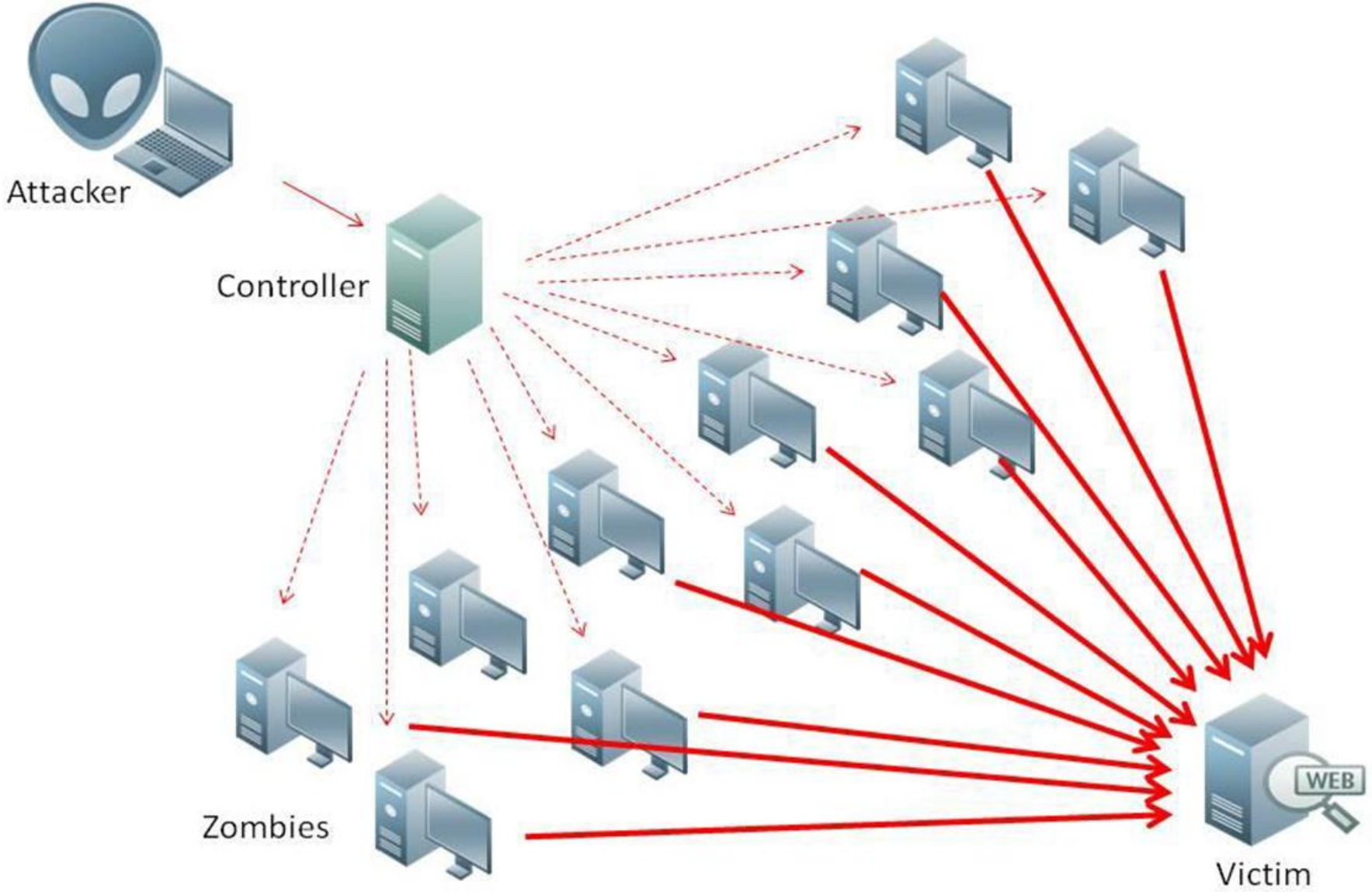
Cybercriminalité et protection des données

Jean-François De Rico, Langlois avocats

Et

Luc Lefebvre, Landry & Associés

1- Déni de service (ou « DDoS »)



LCCJTI – C-I-A

TÉLÉCOMMUNICATIONS XITTEL INC.

et

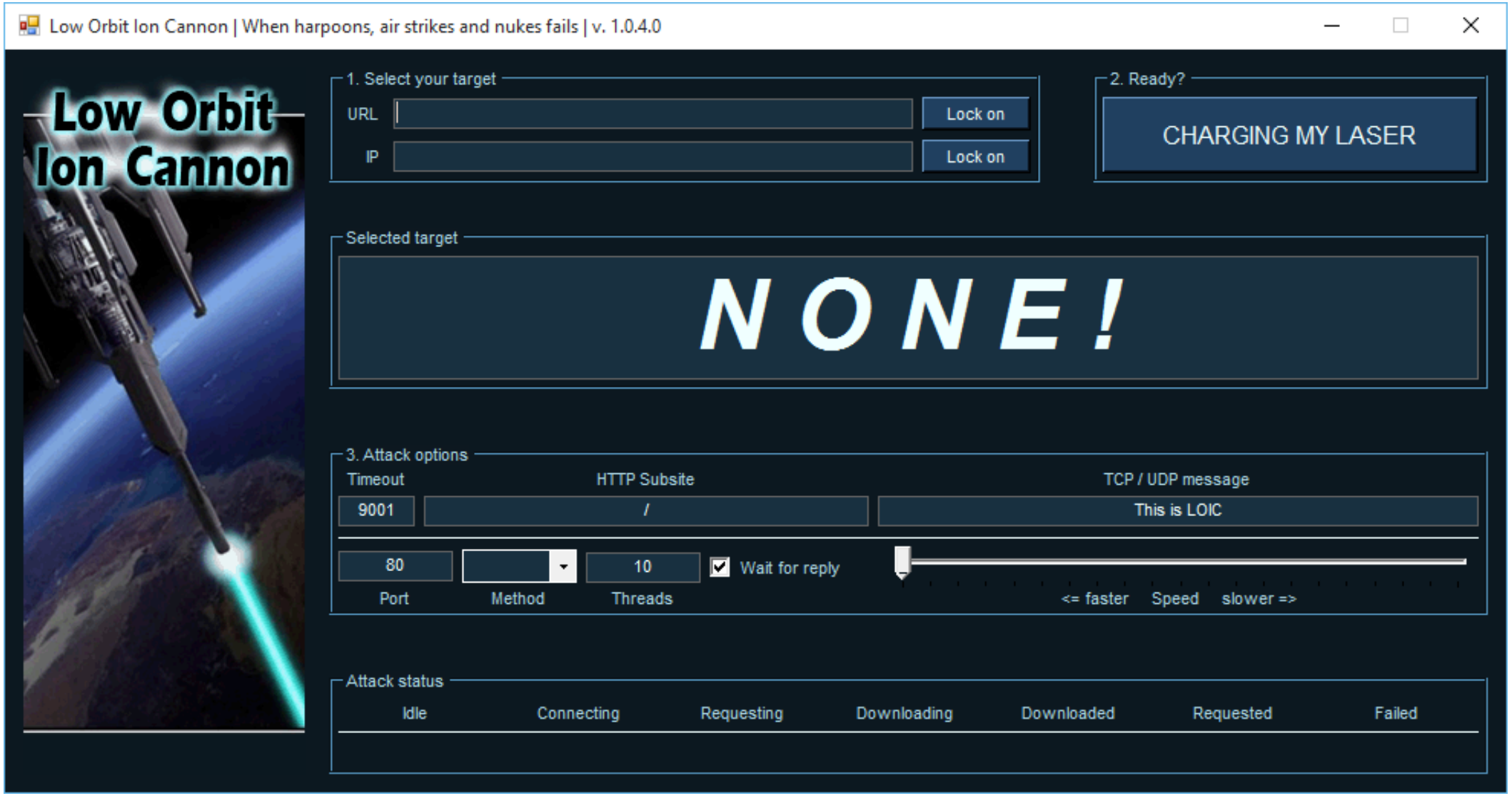
9116-6033 QUÉBEC INC., société légalement constituée faisant affaires sous le nom de **LES SYSTÈMES INFORMATIQUES CONCEPTA**

