FROST & SULLIVAN

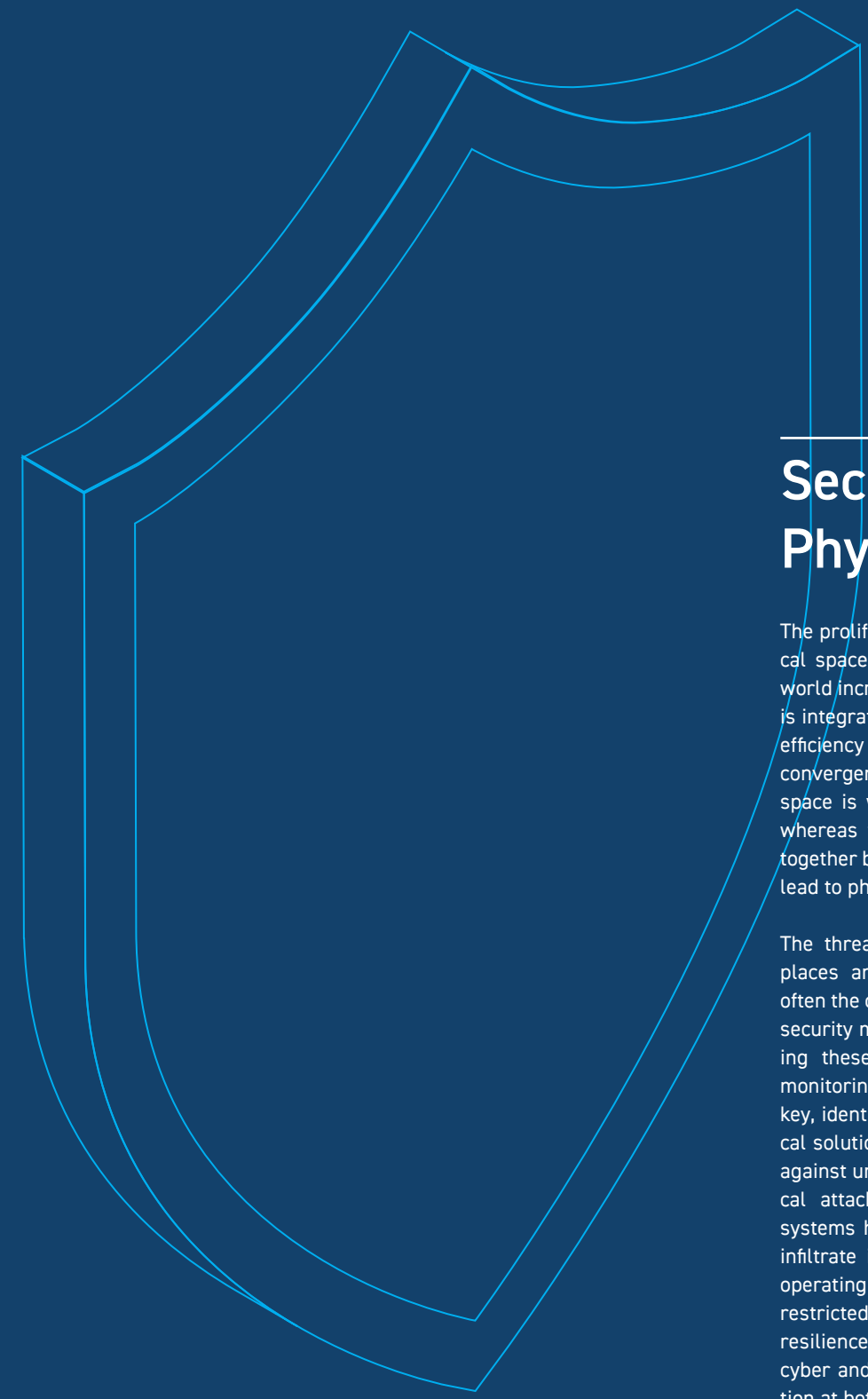
Securing Experiences via Digital Identity

Sponsored by

NEC

A Frost & Sullivan Executive Briefing Paper

The Rule of Three



1 Securing Cyber and Physical Spaces

The proliferation of technology has transformed physical spaces as the Internet of Things (IoT) makes the world increasingly connected. Technology convergence is integrating the cyber and physical spaces, achieving efficiency levels not previously possible. However, this convergence presents new challenges. The physical space is where people and ubiquitous objects reside whereas the cyber space is virtual. Putting the two together brings about cyber threats that can potentially lead to physical harm.

