\Orchestrating a brighter world NEC

ENSURING DIGITAL SAFETY

WITH ROBUST CYBER SECURITY

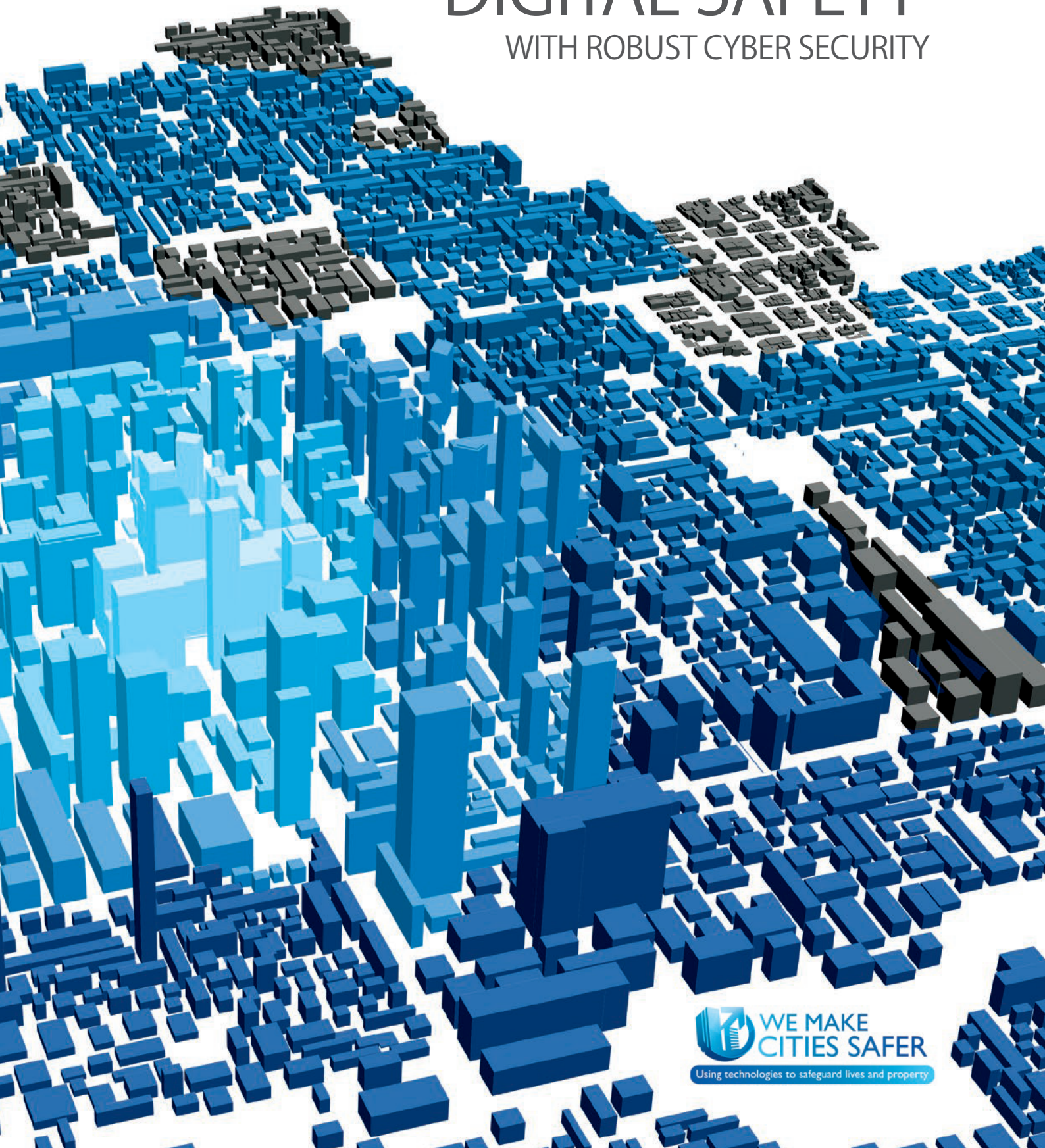
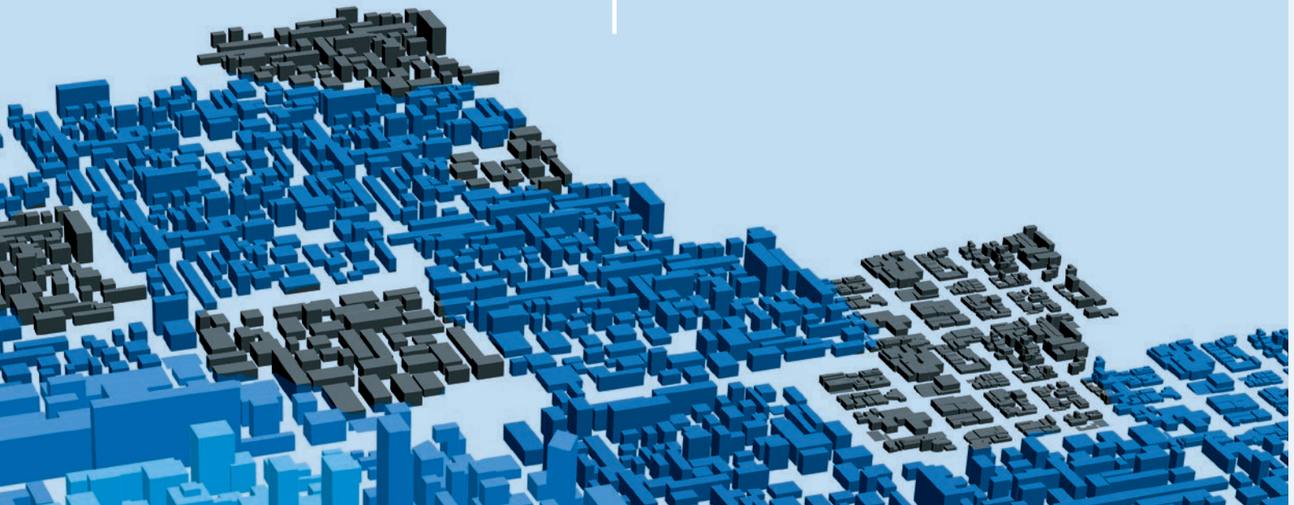


