



# Cybersecurity Advisory

## Threat Intelligence

This outcome-driven engagement identifies gaps in your **information security management policies, standards, processes and threat intelligence capability and/or services.**

**Security boundaries have moved. No longer can you rely solely on traditional network security controls to provide adequate protection for your most valuable business assets. Threats continue to rapidly evolve and, driven by new business demands, your IT landscape includes more mobile access, more web-based applications, and hybrid IT environments. You need to think strategically about planning, designing, and operating your enterprise security.**

A review of the current state of your security posture is required as part of your ongoing security improvement initiatives. A robust security roadmap includes the unified and integrated

design, implementation, and operation of security 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. Insight gained from optional assessments allows you to apply your resources and controls in the most effective way to protect key data.

The current explosion in the number of vulnerabilities has only served to increase complexity **as organizations strive to keep up with patches and migrating controls on a weekly and daily basis.**

*Source: 2019 Global Threat Intelligence Report*

## Business outcome

Business outcome	Benefits
Identification of gaps in your organizations information security management policies, standards, processes and threat intelligence capability and/or services.	Reduction in security risk by implementing and better leveraging threat intelligence capabilities to predict and prevent, protect, and respond to cyberattacks.
Prioritized roadmap and implementation recommendations.	Improvement in security posture across your environment focused on implementing and better leveraging threat intelligence capabilities to predict and prevent, protect, and respond to cyberattacks.

## 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 Threat Intelligence module uses workshops and interviews to analyse the maturity levels of levels of an organizations current threat intelligence capability and/or services.



Our consultants work with your stakeholders to determine the gaps between your security posture today, where you want 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 recommended roadmap to best leverage threat intelligence capabilities to predict and prevent, protect, and respond to cyberattacks.

The recommended roadmap can be used to build a budget and resource plan, or simply aligned to an existing strategy for confirmation and reassurance.

## Key service features:

- Globally consistent methodology, reporting and benchmarking.
- Provides a comprehensive baseline review of the people, process and control aspects of your threat intelligence capability and/or services and identify any gaps.
- Provides a prioritized, actionable security roadmap that is business aligned.

## Additional Cybersecurity Security Modules for consideration

**Digital Workplace** evaluates the data protection, identity and device protection, secure collaboration and cloud access management.

**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.

**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.

**Application Security** for the development and implementation of a strategy for software security that is tailored to specific risks facing the organization.

**Multi-cloud** evaluates your security capabilities for all aspects of a multi-cloud environment, 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](#)