Cybersecurity Incident Response Planning

Checklist

This checklist can be used to support your incident response planning process. It is not exhaustive but identifies critical elements emphasizing a risk-based approach.

- ☐ We have identified all of the critical assets (data, software and systems) within the organization.
- ☐ We have mitigated vulnerabilities that expose critical assets. If not, there is a mitigation plan in place.
- ☐ We have an incident response plan (IRP).
- ☐ There is a leader assigned for cybersecurity incident response activities who is apprised of the organizational priorities and risks and has specific authorities to act in the event of an incident.
- ☐ We have access to legal advice either through in-house or external counsel or through our cyber insurance provider.
- ☐ We have retained, or have reliable access to, specialist cybersecurity services.
- ☐ We have communications protocols in place to support internal and external communications and media engagement. This includes the use of alternative communications channels if organizational systems are not available.
- ☐ External reporting requirements have been established and there is a reporting process in place (e.g., law enforcement, Cyber Security Ontario, the Privacy Commissioner, other regulatory authorities).
- ☐ We have a triage process, either internally or with a third-party service provider, which ensures that the initial impact assessment includes an appreciation of organizational risks.
- ☐ We have an escalation protocol that is based on potential organizational impacts.
- ☐ Everyone with a role in cybersecurity incident response has been informed of and is capable of fulfilling their responsibilities. This includes third-party services that may have response functions.
- ☐ We have the necessary tools, processes and procedures in place to support incident response, containment, eradication and recovery.
- ☐ We have a process for risk-based assessment prior to taking courses of action during incident response.
- ☐ We have adequate, tested and reliable back ups including a segregated, immutable back up of data, software and operating systems for all critical IT and OT.
- ☐ The IRP has been developed in concert with and is reflected in other critical plans such as business continuity, emergency management and disaster recovery plans.
- ☐ We have a mechanism within the IRP for feedback and continuous improvement.
- ☐ We review the plan and exercise the organizational incident response team at least annually.

Toronto Metropolitan University

ROGERS cybersecure catalyst

Cybersecurity Incident Response Planning

Rogers Cybersecure Catalyst

Rogers Cybersecure Catalyst is Toronto Metropolitan University's national centre for training, innovation and collaboration in cybersecurity. Headquartered in Brampton, Ontario, and offering programs and services across Canada, the Catalyst empowers individuals and organizations to seize the opportunities and tackle the challenges of cybersecurity. Together with our partners and collaborators, we work to realize a vision of healthy democracies and thriving societies, powered by secure digital technologies.

Through our groundbreaking training and certification programs; unique innovation programming for start-ups and scale-ups; first-of-its-kind cyber range; and wide-ranging public education programs, the Catalyst helps drive Canada's global competitiveness in cybersecurity.

The Catalyst's Corporate Training & Cyber Range team offers on-site and virtual training opportunities to organizations across Canada. Our range of services are:

- **Interactive experiential**
  minds-on, hands-on training that is engaging and practical.
- **Customizable**
  we tailor our offerings to your specific organizational needs and sector.
- **Inclusive**
  we offer targeted training for every level of employee - executive, technical, non-technical.

Our Training Solutions include:

- Catalyst Tabletop Exercises (TTX)
- Catalyst Cyber Range Program
- Incident Response Planning Workshop
- Cybersecurity for Elected Officials Training
- Resilience & Risk Webinars

Contact us today

Our team of cyber experts and trainers will work with you to develop a training solution that meets your needs, goals and budget.

Email: publicsectorcatalyst@torontomu.ca

Toronto Metropolitan University

ROGERS cybersecure catalyst