Demanderesses

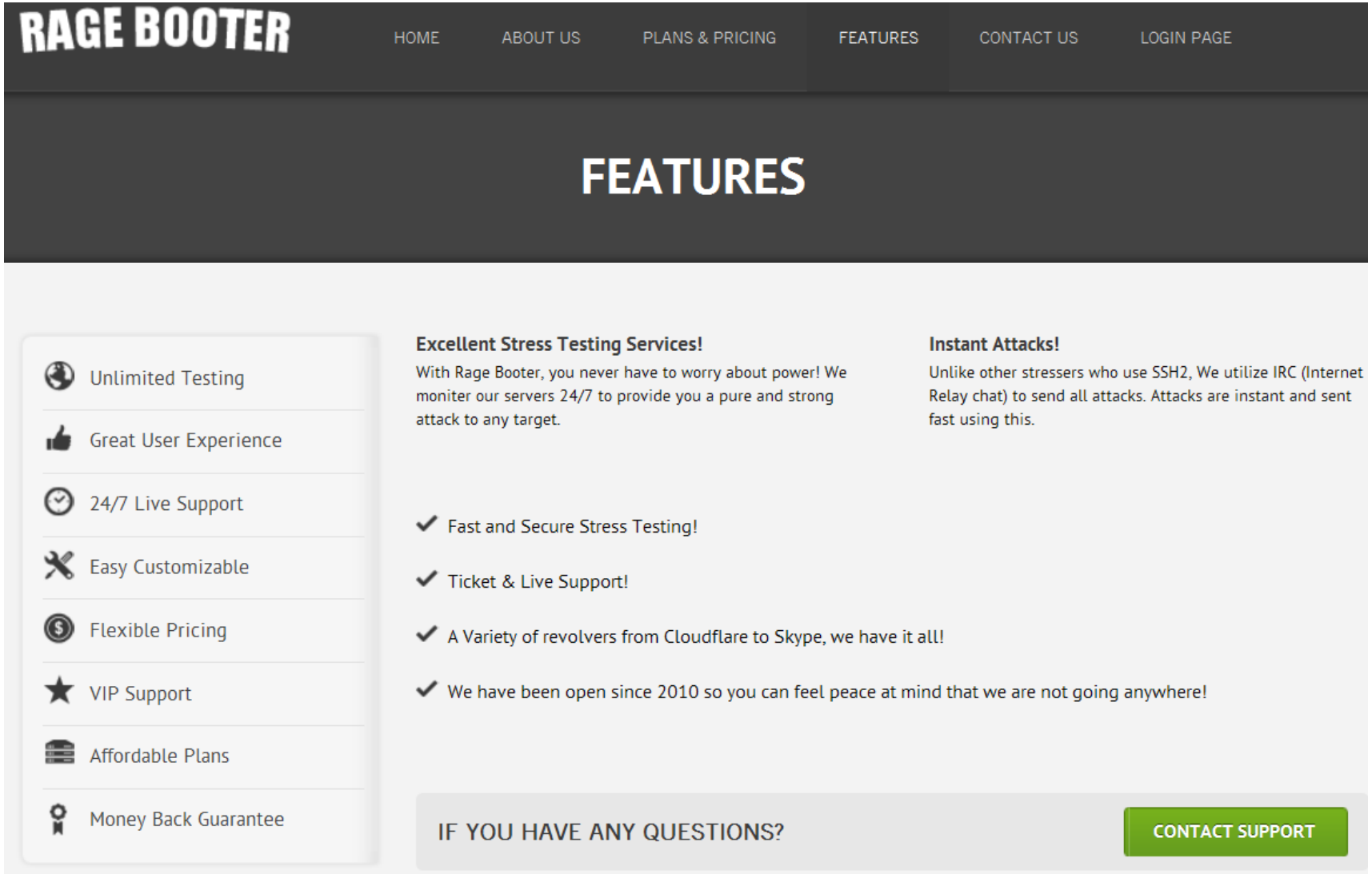
c.

