Deloitte.

Cyber incident response

Prepare for the inevitable.
Respond to evolving threats.
Recover rapidly.

“Today, no Canadian business is immune from a potential attack. It’s no longer a question of *if* your organization will be attacked. It’s a question of *when*.“

Staying ahead of adversaries

The cyber threat landscape continues to expand rapidly. With each passing day, the cyberattacker ranks grow larger, as does their level of sophistication and the number of organizations they target.

Preparing for the inevitable cyber incident involves more than preparing to react—to merely neutralize a one-off attack. It involves the ability to respond effectively and repeatedly—to plan proactively, to defend your critical systems and data assets vigorously, to get ahead of evolving threats, and to recover thoroughly when attacks do occur.

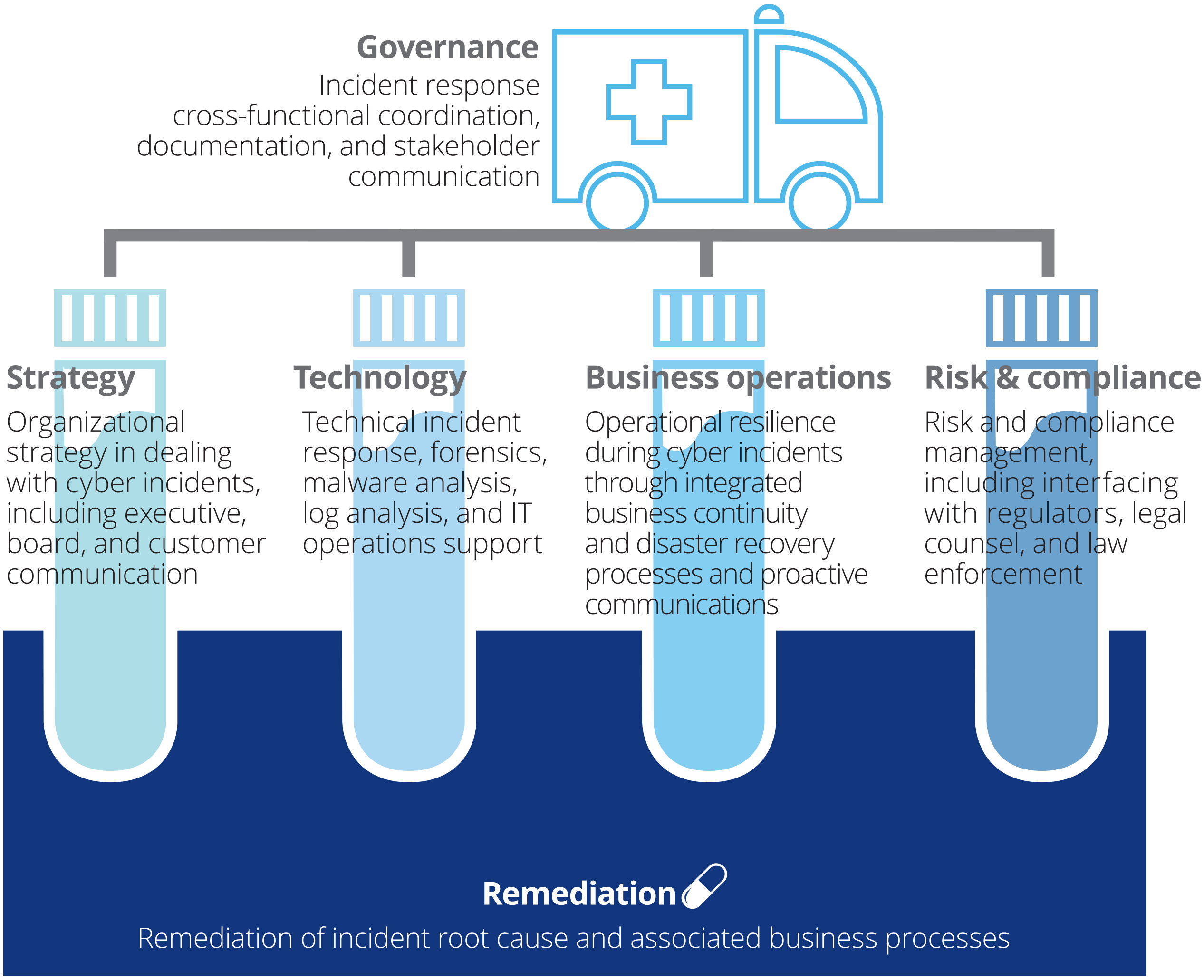
As cyberattacks increasingly take a toll on corporate bottom lines and reputations, developing a strong cyber incident response (CIR) capability becomes essential for businesses that seek to build secure, vigilant, resilient organizations. A strong CIR capability can help your organization:

- Quickly understand the nature of an attack—to help answer and address the questions of what, where, how, and how much
- Minimize the costs associated with data loss—in terms of the cost of time, resources, and diminished customer confidence
- Introduce a heightened level of management and controls that can strengthen your IT and business processes, helping your organization focus on core activities that deliver value for the enterprise

"Deloitte is the only organization in Canada that offers complete incident response services (including crisis management, privacy advisory, forensic analysis and investigations) and works closely between clients, law firms, and insurance companies throughout the incident. Our experience dealing with some of the largest breaches in the world has allowed our clients to efficiently and effectively recover from cyber incidents."