Table of Contents



SAFER CITIES
WITH ROBUST CYBER SECURITY

As cities wire up with more smart sensors, security efforts have to overcome various challenges to protect the critical infrastructure.

Ask any chief information officer (CIO) or IT manager what keeps him up at night and cyber security is surely at the top of the list.

While threats used to come from the outside, which can be effectively warded off with strong external defenses, today's hackers can strike from anywhere, be it through social engineering or by planting increasingly complex malware to trigger an attack from the inside.

Hackers too are becoming more sophisticated and organized. No longer one-man efforts, many are often state-sponsored and financially-motivated today.

From stealing information from PCs, they have graduated in recent years to learning how to damage public infrastructure as well. From crashing Web servers, they have gone on to target industrial systems that used to be "safe" from such hacking because of their uncommon interfaces.

In 2010, Iran was the target of an unprecedented cyber-attack that shut down the centrifuges that the country relied on for enriching uranium at its facilities. Tellingly, it managed to stay dormant for years before taking over computers at a nuclear facility to overload and damage the equipment there. Iran's nuclear plans were set back by several years, as a result. The culprit was the Stuxnet malware, an APT (Advanced Persistent Threat) which became the first of its kind to be uncovered and found to be so sophisticated that it could infiltrate and subvert industrial control systems of a critical infrastructure such as Iran's nuclear facility.

Since its initial appearance, Stuxnet has been found lurking in the data banks of traffic control systems, power plants and factories, packing software code that is believed to be 20 times more complex than other malware. Its obvious targets are public infrastructure, on an unprecedented scale.

It could turn off oil pipelines and change the pressure in nuclear plants, while keeping the readings at normal levels to deceive operators that everything was going fine. Turning on a nuclear plant under construction, Iranian authorities later conceded, could lead to electricity blackouts in its cities.