KEVIN COURTOIS

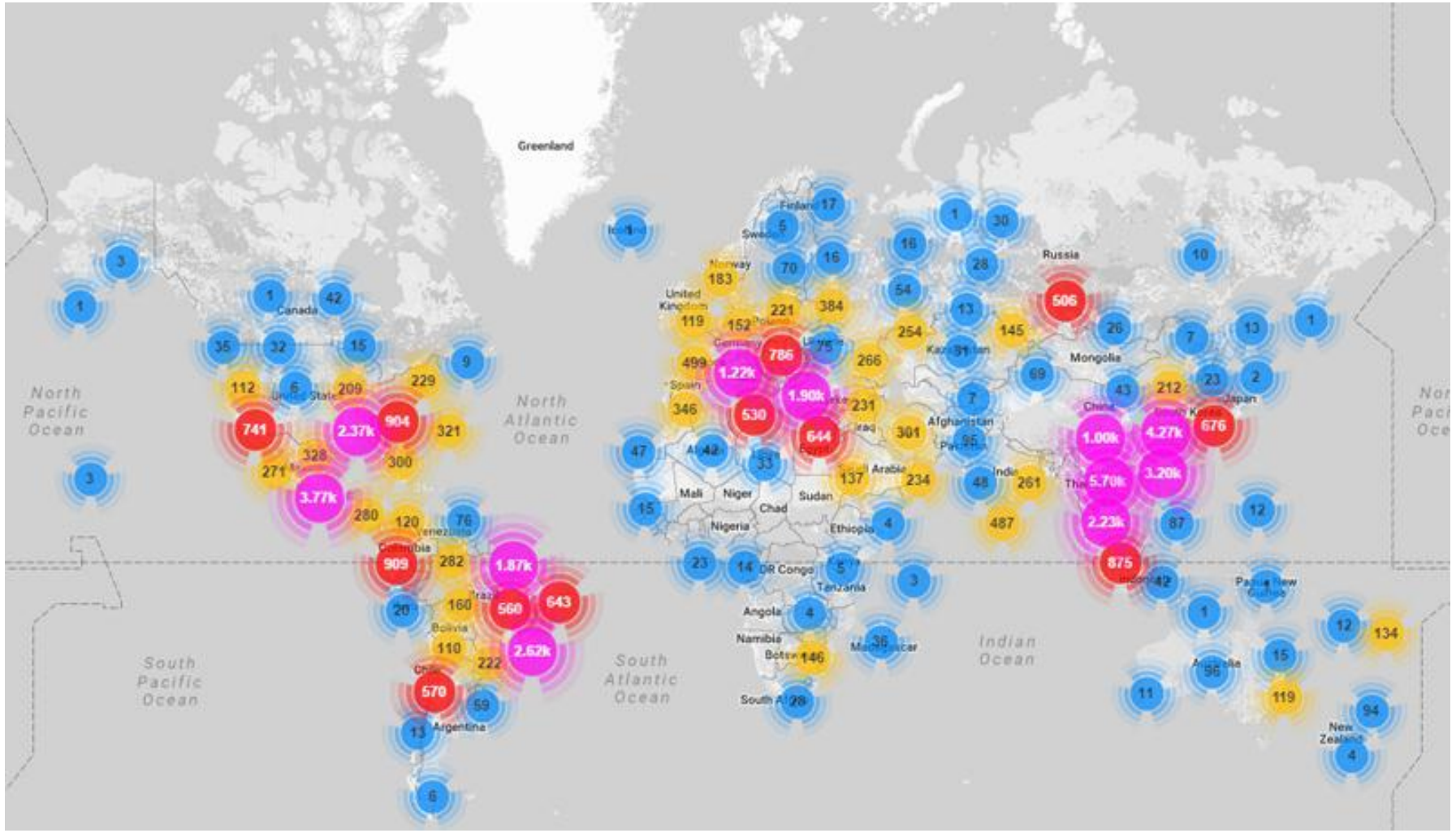
1- « DDoS » - services



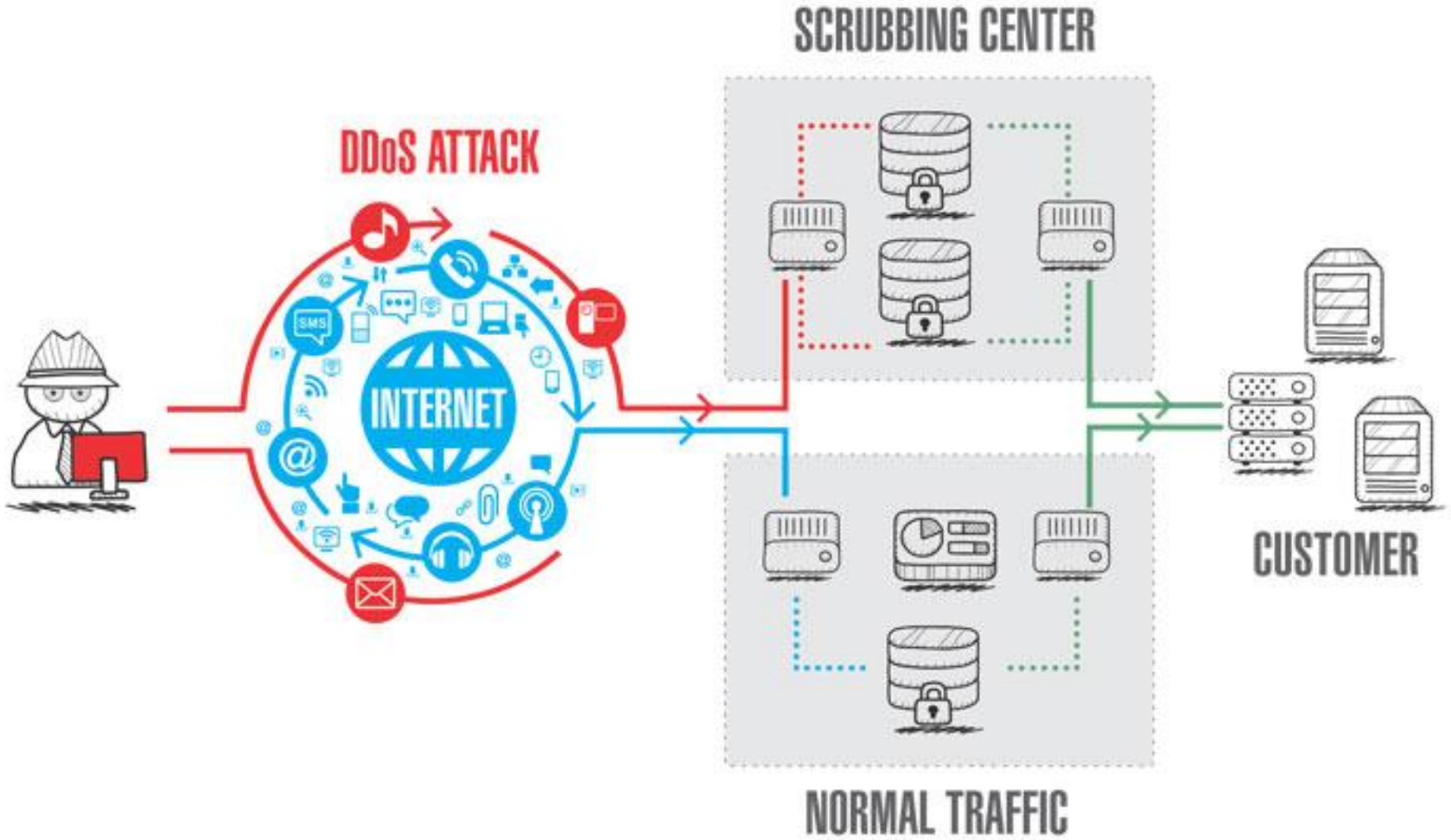
1- « DDoS » - services



1- « DDoS » - services



1- « DDoS » - mitigation



Internet of things

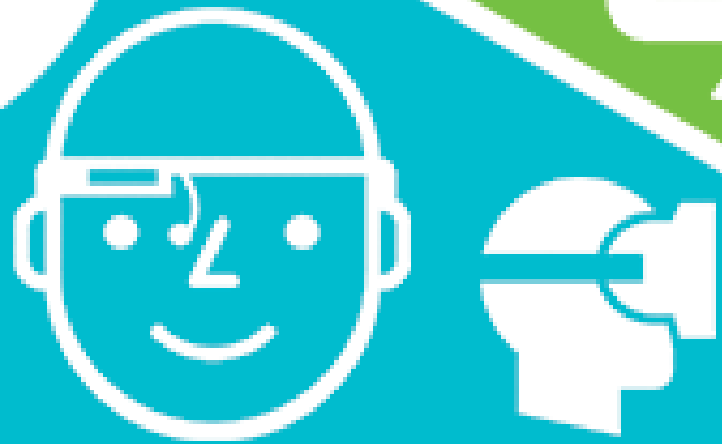
CAPITA

DEVICES WE ALREADY USE

DEVICES USING CONNECTIVITY IN NEW WAYS

DEVICES PREVIOUSLY INACTIVE, BUT NOW INTELLIGENT

