



## 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 cyber attacker ranks grow larger, as does their level of sophistication and the number of organizations they target.

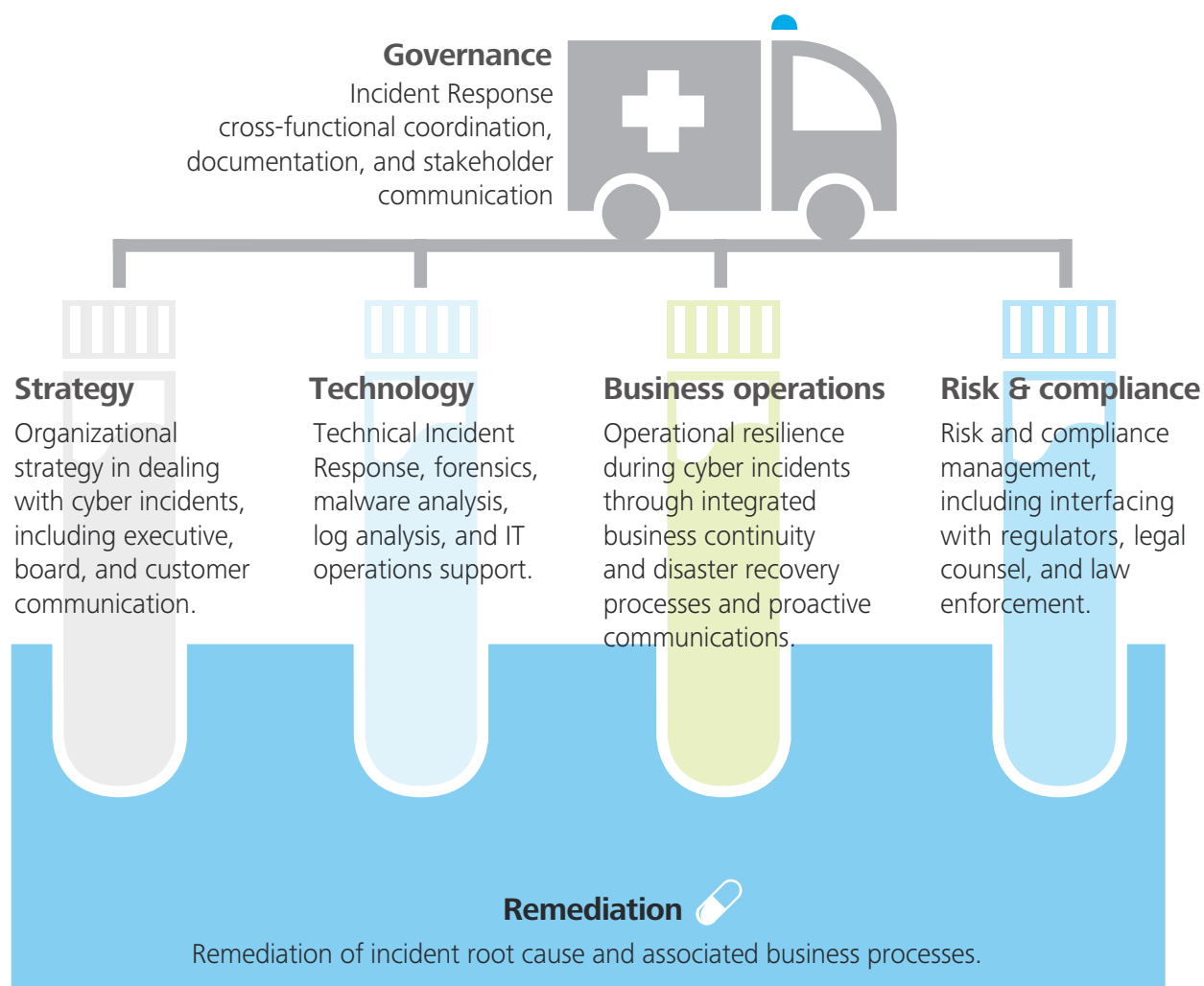
Preparing for the inevitable cyber incident involves more than preparing to react—to merely neutralize a one-off attack. It involves the ability to respond effectively and repeatedly—to plan proactively, to defend your critical systems and data assets vigorously, to get ahead of evolving threats, and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

As cyber attacks 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

# 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

- Set tone at the top
- Align strategy with organizational goals
- Provide mechanism for cross-functional communication



