IT INTELLIGENCE.
HUMAN INTELLIGENCE.

WOULD YOUR ORGANIZATION SURVIVE A MAJOR INCIDENT?

Faced with the growing complexity of digital threats, it is essential to assess your organization's ability to maintain its operations in the event of a major incident. This questionnaire aims to identify your strengths and weaknesses in terms of business continuity and cyber resilience.

What result did your organization achieve?
If several of your answers are negative, your organization may not be ready to handle a cyberattack or a major crisis. This finding should serve as a starting point for strategic reflection and corrective action.

Contact us 1-888-251-1622 • iti.ca

Learn more about our major incident simulation workshops to assess your teams' preparedness for ensuring the continuity of your operations.

Governance and strategic planning

	NO	YES
Is business resilience included as part of the organization's overall strategy?		
Are members of the leadership team (operations, human resources, finance, suppliers, legal service, etc.) involved in planning or managing business continuity?		
Are risk thresholds clearly defined and communicated to all relevant stakeholders?		
Are lessons learned from previous exercises or incidents systematically taken into account in future planning?		
Is someone specifically designated to update continuity plans (BCP, IRP, DRP)?		

Risk and Dependency Analysis

	NO	YES
Have you recently conducted a business impact analysis (BIA) to map your dependencies (personnel, technologies, suppliers) and principal risks?		
Is the business impact analysis re-evaluated on a defined schedule?		
Are the financial, reputational, and operational impacts measured for each critical process?		
Do you have a specific communication plan in case of disruption to your supply chain or critical dependencies?		

Preparation and Incident Response

	NO	YES
Are technological solutions, such as intrusion detection/prevention systems (IDS/IPS) or threat analysis and response tools (EDR/MDR), deployed to ensure the detection of security incidents?		
Have you defined and tested your RTO (Recovery Time Objective) and RPO (Recovery Point Objective) for each critical activity?		
Are incident response plans adapted to different types of threats (cyber, operational, human, natural disasters, etc.)?		
Are offsite backups and recovery tests performed and tested regularly?		
Do simulation exercises include scenarios involving employee relocation outside the office or manual work?		

Training, Awareness, and Communication

	NO	YES
Are ongoing trainings offered to strengthen vigilance and foster a culture of cybersecurity?		
Is the effectiveness of awareness campaigns measured and adjusted?		
Do new employees receive specific training on incident management and business continuity upon arrival?		
Are there initiatives that encourage a no-blame alert culture within the organization?		
Are feedback procedures (post-mortems) put in place following each exercise or incident?		
Are there established procedures for communicating with internal and external stakeholders (customers, media, regulatory bodies) in the event of a crisis?		