KPMG

Cyber Resilience:

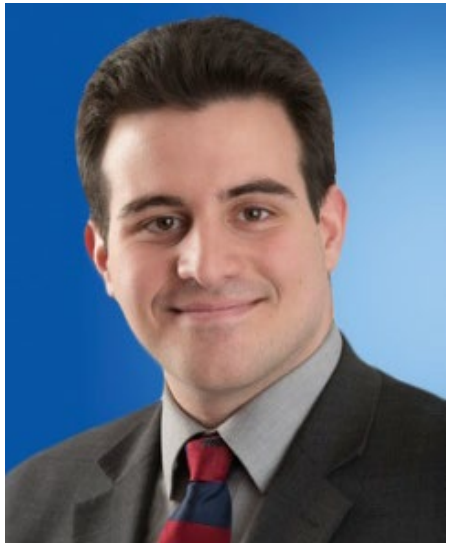
Focusing your resilience program on cyber-attacks

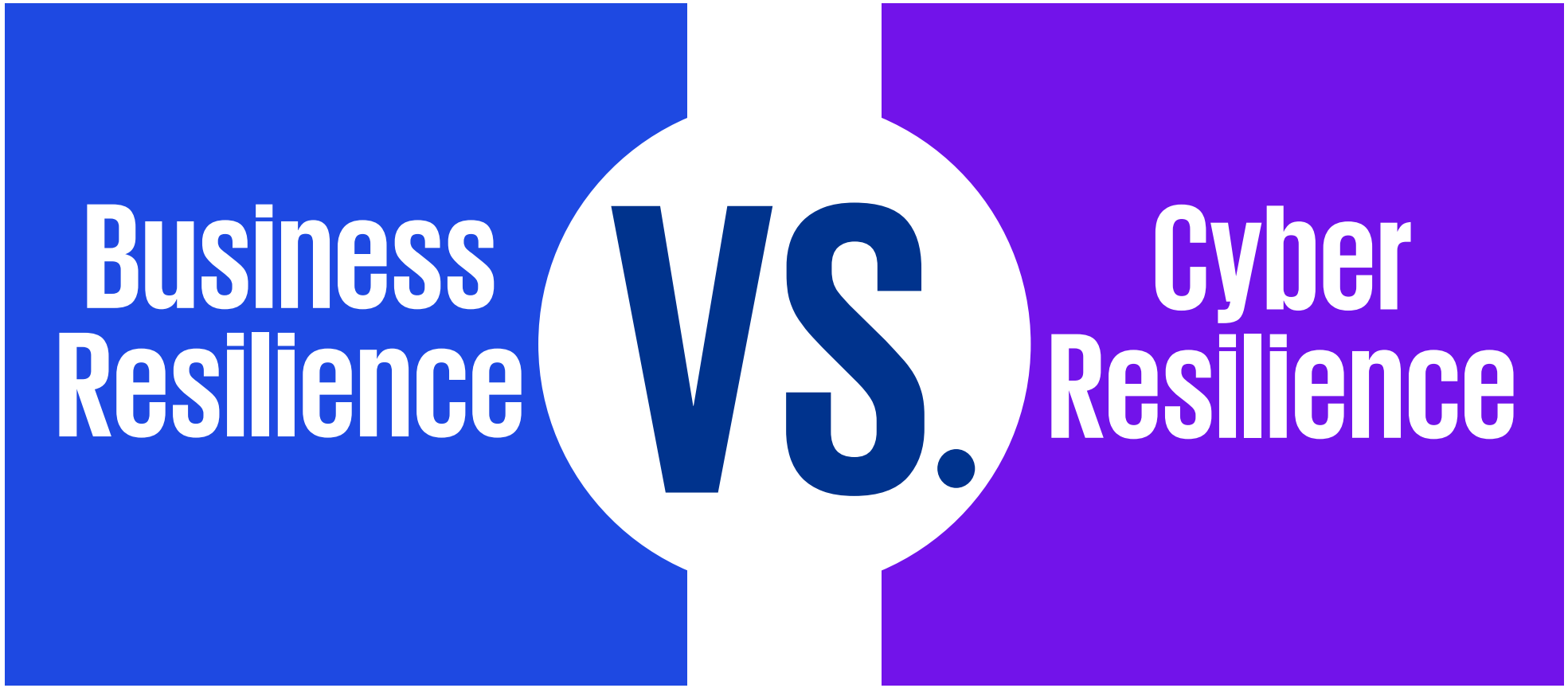
Presentation By: Tarek Habib

October 25, 2022

About the speaker

- Senior Manager in KPMG Canada's Risk Advisory practice, based in Halifax
- Focused on business resilience & cyber security
- Certified information systems auditor (CISA) from ISACA
- Certified business continuity professional (CBCP) from DRI Canada
- Certified information systems security professional (CISSP) from ISC^2
- Working with organizations of various sizes and industries to build business and cyber resilience programs, conduct business impact assessments (BIAs), conduct risk assessments, identify and implement resilience measures, design recovery strategies and test them.





