_la force de l'engagement[MC]

Être ou ne pas être?

Telle est la question en gestion de l'identité

UNITÉ D'AFFAIRES de Québec
1er mars 2011

Claude Perreault, directeur services-conseils
Vice-présidence Prospective, Affaires et Transformation
Centre de compétence en sécurité de l'information

La gestion de l'identité est traditionnellement associée à la gestion des accès et à des mesures de contrôle technique pour discriminer et, parfois, reconnaître des personnes connues ou liées par un cadre contractuel quelconque, tel un contrat d'abonnement ou un contrat d'emploi. Elle vise, entre autres, à leur permettre de consulter des données personnelles ou d'entreprises ou, le cas échéant, d'effectuer des transactions en leur propre nom ou pour le compte de leur employeur.

De nos jours, l'accessibilité accrue à l'Internet et le déferlement des technologies, notamment par les appareils mobiles et les applications dans le nuage, permettent à l'internaute moyen d'accéder à des contenus informationnels de plus en plus sensibles ou stratégiques et de transiger en ligne avec un simple clic. Cette accessibilité accrue contribue néanmoins à ramener l'identité au centre des préoccupations :

- celle des internautes, qui veulent demeurer plus ou moins anonymes lorsqu'ils naviguent sur le Web, tant à titre personnel que de représentant d'une entreprise; et

- celle des entreprises, des ministères et des organismes publics dispensant des services sur le Web qui veulent être en mesure d'identifier sans équivoque les personnes transigeant avec eux.

Internet : la rencontre des extrêmes

Deux tendances se dessinent actuellement en gestion de l'identité à la suite de l'apparition du WEB 2.0, de la mobilité et l'utilisation de l'informatique en nuage, soit :

- l'une centrée sur les entreprises, les ministères ou les organismes publics, que nous désignerons ci-après comme étant les «entreprises», dispensant des services sur le Web (Enterprise or Service Centric Identity); et
- l'autre centrée sur l'internaute qui est roi et maître (User or Consumer Centric Identity) lorsqu'il navigue dans l'univers d'Internet.

La première tendance consiste à exposer différentes facettes de sa personnalité et bien souvent de son identité au grand jour, notamment sur Facebook, Twitter et les autres réseaux sociaux, tout en voulant demeurer anonyme, mais sans nécessairement se rendre compte des bris de confidentialité potentiels et des risques de vol d'identité rendus possible par la simple divulgation de ces informations personnelles.

La deuxième tendance consiste à dématérialiser[i], à décloisonner[ii] et à délocaliser[iii] certains actifs informationnels, plus ou moins critiques ou essentiels, pour les rendre accessibles sur Internet, tel le dossier de santé d'un patient que ce dernier peut consulter et/ou alimenter lui-même ou qui peut l'être par les intervenants du secteur de la santé ou par des appareils médicaux. Dans ce contexte, les entreprises doivent être conscientes des risques d'exposer des données hautement critiques ou très sensibles dans des réseaux privés ou publics et de l'importance d'identifier sans équivoque les personnes pouvant être autorisées à les consulter ou à les alimenter.

Ces deux tendances réfèrent évidemment à deux réalités qui s'opposent et qui commandent une gestion du risque et un niveau de confiance envers l'identité d'une personne fort différents.

La gestion de l'identité : une facette de la gestion du risque

Les gouvernements et l'industrie, notamment par l'établissement de normes et de standards, réagissent actuellement à cette réalité en définissant des paramètres permettant de gérer adéquatement le risque lié à l'identité d'une personne en regard de l'information qu'elle consulte ou qu'elle fournit.

Au Québec, la démarche gouvernementale d'analyse de risque, par exemple, s'appuie sur le modèle de sécurité à quatre (4) niveaux de confiance proposés par le National Institute Of Standards And Technology (NIST)[iv], retenu par le Liberty Alliance Project[v] pour son cadre de référence sur la fédération de l'identité, et adopté par plusieurs pays de tradition de droit civil ou de droit commun (Common Law).

