



## **Cyber Risk Services**

Cyber Incident Response  
Capabilities – Caribbean &  
Bermuda Countries

# Why Deloitte?

With a global network of over 11,000 cyber security and forensics professionals, we have the capacity to offer a full range of best-in-class services to address the various aspects of a cyber threat, while assisting your organization through proactive education on current threats, process improvements, and risk mitigation.

## Comprehensive Suite of Cyber Incident Response Services

We provide end-to-end cyber incident response services that help our clients prepare for, respond to, and recover from cyber incidents across the entire incident lifecycle.



### Global Reach

Leveraging our member firm network, we can provide seamless support across the globe to many major markets.

### Deep Cyber Security Experience

Having performed many cyber risk and incident response projects in the Caribbean, we bring deep industry and technical expertise to organizations. Deloitte's global acquisitions such as of Vigilant, Inc., have further strengthened our threat intelligence and monitoring capabilities.

### Resources, Tools, & Facilities

We have a dedicated team of practitioners with extensive background in incident response and forensics, coupled with state of the art tools and facilities that allows for an immediate response in almost any setting.

## Caribbean Reach

In the Caribbean, we have the ability to use local management teams with highly specialized cyber incident team resources and access to a state of the art Forensics lab, to deliver high-quality services around the region.

### Atlantic Ocean

**Grand Bahama**  
Freeport

**Bahamas**  
Nassau

**Bermuda**  
Hamilton

**British and US  
Virgin Islands**  
Road Town

**Cayman Islands**  
George Town

**Jamaica**  
Kingston




### Caribbean Sea

**Barbados**  
St. Michael

**Trinidad &  
Tobago**  
Port of Spain

# Our Broad Incident Response Services

Leveraging our cyber incident response framework, we can deliver a broad end-to-end experience. The following capabilities will enable you in becoming resilient and will facilitate a comprehensive response when dealing with cyber incidents:

Capability	Description
 <p><b>Prepare</b></p>	<ul style="list-style-type: none"> <li>• Incident Response plan assessment across people, process, and technology</li> <li>• Enterprise-wide Incident Response plan design, development, training, and implementation</li> <li>• Leadership to executives to drive an understanding of impact and management of response</li> <li>• Retainer services to assist clients in their response in the event of an incident</li> <li>• Cyber simulation exercise that immerses clients in a simulated cyber attack scenario, to help evaluate the effectiveness of the Incident Response plan</li> </ul>
 <p><b>Respond</b></p>	<ul style="list-style-type: none"> <li>• Leadership to drive response based on the strategic, business, compliance and technical impacts</li> <li>• Technical analysis to triage incidents, determine operational and business impact and perform root cause analysis to determine cause of incident</li> <li>• Support in containing the incident</li> <li>• Provide public relations and legal advice as needed via partnerships with leading third parties</li> <li>• Provide risk and compliance support to help you better understand legal, regulatory, and customer impact</li> <li>• Provide assistance in working through business interruptions</li> </ul>
 <p><b>Recover</b></p>	<ul style="list-style-type: none"> <li>• Leadership to organize and manage recovery based on the strategic, business, compliance and technical impacts</li> <li>• Lead or support in remediation, sustainment, and recovery from an incident, whether a small isolated incident, or a large scale attack that prevents you from conducting business</li> <li>• Provide integrated technical and business capabilities to support post incident management</li> </ul>

