You Can’t Stop Bad – Continuing Your Operations When “Bad” Occurs

Presented to Emergency Preparedness & Business Continuity Conference
John Yamniuk, MBCP, MBCI
President DRI CANADA
Wednesday, November 1, 2017

DRI CANADA
the institute for
continuity management

Presentation Objective

- About DRI CANADA
- What are we facing?
- Case study
- Takeaways
- Q&A

About DRI CANADA

DRI CANADA

the institute for continuity management

DRI CANADA

Formed in 1996 as a member owned, Non-Profit organization, DRI CANADA operates as an affiliate of DRI International.

DRI Canada provides internationally recognized education and certification to business continuity, disaster recovery, and emergency management professionals in Canada. These professionals empower Canadian organizations, communities and businesses to be resilient and better prepared for any emergency or disaster.

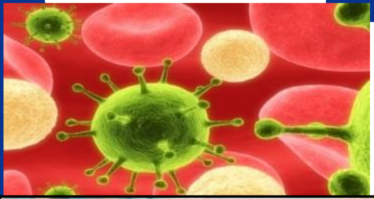
By developing a base of common knowledge for the continuity management profession and certifying qualified individuals, DRI encourages credibility and professionalism in the field.

What are we facing?

CANADA

the institute for
continuity management

What does ‘bad’ look like?



Will your organization survive – from an operational, reputational, financial perspective?

Is your organization prepared?

Things Happen!

Case Study

DRI CANADA

the institute for continuity management

Case Study

- Friday, May 27, 2016
- University of Calgary victim of kidnapping

Takeaways

DRI CANADA

the institute for
continuity management

Takeaways

- “Never let a good crisis go to waste!”
  - **Eve-Marie Cormier, National Bank; June 2017**

Takeaways

- Continually review legislation, standards, legal/regulatory requirements for your EM/CM programs. Ensure compliance with applicable legislation/regulations (includes data storage and ownership) and the program is aligned with key drivers (customer, reputation, audit, etc.).
- Continually review 'business' processes – i.e. JIT inventory
- Establish 'life cycle' approach for your programs/plans
- Continually assess new and emerging threats - i.e. cloud – legal implications re data; terrorism – vehicle rentals to launch attacks; cyber (ransomware, phishing, malware); CI threats; Internet of Things, Insider Threat; regional event implications
- Promote a culture of risk awareness

Takeaways - continued

- Review existing controls/safeguards – adjust and implement new as required
- Identify core and support processes for your organization and dependencies – internal and external – map to supply chain
- Ensure strategies driven from risk assessment and impact analysis are still valid – assess potential risk(s) of new strategies
- Strengthen supply chain
- Verify credibility of social media

Takeaways - continued

- Conduct penetration testing
- Conduct horizon scanning
- Review/adjust asset location
- Implement mitigation efforts
- Perform regular maintenance activities
- Implement enablers/policies
- Implement lessons identified (events/threats/exercises)
- Establish Mutual Aid/Assistance agreements
- Conduct awareness & training

Takeaways - continued

- Include external stakeholders in your organization’s training and awareness programs
- Integrate cyber into your BCM program (includes incident management and exercises)
- Practice, practice, practice – internally and with partners/suppliers
- Establish and maintain relationships processes with external agencies/organizations early in the process
- Continually improve your programs

Questions????

DRI CANADA

the institute for
continuity management

Thank You!

John Yamniuk, MBCP, MBCI
john@dri.ca

DRI CANADA
the institute for
continuity management