The same sophistication is being seen in increasingly common attacks that are coordinated and well-planned. Since Stuxnet, the threat of cyber attacks on critical infrastructure has become more serious and real for many city planners.

What makes malware such as Stuxnet even more dangerous is that it is open source. Since being out in the open, it has been taken apart and reassembled to target various different public infrastructures. It is available to people with a motive to attack such installations.

However, despite its reputation for targeting industrial control systems of nuclear and power facilities, this in no way means that the potential destructiveness of APTs is confined to just that space. The fact that it has up until now targeted such an infrastructure does not mean that it will continue to be that way in the very near future. Stuxnet was but a taste of the terror that APTs are capable of unleashing; a tip of an incredibly deep iceberg. Other critical infrastructures such as banks and transport companies could be subjected to similar, if not higher risk levels of being breached. This is further exacerbated by the fact that many critical infrastructures are primarily owned by private entities nowadays. Such organizations are profit driven and would generally not make it the utmost priority to expend resources on strengthening cyber infrastructure. Specific regulations from government may be required, but this will likely take time as such risks to safer cities are still relatively new to many policy makers

In 2013, a former director of the United States' National Security Agency claimed that 90 per cent of the world's computers holding strategic, monetary or intellectual value may have been infected by malware.

And at the start of 2014, the unrest in Ukraine was marked by the use of sophisticated cyber weapons. One known as Snake is said to have infected dozens of government systems, and could potentially prevent many public services from being provided.

In the years ahead, it's clear that city planners and leaders have to make cyber security a key focus in their critical infrastructure. As they roll out safe cities wired up with sensors to measure everything from flood water to human traffic, the challenge is to develop a robust strategy for protecting all that the new connectedness offers.

What is also critical is having well-trained manpower with the necessary technical skills to counter cyber attacks. These skills cannot be taught just in classroom environments, but also through realistic simulations that truly test a system and its operators' robustness in dealing with threats.

LIVING WITH THE CONSUMERIZATION OF IT

One phrase that often worries CIOs is BYOD, or bring your own device. Rather than provide corporate devices that are "hardened" for security, today's IT departments are facing strong demand from users who want to access corporate resources through their own smartphones, tablets and laptops.

While convenience is clearly an advantage in an era of always-on, mobile computing, having unsecured devices access an organization's computer networks can potentially open up security loopholes in an otherwise well set-up system.

All it takes, for example, is for a user to be infected by a key logging malware, say, while visiting a malicious website or downloading some malware inadvertently, for a hacker to have access via his account.

Another issue is zero-day exploits. These are essentially loopholes found on new systems that are yet to be discovered, and they can be traded on the black market for about US$100,000. The Stuxnet malware targeting public infrastructure, for example, made use of 20 such zero-day exploits.

Many tools have been developed to counter this. For example, some PCs are not allowed to connect up to sensitive parts of a network unless they have the latest software updates and are protected by anti-virus software. However, these measures have to contend with the increasing number of threats and potential entry points through users' weakly protected PCs.

Indeed, the BYOD development is part of a bigger trend, one where IT is increasingly consumerized and uses highly common components and interfaces.

For safe cities, this is a trend that can bring challenges. As the computing hardware used to monitor car park spaces or compile data from sensors city-wide becomes commoditized, it also becomes easier to target.

That is because common, open interfaces make them easy for cyber attackers to learn, master and exploit. This is especially true of zero-day exploits, which refer to newly discovered exploits that are not yet patched up by security measures.

This is not to say CIOs and city planners should avoid the consumerization of IT – they cannot, in all honesty. What they have to do is implement more intelligent, rigorous checks on a system-wide level.

One way to start is to have strict policies on users and machines that are connected to critical systems. Something as simple as a USB drive brought from the outside could be the source of an infection – and may be restricted on more sensitive systems.

BUILDING
SECURITY INTO DEVICES

While the commercialization of IT has led to advances, such as touch screens, that are faster than before, some technologies can also come without the security checks required for a robust defense against cyber attacks.

