DATA SHEET

Cybersecurity Advisory

Digital Forensics and Incident Response

This outcome-driven engagement identifies gaps **in your Digital Forensics and Incident Response planning and provides a baseline Incident Response Plan.**

Cybersecurity incidents and the potential for breaches are an unpleasant fact for organizations. NTT provides a service to clients where all aspects of a potential major incident/breach are assessed and the appropriate Incident Response Plan is drafted, tested and implemented. The ability to reduce breach exposure time requires an efficient and effective process for incident handling.

Our team works closely with a client's security team to understand the nature of their business and the threats that they face before working to create an appropriate Incident Response Plan. Our service enables us to review an organization's current capabilities and gaps analysed via workshops and a table-top exercise. Once gaps in capability have been identified an appropriate Incident Response Plan can be created.

By developing a programmatic and methodical approach to incident handling, secure organizations are able to protect their business objectives, evolve with the changing threat landscape and maximize operational efficiency and effectiveness.

Our Cybersecurity Advisory service is a business-outcome-driven consulting engagement with a flexible, modular framework that spans the entire lifecycle of security from developing a strategy and plan aligned to your business needs, optimizing existing security controls, to designing your next-generation enterprise security architecture, policies and framework.

Prevention is about taking the appropriate steps prior to an incident and is preferable to poor response. **Constantly update your plans to be resilient and maintain business continuity.**

Source: 2019 Global Threat Intelligence Report

Business outcome

Business outcome	Benefits
Identification of gaps in cybersecurity incident response capability.	Reduction in security risk, achievement of your governance, risk and regulatory compliance requirements and enablement of an effective and secure ICT environment.
Proactive response plan for cyber threats in place.	Reduced time taken to respond to threats. Staff and departments know their responsibilities, when to escalate an issue, and to whom to escalate.

How we deliver

The Cybersecurity Advisory is delivered in a flexible way, allowing the engagement to be customized based upon the level of detail required.

Our Digital Forensics and Incident Response (DFIR) module uses workshops and interviews to analyse the maturity levels of an organizations incident response policies, standards, processes and controls aligned to NIST SP 800-61 Rev. 2.

Our consultants work with your stakeholders to determine the gaps between your breach detection and response and security posture today, where you need to be in the future and how your organization bridges the gap to meet those future requirements. We then benchmark you against other clients in your industry and region and develop a highly tailored improvement plan able to protect your business/ mission, which evolves with the changing threat environment and maximizes operational efficiency and effectiveness.

This Incident Response Plan will present all the necessary workflow and processes in order to resolve a security incident.

Key service features:

- Globally consistent methodology, reporting and benchmarking.
- Provides a comprehensive baseline review of the people, process and control aspects of your ability to respond to cybersecurity Incidents and identify any gaps in coverage (process, procedure or tools).
- Provides an Incident Response Plan that is business aligned.

Additional Cybersecurity Security Modules for consideration

Digital Infrastructure evaluates your security capabilities for all aspects of physical/virtual networking and computing, so your organization is able to manage risks from the countless entry points into your environment from potentially insecure devices and applications.

Breach Detection evaluates your capabilities, so your organization is able to detect, investigate, control and mitigate security breaches.

Threat Intelligence evaluates your capabilities, so your organization is able to predict and prevent, protect, and respond to cybersecurity attacks.

Identity and Access Management evaluates identity and access management practices so that your organization is able to protect the Identity of users and accounts and the associated access across applications, data, devices and cloud services.

Micro Segmentation evaluates your organizations maturity for your infrastructure and network security policies, standards, processes and controls so your organization is prepared for micro segmentation of your physical and virtual network and infrastructure.

Multi-cloud evaluates your security capabilities for all aspects of multi-cloud, so your organization is able to manage risks from the virtual machines and applications that process, store and transmit your data.

Why NTT?

Global experience
More than 15,000 security engagements with clients spanning 49 countries across multiple industries.

Track record
Decades of experience in providing professional, support, managed, and fully outsourced security services to over 6,000 clients.

Expert skills
Highly certified security consultants with expertise across various infrastructures, systems, and application technologies.

Proven approach
Client-centric, pragmatic approach using proven assessments, methodologies, frameworks, and best practices to deliver consistent, high-quality engagements.

For more on cybersecurity advisory, click here