What it takes

Developing a CIR capability that can position your organization to meet evolving threats requires both an operational framework as well as an understanding of the cyber incident life cycle. Building a framework—your CIR "house"—and building knowledge of the phases of threat management gives your organization essential tools for proactively responding to cyber incidents.



Governance
Incident response cross-functional coordination, documentation, and stakeholder communication

Strategy
Organizational strategy in dealing with cyber incidents, including executive, board, and customer communication

Technology
Technical incident response, forensics, malware analysis, log analysis, and IT operations support

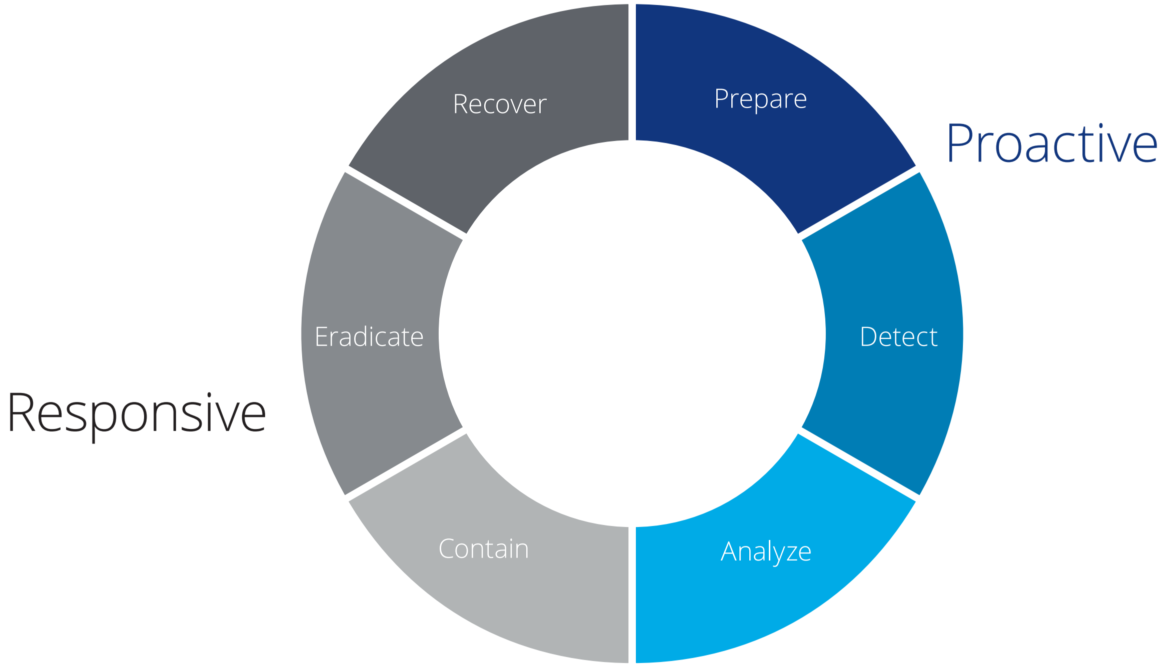
Business operations
Operational resilience during cyber incidents through integrated business continuity and disaster recovery processes and proactive communications

Risk & compliance
Risk and compliance management, including interfacing with regulators, legal counsel, and law enforcement

Remediation
Remediation of incident root cause and associated business processes

Incident response life cycle

The incident response life cycle begins before an incident even occurs. Vigilant organizations can develop a *proactive* and *responsive* set of capabilities that allow them to rapidly adapt and respond to cyber incidents—and to continue operations with limited impact to the business.



Proactive	**Prepare**	• Encompasses design and development of an incident response program covering organization, processes, and procedures • Involves design and implementation of a resilient IT infrastructure to sustain business operations • Includes proactive red team exercises to test incident response processes and procedures
	Detect	• Leverages cyber threat intelligence (CTI) capabilities and other CIR methods to develop a comprehensive cyber monitoring program and to support ongoing monitoring and detection • Includes cyber compromise assessments to detect unknown compromises or validate the health of the network environment
	Analyze	• Involves gathering information and then prioritizing individual incidents and steps for incident response • Comprises the forensic preservation and analysis of client data to determine the extent and impact of the incident
Responsive	**Contain**	• Focuses on taking risk-mitigating actions to prevent further impact and damage to the organization
	Eradicate	• Focuses on taking actions to remove the known existing threats from the network
	Recover	• Emphasizes near-term incident remediation, remediation strategy, and roadmap development • Concentrates on resuming normal business operations, as well as developing long-term risk mitigation and documenting lessons learned • Includes claims management, privileged/legal advisory work, and privacy consultation

A broad set of capabilities

When it comes to incident response services, Deloitte understands the spectrum of capabilities organizations need to provide end-to-end protection—from preparation to recovery. Maintaining a proactive stance, responding strategically to incidents, and recovering in a sustained manner can help organizations develop the *secure, vigilant, and resilient* posture they need to fight evolving cyber threats.