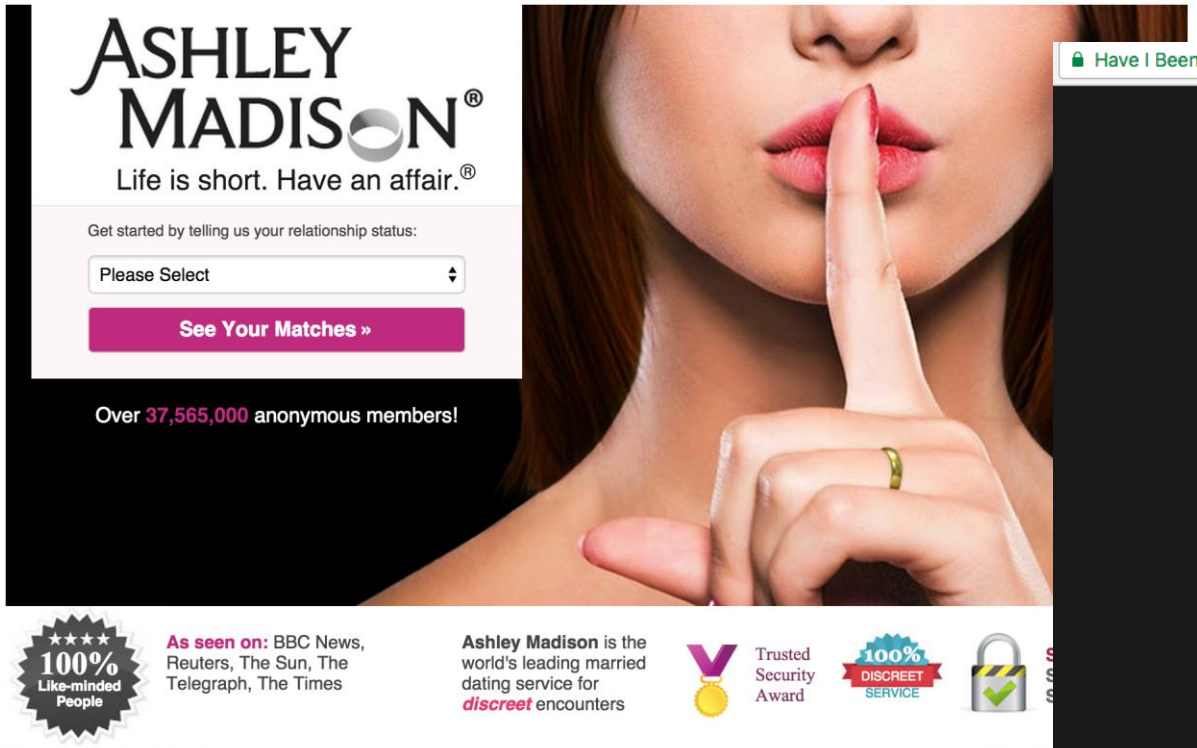
COMPLETELY NEW DEVICES

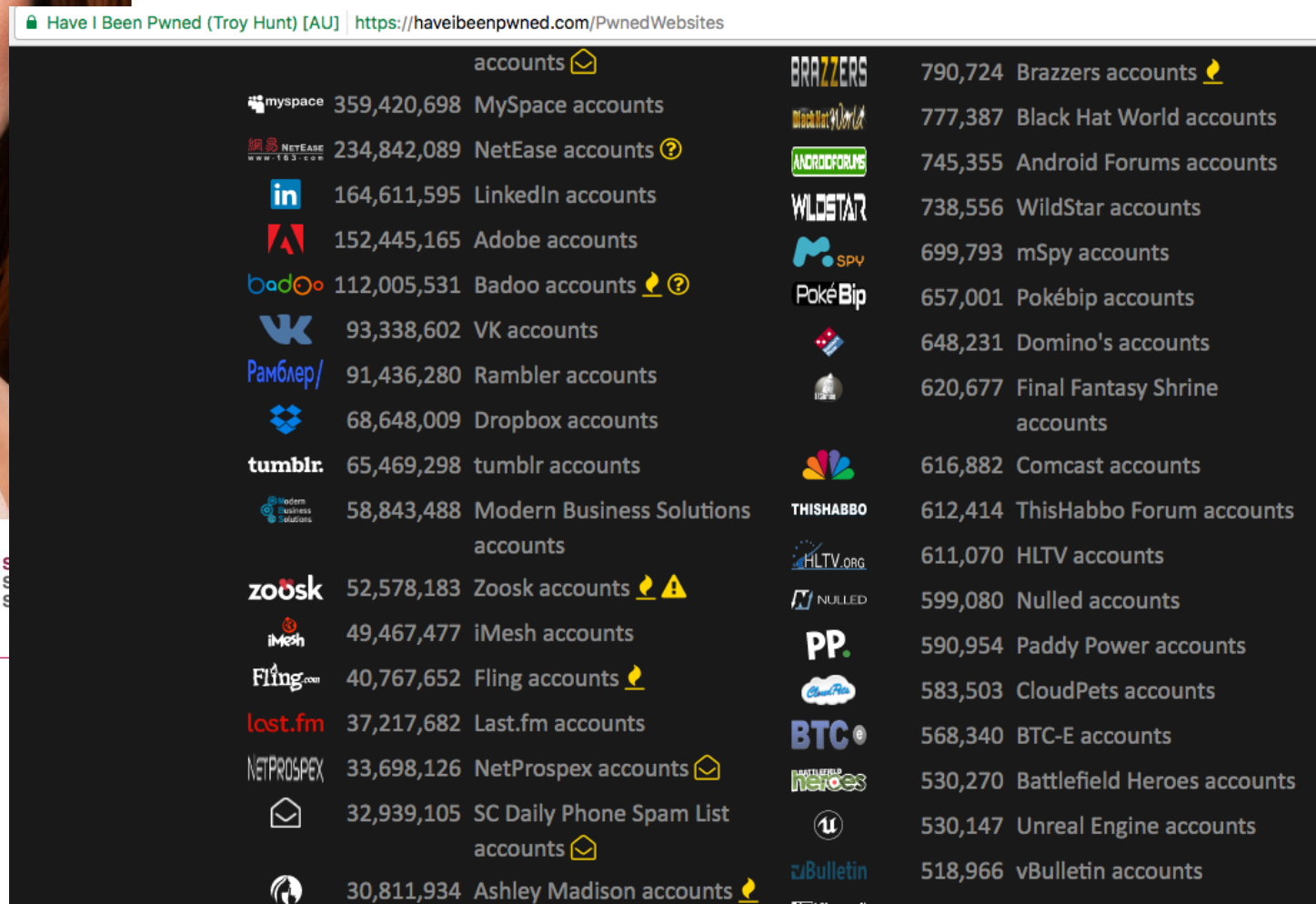


1- « DDoS » - responsabilité

En janvier 2012, un hacker a identifié une faille dans la sécurité d'un système de télésurveillance , qui a ensuite été exploitée par des "confrères" qui ont diffusé/rendu accessible le contenu de 700 caméras.

