



Introduction à la sécurité

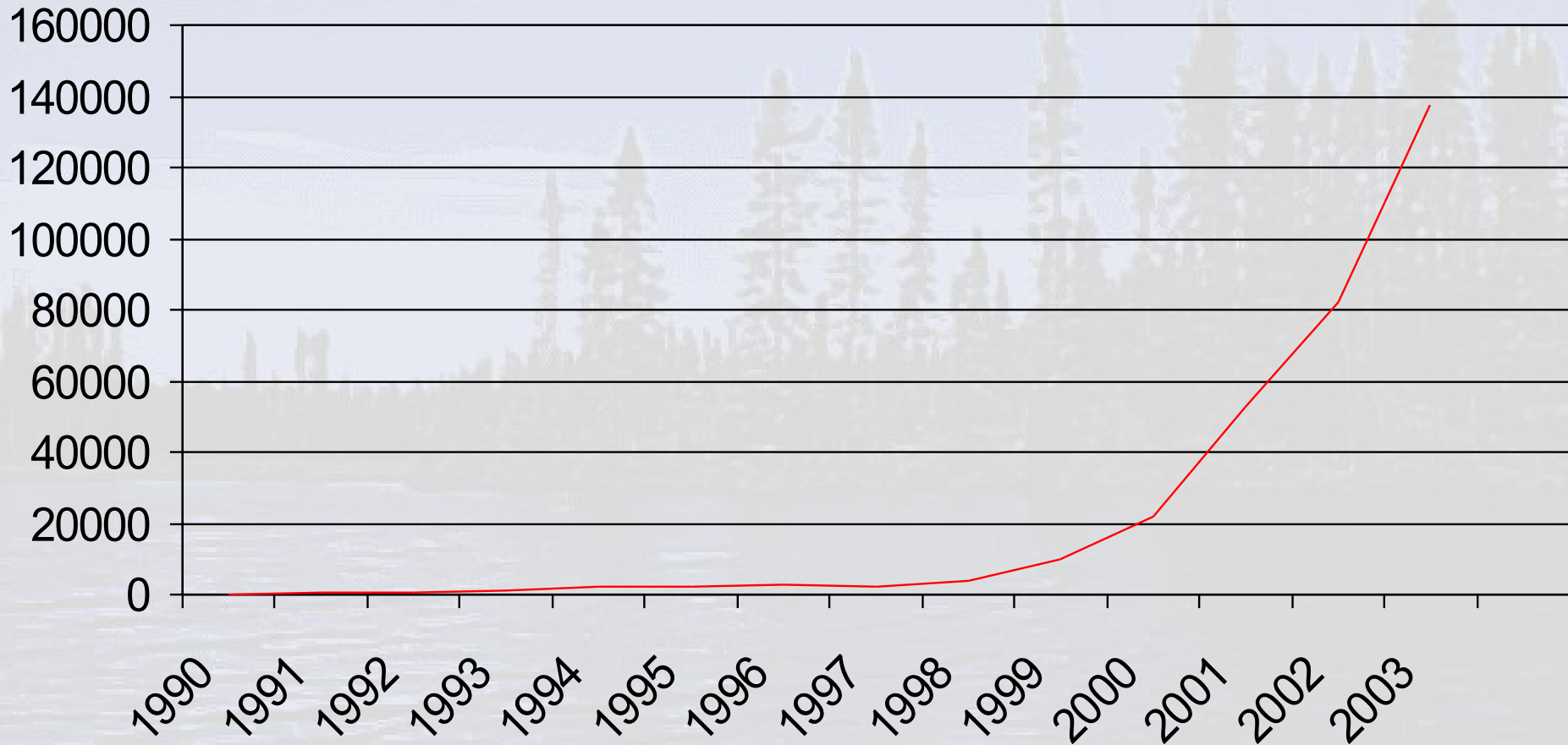
Octobre 2004

Marc-André Léger, MScA

Plan du cours

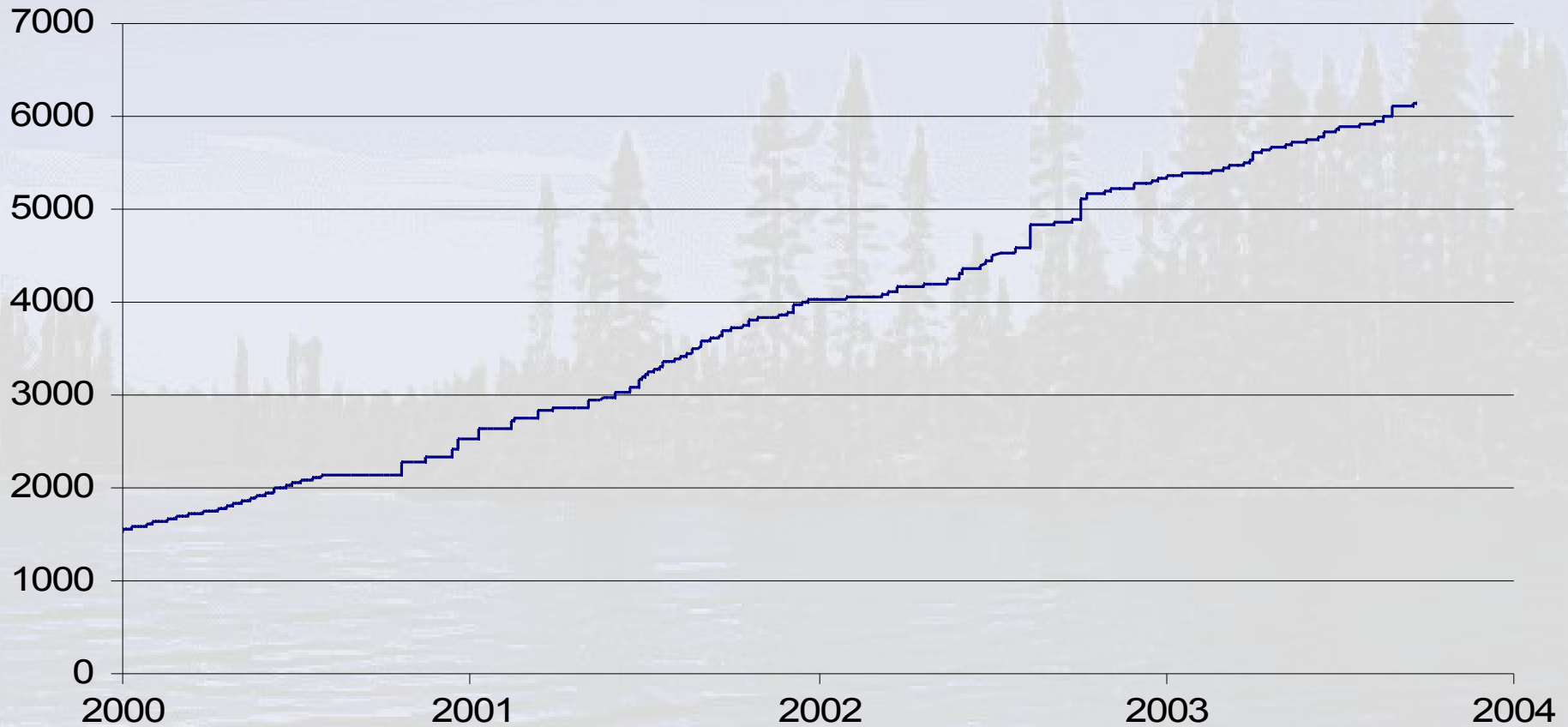
- Principes de base de la gestion de risque et de la sécurité
- Gouvernance
- Diligence raisonnable
- Besoins légaux et réglementaires (Sarbanes-Oxley)
- Loi sur l'accès
- Cadre juridique québécois
