Cyber Incident Response
Prepare for the inevitable. Respond to evolving threats. Recover rapidly.
Today, no South African business is immune from a potential attack. It’s no longer a question of *if* your business 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 businesses they target.

Preparing for the inevitable cyber incident involves more than preparing to react or merely neutralising a once-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 business that seek to build secure, vigilant and resilient. A strong CIR capability can help your business:

- Quickly understand the nature of an attack to help answer and address the questions of what, where, how and how much
- Minimise 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 business focus on core activities that deliver value for the enterprise

[0x0]
What it takes

Developing a CIR capability that can position your business 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 business essential tools to proactively respond to cyber incidents.

**Governance**
Incident Response cross-functional coordination, documentation and stakeholder communication.

**Strategy**
Business 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.
Cyber Incident Response | What it takes

Governance
- Set tone at the top
- Align strategy with business 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 CIR efforts with security management and IT engineering initiatives

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

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

Risk & 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
The incident response lifecycle begins before an incident even occurs. Vigilant businesses 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.

### Incident response lifecycle

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive</td>
<td>Governance and strategy: Encompasses design and development of an incident response program covering business, processes and procedures.</td>
</tr>
<tr>
<td></td>
<td>Incident detection: Leverages Cyber Threat Intelligence (CTI) capabilities such as, CTI sharing with industry peers, other CIR methods in order to develop a comprehensive cyber monitoring program and to support ongoing monitoring and detection. Efforts can integrate with Cyber Intelligence Centre (CIC)</td>
</tr>
<tr>
<td>Responsive</td>
<td>Triage: Involves gathering information on multiple incidents and then prioritising individual incidents and steps for incident response.</td>
</tr>
<tr>
<td></td>
<td>Recover: Emphasises near-term incident remediation, remediation strategy and roadmap development.</td>
</tr>
</tbody>
</table>
Putting the pieces together with Deloitte

Deloitte offers businesses 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 businesses 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 the attackers’ motives, 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 businesses face. The approach is customised for each client as we 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 businesses 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 what data has been accessed or exposed, as well as attempting to understand a cyber adversary’s motives and possible next steps. The assessments 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 business 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 business’s security posture.
## A broad set of capabilities

When it comes to incident response services, Deloitte understands the spectrum of capabilities businesses 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 businesses develop the secure, vigilant and resilient posture they need to fight evolving cyber threats.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
</table>
| Proactive  | • Governance and strategy  
             • Architecture & operations  
             • Incident detection  
             • Enterprise-wide CIR plan assessment, design, development, training and implementation  
             • Leadership guidance for understanding response impact and management  
             • Retainer services to assist clients with CIR in the event of an incident  
             • Cyber-attack simulations  
             • CTI and CTI sharing with peers |
| 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 organise 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 |
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 perform more than 1,000 cyber risk assessments annually globally.

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

**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 Africa, providing a range of customised, integrated security services that deliver round-the-clock business-focused security for critical systems and data.

<table>
<thead>
<tr>
<th>Features</th>
<th>Gold</th>
<th>Silver</th>
<th>Bronze</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-negotiated terms and conditions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Access to 24/7 hotline</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Discounted rate per hour</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cyber Incident Response Plan*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cyber Incident Crisis Simulation*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cyber Maturity Assessment (current state)*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cyber Awareness*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
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 customised and integrated security services that deliver 24/7, 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 CIC can help your business become more secure, more vigilant and more resilient.

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

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

Some cyber incidents can cause serious business crises. Enhancing your ability to detect and respond to threats helps you minimise losses and get back to “business as usual” faster.
Bottom-line benefits

Enhancing your CIR capabilities can help your business 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 business, strengthen partner and customer confidence and solidify 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 and 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 business to develop a CIR strategy.
- Make behaviour change part of your strategy to ensure a proactive stance on incident response.
Contact us

Southern Africa

Navin Sing  
Managing Director: Risk Advisory Africa  
Mobile: +27 83 304 4225  
Email: navising@deloitte.co.za

Derek Schraader  
Risk Advisory Africa Leader: Cyber Risk Services  
Mobile: +27 79 499 9046  
Email: dschraader@deloitte.co.za

Cathy Gibson  
Director: Risk Advisory Southern Africa  
Mobile: +27 82 330 7711  
Email: cgibson@deloitte.co.za

Yolande Kruger  
Associate Director: Risk Advisory Southern Africa  
Mobile: +27 83 265 3522  
Email: ykruger@deloitte.co.za

Central Africa

Tricha Simon  
Risk Advisory Regional Leader: Central Africa  
Mobile: +263 772 234 932  
Email: tricsimon@deloitte.com

Rodney Dean  
Director: Risk Advisory Central Africa  
Mobile: +263 867 700 0261  
Email: rdean@deloitte.co.zw

West Africa

Anthony Olukoju  
Risk Advisory Regional Leader: West Africa  
Mobile: +234 805 209 0501  
Email: aolukoju@deloitte.com.ng

Temitope Aladenusi  
Director: Risk Advisory West Africa  
Mobile: +234 805 901 6630  
Email: taladenusi@deloitte.com.ng

East Africa

Julie Nyangaya  
Risk Advisory Regional Leader: East Africa  
Mobile: +254 720 111 888  
Email: jnyangaya@deloitte.co.ke

William Oelofse  
Director: Risk Advisory East Africa  
Mobile: +254 20 423 0000  
Email: woelofse@deloitte.com