\Orchestrating a brighter world NEC

CONNECTING THE BITS:
Cyber-Security and the Physical World

New technologies are bringing massive change and opportunity for cities globally. The Internet of Things (IoT) and advanced analytics are bringing great improvements to the critical infrastructure of cities. However, such technologies heighten the risk of cyber-attack because of the difficulty in encrypting the devices used and the ease at which these devices can be penetrated.

A study by The Economist Intelligence Unit, Securing the digital city: Cyber-threats and responses, brings the need for cyber-security amid technology innovation into perspective. More than 80 percent of global executives surveyed for the report agree that 'the proliferation of connected devices', the 'IoT' and 'Big Data' will make their organisation more vulnerable to cyber-attack. Moreover, over 74 percent of respondents believe their organisation is likely to encounter a serious cyber-attack within the next three years. They expect ICT systems, telecommunications, industrial and financial networks to be the most targeted. These components of critical infrastructure are often privatised, hence private and public sector enterprises must work together to prepare for these threats and maintain the safety of their city's ecosystem.

Interconnectivity of the Physical and Digital Worlds

Mr Toshiya Matsuki, Executive Vice President of NEC Corporation, explains that the security of a city has moved beyond just protecting the physical infrastructure. "ICT infrastructure management is used for cities in a number of different ways which unconsciously creates various vulnerabilities," he says. "Attacks aimed at critical infrastructure supporting a city have the potential to shut down essential functions in cities, causing panic or chaos. Previously, security was largely focussed on physical solutions, such as surveillance and access control. Now, however, cyber-security has become equally important."

Mr Toshiya Matsuki, Executive Vice President, NEC Corporation

Mr Matsuki adds that the first step an organisation should take is to build comprehensive understanding of their physical and cyber activities, and address any vulnerabilities. The second step, and consciously a tougher one, is to identify threats within systems and respond to them swiftly.

"A cyber-attack isn't something that will happen once," Mr Matsuki elaborates. "To reduce the possibility of an attack or a recurring attack, organisations need to know what to protect and how they can best protect it. The attackers are continuing to attack, in as many ways as they can, and, at the same time, are preventing themselves from being hacked or identified. So, it becomes very important to be vigilant and to actively prevent such attacks from occurring."

From Intent to Implementation

While governments are beginning to create cyber-safety guidelines for their cities, Mr Matsuki is of the opinion that industries must also give security a higher priority and increase their investment in it. The role of top management is critical to ensure that investment and corporate priorities are in-line with both physical and cyber-security objectives. "It is important that top management at a company understands these issues, and is willing to take steps to ensure that their company is protected from threats," he says. Today leading companies assign a chief information security officer, whose role is to take initiative that resources and investment are adequately allocated to cyber-security measures, and that systemic risks of a cyber-attack on their ecosystem and supply chains are measured and monitored. It is a strategic option for them to make use of the expertise of external ICT professionals. "NEC has made a strategic move to set up several Cyber-Security Factories across the globe to help both governments and industries protect themselves from cyber-threats. They are staffed with highly trained professionals and so-

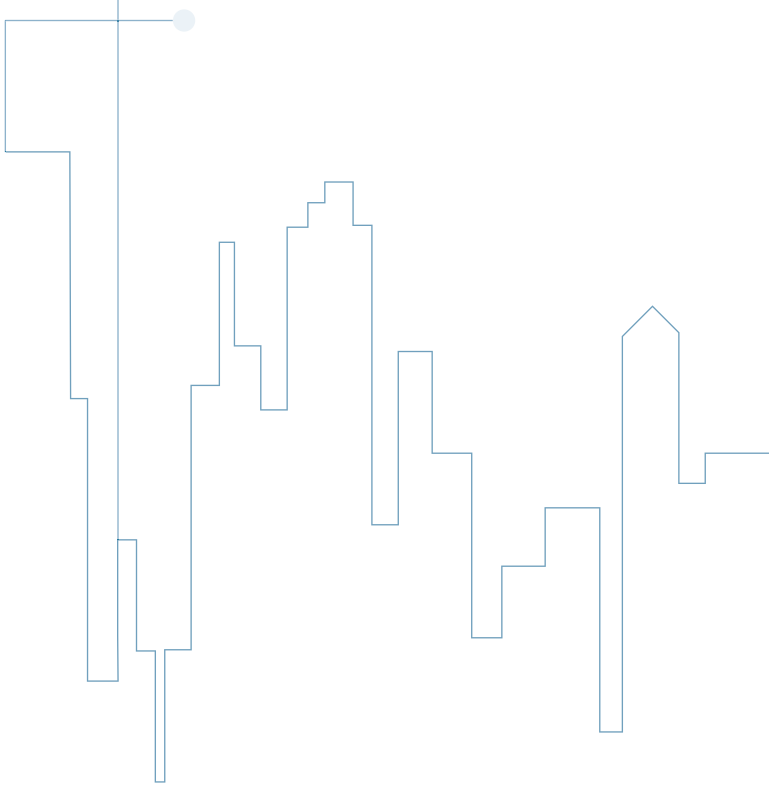
phisticated security systems," says Mr Matsuki. The EIU study suggests that third parties are becoming increasingly important in the cyber-security plans of critical infrastructure organisations today. Among survey respondents, 35 percent said they employ a third party to manage all or most of their cybersecurity needs, while 27 percent use a commercial off-the-shelf solution that they manage themselves. Mr Matsuki says that security management in this new age requires sophistication in both strategy and technology. The NEC system, he elaborates, encompasses a smart visualisation enabled by artificial intelligence (AI) to detect even unknown cyber-attacks. Through machine learning, NEC's AI-enabled cyber-security system is able to comprehend the normal state of operations of an entire ICT system, which would take an enormous amount of man-hours for humans to map. It will automatically alert operators to actual points of deviation from the normal systemic state and allow them to quickly rectify the situation.

Evolving technological advancements diminish the lifecycle of cyber-security products as attackers become more resourceful. Mr Matsuki explains that today's systems must be agile, robust and flexible enough to adapt in a way that mitigates cyber-threats, yet they must be capable of preventing major disruptions or shutdowns of entire systems. NEC's Software-Defined Networking control function, for instance, is able to localise and block any malware-infected terminals and automatically instigate appropriate responses to allow the system to continue its functions. Without such functions, it would take the organisation several weeks to get its system restored.

Rising to the Challenge

The world is entering into an era of technology-dominated progress. Cities and corporates are keenly focused on the benefits of sophisticated technology, which has increased their mobility, information management and awareness. But they must all consider the risks of such a future. Enterprises, governments and technology experts should work together to take a co-operative approach to the systemic security of critical infrastructure. NEC believes that multi-agency collaboration is essential in this new age, where selected data from different systems in both the public and private sectors can be integrated into one command centre, providing a coherent view of the situation and the actions required to protect and progress.

To keep their cities safe, governments are steadily working towards building cyber-security mechanisms alongside physical security systems. As Mr Matsuki foresees "Moving forward, security is going to become a vital function for companies and cities. Focussing on sound cyber-security practices will allow both developed and developing cities to reassure stakeholders on the safety of their city, and thereby build sustainable economic and societal betterment."



NEC Corporation
7-1, Shiba 5-chome, Minato-ku, Tokyo 108-8001, Japan
www.nec.com