	Capability	Description
Proactive	• Governance and strategy • Architecture and operations • Incident detection	• Enterprise-wide incident response (IR) plan assessment, design, development, training, and implementation • Leadership guidance for understanding response impact and management • Retainer services to assist clients with IR in the event of an incident • Cyberattack simulations • Cyber threat intelligence (CTI) and CTI sharing with peers • Red teaming and compromise assessments • Privacy advisory services
Responsive	• Triage • Respond	• Leadership to drive incident response based on strategic, business, and technical needs • Technical analysis to triage incidents, determine the impact, and investigate the root cause • Support to contain the incident • Support with post-incident public relations • Risk and compliance support for managing legal, regulatory, and customer impacts • Assistance in working through business interruptions
	• Recover • Sustain	• Leadership to organize and manage recovery efforts based on strategic, business, and technical needs • Remediation, sustainment, and recovery support after an attack, whether large or small • Integrated technical and business capabilities to support post-incident management support

Bottom-line benefits

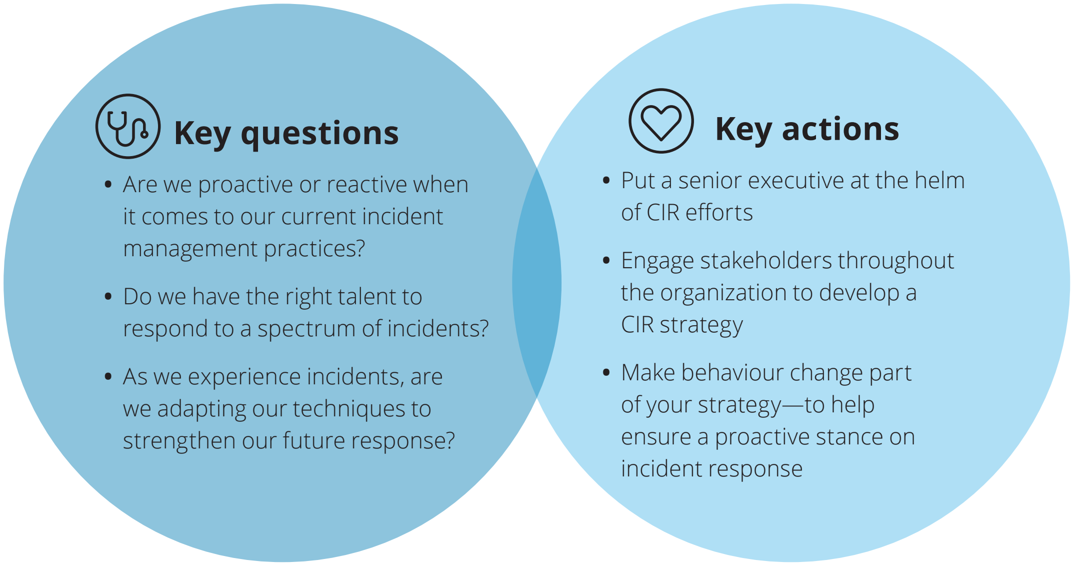
Enhancing your CIR capabilities can help your organization identify and address threats early—and rapidly remediate cyber incidents.

A stronger posture on CIR can help you:

- Maintain business continuity
- Prevent the loss of data assets that are critical to your operations
- Improve the overall security of your organization, strengthening partner and customer confidence, and solidifying reputation
- Devote more time and resources to fundamental business improvements, innovation, and growth

Questions and actions

Strengthening your CIR posture requires comprehensive guidance that's based on experience. It also requires the ability to ask the right questions and to take the right actions.



Key questions

- Are we proactive or reactive when it comes to our current incident management practices?
- Do we have the right talent to respond to a spectrum of incidents?
- As we experience incidents, are we adapting our techniques to strengthen our future response?

Key actions

- Put a senior executive at the helm of CIR efforts
- Engage stakeholders throughout the organization to develop a CIR strategy
- Make behaviour change part of your strategy—to help ensure a proactive stance on incident response

Contact us

To start the conversation on how your organization can begin developing cyber incident response capabilities that can help you stay ahead of threats, visit us online or contact us directly.

Toronto

Nathan Spitse
Partner
Cyber Risk Services
nspitse@deloitte.ca
416-874-3338

Corey Fotheringham
Partner
CyberCrime &
eDiscovery Services
cfotheringham@deloitte.ca
416-618-4253

West

Justin Fong
Partner
Cyber Risk Services
jfong@deloitte.ca
403-503-1464

East

Rob Masse
Partner
Cyber Risk Services
rmasse@deloitte.ca
514-393-7003

Cyber incident response email:
increspose@deloitte.ca

If you are currently experiencing an issue, please call: 1-800-CIC-HELP

www.deloitte.ca/cyber

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Designed and produced by the Deloitte Design Studio, Canada. 16-4161H