



Conférence RECO-Québec, cybernétique

Présenté par: Stephen Atkinson, Vice President, Financial Institutions

Le jeudi 17 novembre 2016



Stephen Atkinson

Vice-président
Institutions Financières, Aon
Conseillers en gestion des risques
Montréal

Stephen Atkinson représente la pratique d'Aon en institutions financières au Québec et dans les Maritimes. En travaillant en collaboration avec des collègues locaux, nationaux et internationaux, il offre le meilleur d'Aon Risk Solutions en matière de courtage en assurance et de services de consultation en gestion des risques à des gestionnaires d'actifs, des sociétés de capital d'investissement et de capital de risque, des assureurs

Situation actuelle : Perception du cyberrisque

- World Economic Forum – Global Risks 2015 Report (10th edition) – (www.weforum.org/risks)
 - vol de données et fraude (9^e rang comme probabilité de survenance)
 - Cyberattaque (10^e rang comme probabilité de survenance)
 - « critical information infrastructure breakdown » (7^e rang parmi les 10 risques les plus importants)
- Évaluation dans le monde des assurances

Ce n'est plus « Si » ça arrivera mais plutôt « Quand »

10 principaux risques



Qu'en est-il des menaces physiques?

2010	Stuxnet – 1ère arme digital (virus attaque centrifugeuses iraniennes)
2014	Cyber-piratage d'une aciérie allemande
2015	Cyber-piratage des jeep Cherokee Rapport publié par Lloyd concernant la panne d'électricité découlant d'une cyber-attaque
2016	(sept.) Tesla Modèle S piraté dans un laboratoire chinois

... et la liste continue...

Création en 2010 du
United States
Cybercommand
(USCYBERCOM)

Le directeur de la CIA,
Leon Panetta, a lancé
cette mise en garde : « *Le
prochain Pearl Harbour
pourrait être cyber-
attaque* ».

Visez la cyber-résilience / assurances

Combien de temps, de ressources et d'argent une entreprise doit-elle consacrer au problème de la sécurité informatique?

Il n'existe pas de solution universelle et à ce titre, il revient à chaque entreprise de prendre les décisions en la matière qui lui semble les plus appropriées.

Une approche cyber-résiliente peut permettre :

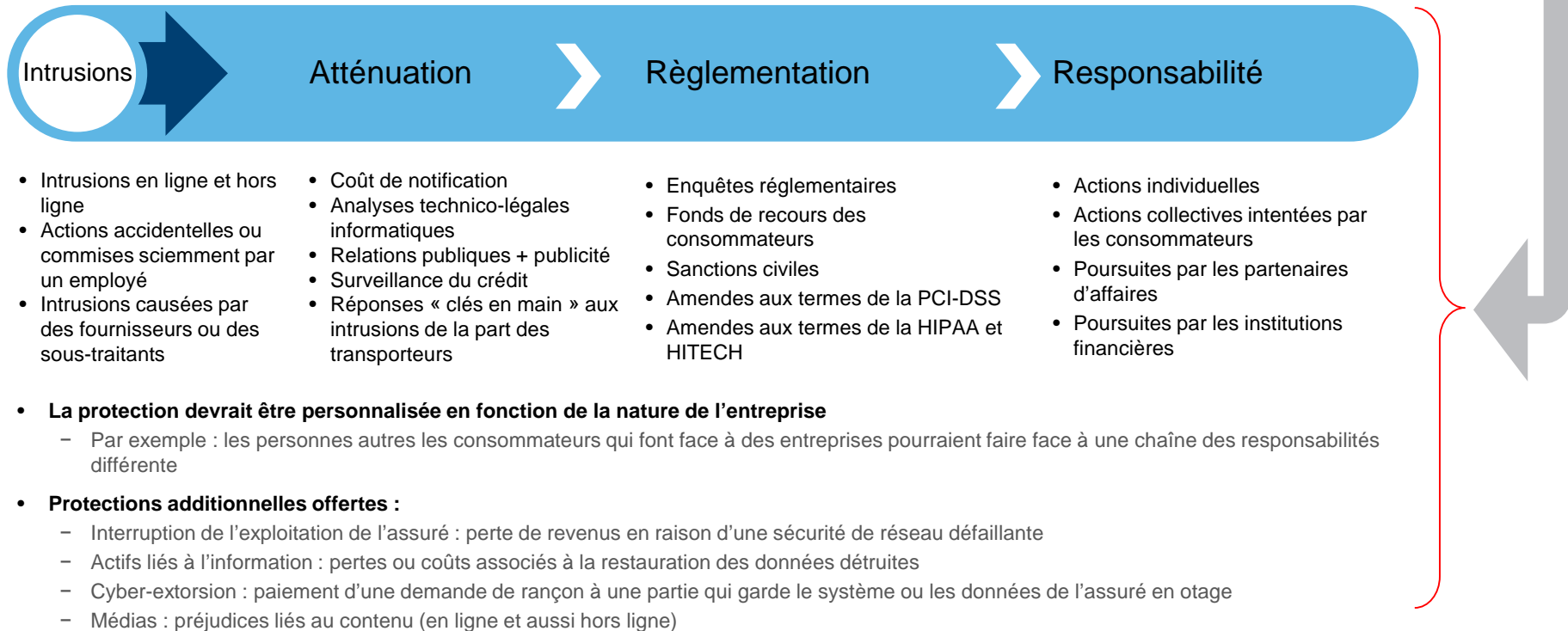
- Une réaction efficace après une intrusion ou une attaque informatique ou une autre forme d'incident
- Une défense de vérification diligente pour le conseil, le chef de la direction et le chef des finances
- La réduction de l'attention portée par les médias en cas d'intrusion et moins de répercussions politiques
- La protection globale de votre marque
- La réduction des probabilités d'amendes imposées par des organismes gouvernementaux ou de réglementation

