NTT Security

Global Overview

Cybersecurity Expertise in Government and the Public Sector

Cyber attacks on governments, councils, agencies and statutory bodies are increasing year-on-year in scale and severity. The public sector faces a rising tide of threats, and growing public concern over the resilience of government systems and the safety of personal data.

Senior officials and even ministers frequently find themselves on the back foot after a breach, forced into damage control mode and allocating precious resources from limited budgets to quell public concern and rebuild confidence in government IT readiness. A cyber attack can have long-term cascading effects, from impacting critical infrastructure capabilities, to exposing both the private data of individuals and the military and diplomatic secrets of nations.

Over the last 18 months there has been a significant increase in malicious cyber activity globally. The WannaCry ransomware attack of 2017 affected government bodies around the globe, including the US, Australia, and 48 of the UK's National Health Service Trusts. The Nyetya 'wiper' malware shut down parts of Ukraine's national power grid with a state-sponsored hacking cell suspected of involvement. Adversarial governments and hacktivist groups meanwhile are becoming bolder and more creative, as they attempt to steal sensitive information, disable systems, or wipe important data entirely.

That's why increased cyber resilience has become a central issue for government. From local to national government departments, and across major institutions, the need to protect services and infrastructure from cyber attacks which expose confidential data can be critical to ensuring public safety and a functioning society; attacks strike at the confidence we have in our governments to deliver services, maintain critical infrastructure, and sustain diplomatic relations with allies and partners. These major bodies need to step up their readiness, but how can that best be achieved?

Cybersecurity challenges in government

Today's public sector IT professionals face a number of challenges and information security concerns including:

- A constantly changing threat landscape with new threats emerging and existing threats becoming more sophisticated
- Governments and state bodies hold sensitive and confidential information about individuals and organizations, making them prime targets for advanced persistent threats and ransomware attacks
- The ongoing rise of state-sponsored hacking
- GDPR – understanding where all personal data is held, ensuring that it is secure, and clarity around how it can be accessed and shared are top of today's agenda across the public and private sectors
- A heightened insider threat risk from employees mistakenly or maliciously causing data breaches
- An increasing number of personal devices on the network, resulting in a higher level of vulnerabilities to be checked and made safe
- Interactions with third parties and the use of contractors as part of the workforce
- An expanding attack surface comprised of mobile devices, cloud data storage, and legacy systems that may be incompatible with the latest cyber defenses

The WannaCry ransomware attack demonstrated the real-world harm that can result from cyber attacks on the public sector, particularly when they are designed to self-replicate and spread.

UK National Cyber Security Centre 2017-2018 Report

- Concerns that if a government body or database is breached, you should have been able to prevent it and need to explain how it happened
- Tightening compliance requirements from regulatory authorities

Our unique capabilities

We offer a broad range of managed security, risk and compliance services that we can deliver to your organization. Our experts have global reach and local resources, and understand the specific challenges that you face in the public sector at both a regional and an international level.

Clients we engage with include major state agencies, utilities, and public sector organizations. Working with a network of trusted partners and NTT Group companies, we enable your cyber resilience using a combination of consulting, managed, cloud, and hybrid security services.

Managed Security Services

The threat landscape is evolving, threats are becoming more frequent and more sophisticated and many government bodies are struggling to manage all aspects of cybersecurity in-house. Partnering with NTT Security as your Managed Security Services provider gives you access to our world-class specialist organization and security experts.

We're here to provide you with end-to-end 24/7 monitoring, management, and support of your client data and security infrastructure. What really sets our Global Managed Security Services apart are our unique threat detection, advanced analytics, and unrivalled threat intelligence capabilities focused on the public sector. Wherever policy decisions take your organization, you'll have peace of mind and the convenience of being able to engage with one global provider for all your cyber security needs.

Our Managed Security Services also allow you to easily fulfil any recommendations made by our own consulting services, and ensure you receive a unique end-to-end cybersecurity service relevant to the provision of government services and protection of public assets.

Continuous Consulting and Compliance

The consequences of data loss in cost, compliance and regulatory violations, and damaged confidence in government can't be ignored. Creating, implementing and managing a data loss prevention strategy is a significant challenge. That's where NTT Security comes in.

As consultants to governments around the globe, NTT Security well understands the requirements of information security and risk mitigation for the public sector. Our proven methodology will significantly improve the security of sensitive data, protecting your responsibilities to stakeholders and your reputation.

57% of Government agencies believe that if information was stolen in a security breach, the greatest impact would be damage to brand and reputation.

NTT Security Risk:Value 2018 Report

The threat landscape continues to evolve, as adversaries exploit mobile devices, cloud technology, and the expanding Internet of Things (IoT) in all levels of attacks.

NTT Security 2018 Global Threat Intelligence Report

In the UK, government bodies must also be sure they handle notification of any data breaches correctly, because if a breach is subsequently found to be a serious infringement of the General Data Protection Regulations (GDPR), potentially very large fines are available to the Information Commissioners Office (ICO). And in Germany, the GDPAA has substantially changed the current German Federal Data Protection Act in order to align it to the GDPR.

Knowing about your compliance commitments and gaps is one thing – effectively dealing with them is another.

When you engage with NTT Group companies, you can be assured that NTT Security experts will help shape each governance, risk and compliance policy and process from a strategic and technical standpoint. This ensures that you are able to create a security infrastructure with the right security policies, processes, architecture, and expertise in place.

External advice can be invaluable to evolve a comprehensive security strategy and, using our proven Global Enterprise Methodology consultancy delivery approach, we will enable you to understand your risk exposure and make informed risk management decisions.

Recent cyber attacks on governments and public sector bodies

- In early January, personal data and documents from large numbers of German politicians including the Chancellor were discovered to have been published online, in what appeared to be one of the country's biggest data breaches
- Hacking of electric utilities and distribution grids in the US and Ukraine by suspected state actors
- Infiltration of 144 US universities and other targets including the United Nations, the US Federal Energy Regulatory Commission, and the states of Hawaii and Indiana – again by state-sponsored hacking groups
- Detection by the US Department of Homeland Security of malicious cyber activity targeting election infrastructure ahead of the 2018 US midterm elections
- Exposure of the personal data of 75,000 people in the databases of the Centers for Medicare and Medicaid Services from a hack of a government computer system
- Discovery of malware targeting the Italian navy designed to insert a backdoor into infected networks
- State-sponsored hacking of Singapore's largest healthcare institution leading to leakage of personal information for 1.5 million patients, along with prescription details for 160,000 others
- Disruption of all government services on the Caribbean island of Sint Maarten after a cyber attack, with most offline for a full week

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.