Deloitte.

Cyber Incident Response

Fast, thorough and decisive

Overview

The increase of cybercrime and data breaches continue to pose major problems for organizations in today's digital world. While adversaries can create service disruptions through cyber attacks, the most advanced methods of penetrations and breaches are specifically designed to remain undetected on your network as they collect and capture valuable data.

With cyber attacks becoming more commonplace throughout the world, responding to a data breach is not just about quickly securing your data. In addition to neutralizing threats as soon as they occur, an effective cyber incident response plan can help you understand the nature of an attack, help you reduce the cost of data loss, and introduce management rigor and controls that benefit enterprise value.

Our Solution

Deloitte helps organizations with cyber incident response in their information environments to protect their important data as well as their reputations and operations. Our Cyber Incident Response (CIR) practice delivers timely and actionable information as a data breach investigation unfolds so that you can make business and system protection decisions, and understand the adversaries' motives and the data they seek.

Our professionals understand the uncertainties, risks, challenges and opportunities in the operating environments of large, complex organizations. Coupled with our industry experience we can deliver services, perspectives and solutions that best suit you, your business, your goals and, most importantly, your data.

Deloitte's Cyber Incident Response team addresses core areas that apply to different cyber events such as:

Compromise Investigation

The primary focus of the compromise investigation is to confirm the indicated avenue of the event and identify the post event network activity related to system infiltration and data exfiltration. Additionally, the compromise investigation further attempts to identify additional compromised endpoints and user accounts.

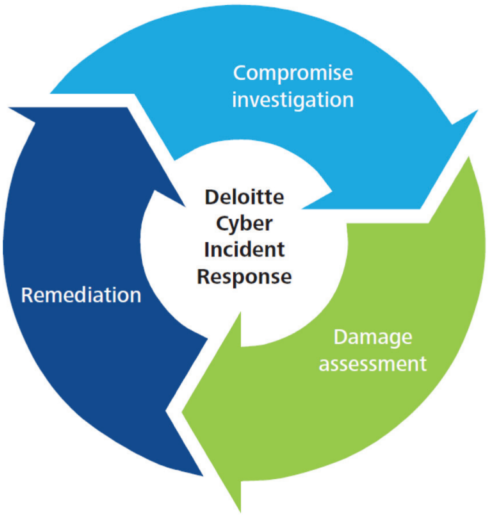
- Understand potential breadth and scale of the incident.
- Identify locations of potentially compromised systems.
- Identify and examine logs available for the incident.
- Determine any priority systems or logs with a tier based system for further collection and examination.
- Identify if an immediate, remote assessment or collection is required.

> Knowing how to respond to an incident quickly, appropriately and effectively is key to minimising the impact on your business.

Damage Assessment

The damage assessment focuses on ascertaining the data accessed or exposed, as well as providing an understanding of what the adversary sought, and what relevant issues will need to be addressed in future actions. The damage assessment can also provide further guidance on the impact of the data exfiltration on your business.

- Files accessed.
- Indicators of file use and adversary intelligence gathering.
- Files potentially or actually exfiltrated.
- Adversary's next steps.



Remediation

During remediation, we can help you get your systems back to normal as quickly as possible while ridding the systems of your adversary. Additionally, we use incident indicators and system/application patch levels to identify short-, mid- and long-term remediation efforts that can further bolster your organization's security posture

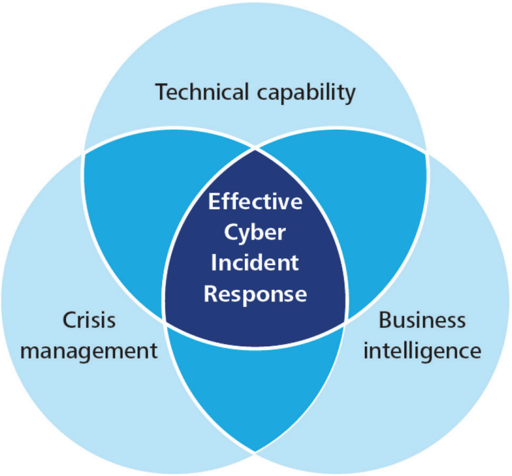
- Identify exploited known vulnerabilities.
- Identify unknown vulnerabilities.
- Recommend patching and upgrades.
- System off-lining and rebuilding.
- Long term remediation project.

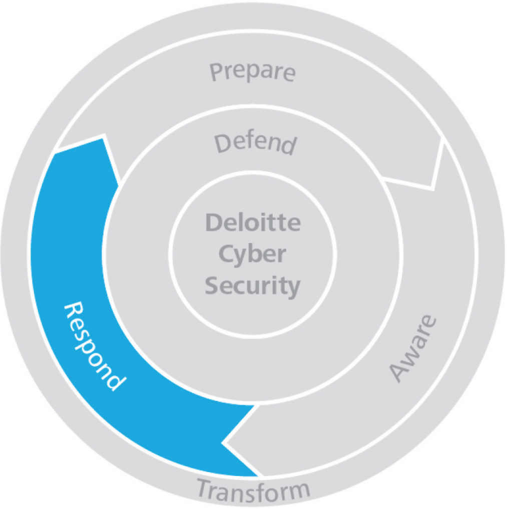
Control the Incident, Manage the Risk

Our approach to Cyber Incident Response blends deep technical skills, crisis management expertise and business intelligence to deliver a complete service, when and where organisation need it most.

- Using our technical skills and field experience, forensic and "white hat" security specialists minimise the time and resources needed to find valuable digital evidence.
- Our cyber crisis management team works with an organisation to quickly define roles and responsibilities, complete a risk and impact assessment and agree response work streams and strategies.
- Understanding your strategic business risks and organisational operations ensures that suggested response options are appropriate for your organisation.

Our response approach makes up part of a wider suite of cyber services. These help organisations to be aware of their threat profile and vulnerabilities, be prepared before an attack, and respond effectively should an attack happen.





Cybercrime.
Be ready.

Deloitte.

For more information on Deloitte's Cyber Risk Services, please contact:

Panicos Papamichael
Partner, Enterprise Risk Services
Tel.: +357 22 360805
E-mail: ppapamichael@deloitte.com

Deloitte Limited is a private company registered in Cyprus (Reg. No. 162812). Offices: Nicosia, Limassol, Larnaca.