Even as they plan for safe, connected cities, city planners have to consider the cyber security issues that new technology brings.

What is there to prevent the smart sensors collecting weather or other information from being spoofed? What's there to stop a server collecting such information from being compromised and thus destroying the "intelligence" provided by such smart sensor networks?

What about shopping carts? Can they be spoofed as well? And water headers that are remotely controlled? Can they be hacked into in future? If these smart devices are not secure, then the damage wrought from a nationwide network of devices could be multi-fold afterwards.

What city planners have to ask for is security to be built into these smart sensors and devices that act as the eyes and ears of a connected neural network for a city. Encryption could be one way to ensure that communications are kept secure between devices, for example. Sensors may also have to be able to authenticate and identify themselves.

All this could mean increased processing power and, very likely, increased deployment costs as well. Yet, in a new Internet of Things in future, where wearable computers and other small computing items are all hooked up online, it may be even more important that the critical data collection sensors and servers be protected by adequate cyber security.

The worry is that manufacturers and integrators of such smart sensors will rush out solutions that promise a quick rollout, only to worry about security later on. That's one issue that city planners cannot ignore when evaluating a safe city solution.

PREPARING
THE INFRASTRUCTURE FOR AN ATTACK

A holistic approach is what city leaders require when preparing a city's infrastructure to defend a cyber attack. With so many devices connected to a multi-faceted network of networks, it is important to have monitoring devices built in to watch out for "choke points" that may turn out to be potential targets.

It is always better to pre-empt an attack than be caught unawares when critical infrastructure is damaged or disrupted by online threats. Increasingly, one way to go about this is through ambient security.

Virtual security agents can be deployed in critical systems, much like the white blood cells in a human body, to patrol for potential threats and pick them up through potential attack signatures or patterns that may be suspicious. Big Data, with its analysis of attack patterns, can be a vital tool in gaining a step up over emerging malicious threats.

Some of the most sophisticated attacks today rely on malware that is planted months, maybe even years, in advance to slowly spy on what is going on in a network. This is before unleashing a payload that could send a machine spinning out of control or turn off street lamps to create chaos in a city in an instant.

One way to counter this is to have sophisticated defenses that don't just look for known patterns from past attacks, but ones that can adapt and learn to identify potential malware such as dormant ones that "wake up" only once in a while to "report back" to its owners.

While city planners beef up defenses to ward off potential attacks, they also have to consider how to recover from a situation where systems are compromised. There is an expectation from the public that a public network should be able to protect users from being attacked.

For example, a spoofed government website or information source on a trusted network could be used to steal information from unsuspecting users in a crisis. Security measures have to be built in to ensure that users are not inadvertently exposed if there happens to be a breach in public cyber infrastructure.

MANAGING
ALL THE DEFENSES

As cyber defenses get more sophisticated, the challenge is to manage all of them in a way that assists rather than confuses. The challenge is multiplied as a city-wide network often contains devices that are both new and old.

