DATA SHEET

Cybersecurity Advisory

Digital Workplace Module

This outcome-driven engagement identifies gaps in your information security management policies, standards, processes and controls for data protection, identity and device protection, secure collaboration and cloud access management and provides a recommendation and prioritized roadmap for improvement.

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 evolve rapidly and driven by new business demands your IT landscape changes with 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 allow you to apply your resources and controls in the most effective way to protect key assets.

‘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.’

Executive Summary -
2019 Global Threat Intelligence Report

Business outcomes

Business outcome	Solution/services benefit
Identification of gaps in your information security management policies, standards, processes and controls for your digital workplace.	Reduction in security risk, achievement of your governance, risk and regulatory compliance requirements and enablement of an effective and secure digital workplace.
Prioritized roadmap and implementation recommendations.	Improvement in security posture across your digital workplace for current and future architectures.

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 Workplace Module uses workshops and interviews to analyse the maturity levels of security policies, standards, processes and controls for data protection, identity and device protection, secure collaboration and cloud access management.

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 improve the efficacy of your security policies, processes, standards and controls to enable a secure digital workplace.

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

Why NTT Ltd.?

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.

Key service features:

- Globally consistent methodology, reporting and benchmarking.
- Provides a comprehensive baseline review of the people, process and control aspects of your digital workplace environment and identify any gaps.
- Provides a prioritized, actionable security roadmap that is business aligned.

Additional Cybersecurity modules for consideration

- **Breach Detection** evaluates your capabilities, so your organization can detect, investigate, control and mitigate security breaches.
- **Threat Intelligence** evaluates your capabilities, so your organization can 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.
- **Application Security** for the development and implementation of a strategy for software security that is tailored to specific risks facing the organization.
- **Reputation, Compliance & Customer Data** for the protection of data, visibility into where data is stored, who has access to the data, and what the end users do with it to mitigate risk to data compromise or loss and to protect your reputation.
- **GDPR** for compliance with the General Data Privacy Regulation (GDPR) to improve the efficacy of your current governance and compliance posture.

For more on Cybersecurity Advisory, click here.