## Strategy

- Avoid “tunnel vision” when planning response and recovery strategies
- Reduce adverse impact to operations and revenue streams during incidents
- Align IR efforts with security management and IT engineering initiatives



## Business operations

- Protect revenue, IT, physical assets, and personal assets
- Respond to unplanned events with minimal disruption
- Plan for and recover from any disruption quickly



## Technology

- Create an architecture that can rapidly adapt to and recover from cyber incidents
- Improve situational awareness
- Confirm that applications are highly resistant to standard attack vectors



## Risk and compliance

- Demonstrate alignment with obligations
- Embrace a risk-based approach focusing on high-impact areas
- Strengthen ability to address regulator and law enforcement inquiries

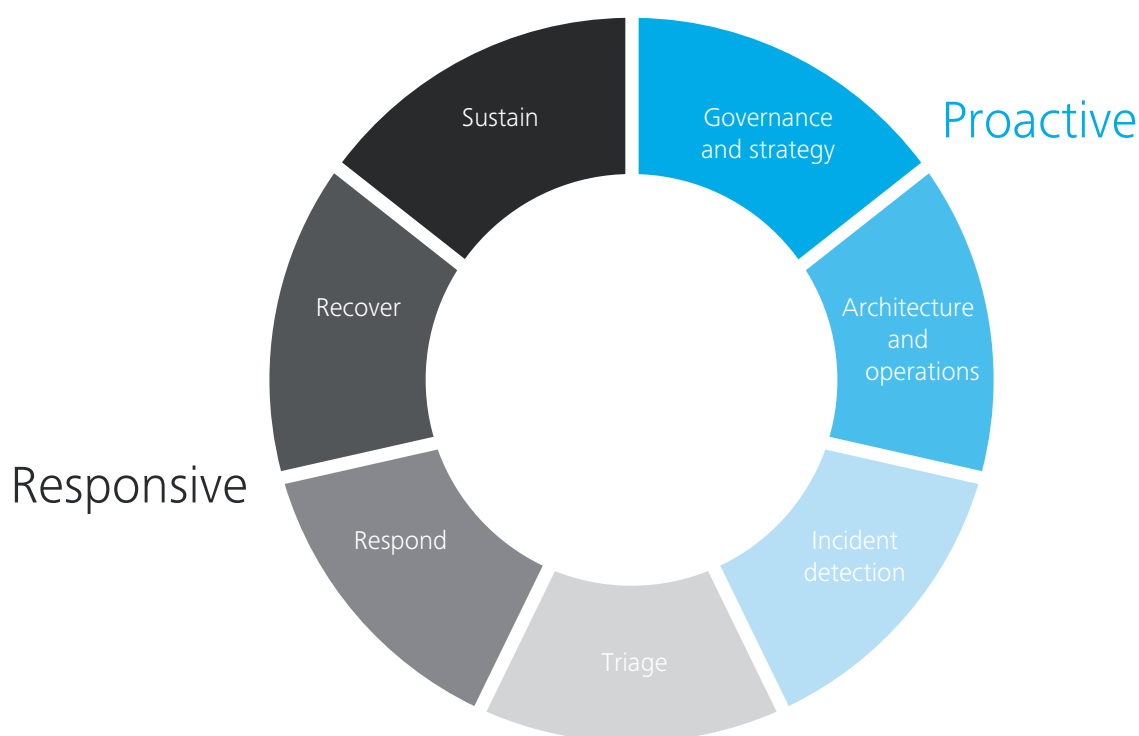


## Remediation

- Develop a remediation plan that includes short-term and long-term goals
- Close identified gaps in technical and business processes
- Monitor technology infrastructure for repeat events

# Incident response lifecycle

The incident response lifecycle 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	<b>Governance and strategy</b>	Encompasses design and development of an incident response program covering organization, processes, and procedures
	<b>Architecture and operations</b>	Involves design and implementation of a resilient IT infrastructure to sustain business operations
	<b>Incident detection</b>	Leverages cyber threat intelligence (CTI) capabilities—such as CTI sharing with industry peers—and other CIR methods to develop a comprehensive cyber monitoring program and to support ongoing monitoring and detection; efforts can integrate with Deloitte’s Fusion SIEM monitoring services
Responsive	<b>Triage</b>	Involves gathering information on multiple incidents and then prioritizing individual incidents and steps for incident response
	<b>Respond</b>	Focuses on taking risk-mitigating actions to prevent further impact to the organization
	<b>Recover</b>	Emphasizes near-term incident remediation, remediation strategy, and roadmap development
	<b>Sustain</b>	Concentrates on resuming normal business operations, as well as developing long-term risk mitigation and documenting lessons learned