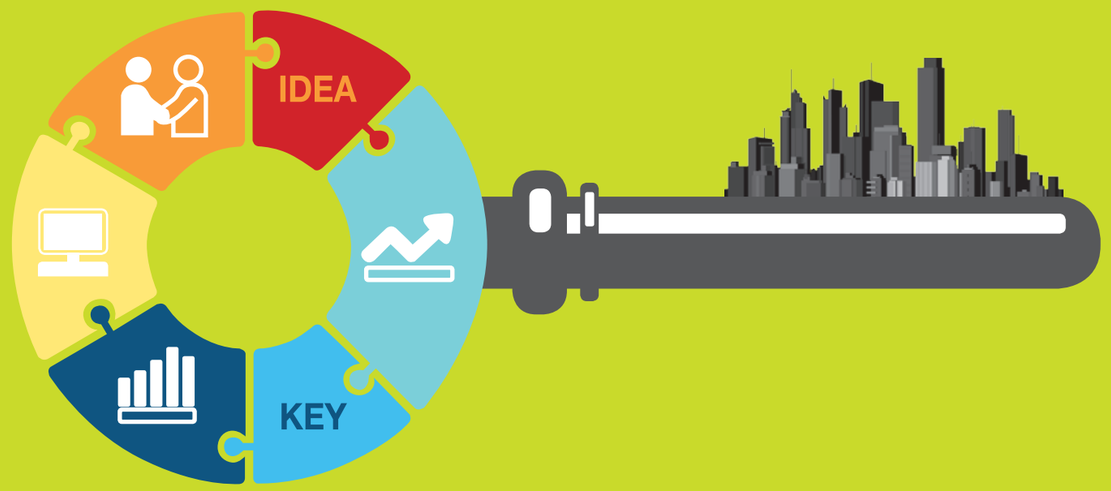
Be it connected cameras or roadside sensors assisting drivers, these devices have to be easily managed at a nerve center that coordinates a city's cyber defenses. For old devices, the solution may be to find adapters and software agents that can talk to them to bring them into the fold in an integrated defense system.

Defense solutions have to be able to scale as well, as millions of smart devices join the network eventually. While building up access is often the first job for city planners eager to bring new capabilities to users, the cyber security involved has to be able to scale at the same pace.

A robust cyber defense solution should be able to work with the thousands of hours of video feeds from surveillance cameras, location-based car sensors and other data to detect where a threat is coming from. This means that not only do the processing power and turnaround time of the cyber defense solution have to be extremely scalable; its architecture will have to be flexible enough to accommodate various technological platforms as cyber and physical defense technologies mesh together. This adds countless key variables into the picture, all of which both end-users and system providers need to grapple with.

One other challenge is to keep the state of cyber defenses secret. Even if a country has a solid cyber defense architecture, skilled hackers might be tempted to have a go at breaching the defenses if they get wind of any details.

A key challenge is in tactically tapping on all monitoring devices available to solicit the necessary data required in a crisis. For example, can there be a better fusion of both cyber and physical signals to pinpoint potential suspects in a cyber attack?



EDUCATION
IS MUCH NEEDED

Clearly, much education is required in not just the IT field but also leaders at various critical infrastructure operators. This is especially important as many systems go "smart" in the coming years, after being "closed" industrial systems for decades.

Consider critical power generation and distribution systems, for example. These used to be unconnected and "dumb" systems without much digital configurations. But they are becoming increasingly sophisticated, bringing more convenience to the hands of operators and potentially that of a hacker who has successfully sneaked past cyber defenses.

The same could apply to, say, subway operators, companies which have probably spent more time looking at how IT can assist in smoother rides and faster connections, rather than shoring up defenses against potential cyber threats.

A gradual education process is required to have operators of critical infrastructure aware of cyber threats and ways to counteract a potential crisis. In simulated environments, NEC is able to train staff on how to respond to a cyber attack. Running a system that is under attack by a "red team" of hackers will bring insights and improvements on a critical system as well as test the effectiveness of contingency plans.

In a realistic simulation, common attacks can be fired, like in a rifle range, to test how resilient and robust an organization's cyber defenses are. This is not aimed at testing the weapons or tactics used by hackers, but to detect where the actual weaknesses are in an organization's infrastructure.

The range will allow professionals – including non-IT savvy operators, say, in a power generation company – to see how a cyber attack will directly affect their operations. A power plant may be shut down, or a government's website could be spoofed, if their defenses are taken down by real-life "white hat" hackers deployed in these realistic tests.

Such training will enable operators of key infrastructure – both IT and non-IT personnel – to directly experience the issues that could play out in a real scenario. Instead of a false sense of security, they will more realistically assess their current situation and improve their response to a real crisis through practice drills. In a world where cyber attacks can come in various forms, the only defense is to be well-prepared.

NEC SOLUTIONS
CAN HELP

At NEC, we have the solutions to help create a better, safer city. We have decades of experience working with governments, city planners and other public agencies in projects as varied as identification to public transport. Besides the protection of critical installations and safeguarding of cyber infrastructure, our solutions include national identification, law enforcement, immigration, and emergency and disaster response.