- TP : travail de recherche personnel à remettre au cours 16 (20%)

Pourquoi se protéger ?



Croissance exponentielle des incidents

Vulnérabilités

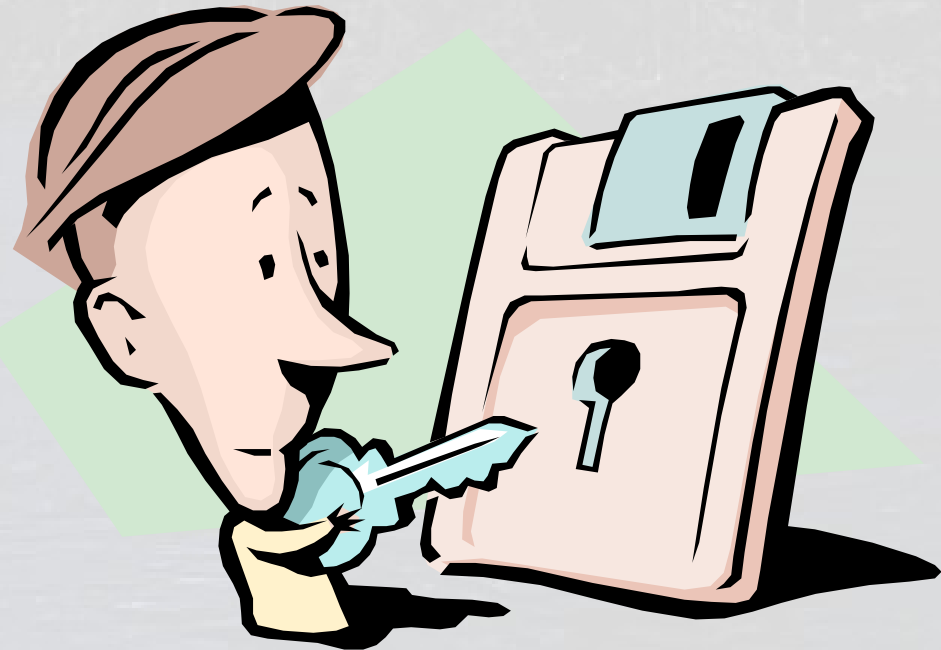


Croissance rapide des vulnérabilités

Protéger tout les actifs

“L'information est un actif qui, comme les autres actif importants pour l'organisation, a une valeur et par conséquent a besoin d'être protégé.”