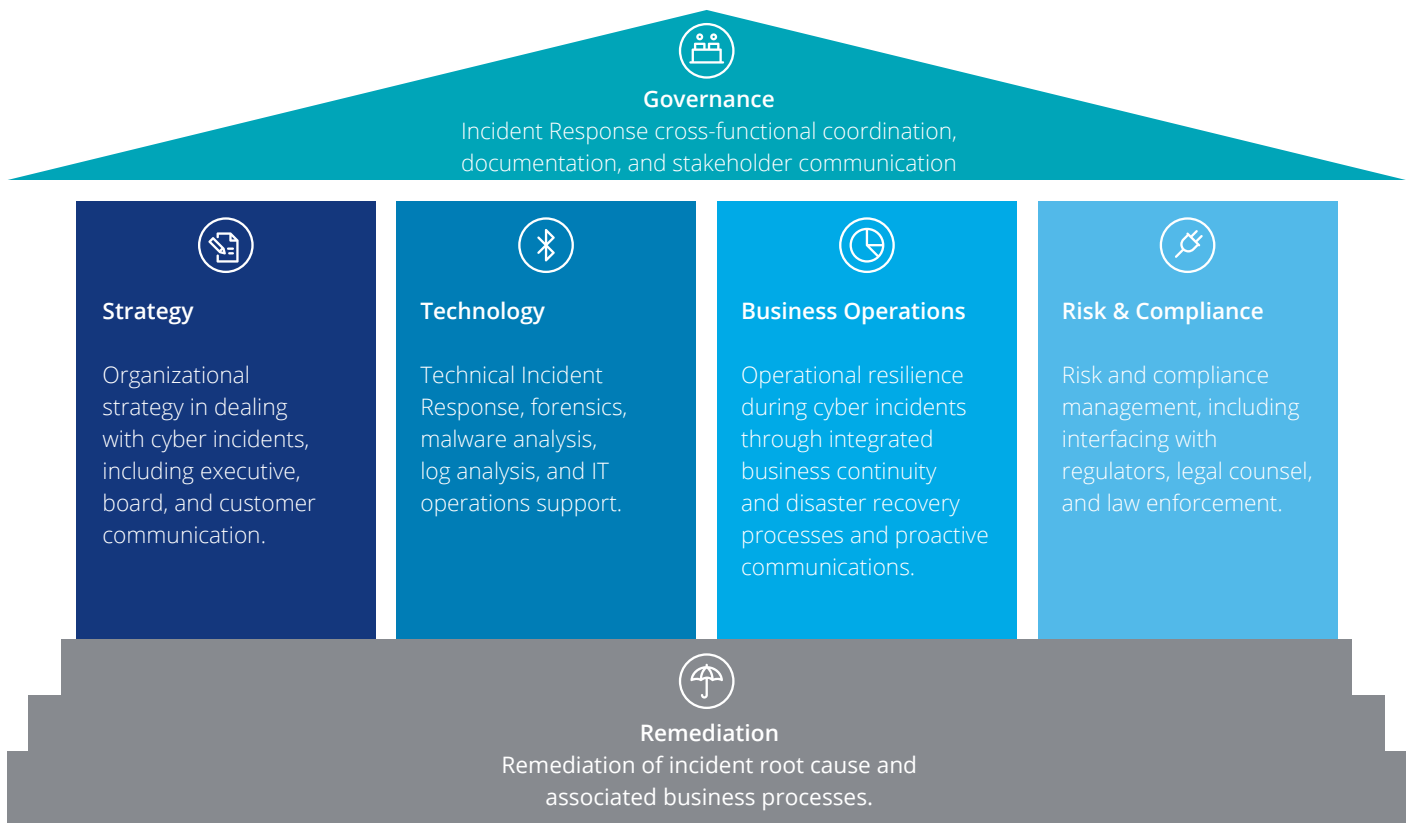
**We can be the one phone call you make to assist you in navigating a cyber incident.**