Le modèle de confiance est la fondation qui soutient le processus de gestion de l'identité mis en place par une entité, un groupe, un secteur d'activités ou une industrie, ci-après globalement désignée comme étant une « entité ». Il contient généralement plusieurs niveaux de confiance intimement liés aux niveaux de risques que cette entité est appelée à encourir dans le cadre de ses échanges d'information. Chacun de ces niveaux de confiance comporte des exigences spécifiques en termes de vérification, de gestion du cycle de vie et de validation de l'identité à respecter pour obtenir le niveau de risque résiduel acceptable recherché, et ce, tant pour la disponibilité, l'intégrité ou la confidentialité de l'information à protéger.

Le modèle de confiance du gouvernement du Québec comprend la définition des critères minimaux permettant d'atteindre un niveau de confiance requis envers l'identité présentée par un internaute :

- ces critères minimaux sont en lien avec les niveaux d'impact selon les besoins de disponibilité, d'intégrité et de confidentialité;

- les quatre niveaux de confiance (minimal, raisonnable, élevé et très élevé) sont généralement alignés sur les quatre niveaux d'impact (bas, moyen, élevé et très élevé) définis dans les outils de gestion de risques généralement utilisés au gouvernement du Québec et dans la plupart des ministères et organismes publics (guide de catégorisation de l'information, méthode Méhari, AGSI, etc.).

De la méfiance à la confiance : tout un changement de paradigme

Les modes d'authentification retenus et le choix des facteurs d'authentification varient suivant la finalité et le type de protection recherchée par le gestionnaire de dossiers contenant des données confidentielles ou sensibles relatives à une personne.

Dans l'appréciation de l'identité présentée par une personne accédant à un service Web ou une application Web, deux appréciations du risque diamétralement opposées mais parfois complémentaires donnent lieu à deux approches de gestion de l'identité, l'une basée sur la méfiance envers l'identité présentée par une personne qui réfère à la mitigation des risques; et l'autre basée sur la confiance envers l'identité présentée qui réfère à l'imputabilité de cette personne.

Ces deux appréciations du risque commandent des mesures de contrôle différentes, soit des contrôles de sécurité technique ou des contrôles de sécurité basés sur l'identité d'une personne. Ils nécessitent un changement de paradigme en termes de gestion de l'identité qui exige de concilier à la fois des éléments de sécurité informatique et des processus de vérification, de gestion du cycle de vie et de validation de l'identité au fur et à mesure que les données relatives à une personne se dématérialisent et reposent dans un univers virtuel.

Le choc des cultures : la rencontre entre le numérique et le juridique

Avec la dématérialisation, la délocalisation et le décloisonnement progressifs des actifs informationnels et des transactions, la gestion de l'identité risque de devenir la principale préoccupation des dirigeants d'une entreprise offrant des services Web.

Dans les faits, la gestion de l'identité des internautes risque de devenir graduellement la pierre d'assise de la gestion des risques relatifs à ces actifs informationnels et va contribuer grandement à rehausser la sécurité de l'information et des transactions. Et c'est là que se produit l'inévitable choc entre le numérique et le juridique, car le concept de l'identification fait appel à des notions juridiques qui remontent à l'aube des temps et qui comportent des règles qui s'appliquent tant dans l'univers virtuel que dans l'univers matériel. C'est là également que le volet technique ne devient qu'un moyen pour s'assurer de l'imputabilité d'un internaute par rapport à l'identité qu'il présente et de l'irrévocabilité des actes et des gestes qu'il pose dans l'exercice de ses fonctions, et ce, tant à titre personnel que de représentant d'une entreprise.

La protection recherchée est de nature juridique et consiste à identifier formellement à travers un processus d'authentification, plus ou moins robuste, les internautes voulant accéder à de l'information ou en fournir dans un réseau, dans un système, dans une application, dans un service ou à une ressource, pour :

- les rendre imputables de leurs faits et gestes, notamment de l'utilisation qu'ils font ou pourraient faire de l'information mise à leur disposition sur la base de cette identité;
- rendre leurs actes ou leurs gestes irrévocables par l'utilisation d'une signature numérique.