2- Intrusion et sécurité des bases de données





2- Intrusion et sécurité des bases de données

LCCJTI – C-I-A

2- Intrusion et sécurité des bases de données

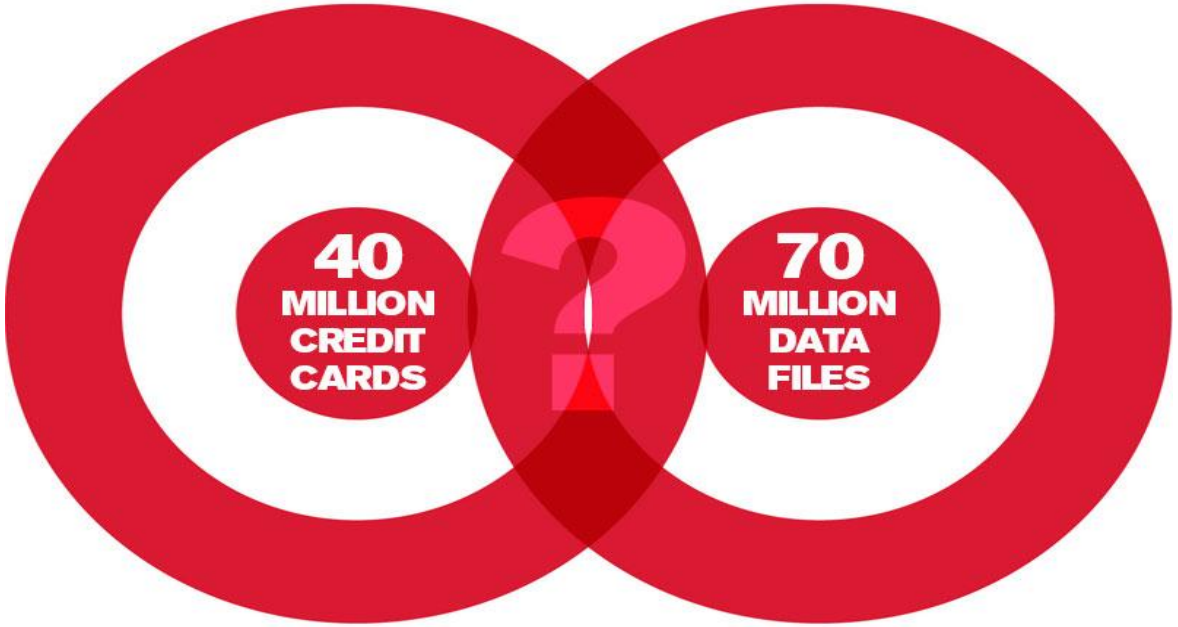
- **Tests d'intrusions (pentests)**
  - Hackers éthiques
  - Standards à suivre : ISO 27000, PCI DSS
  - Méthodologies à suivre: NIST framework, OWASP
- **Pour éviter dans le futur?**
  - Chiffrement
  - Audit indépendant
  - Rapport de transparence
  - Modèle d'affaire

2- Intrusion et sécurité des bases de données

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation This Document Relates to: All Financial Institutions Cases	MDL No. 14-2522 (PAM/JJK) **CONSOLIDATED CLASS ACTION COMPLAINT**

Umpqua Bank, Mutual Bank, Village Bank, CSE Federal Credit Union, and First Federal Savings of Lorain, Individually and on behalf of a class of all similarly situated financial institutions in the United States, Plaintiffs, v. Target Corporation, Defendant.	JURY TRIAL DEMANDED



In re: Target Corporation Customer Data Security Breach Litigation,

RÉGLEMENTS INTERVENUS

- $39 million avec les banques visées par le recours collectif
- $67 million avec VISA
- $10 million avec des clients

AM AND EM MUST SHUT DOWN IMMEDIATELY PERMANENTLY

Avid Life Media runs Ashley Madison, the internet's #1 cheating site, for people who are married or in a relationship to have an affair. ALM also runs Established Men, a prostitution/human trafficking website for rich men to pay for sex, as well as cougar life, a dating website for cougars, man crunch, a site for gay dating, swappernet for swingers, and the big and the beautiful, for overweight dating.

Trevor, ALM's CTO once said "Protection of personal information" was his biggest "critical success factors" and "I would hate to see our systems hacked and/or the leak of personal information"

Well Trevor, welcome to your worst fucking nightmare.

We are the Impact Team. We have hacked them completely, taking over their entire office and production domains and thousands of systems, and over the past few years have taken all

