DATA SHEET

Cybersecurity Advisory

Breach Detection

This outcome-driven engagement identifies gaps in your current policies, standards, processes and controls for security breach detection and response.

Cybersecurity breaches are an unpleasant occurrence for many organizsations. We provide a service to clients where all aspects of their ability to detect and respond to a breach are assessed and detailed recommendations are made. The ability to reduce breach exposure time is critical to continuation of core business services and limiting liability.

A review of the current state of your cybersecurity breach detection and response capability is required as part of your ongoing security improvement initiatives. A robust security roadmap includes the implementation, and operation of breach detection and response practices across your organization.

This will enable you to formulate a plan to manage risks, maintain compliance with external regulations and contractual mandates, and align to industry best practice.

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 breach detection and response capability	Reduction in security risk, breach detection and response, achievement of your governance, risk and regulatory compliance requirements and enablement of an effective and secure ICT environment.
Proactive improvement plan for cybersecurity breach detection and response in place	Reduced time taken to detect and respond to breaches. Staff and departments know their responsibilities and when to escalate a potential breach and who to escalate it to.

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 Breach Detection module uses workshops and interviews to analyse the maturity levels of an organization's breach detection and response policies, standards, processes and controls.

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.

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 detect and respond to cybersecurity breaches and identity any gaps in your capability (process, procedure or tools).
- Provides a prioritized, actionable security roadmap that is business alilgned.

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.

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 organization's 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.

Digital Forensics and Incident Response evaluates your digital forensics and incident response capabilities, so your organization is able to reduce the time taken to respond to threats and potential breaches.

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**