While bringing together the latest cutting-edge technology, NEC's team also possesses the experience and expertise to deal with projects – both private and government – on municipal and international levels.

In December 2012, NEC signed a three-year-agreement with Interpol to develop core elements of the Digital Crime Centre established at the Interpol Global Complex in Singapore. NEC will provide technical and human resources worth some EUR 7.6million to establish a Digital Forensic and Cyber-Fusion Centre at Interpol's complex.

This lab will focus on identifying and test-bedding digital forensic technology and methodologies to help investigators better coordinate and conduct digital crime investigations.

Among the cutting edge technologies is NEC's Cyber Fusion platform. This powerful platform works in tandem with NEC's cutting edge City Operations Centre, enabling city authorities to tactically tap on connected devices and sensors throughout a city to solicit the necessary signals, for example, to locate suspects of a cyber-attack. The alliance between the Cyber Fusion platform and City Operations Centre will allow for a more holistic approach towards defending cities from cyber-attacks and beyond.

By combining the signals from a computer network and feeds from physical sensors such as cameras, the platform works like a sensory brain that offers greater insight into a fast developing situation. It can search through online channels for a suspected terrorist's logons to various networks online to look for traces he has left, say, when changing server records or stealing data to execute a physical attack.

For example, if a suspected terrorist is detected to be chatting online and stealing data related to some tenants in a building, law enforcement officers can draw on that intelligence to help determine his whereabouts quickly. They can also activate CCTV cameras to look out for persons who might be identified visually.

Training operators of critical infrastructure to realize the vulnerabilities of their systems is another area where NEC can assist in. With a virtual "firing range" running on virtual machines, NEC can simulate actual mission-critical systems and test them against a variety of cyber attacks carried out by "red team" hackers.

Some of them can look out for known or new vulnerabilities in enterprise apps, while others with specific knowledge in industry control systems, such as SCADA (supervisory control and data acquisition), can put operators of critical infrastructure, such as a power or water control system, to a realistic test through a cyber attack.

Through such cyber defense training, NEC would enable the relevant personnel to watch out for suspicious activity, as well as evaluate the readiness and resilience of their existing systems. Issues with technology – say, patches not being applied on time – or processes that may be insecure can be surfaced through such training scenarios.

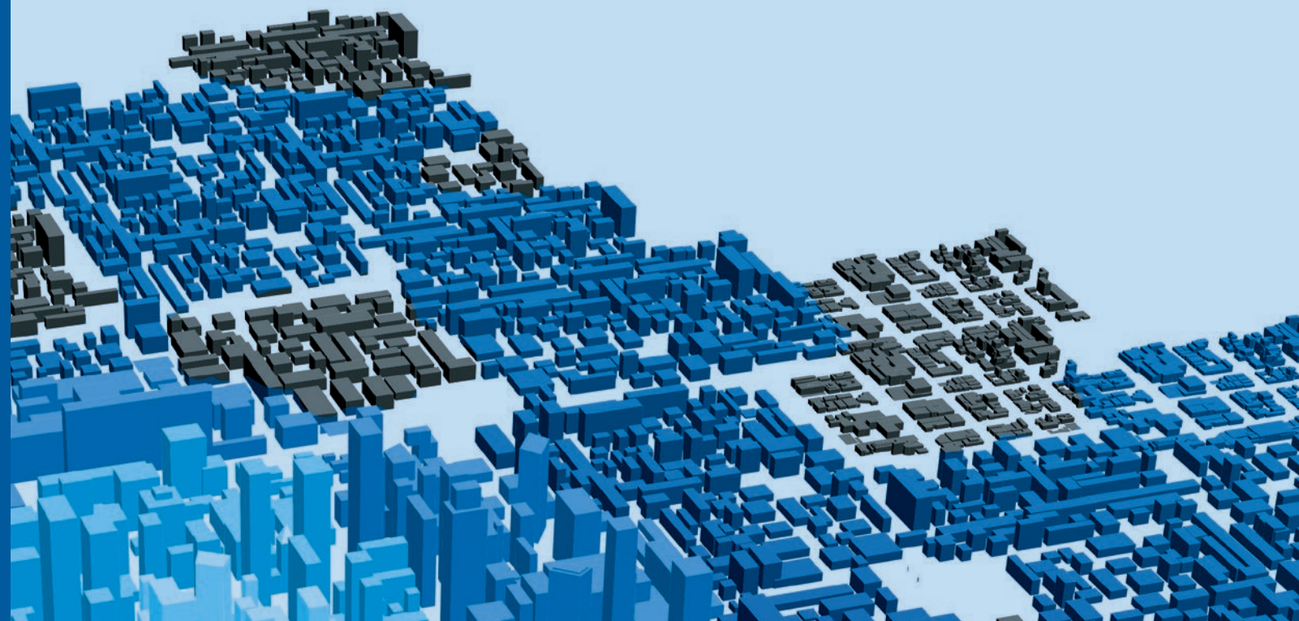
Coupled with e-classroom sessions, such education will raise awareness and provide real hands-on practice to boost competency and preparedness. Whether an attack is from an insider in an otherwise secure network, or from repeated attacks, these virtual exercises are valuable in preparing for cyber attacks in the future.