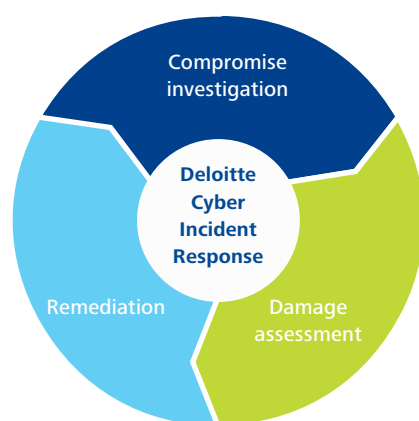
# Putting the pieces together with Deloitte

Deloitte offers organizations critical guidance for building the pieces of a strong CIR capability and for putting those pieces together. We also offer a suite of focused CIR offerings to help organizations proactively monitor and respond to threats.

Deloitte's comprehensive approach aims to deliver timely and actionable information for investigating and responding to data breaches—so you can understand attackers' motives and the data they seek and so you can make timely decisions about business and system protection.

The approach is one that leverages our deep experience across industries and our understanding of the challenges, risks, and opportunities that large, complex organizations face. And it's an approach that we customize for each client as we work to provide guidance and solutions that can work for you, your business goals, and your data needs.

Here's a look at three key areas on which we focus as we help organizations put together the pieces of a strong CIR capability.



**Compromise investigations** seek to confirm the avenues of attack involved in cyber incidents, identify related post-event network activity, and identify additional compromised endpoints and user accounts. Attempting to understand the potential breadth and scale of an incident is central to a compromise investigation.

**Damage assessments** focus on determining which data have been accessed or exposed, as well as attempting to understand a cyber adversary's motives and possible next steps. The assessments can bring to light issues that need to be addressed and can provide insights on how a loss, leakage, or exfiltration of data might affect your business.

**Remediation activities** help you get your systems back to normal as quickly as possible, while fortifying your organization against your attacker. Deloitte examines various incident indicators, known vulnerabilities, and software patch statuses to develop short-range, mid-range, and long-range remediation efforts that can further bolster your organization's security posture.

# 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
<div>Proactive</div> <div><ul style="list-style-type: none"><li>• Governance and strategy</li><li>• Architecture &amp; operations</li><li>• Incident detection</li></ul></div>	<ul style="list-style-type: none"><li>• Enterprise-wide IR plan assessment, design, development, training, and implementation</li><li>• Leadership guidance for understanding response impact and management</li><li>• Retainer services to assist clients with IR in the event of an incident</li><li>• Cyber attack simulations</li><li>• Cyber threat intelligence (CTI) and CTI sharing with peers</li></ul>
<div>Responsive</div> <div><ul style="list-style-type: none"><li>• Triage</li><li>• Respond</li></ul></div>	<ul style="list-style-type: none"><li>• Leadership to drive incident response based on strategic, business, and technical needs</li><li>• Technical analysis to triage incidents, determine the impact, and investigate the root cause</li><li>• Support to contain the incident</li><li>• Support with post-incident public relations</li><li>• Risk and compliance support for managing legal, regulatory, and customer impacts</li><li>• Assistance in working through business interruptions</li></ul>
<div><ul style="list-style-type: none"><li>• Recover</li><li>• Sustain</li></ul></div>	<ul style="list-style-type: none"><li>• Leadership to organize and manage recovery efforts based on strategic, business, and technical needs</li><li>• Remediation, sustainment, and recovery support after an attack, whether large or small</li><li>• Integrated technical and business capabilities to support post-incident management support</li></ul>



# The Deloitte difference

Deloitte delivers a powerful blend of technical skills, business experience, and industry insights when helping clients put in place effective CIR capabilities.



**Our solutions are comprehensive.** Deloitte's end-to-end CIR services help our clients prepare for, respond to, and recover from incidents across the entire incident life cycle.



**Our CIR experience is deep.** We annually perform more than 1,000 cyber risk assessments throughout North America, and our acquisition of Vigilant Inc. has bolstered our security monitoring and cyber threat intelligence capabilities.