Pour adopter une approche cyber-résiliente, vous devez :

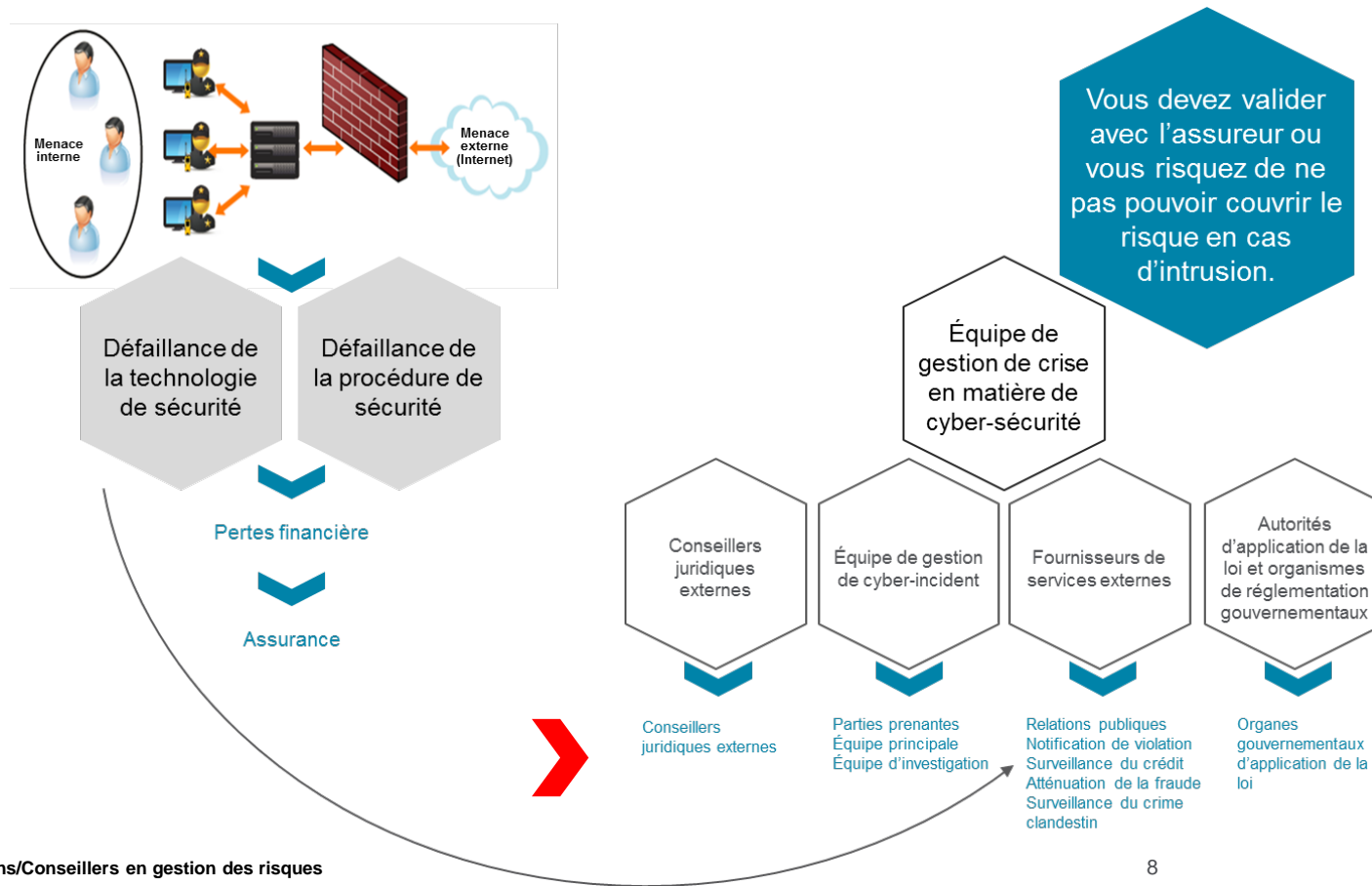
- **Identifier vos risques, menaces et actifs**
- Comparer vos pratiques en matière de sécurité aux pratiques exemplaires d'après vos risques, menaces et actifs
- **Mettre en place un plan pour atténuer ou accepter officiellement les risques**
- **Cerner ce qui peut être transféré, négocier les contrats et coordonner les plans d'intervention en cas d'attaque**