## Deep Cyber Security Experience

<p><b>Market leaders with a broad cross-section of complex, risk-sensitive organizations</b></p> <ul style="list-style-type: none"> <li>• The only organization with the breadth, depth and insight to help complex organizations become <b>Secure, Vigilant, and Resilient.</b></li> <li>• 11,000 risk management and security professionals globally through the Deloitte Touche Tohmatsu Limited network of member firms.</li> <li>• We have strengthened our cyber threat detection offerings via acquisition of Vigilant, Inc.</li> <li>• Extensive experience working with all facets of data breaches and cyber incidents, including the navigation of multi-faceted decision points that arise when dealing with law enforcement, technology issues, and beyond to the broader business.</li> </ul>		<ul style="list-style-type: none"> <li>• Named a leader in Global Risk Management Consulting Services, based on completeness of vision and ability to execute by Gartner. - <b>"Magic Quadrant for Risk Management Consulting Services, Worldwide"</b> report, 2015</li> <li>• Ranked #1 globally in Security Consulting Services, based on 215 Revenue by Gartner. - <b>"Market Share: Security Consulting Services, Worldwide, 2015"</b> report.</li> <li>• Named the global leader in Analytics IT Consulting based on capabilities by ALM Intelligence (Kennedy Information, LLC). - <b>"IT Consulting: Analytics 2014"</b> report.</li> </ul>
<p><b>Experience helping our CBC clients stay ahead of the curve</b></p> <ul style="list-style-type: none"> <li>• Provided incident response and investigation services of a potential breach to a government entity along with additional internal and external security assessments resulting in a comprehensive security posture report and recommendations.</li> <li>• Assisted a financial institution to evaluate and enhance their cyber threat management program.</li> <li>• Performed numerous security assessments.</li> <li>• Consult clients on cyber issues on an ongoing basis.</li> </ul>	<p><b>Deloitte is contributing to the betterment of cyber risk management practices</b></p> <ul style="list-style-type: none"> <li>• Selected by National Institute of Standards and Technology to assist in developing their cyber security framework in response to the 2013 Executive Order for Improving Critical Infrastructure Cybersecurity.</li> <li>• Selected as third party observer of the Quantum Dawn 2 Cyber Attack Simulation, conducted by the Securities Industry and Financial Markets Association in July 2013.</li> <li>• Worked with leading Government agencies on advanced threat solutions.</li> </ul>	