De la délivrance à la gouvernance

Ce changement dans la protection recherchée exige également que les entreprises, les ministères et les organismes publics dispensant des services sur le Web adaptent leur vision de la sécurité, passant d'un mode forteresse contrôlée par les services techniques à une gestion intégrée du risque impliquant plusieurs directions de l'entreprise et, plus important encore, la haute direction qui doit se l'approprier pour répondre à ses obligations et être en mesure d'effectuer la reddition de compte attendue d'elle.

Le gouvernement du Québec a, par exemple, initié ce changement en matière de sécurité en mettant en vigueur, au printemps 2008, le Règlement sur la diffusion de l'information et sur la protection de renseignements personnels. Ce règlement rend la haute direction des ministères et organismes publics, soit le sous-ministre ou le principal dirigeant, imputables de la mise en œuvre des responsabilités et des obligations attribuées par le règlement, notamment la mise en place d'un cadre de gouvernance sur l'accès à l'information et la protection des renseignements personnels.

Cette tendance se répercute dans tous les domaines d'intervention de la sécurité, y compris la gestion de l'identité. Jusqu'à tout récemment, la gestion de l'identité était perçue par l'industrie comme une opération purement technique sous la responsabilité entière du département informatique alors que dorénavant, comme le suggère le modèle de gouvernance proposé par Gartner[vi], l'intervention de la haute direction s'inscrit dans un cadre plus global de gouvernance de la sécurité de l'information et doit mettre à contribution des membres des volets affaires et technique.

La gestion, la mise en place et l'opérationnalisation de ce cadre de gouvernance impliquent la mise en place d'un comité de gouverne, d'une équipe dédiée à la gestion de l'identité. Elles nécessitent la collaboration de

ressources concernées par la gouvernance de la sécurité, la gestion du risque, la conformité et la continuité des affaires.

Ce changement signifie également que les entreprises, les ministères et les organismes publics dispensant des services sur le Web se dotent graduellement d'un cadre global de gestion couvrant l'ensemble des activités requises pour la mise en place d'un service de gestion de l'identité.

Le cadre global de gestion de l'identité couvre deux aspects fondamentaux de la gestion de la sécurité pour légitimer la démarche d'une entreprise dispensant des services sur le Web, toujours selon le modèle proposé par Gartner[vii], et pour s'assurer du succès de son programme de gestion de l'identité, soit :

- d'un point de vue gouvernance : en matière de gestion de l'identité, orienter, guider et encadrer les propriétaires d'actifs informationnels qui veulent ou doivent mettre en place un service de gestion de l'identité;
- d'un point de vue conformité : prendre les mesures nécessaires pour s'assurer que les services de gestion de l'identité implantés et utilisés par les propriétaires d'actifs informationnels sont conformes au cadre normatif régissant la gestion de l'identité au sein d'une entreprise dispensant des services sur le Web.

La gestion de l'identité : un monde à découvrir

Les gestionnaires d'entreprises, de ministères ou d'organismes publics dispensant des services sur le Web, tant aux individus qu'aux entreprises, vont devoir tôt ou tard s'intéresser à la gestion de l'identité s'ils veulent éviter de devoir, malgré eux, endosser la responsabilité ou rendre compte de certains faits et gestes sur lesquels ils n'ont actuellement aucun contrôle.

---

i Dématérialiser : rendre des données accessibles sous forme numérique sans support physique.

ii Décloisonner : rendre des données accessibles sous forme numérique à l'extérieur de son domaine de confiance ou rendre accessible les données d'un système source local, sectoriel ou régional pour alimenter un système de partage de données.

iii Délocaliser : externaliser, sans référence au lieu physique, ses équipements, ses données, ses logiciels et ou/ou ses processus d'affaires hors de son domaine de confiance pour le confier à un hébergeur, un impartiteur, à un fournisseur de services de type SAAS ou en mode de gestion de service.

iv http://csrc.nist.gov

v http://www.projectliberty.org/

vi Gartner Identity and Access Management Summit, «The Death of IAM and the Loss of Identity Innocence — A Review of Program Maturity, Service-Driven Change and New-Era Threats», San Diego (CA), November 9-11, 2009.

vii Gartner Identity and Access Management Summit, « The Death of IAM and the Loss of Identity Innocence — A Review of Program Maturity, Service-Driven Change and New-Era Threats », San Diego (CA), November 9-11, 2009.