Assurance en matière de sécurité des renseignements personnels et des réseaux (cyber-assurance)

La « cyber-assurance » couvre les coûts suivants de l'assuré



Post-intrusion : fournisseurs de services et assurance



Example of project: Our objectives today

- Start a structured conversation regarding the integration of external vendors into cyber-incident response plan
- Define scope of the project and responsibilities
 - Identify team members
 - Agree on tentative timeline
 - Identifying and vetting vendors
 - ▶ validate vendors with client's objectives, procurement procedures and insurer (cyber and other)
 - Expand IRP, BCP and DRP currently in place to include external vendor information and coordination strategy
 - ▶ Create external vendor infographic / roadmap to help communicate change
 - Engage client and prospective insurers, e.g., Insurer in tabletop simulation to test strategy
- Leave meeting with understanding of next steps, deliverables, milestones and KPIs

Example: Questions for the group...

- What does an orderly cyber-incident response plan look like?
 - What are its component parts; how are roles and responsibilities allocated; how are timelines managed?
 - What is the “ideal” sequence of events?
- Who needs to be involved in its conception?
 - Internally and externally?
- Who needs to be involved in its execution?
 - Internally and externally

*Again, Consultant's
focus will be on
helping client with the
identification and
validation of external
vendors*

Example: Few organizations are well prepared for a cyber security incident in terms of:

- People (e.g., an incident response team or individual, technical experts, fast access to decision-makers, representation from key suppliers)
- Process (e.g., knowing what to do, how to do it and when to do it –when detecting, containing, eradicating or recovering from a cyber security incident)
- Technology (e.g., knowing their network topology, providing the right event logs)
- Information (e.g., having information close at hand about business operations and priorities; critical assets; and key dependencies, such as on third parties, important locations or where relevant information resides).
- Question: How does your incident response plan, business continuity plan, crisis management and crisis management communications plan support each other? Are they harmonized? Have they been tested?



Questions et réponses

The Aon logo, consisting of the word "Aon" in a bold, white, sans-serif font, centered on the page. The background of the entire slide is a long-exposure photograph of a highway at night, showing light trails from cars in yellow and red against a dark sky with a sunset or sunrise glow.

Aon Risk Solutions/Conseillers en gestion des risques