Types of Disruptions

Deliberate threats

- Cyber-attack (sabotage such as ransomware)
- Labor strike/protest
- Physical vandalism / attack
- Theft of critical assets

Accidental threats

- Fire / explosion
- Equipment/hardware malfunction
- Power failure
- Chemical/hazmat spill
- Software malfunction
- Supplier failure/bankruptcy
- Industrial accidents

Natural hazards

- Epidemic/pandemic
- Snowstorm
- Earthquake
- Hurricane
- Flooding / tidal wave
- Extreme cold temperatures

Recent business resilience lessons

Business resilience domains

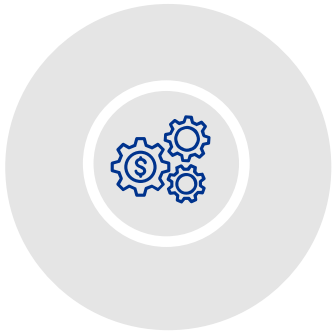
Incident & Emergency Response

Scenario example

A fire/explosion severely damages the head office campus and several employees are hurt, and the entire campus must be evacuated

Crisis Management

The organization is blamed for carelessness in the media, and needs a coordinated public relations response



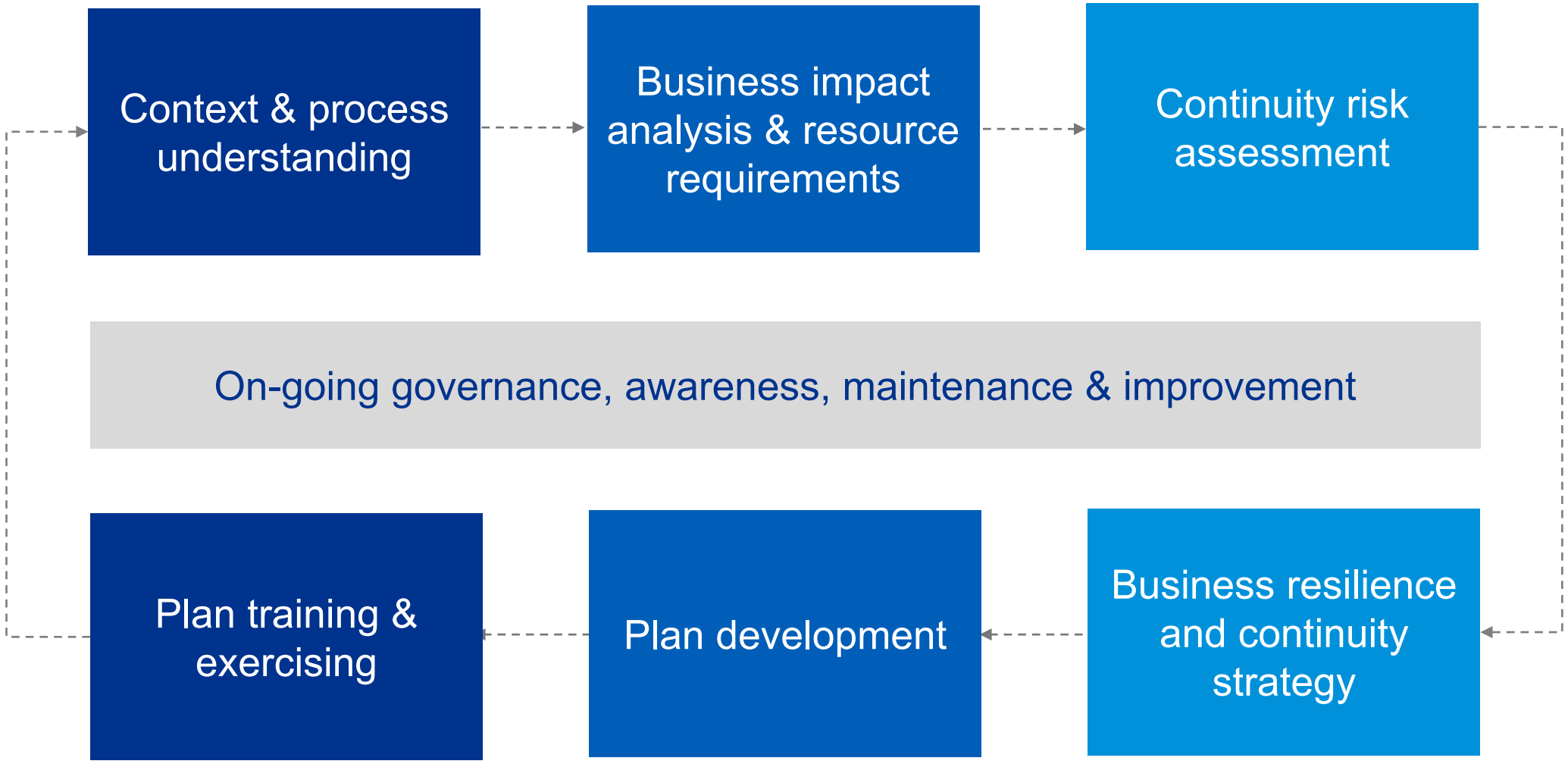
Business Continuity Planning