ISO/IEC 17799:2000



Types d'informations

- Fichiers stockés numériquement;
- Informations sur support papier, imprimé ou manuscrit;
- Images, films, radiographies;
- Vidéo, musique;
- Conversations.



Protection de l'informations

Quelle que soit la forme prise par l'information ou quels que soient les moyens par lesquels elle est transmise ou stockée,

il faut qu'elle soit toujours protégée de manière appropriée.

ISO/IEC 17799:2000

Définitions

La **sécurité de l'information** est définie comme l'ensemble des actions et des procédures conçues pour prévenir, avec un niveau de certitude démontrable, la divulgation, le transfert, la modification ou la destruction non autorisée, volontaire ou accidentelle de données.

Définitions

Une **menace** consiste en une situation ou une condition avec le potentiel de compromettre la sécurité de l'information.



Définitions

Le **risque** est l'impact négatif net résultant de l'exploitation d'une menace en considérant sa probabilité et ses impacts.

Définitions

Les **mesures de protection** sont les éléments, les outils ou les processus mis en place pour réduire le niveau d'exposition, mitiger les conséquences d'une vulnérabilité technologique, contrer une menace ou solutionner un problème de sécurité particulier. En général, des mesures de protection pertinentes et bien utilisées réduisent le risque.

Définitions

L'évaluation des menaces et du risque consiste à observer, dans un processus formel, la relation entre la menace et le risque pour en évaluer la probabilité. Cette analyse aidera l'organisation à déterminer les mesures de protection disponibles et prendre des décisions concernant la pertinence de leur mise en place.

Définitions

Une **cyber attaque** est définie comme l'exploitation d'une menace par l'intermédiaire des systèmes d'information ou de réseaux de télécommunications, tel que le réseau InterNet.

Fondements d'une solution

- Utilisation de normes
- Utilisation de méthodes
- Engagement de haut niveau
- Création d'un comité de gouvernance
- Audit
- Définition des objectifs
- Politique de sécurité
- Création de comité(S) de sécurité(S)

Définition des objectifs

L'organisation doit déterminer ses objectifs de sécurité en alignement avec ses objectifs d'affaires

Objectifs de la sécurité

- la confidentialité des données;
- l'intégrité des données;
- la disponibilité des données;
- la non répudiation des transactions;
- l'authentification des utilisateurs;
- l'authentification de l'origine des données; et
- le contrôle des accès.

Confidentialité

La **confidentialité** identifie la sensibilité de l'information ou des biens à une divulgation non autorisée.

Intégrité des données

L'**intégrité** est l'exactitude et l'intégralité des renseignements et des biens ainsi que l'authenticité des transactions.

Disponibilité des données

La **disponibilité** est l'accessibilité d'un système d'information ou des données qu'il contient, au moment opportun, pour exécuter certains processus.

Non répudiation des transactions

La **non répudiation** ou l'**irrévocabilité** réfère à la permanence dans le temps et à la démontrabilité tangible de l'existence d'une transaction.

Authentification des utilisateurs

L'**authentification** des utilisateurs définit des mécanismes et des processus qui sont utilisés pour identifier, avec un niveau de certitude déterminé, l'identité d'un utilisateur d'un système d'information.

Authentification de l'origine des données

L'**authentification** de l'origine des données définit des mécanismes et des processus qui sont utilisés pour identifier, avec un niveau de certitude déterminé, la source d'une donnée stockée dans un système d'information.

Contrôle des accès

Le **contrôle des accès** aux informations contenues dans un système d'information d'une organisation devrait être établi en fonction de ses objectifs et de ses obligations.

Les pistes de solution

- Analyse de risque
- Analyse de vulnérabilités
- ISMS
- ISO 17799
- Conformité (Gouvernance)
- ITSM (ITIL)
- Gestion du changement
- Architecture de sécurité

Gouvernance

- Règles de gestion
- Emmené par Nortel, Enron, Parmalat
- Respects des aspects d'éthiques des affaires

Diligence raisonnable

- Principe juridique
- Ce qu'un bon père de famille ferait dans la même situation
- La responsabilité (\$\$\$) comme conséquence

Besoins légaux et réglementaires (Sarbanes-Oxley)

- Lois américaines
- Lois canadiennes
- Autorité des marchés financiers
- Nouvelles lois à venir

TP : travail de recherche personnel à remettre au cours 16 (20%)

- Effectuer une recherche sur un des éléments dictés dans le cours
- 4-10 pages
- Références

Laboratoire

- Configuration des postes de travail avec Red Hat Linux
 - Installer Apache
 - MySQL
 - Xwindows
 - Etherreal