de laisser cette grosse responsabilité à une personne qui ne représente aucun risque de fuite à l'interne. Au final, concrètement, que devrez-vous faire pour protéger les données personnelles et avoir un plan concret pour améliorer votre niveau de cyber sécurité?

Pour mobiliser votre équipe à la cybersécurité

Vous aurez à parler de ce qui s'en vient en lien avec le projet de loi 64 avec vos employés. Qu'est-ce qui changera dans leurs outils informatiques, qu'est-ce qu'ils devront faire pour protéger les données de vos clients. Une approche de « design thinking » est efficace pour mobiliser vos employés et collègues puis travailler en équipe avec tous ces gens. Puis, le *design thinking* vise à innover et à évoluer, tout le monde ensemble. Certes, une évolution sera de mise avec ce nouveau projet de loi, puis mobiliser tout le monde de votre équipe à travailler ensemble pour trouver des solutions et s'ajuster aux nouvelles normes ne peut être que bénéfique pour la prospérité des PME du Québec.

Vous devrez expliquer de manière exhaustive, mais compréhensible par vos employés, les nouvelles normes en vigueur et donner à chaque employé un rôle dans cette transition vers un environnement informatique sécuritaire. Pour ce faire, il est possible que vous ayez besoin de support ou de formations ponctuelles pour bien assimiler tout ce qui touche à la sécurité informatique

dans votre environnement entrepreneurial interne, puis externe. Comment une fuite de données ou une cyberattaque peuvent-ils entraver le bon déroulement de vos activités? Il y a des attaques qui ne pardonnent pas, où des vols d'identité surviennent par la suite. Votre réputation et celle de votre entreprise en seront directement entachées. De ce fait, en quoi consiste le projet de loi et comment vous protège-t-il, vous et vos clients?

La mise en application du projet de loi 64

Graduellement, d'ici septembre 2024, le décor informatique et numérique des entreprises québécoises risque de changer, d'une certaine façon, avec la mise en application du projet le loi 64. Vous devrez mettre en place un système fiable, d'ici septembre 2022, pour assurer la sécurité de vos données et de celles de vos clients, fournisseurs et partenaires d'affaires. Ces mesures de sécurité peuvent passer par un serveur sécurisé, des copies de sauvegarde de votre système informatique, une sensibilisation de votre équipe aux manœuvres de cyberfraude ainsi que le chiffrement de vos activités sur les plateformes de type « infonuagiques ». Si vous êtes en mesure de vous prémunir d'un serveur sécurisé pour empiler les données sensibles, le fait d'aller de l'avant avec cette initiative vous assure un meilleur niveau de protection. Il y a premièrement vos équipements informatiques qui entrent en ligne de compte (sont-ils suffisamment fiables). Puis vient ensuite votre responsabilité personnelle. Vous aurez besoin de connaître les risques de cyberfraudes possibles et de comprendre comment les contrer.

Il faut comprendre ici que le projet de loi 64 n'est pas une proposition : c'est une obligation que va imposer le gouvernement du Québec, autant pour la sécurité de vos clients que pour la vôtre. Le projet de loi 64 deviendra la loi 25. Bref, il y aura bientôt une culture de la cybersécurité à inclure dans votre culture d'entreprise. Ceci est une révolution somme toute majeure dans l'écosystème entrepreneurial québécois. Le dit projet de loi sera graduellement mis en application d'ici septembre 2024 afin de laisser le temps aux entreprises de s'ajuster. En effet, un changement aussi majeur ne se met pas en place en un simple claquement de doigts.

L'éducation sert aussi à prévenir les cyberattaques

Un gestionnaire avisé vaut une armée de soldats de l'informatique! Ce qui signifie qu'en tant que contrôleur, le gestionnaire a sa part de responsabilité dans une cyberattaque. En comprenant où et comment les attaques surviennent et comment les éviter, un bon gestionnaire d'entreprise arrive à éliminer environ 90% des risques liés à son environnement informatique direct. Autrement, quel type de cyberattaque peut survenir dans un environnement d'entreprise numérique?

Les virus, les pirates informatiques sont les formes les plus

connues de menaces numériques

Qui n'a jamais entendu parler d'un ami qui a vu son appareil infecté par un virus. Cela peut effectivement être frustrant pour la personne qui en est la victime. Cependant, les virus ne ciblent pas nécessairement des individus précis, mais plutôt des failles dans les systèmes d'exploitation (Windows, Mac, Linux). À l'échelle d'une entreprise, ces attaques, bien plus que déconcertantes, inquiètent chaque membre de l'équipe! Une forme courante est une attaque par rançongiciel. Un virus empêche votre appareil de redémarrer et vous envoie un message comme quoi votre appareil ne démarrera pas tant que vous n'aurez pas envoyé une somme d'argent, des bitcoins ou même parfois des données personnelles. Même si vous parvenez à contrer l'attaque, les chances que votre travail de plusieurs mois soit perdu sont réelles!