The organization conducted most front-office activities at the head office campus, and needs to activate its BCP to continue delivering services

Disaster Recovery Planning

The primary datacenter was also impacted in the fire/explosion, and the organization needs to activate its DRP to restore IT systems

Business resilience lifecycle



How to approach the business impact analysis (BIA)

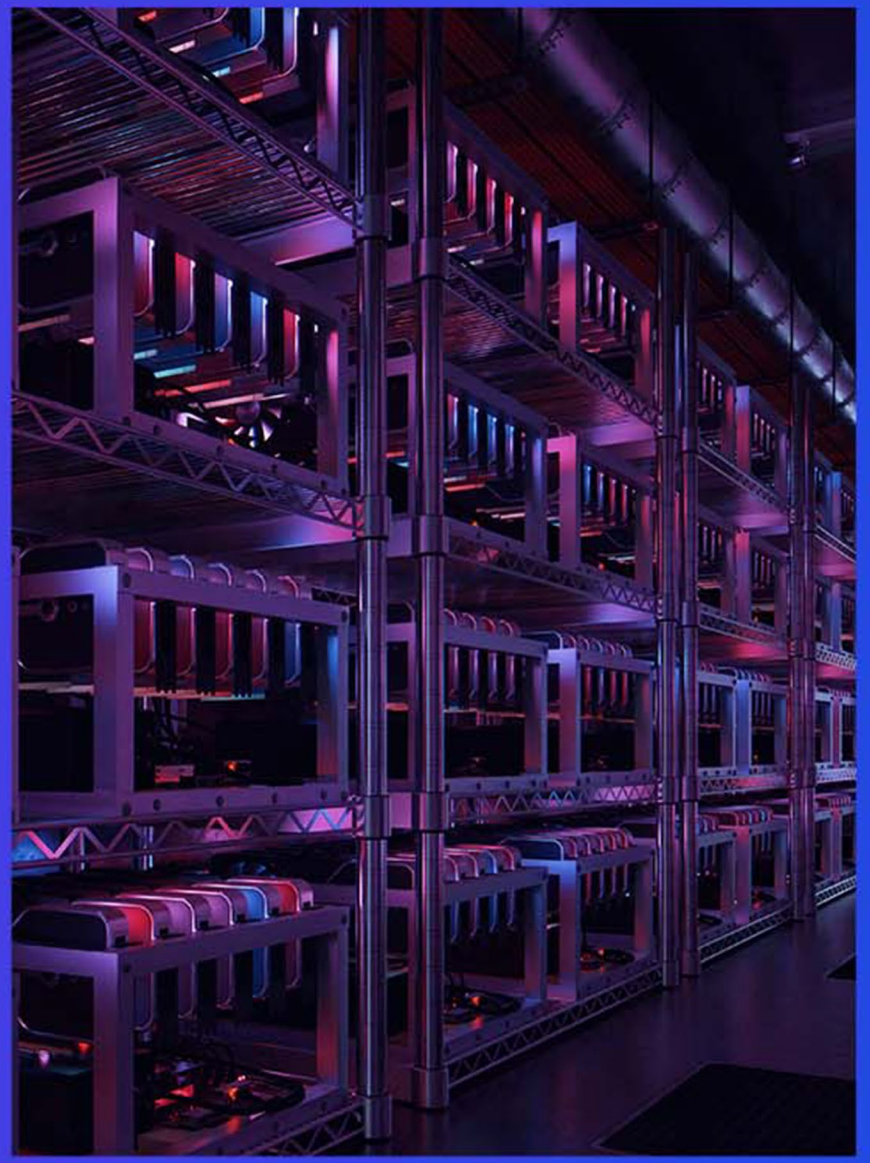
Pre-BIA (preparation)	BIA (workshops)	Post-BIA (reporting)
Step 1: divide the organization into multiple “BIAs” to streamline workshops	Step 1: assess impact-over-time of disruption on each process (should consider all-perils)	Step 1: resolve any conflicts over resource requirements or interdependent processes
Step 2: document an inventory of processes to be analyzed in each BIA	Step 2: identify minimum resource requirements for processes to operate at the minimum acceptable level (can be scenario-specific)	Step 2: summarize impact results and resource requirements in a BIA report for management review and use in next steps