2- Intrusion et sécurité des bases de données

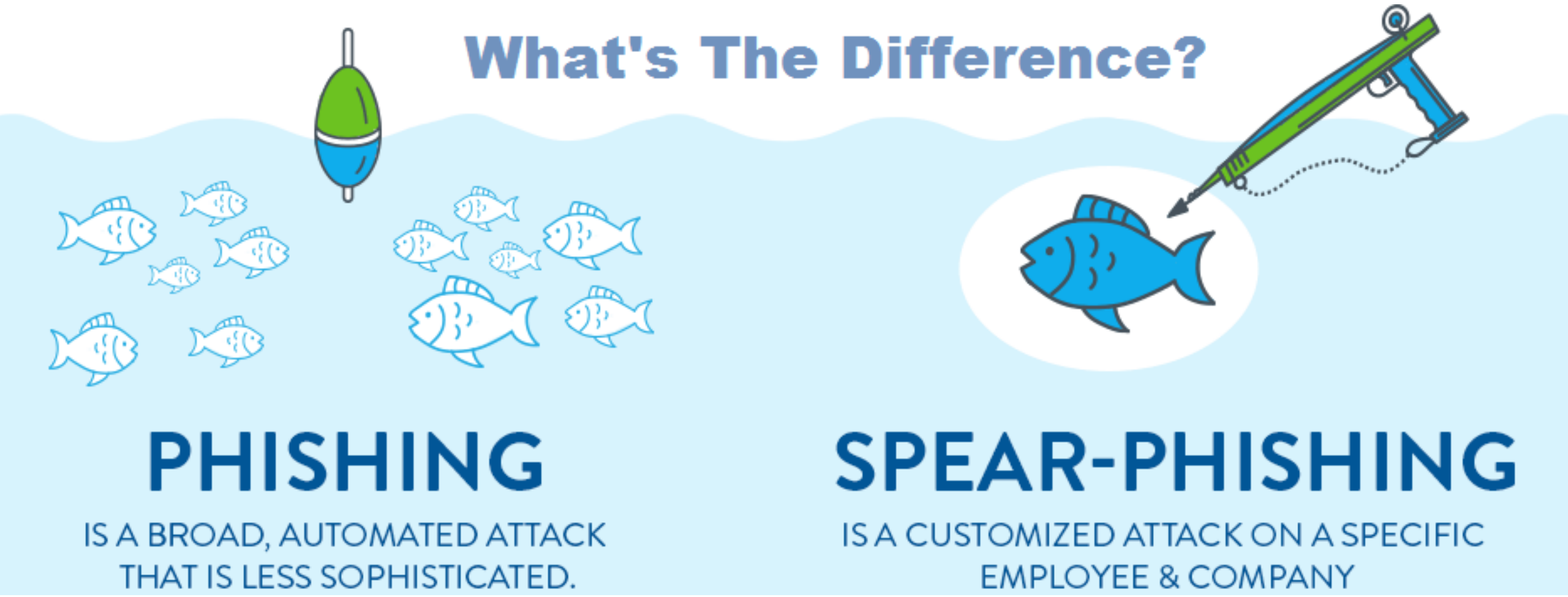
CRITÈRES D'ANALYSE:

- Les mesures de sécurité doivent être proportionnellement élevées:
  - Sensibilité des renseignements personnels détenus par ALM
  - Conséquences négatives prévisibles pour les utilisateurs du piratage de leurs RP
  - Déclarations faites par ALM en ce ui a trait à la sécurité de ses systèmes d'information,

QUESTIONS:

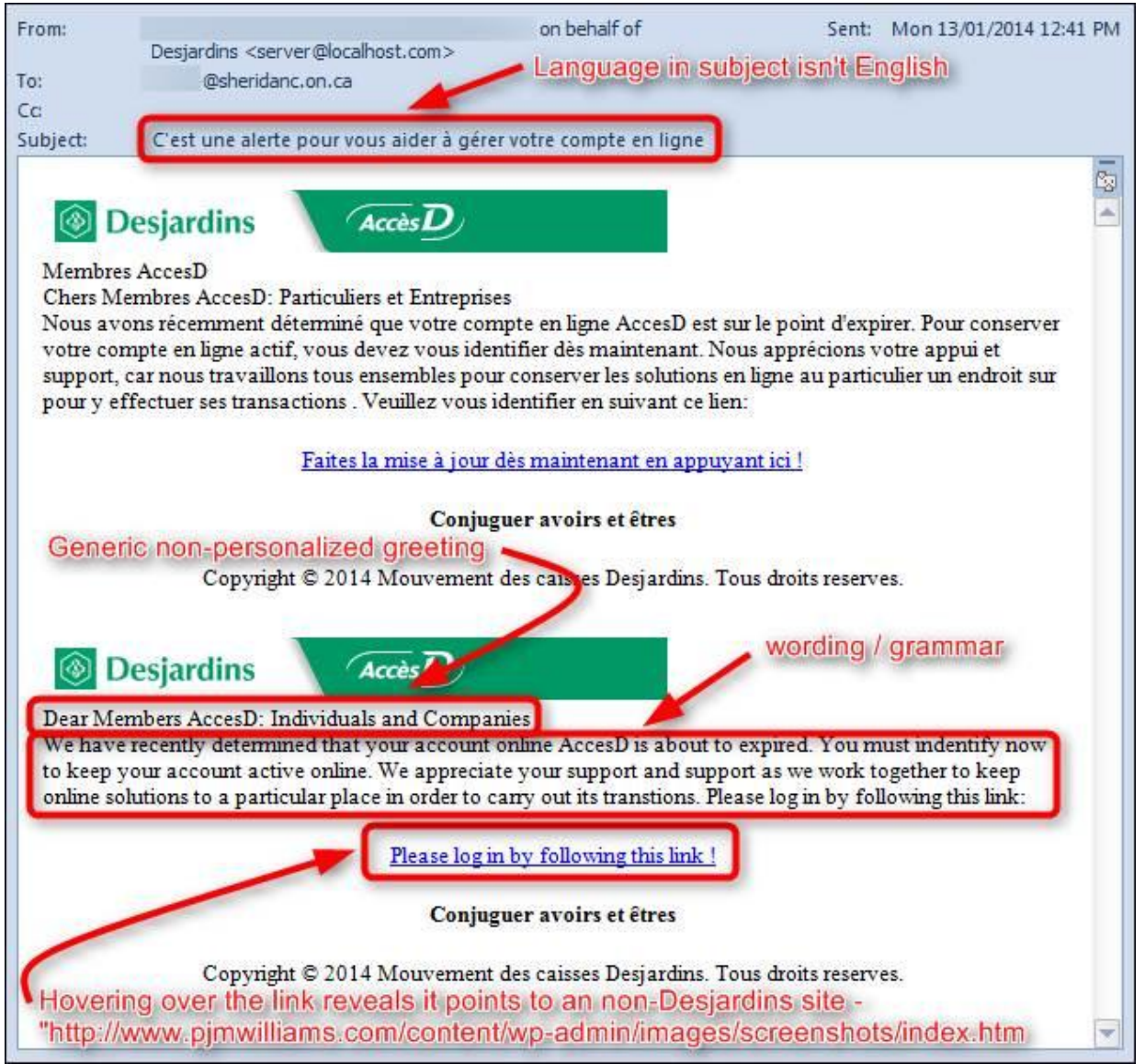
- L'organisation avait-elle un motif raisonnable pour conserver les renseignements personnels touchés par la brèche?
- L'organisation conservait-elle les renseignements conformément à la LPRPDÉ et à la PIPA?
- L'organisation avait-elle mis en place des mesures de sécurité raisonnables afin de protéger les renseignements personnels qu'elle conservait?
- Examen:
  - Étendue et conformité de la conservation
  - Mesures de protection de sécurité sans fil en place au moment de la brèche
  - Mesures adoptées après l'incident

3- L’hameçonnage et l’harponnage



3- L'hameçonnage et l'harponnage

exemples



3- L’hameçonnage et l’harponnage

exemples

www.lapresse.ca/actualites/201701/19/01-5061353-comment-un-escroc-a-vole-55-millions-a-la-coop-federee.php