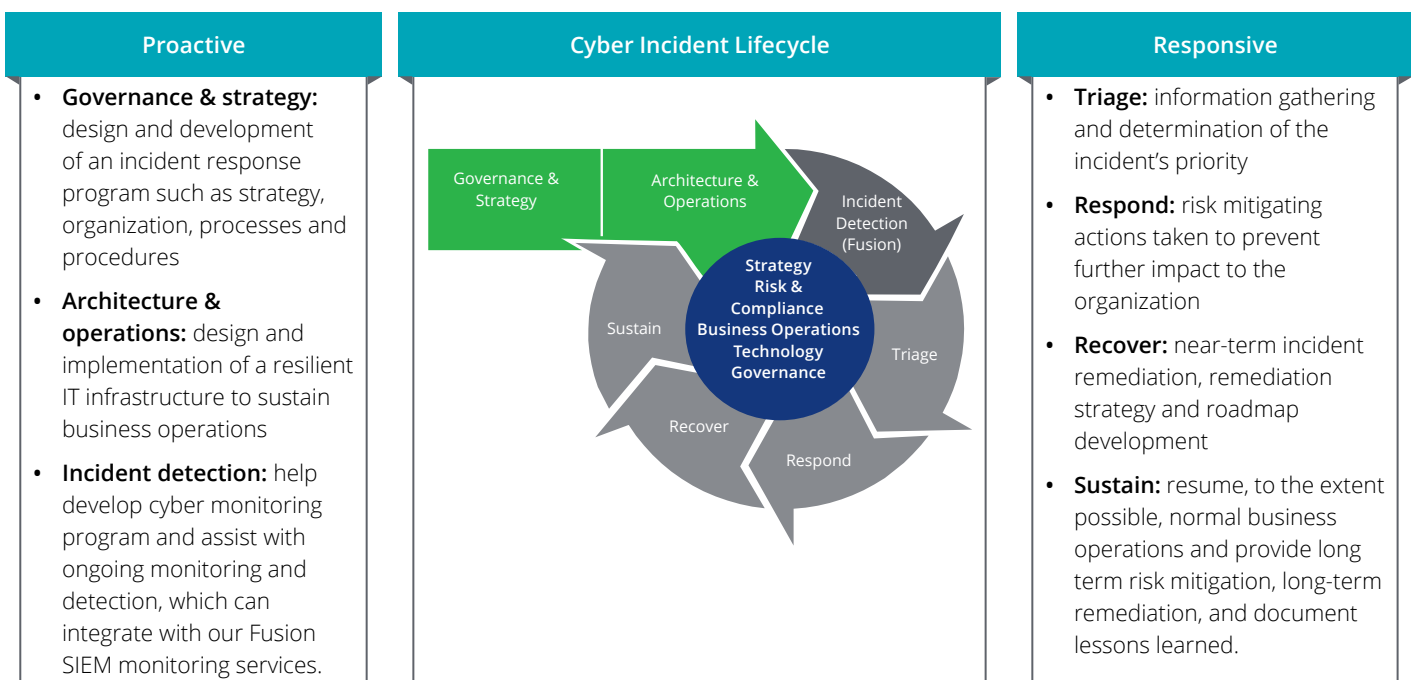
# Cyber Incident Response Framework

Organizations should embrace a broad Incident Response approach across disciplines, stakeholders and environments.



## Cyber Incident Response Lifecycle

The incident response lifecycle begins before an incident occurs. A set of **proactive** and **responsive** capabilities are required for an organization's operations to **rapidly adapt and respond** to cyber incidents and **continue operations** with **limited impact** to the business.



**Our broad cyber incident response framework, methodology and services help organizations to proactively prepare for a cyber incident and, as needed, enable the ability to quickly respond to and recover from an incident.**

## Resources

Our Caribbean and Bermuda Countries practice is supported by the Global Deloitte Network, allowing us to provide immediate responses in almost any setting.

Capability	Description
<b>People (Global)</b>	Through the Deloitte Touche Tohmatsu Limited network of member firms, we have: <ul style="list-style-type: none"><li>• 11,000 risk management and security professionals</li><li>• Over 400 incident response and computer forensics specialists</li></ul>
<b>People (CBC)</b>	<ul style="list-style-type: none"><li>• 50+ risk management and security professionals</li><li>• Over 5 incident response and computer forensics specialists</li></ul>
<b>Certifications</b>	<ul style="list-style-type: none"><li>• CISSP: Certified Information Systems Security Professional</li><li>• CEH: Certified Ethical Hacker</li><li>• EnCE: EnCase Certified Examiner</li><li>• CFE: Certified Fraud Examiner</li><li>• ACE: AccessData Certified Examiner</li><li>• Cellebrite Certified Examiner</li></ul>

## Facilities

### Deloitte data forensics and electronic discovery laboratories

Our Computer Forensics Lab, located in the Cayman Islands, is built on American Society of Crime Laboratory Directors (ASCLD) legacy standards and we are constantly seeking improvement in implementing new technology to meet our clients' needs. We maintain two regional Computer Forensics Labs around the Caribbean that allow for analysts to remotely work in our Discovery Data Centre in Grand Cayman, Cayman Islands, virtually. The environment is composed of:

- Storage capacity of approximately 50 terabytes and expanding
- 20 Servers
- Designed as a highly scalable and highly available processing architecture
- Hosted VMware Forensics Workstation environment for Discovery and Computer Forensics
- State-of-the-art fully redundant storage architecture
- Systems that can be securely accessed and operated by Deloitte personnel from another city or country
- Owned and operated by Deloitte

## Key Contacts

### Taron Jackman

Cyber Risk Leader  
+1 345 814 2212  
tjackman@deloitte.com

### Nick Kedney

Partner, Deloitte Forensic  
+1 345 743 6287  
nkedney@deloitte.com

### Alexandra Simonova

Senior Manager, Risk Advisory  
+1 345 743 6333  
asimonova@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

Deloitte & Touche is an affiliate of DCB Holding Ltd., a member firm of Deloitte Touche Tohmatsu Limited.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.