La fraude au fournisseur

En quoi consiste une fraude au fournisseur? Il s'agit d'un pirate ou d'un logiciel qui copie l'adresse courriel de votre fournisseur ou trouve tout autre moyen de se faire passer pour lui (par téléphone, par exemple). La personne qui vous escroque, si elle se fait passer pour votre fournisseur de cartouches d'encre, par exemple, demandera souvent à un de vos employés des renseignements sur votre entreprise et la plupart du temps, demandera à être payée comme l'est votre vrai fournisseur de cartouches d'encre. Ainsi, non seulement un paiement sera envoyé à une personne à qui il n'est pas destiné, mais de surcroît vous aurez peut-être des paiements qui passeront sur votre compte bancaire d'entreprise si c'est le moyen de paiement qui a été utilisé pour la transaction. Des comptes bancaires d'entreprises ont déjà été vidés de cette façon. Vous comprenez donc qu'il y a un besoin flagrant, dans notre société, d'agir de sorte à ne pas augmenter les risques. La fraude au président est une autre forme sournoise d'arnaque, puis il en existe plusieurs autres. Le gestionnaire qui connaît ces menaces et qui ne « mord » pas à l'hameçon aura beaucoup moins de chances de vivre des situations embarrassantes liées à la sécurité des données.

Les conséquences sur les outils informatiques

Bien évidemment, comme la majorité des données personnelles ou sensibles passent par l'informatique aujourd'hui, il sera donc bien important de sécuriser vos systèmes adéquatement grâce à un antivirus fort, à des systèmes internes de contrôle de l'intégrité des données personnelles, à un plan d'urgence en cas de fuite de données. Vos bases de données devront donc être sécurisées elles aussi, puisque celles-ci sont toujours susceptibles de contenir des informations dites sensibles.

En ce qui concerne les bases de données de forme SQL, elles seront à protéger par un mot de passe fort probablement, à stocker dans un espace réellement sécurisé, puis à « camoufler » de toute personne mal intentionnée qui aurait réussi à pénétrer votre système informatique. À titre d'exemple, dans un site

web, vous pouvez rendre invisible un fichier contenant des données sensibles avec les fonctionnalités de votre hébergeur web.

Les formulaires de contact sont directement liés à des bases de données qui stockent des courriels, numéros de téléphone et autres informations possibles pour contacter vos clients. La base de données qui est liée à votre formulaire de contact devra elle aussi être bien protégée des entités malveillantes qui pourraient en prendre possession sur votre site web.

De plus, tout ce qui est contenu sur votre disque dur pourrait potentiellement contenir des infos sensibles de vos clients ou de votre entreprise, telles que des numéros de téléphone, des courriels, voire même des numéros de cartes de crédit, des informations aussi personnelles!

Adopter un management cyber-sécuritaire devient une pratique gagnante

Avant le fameux projet de loi, nous protégions les données de nos clients, mais sans nécessairement prendre en considération la partie informatique de la chose ou en ne voyant le concept que d'un point de vue face-à-face. Or, les données peuvent désormais être subtilisées sournoisement, et à distance, par un pirate informatique ou un virus.

C'est pourquoi nous devons assurer que nos systèmes sont en ordre, qu'il n'y a pas eu de données corrompues, mais surtout nous assurer que nos employés, collègues et partenaires d'affaires soient au fait des pratiques cyber-sécuritaires et que tous puissent les mettre en pratique, sans que leur travail habituel ne soit affecté.

Il serait important que vous convoquiez vos employés en réunion pour leur parler des changements à venir et des raisons de ces changements : la loi 25, puis un désir de protéger vos clients contre la fraude et le vol d'identité. Si ce n'est pas une réunion, au minimum, parlez à vos employés des pratiques en cybersécurité seul-à-seul ou dans un espace ouvert. Peu importe quand la conformité à un environnement sécuritaire est en jeu.

Visuellement, vous pourriez aussi adopter un schéma, ou un tableau avec points de contrôle, pour que vos collaborateurs puissent voir ce qui va changer, leurs rôles respectifs mais surtout le but poursuivi par chaque action. Un plan d'action sans repères risque souvent de devenir un mélange dans l'esprit de vos interlocuteurs. C'est pourquoi le visuel est fortement recommandé quand des concepts informatiques, abstraits pour certains, risquent d'être moins bien compris avec une simple discussion.

Le plan d'urgence en cas de fuite de données

En septembre 2024, vous devrez avoir un plan d'intervention en cas de fuite de données. Qui allez-vous aviser? Comment allez-vous communiquer

l’information au ministère concerné, aux autorités, aux personnes pour qui la fuite des données a un impact (leurs données)? Il est crucial de savoir quoi faire si une situation d’urgence survient, comme un incendie. Il le devient tout autant de nos jours, ou presque, en cas de vol de données informatiques.

Vous devrez aussi nommer un responsable de la cybersécurité dans votre entreprise. Celui-ci peut être un employé ou une entreprise de consultation externe en TI. Une personne ou une entreprise responsable de la cybersécurité pourra forcément être un atout. De plus, il est recommandé de vérifier les certifications et les compétences de la personne ou de la firme choisie pour assurer votre sécurité. Si vous avez à cœur vos clients, vous serez probablement favorable avec ce projet de loi, même si il implique de nombreux ajustements au final.