Holistically, NEC's cyber security solutions answer the challenges arising from a safe city, ensuring that the connectedness is paired with robust cyber security for the public's peace of mind. The scalability of our solutions pairs well with our integrated offerings in inter-agency collaboration and critical infrastructure management.

Whether this is defending against a zero-day exploit or working with agencies to develop a tested cyber security strategy, NEC is well equipped and the partner of choice for safer cities.

REFERENCES:

1. Gartner Predicts 2014: Smart City Security, Infrastructure and Business Issues Remain Critical *(http://www.gartner.com/document/2633218)*
2. NSA Director Warns Middle East Oil and Gas Firms of Vulnerability Against Cyber Attacks *(http://www.thenational.ae/business/industry-insights/technology/nsa-director-warns-middle-east-oil-and-gas-firms-of-vulnerability-against-cyber-attacks)*
3. Cyber Attacks in the Middle East *(http://www.currentintelligence.net/analysis/2013/7/29/cyber-attacks-in-the-middle-east.html)*
4. Ten Things To Consider When Developing An Enterprise BYOD Security Policy *(http://www.darkreading.com/ten-things-to-consider-when-developing-an-enterprise-byod-security-policy/d/d-id/1140478?)*
5. DDOS Cyber Attacks Get Bigger, Smarter, More Damaging *(http://www.reuters.com/article/2014/03/05/us-cyber-ddos-idUSBREA240XZ20140305)*
6. Report Calls for Better Backstops to Protect Power Grid From Cyberattacks *(http://www.nytimes.com/2014/03/03/business/energy-environment/report-calls-for-better-backstops-to-protect-power-grid-from-cyberattacks.html*



CONTRIBUTORS;

- Paul Wang (PhD), Chief Technology Officer, Global Safety Division, NEC Corporation.
- Douglas Tang, Senior Director & Global Lead of Cyber Security, Global Safety Division, NEC Corporation.
- Quek Joo Khuan, Business Development Director of Cyber Security, Global Safety Division, NEC Corporation.

About NEC Global Safety Division

NEC Global Safety Division, a business division within NEC Corporation, spearheads the company's public safety business globally. The Division is headquartered in Singapore and offers solutions in the following domains: Citizen Services & Immigration Control, Law Enforcement, Critical Infrastructure Management, Public Administration Services, InformationManagement, Emergency & Disaster Management and Inter-Agency Collaboration. Leveraging on its innovative solutions, the Division aims to help government and business make cities safer.

NEC Global Safety Division

Global Headquarters: No.1 Maritime Square #12-10, HarbourFront Centre, Singapore 099253 For enquiries, please contact safety@gsd.jp.nec.com

nec.com/safety