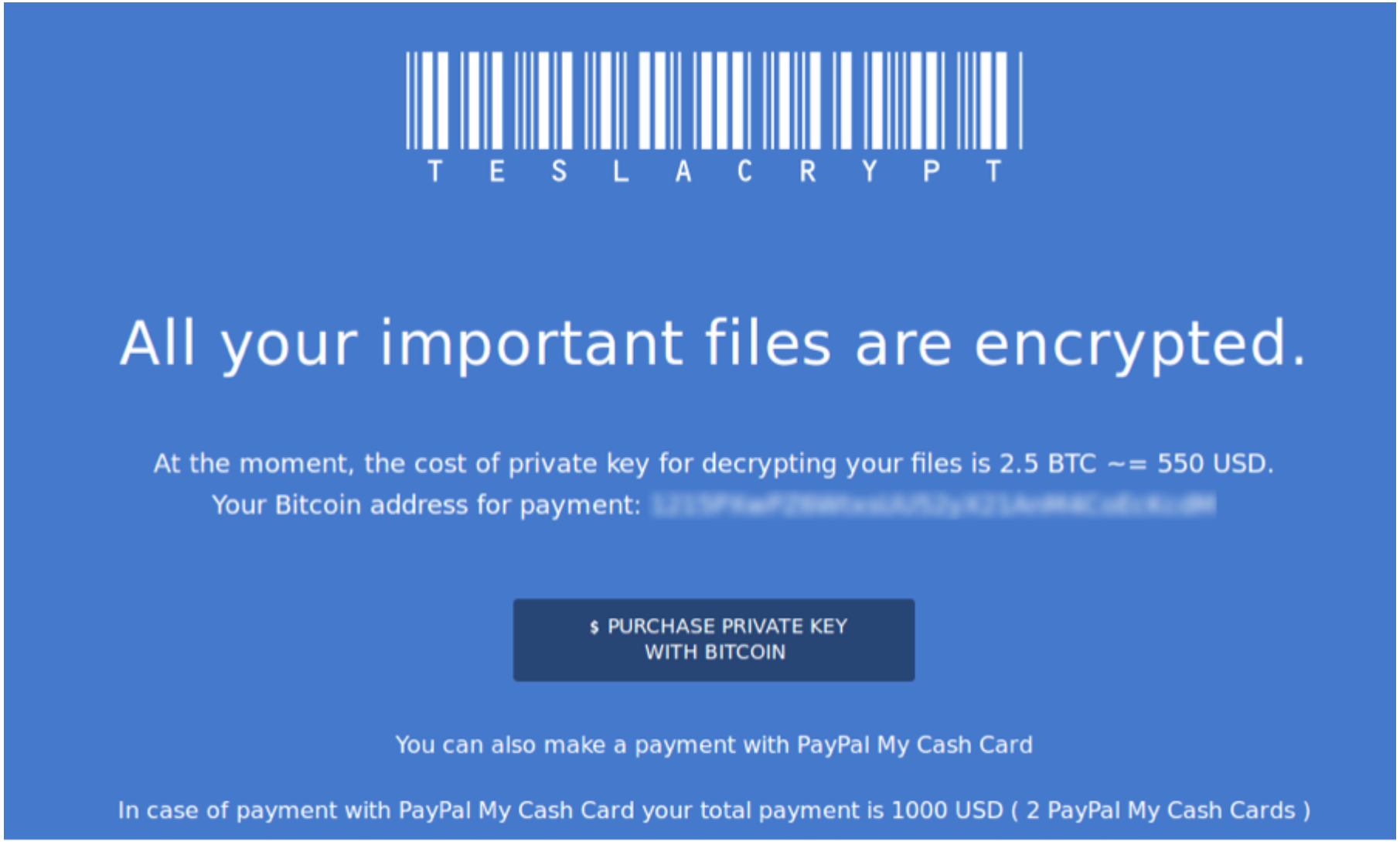
maPRESSE Découvrez Ma Presse

EXCLUSIF **Publié le 20 janvier 2017 à 05h00** | Mis à jour le 20 janvier 2017 à 06h18

Comment un escroc a volé 5,5 millions à La Coop fédérée

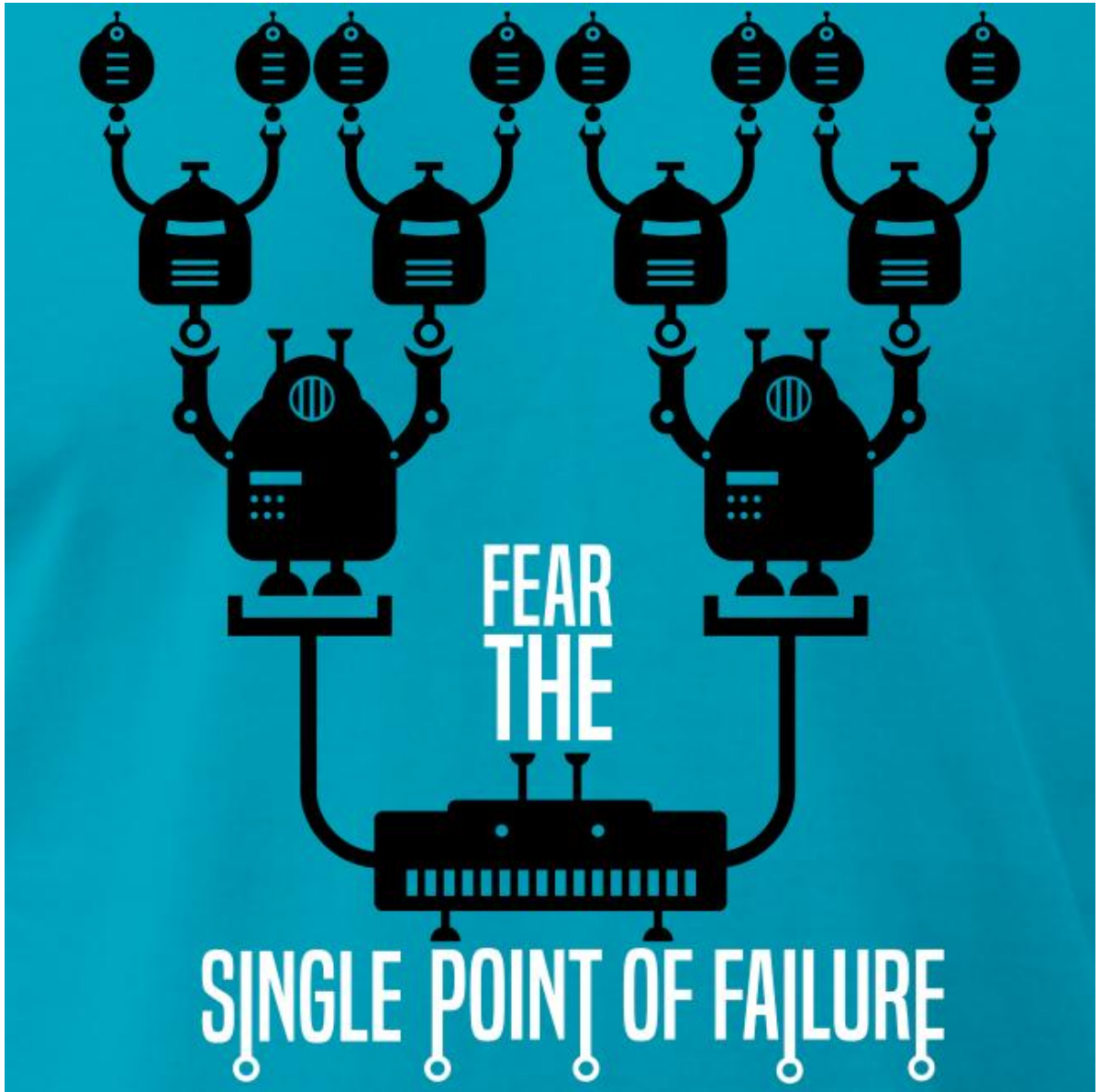
La Coop fédérée est propriétaire notamment des quincailleries BMR et des marques de viandes Olymel. Son chiffre d'affaires avoisine les 10 milliards de dollars annuels.

