XMedius

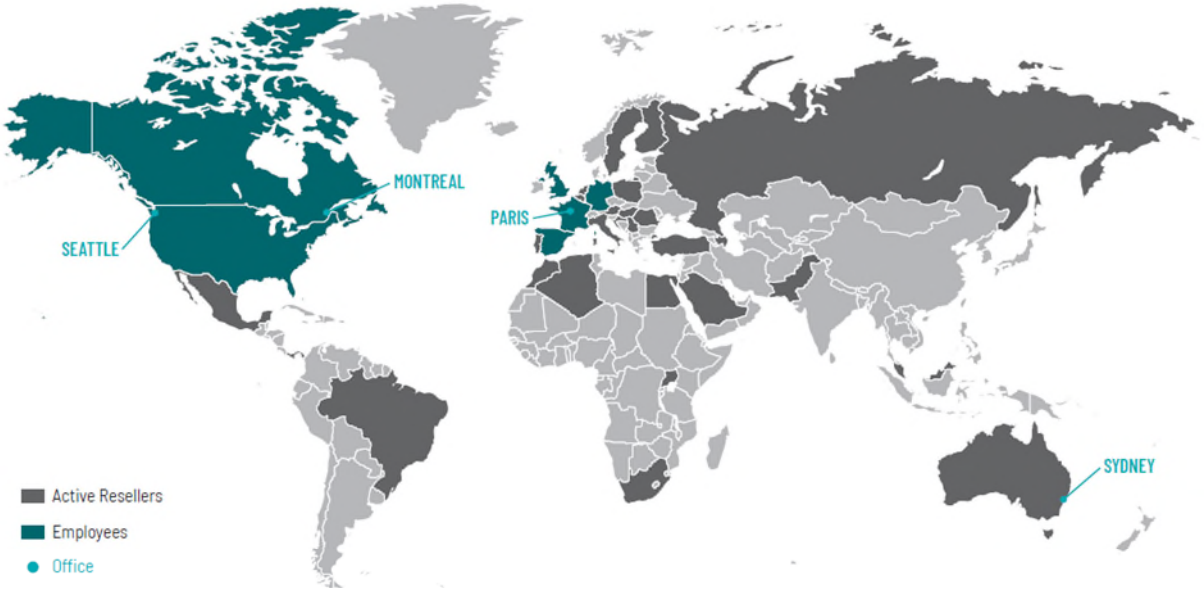
ISO 27001, LA FONDATION D'UN BON PROGRAMME DE SÉCURITÉ

SÉBASTIEN BOIRE-LAVIGNE

BRÈVE INTRODUCTION

Sébastien Boire-Lavigne

General Manager, Data Solutions
CISM



+Fondé 1993 +180 Employés +Actif dans 75 pays

Solution de communication pour les entreprises

Voix	Donnée
XM Connect XM Hospitality XM TeamQ	XM Fax XM SendSecure

On-Premises	Hybrid	Cloud

INFRASTRUCTURE INFONUAGIQUE

- 6 CENTRES DE DONNÉES (EN PAIRE)
- 3 RÉGIONS INDÉPENDANTES
- 6 FOURNISSEURS TELECOM
- 50+ SERVEURS / RÉGION
- INFRASTRUCTURE « MÉTAL » ET VIRTUALISÉS
- CAPACITÉ DE 5 MILLIONS DE PAGES FAX / MOIS / REGION
- CERTIFICATION ISO 27001 / CONFORMITÉ RGPD (GDPR)
- GÉRÉ DE MONTRÉAL
- UTILISE AWS (VIRGINIE DU NORD, IRLANDE, MONTRÉAL)

EN QUOI CONSISTE ISO 27001

- Famille de standard ISO liée à la sécurité de l'information (série 27000)
- Cadre pour établir un système de gestion de la sécurité
- Principaux standards: ISO 27001 & ISO 27002
- Fondement du système: PDCA/PVFR
  - Planifier, Faire, Vérifier, Réagir (Plan, Do, Check, Act)
- 114 objectifs de contrôle organisés en 14 groupes

PDCA EN PRATIQUE POUR LA SÉCURITÉ DE L'INFORMATION

Planifier	Faire	Vérifier	Réagir
Évaluation & plan de traitement des risques	Traitement des risques	Audit & surveillance	Action corrective & réponse aux incidents

LES DOMAINES DE SÉCURITÉ – ISO 27001

- A.5 Politique de sécurité [2 contrôles]
- A.6 Organisation de la sécurité [7 contrôles]
- A.7 Sécurité des ressources humaines [6 contrôles]
- A.8 Gestion des actifs [10 contrôles]
- A.9 Contrôle de l'accès [14 contrôles]
- A.10 Cryptographie [2 contrôles]
- A.11 Sécurité physique et environnementale [15 contrôles]
- A.12 Opération de la sécurité [14 contrôles]
- A.13 Sécurité des communications [7 contrôles]
- A.14 Acquisition, développement & maintenance des systèmes [13 contrôles]
- A.15 Sécurité des fournisseurs [5 contrôles]
- A.16 gestion de la réponse aux incidents de sécurité [7 contrôles]
- A.17 Gestion de la continuité d'activité [4 contrôles]
- A.18 Conformité [8 contrôles]