Scenario Pitfall

1. **Impact should be assessed in an all-perils scenario to measure the true recovery target**

2. **Resource types can be limited based on the scenario:**

   - **Cyber Resilience**: Systems, vital records and third parties
   - **Business Resilience**: Add personnel, facilities and specialized equipment/machinery



How to assess exposure

Examples of risk factors

Internal systems	External systems	Third parties
Widespread vs. narrow use	Widespread vs. narrow use	Contractual safeguards
Current recovery capabilities	3rd party recovery commitment	Resilience track record
Manual alternatives	Cybersecurity posture	Availability of alternatives

Developing a strategy

Prevention

Reduce the impact and/or probability of the risk materializing

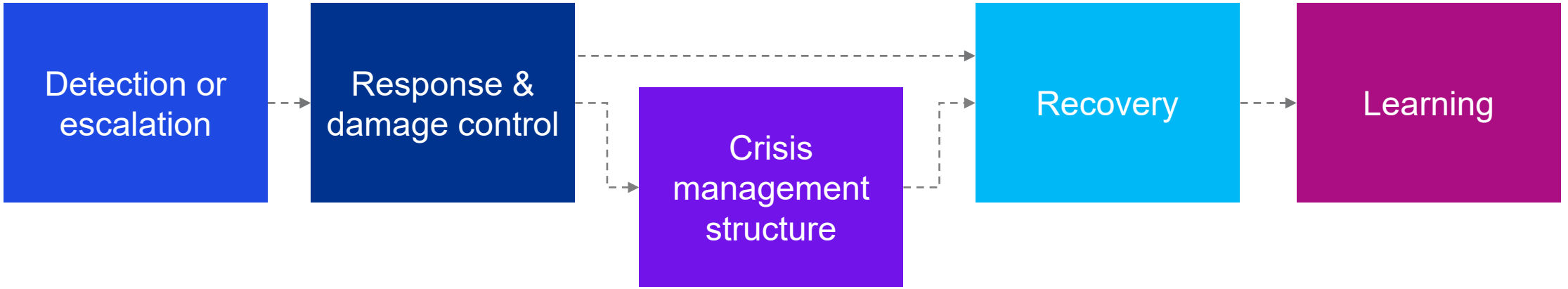
Response

Effectively respond to incidents to minimize losses and damage

Recovery

Recover critical processes within approved recovery timeframes

Response model and flow



Investing & safety nets

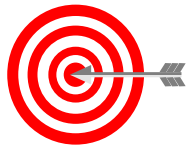
“Big red buttons”

Minimum plan contents

Integrating crisis management

Crisis management activities

- Strategic decisions for containment & remediation
- Crisis communications
- Liaising with external partners, legal counsel, law enforcement
- Customer retention and brand protection decisions



Common objective

Damage control & containment

Cybersecurity IR management activities

- Triage & investigation (post detection)
- Containment of the exposure
- Eradication of the threat
- Recovery of affected systems
- Post-incident learning

Training and exercising

Closing remarks

Keep the business involved and engaged (still not a cyber-only responsibility)

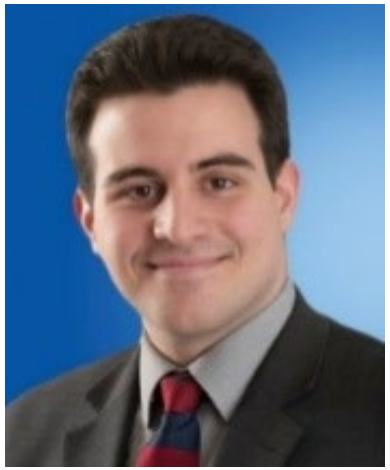
Keep it practical (survival mode)

Understand the appetite for investment

Invest across the lifecycle: prevent, respond, recover

Look outside the box: consider what would happen if a key supplier went bankrupt or experienced a major breach

Collaborate with your industry and peers



Tarek Habib, MBA, CISA, CBCP, CISSP
Senior Manager, Cybersecurity & Privacy
KPMG LLP
tarekhabib@kpmg.ca
T (902) 492-6078
M (902) 292-2091

home.kpmg/ca