4- Le rançongiciel



4- Le rançongiciel

points faibles



4- Le rançongiciel

points faibles

4- Le rançongiciel

Assurance cyber-risques

Méthodes de prévention

- Solution techniques
  - Black list
  - Antivirus
  - Sandbox
- Formation et sensibilisation
- Tests

4- Le rançongiciel

Assurance cyber-risques

COUVERTURES MULTIPLES

- Les réclamations de tiers reliées à des intrusions dans nos systèmes informatiques, incluant les réclamations liées au défaut de protéger la confidentialité des données (pour autant que cela ne fasse pas déjà partie de notre police responsabilité)
- Les coûts reliés à la gestion de crise (professionnels de l'informatique, recouvrement de données, relations publiques, suivi de crédit des clients affectés, etc…)
- Coût associés à une demande de rançon par un pirate
- Pertes de revenus en raison de l'interruption d'accès aux systèmes informatiques

4- Le rançongiciel

Information

Application générale

CcQ

Obligations contractuelles

Protection des renseignements personnels

Responsabilité civile

Règlements et normes sectorielles

Criminel

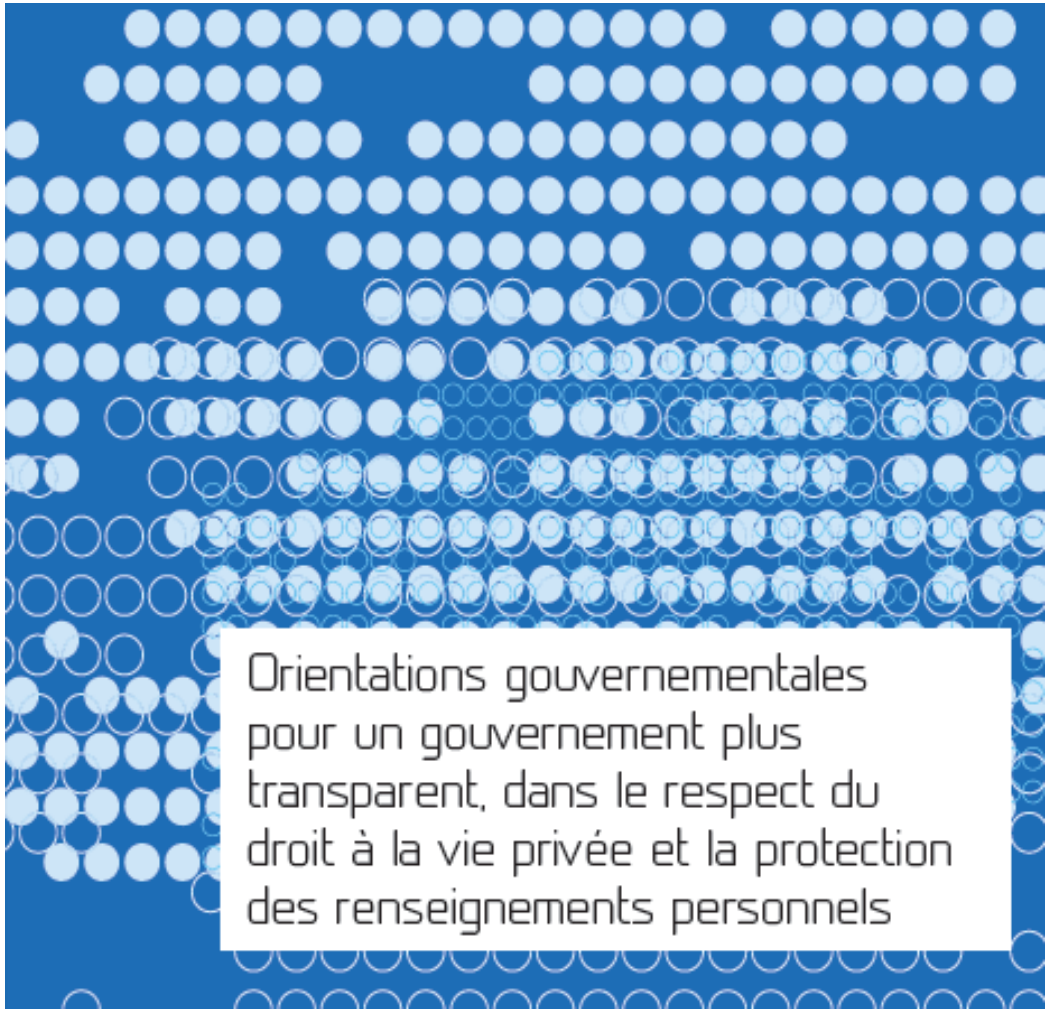
télécommunications

4- Le rançongiciel

Mars 2016

Règlement sur la notification et la déclaration des atteintes à la protection des données

4- Le rançongiciel



4- Le rançongiciel –

Principes directeurs pour les conseils d'administrations

- 1. **Understand and approach cybersecurity as an enterprise-wide** risk management issue, not just an IT issue.
- 2. Directors should **understand the legal implications** of cyber risks
- 3. Boards should have **adequate access to cybersecurity expertise**, and it should be on the agenda and discussed.
- 4. Directors should **set the expectation that management will establish an enterprise-wide risk management framework** with adequate staffing and budget.
- 5. Board-management discussion of cyber risk should include **identification of which risks to avoid, accept, mitigate, or transfer through insurance**, as well as specific plans associated with each approach.
-

Questions?

- Jean-François De Rico
  - Courriel: jean-francois.derico@langlois.ca
  - Tél: 418-650-7923 & 514-842-9512
  - Site Web: www.langlois.ca
  - LinkedIn: www.linkedin.com/in/jfderico
  - Twitter: @jfderico

- Luc Lefebvre
  - Courriel: luc.lefebvre@landryconsulting.com
  - Tél: 514-924-6726
  - Site Web: www.landryconsulting.com
  - LinkedIn: ca.linkedin.com/in/luclefebvre
  - Twitter: @luclefebvre