FEUILLE DE ROUTE VERS ISO 27001

PRÉPARATION

FEUILLE DE ROUTE VERS ISO 27001

MISE EN PLACE

DE L'IDÉE AU RÉSULTAT

bsi. ISO/IEC 27001 Information Security Management

= 24 MOIS

COÛTS DU PROGRAMME DE SÉCURITÉ

- Mise en place
  - $40k, formation, consultants, audit
  - $100k, 1 année de travail (ressources internes, sur 2 ans)

- Maintient du système
  - $15k, consultants (évaluation du risque, audits internes)
  - $25k, auditeurs, voyagement (2 bureaux, 6 centres de données)
  - $24k, 400 heures (2 pers, ≅ 5 semaines / pers.)

- Exclus les coûts de sécurité « directs »
  - ≅ $300k

LA SÉCURITÉ CHEZ XMEDIUS

Contrôles administratifs

- 12 politiques de sécurité:
  - Manuel de la sécurité
  - Cryptographie
  - Contrôle d'accès
  - Utilisation acceptable
  - Continué des activités et reprise après sinistre (BCDR)
  - Fournisseurs
  - Sauvegarde et rétention
  - Contrôles physiques
  - Collection des informations personnelles
  - Réponse aux évènements
  - Mise à pied/sortie
- Programme de formation de sécurité:
  - Sensibilisation à la sécurité
  - Ingénierie sociale
  - Vie privée
  - Traitement des données client
- Audit interne & par un tiers indépendant
- Tests de pénétration
- Évaluation des risques
- Inventaire des équipements, logiciels et informations

Contrôles techniques

- AD / Authentification / contrôle d'accès
- Outils de gestion des comptes privilégiés (PAM)
- VPN/tunnels IPSEC
- Pare-feu, IDS, Antivirus
- Surveillance/SIEM/FIM
- Ségrégation des réseaux
- Cryptage
- Scanneur de vulnérabilité
- Journaux des évènements
- Gestion des correctifs (Patch management) / veille des vulnérabilités
- Aire de travail protégé par carte d'accès
- Accès restreint aux zones critiques (cartes ou cadenas)
- Système de surveillance par caméra
- Système d'alarme
- UPS / Génératrice

LA SÉCURITÉ ET LES FOURNISSEURS

- Dans un monde infonuagique, un élément est de plus en plus important
- De plus en plus de clients sont sophistiqués dans la gestion de la sécurité des fournisseurs
- Risques avec des fournisseurs (infonuagique ou non), pas différents des autres risques d'une organisation:
  - Contrôler, Éviter, Transférer, Accepter
- La RGPD/GDPR force une gestion stricte des risques liés aux fournisseurs

LEÇONS APPRISES

- ISO 27001 est une base solide et extensible
- Garder les choses simples
  - Ne pas être trop ambitieux, être certain de pouvoir livrer sur nos promesses
  - Documenter le strict nécessaire
- La maturité prend du temps
- L’appui de la haute direction est primordial
- Les choses les plus simples sont souvent les contrôles les plus efficaces
  - Gestions des correctifs, ségrégation, surveillance
- La valeur des tests de pénétration est inestimable
  - On ignore souvent des risques importants sans le savoir
- La gestion des fournisseurs est souvent un enfant pauvre des systèmes de sécurité
- La sécurité ne s’arrête pas au pare-feu

POURQUOI MONTER UN PROGRAMME DE SÉCURITÉ

- Pour se différencier
- Pour la confiance (Certificat, rapport d'audit)
- Pour réellement diminuer les risques liés au cyber
- Pour réduire les coûts de se conformer avec la règlementation
  - RGPD (GDPR)
  - HIPAA
  - HDS
- Réduire les coûts des assurances (E&O) contre les risques liés au cyber

LES PROCHAINES ÉTAPES EN CONFORMITÉ CHEZ XMEDIUS

- 2019 Q3
  - PCI-DSS (Fournisseur de service niveau 1, 300k+ transactions)
- 2020 Q3
  - HiTrust
- 2020+
  - NIST 800-53
  - HDS (France)
  - Soc 2
  - FedRamp (USA)

CONCLUSION

- ISO 27001 parce que la sécurité c'est pour tout le monde
  - Fournis un cadre standardisé
  - Pas d'obligation d'obtenir/maintenir la certification ou de rencontrer tous les objectifs

- Si ISO 27001 n'est pas pour vous…
  - Au moins, faire des évaluations de risque annuel, avec plan de traitement des risques:
    - Évaluer vos contrôles de sécurité en place
    - Faire un tour d'horizon des menaces avec un accent sur vos maillons faibles
    - Déterminer les niveaux de risques et s'ils sont acceptables (occurrence & impact)
    - Faire un plan de traitement de risque pour mitiger les risques non acceptés

- ISO 27001 c'est l'attestation qu'un fournisseur a mis en place un système de sécurité compréhensif et efficace

- ISO 27001 ce n'est pas une destination, c'est un commencement

QUESTIONS?