**Our reach is broad.** With professionals working at Deloitte member firms across the globe, we're prepared to address cyber challenges wherever they might occur within your organization.



**Our resources are on target.** To address cyber incidents, Deloitte brings to bear experienced professionals using field-tested tools, leveraging a network of cybersecurity intelligence centres that allow us to respond to incidents immediately in almost any setting.



**Our live support capabilities are unsurpassed.** Deloitte's Cyber Intelligence Centre (CIC) serves as a national resource for businesses throughout Canada, providing a range of customized, integrated security services that deliver round-the-clock business-focused security for critical systems and data.

Package	Features
Bronze	<ul style="list-style-type: none"><li>• Master services agreement</li><li>• No service level agreement</li></ul>
Silver	<ul style="list-style-type: none"><li>• Master services agreement</li><li>• Service level agreement – with response time as follow:<ul style="list-style-type: none"><li>• Remote – 12 hours</li><li>• On site – 36 hours</li></ul></li><li>• Monthly Cyber Threat Intelligence summary</li></ul>
Gold	<ul style="list-style-type: none"><li>• Master services agreement</li><li>• Service level agreement – with response time as follow:<ul style="list-style-type: none"><li>• Remote – 12 hours</li><li>• On site – 24 hours</li></ul></li><li>• Monthly Cyber Threat Intelligence summary</li><li>• Cyber threat assessment</li></ul>

# Cyber Intelligence Centre (CIC)

Cyber threats are evolving in volume, sophistication and impact, making it harder for internal security teams to detect and address advanced threats around the clock.

Deloitte's Cyber Intelligence Centre (CIC) can help you manage cyber risks with a range of customized, integrated security services that deliver 24x7, business-focused security for your critical systems and data.

- Security Information and Event Management (SIEM)
- Advanced threat detection
- Intrusion prevention and detection
- Firewall management
- End point protection
- Data leakage protection
- Web proxy and URL filtering
- Brand monitoring
- Vulnerability management
- Breach detection, incident response and management

Whether you're looking for a fully managed cybersecurity solution or a way to replace or augment your existing solution, the Cyber Intelligence Centre can help your organization become more secure, more vigilant, and more resilient.

## Secure

By adopting a risk-based approach to cyber crime prevention, you can gain access to timely, actionable threat intelligence, positioning you to improve the effectiveness of your security controls.

## Vigilant

With a customized approach to cyber intelligence that takes your specific environment into account, you can more readily predict and prevent security incidents, strengthen your organization's threat profile, and reduce your vulnerability to criminal attack.

## Resilient

Some cyber incidents can cause serious business crises. Enhancing your ability to detect and respond to threats helps you minimize losses and get back to "business as usual" faster.

# Bottom-line benefits

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

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 behavior 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

**Rocco Galletto**  
Partner  
Cyber Risk Services  
[rgalletto@deloitte.ca](mailto:rgalletto@deloitte.ca)

**Adam Crawford**  
Senior Manager  
Cyber Risk Services  
[adcrawford@deloitte.ca](mailto:adcrawford@deloitte.ca)

**Nathan Spitse**  
Senior Manager  
Cyber Risk Services  
[nspitse@deloitte.ca](mailto:nspitse@deloitte.ca)

## West

**Tejinder Basi**  
Partner  
Cyber Risk Services  
[tbasi@deloitte.ca](mailto:tbasi@deloitte.ca)

**Justin Fong**  
Partner  
Cyber Risk Services  
[jfong@deloitte.ca](mailto:jfong@deloitte.ca)

**Albert Yap**  
Partner  
Cyber Risk Services  
[ayap@deloitte.ca](mailto:ayap@deloitte.ca)

## East

**Rob Masse**  
Partner  
Cyber Risk Services  
[rmasse@deloitte.ca](mailto:rmasse@deloitte.ca)

**Francis Castonguay**  
Senior Manager  
Cyber Risk Services  
[frcastonguay@deloitte.ca](mailto:frcastonguay@deloitte.ca)

Cyber incident response email:  
[incresponse@deloitte.ca](mailto:incresponse@deloitte.ca)





[illegible]



**[www.deloitte.ca](http://www.deloitte.ca)**

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](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

© Deloitte LLP and affiliated entities.

Designed and produced by the Deloitte Design Studio, Canada. 15-3207M