CYBERSECURITY CONSULTING

Incident Response: Plans, Playbooks & Tabletop Exercises

Response capability your team can execute under pressure, incident response plans, scenario playbooks, and tabletop exercises for both leadership and technical teams.

When an incident hits, hesitation is expensive. CyberX One builds and tests your incident response capability: a clear IR plan, scenario-specific playbooks for ransomware, data loss, and privacy breach, and realistic tabletop exercises. We run two tabletop tracks, a Senior Leadership Team (SLT) exercise and an IT / technical team exercise, so decision-makers and responders both practise their roles.

Objectives

- Test and refine your existing incident response plans and playbooks so they stay effective.
- Strengthen the crisis management team's decision-making, problem-solving, and critical thinking.
- Validate internal and external communication protocols for clear, timely information flow.
- Expose vulnerabilities in current systems and processes so they can be addressed.
- Raise cyber awareness and foster collaboration across departments and stakeholders.

Outcomes & benefits

- **Confident response**, teams that know the process and their roles under pressure.
- **Tested plans**, an IR plan and playbooks proven against realistic scenarios.
- **Better decisions**, familiarity with ransomware decision points and cyber-insurance concepts.
- **Clear gaps**, a documented after-action view of what to improve.
- **Stronger coordination**, leadership and technical teams working from the same playbook.

Scope of service

- Review of your current incident response plan and playbooks to identify gaps.
- Understand your environment and operations so scenarios reflect operational reality.
- Design realistic threat scenarios (e.g. ransomware, data loss, privacy breach) tailored to you.
- Facilitate the tabletop for the SLT and/or technical team, capturing decisions and gaps.
- Deliver an after-action report with prioritized improvements.

Our process

1. **Review**
   Assess the current IR plan and playbooks and set exercise objectives.
2. **Design**
   Build realistic, tailored scenarios aligned to your environment.
3. **Facilitate**
   Run the SLT and/or technical tabletop, observing decisions and comms.
4. **Debrief**
   Deliver the after-action report and a prioritized improvement roadmap.

What you receive

- Incident response plan and/or scenario playbooks
- Tabletop scenario pack (SLT and technical tracks)
- Facilitated tabletop exercise
- After-action report with prioritized improvement roadmap

Engagement at a glance

TYPICAL DURATION	LED BY	SERVICE TYPE
~3 weeks	Cybersecurity Consultant	Advisory · exercise

NIST SP 800-61 | NIST CSF | ISO 27035

Ready to start?

Email **shah@cyberxone.ca** · **LinkedIn**

CyberX One Inc. · Markham, Ontario · Serving Canada

Book a discovery call