The threat creates a greater need to secure public places and critical infrastructure because they are often the choice for physical attacks despite heightened security measures. The conventional method in guarding these places has been to restrict access and monitoring of premises with solutions that require a key, identification card or a password. However, physical solutions will not be the best measure in guarding against unauthorised access in integrated cyber-physical attacks. The absence of air-gaps in operating systems have made it possible for cyber attackers to infiltrate internal controls with malware that cripple operating systems without the need to physically enter restricted premises. There is a need to strengthen the resilience of control systems by safeguarding both cyber and physical spaces effectively with authentication at both domains.

Securing Customers and Stakeholders' Experience

As the IoT brings the cyber and physical worlds closer together, people are increasingly going through their daily routines in the cyber space such as performing online banking transactions or shopping via eCommerce. Having a digital identity reduces the need for people to be physically present in different places to perform various activities. As these experiences are evolving to become an essential part of our lives today, digital identities have become the core of our virtual experience.

However, such experiences have not been extended to the physical domain because physical security continues to rely primarily on conventional systems to regulate entry. People have to stop to identify themselves be it using passwords, identity cards or screening measures to validate who they are. To empower people to perform their tasks more efficiently, there is a growing demand for the need to get through conventional security systems in a more seamless and faster manner. This calls for technologies that could track, identify, and recognise people and their activities within certain boundaries. Tracking and identification technologies are evolving from environments where individuals are already known by the system such as employees in a corporation, to environments such as an airport where a large number of individuals are not known by the system.

For instance, in the event of an emergency, the ability to conduct physical authentication in the cyber domain will enable security personnel to launch an investigation immediately without wasting time to be physically present. It will be even more critical in situations that require the validation of numerous stakeholders with different access rights. The ability to efficiently authenticate their identity, organisation, credentials and what they can perform will be important. While having a digital identity remains used largely for security reasons, it is increasingly adopted for commercial purposes in securing experiences with the personalisation of the service delivery.

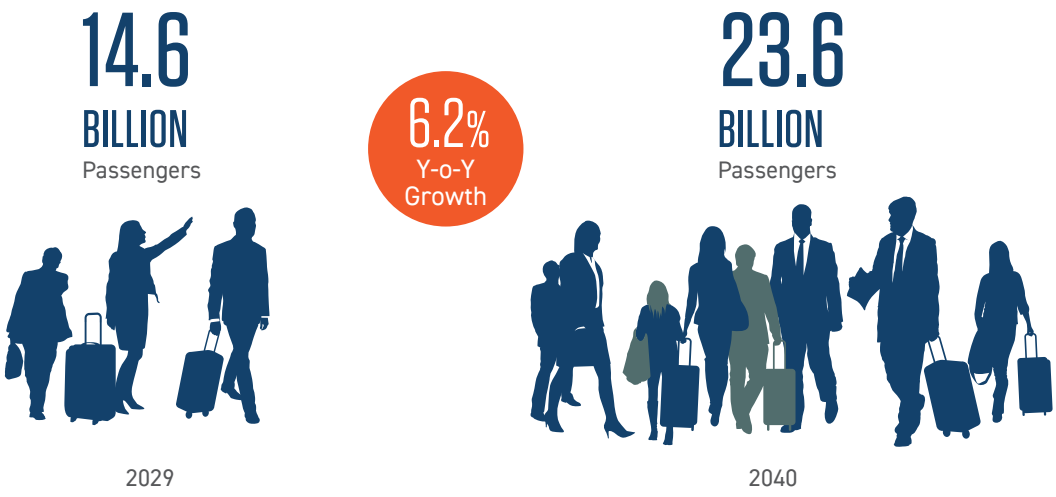
Securing Digital Identity

With the rise of cloud, social and mobility, a person no longer has a single physical identity but multiple identities across applications, devices, and objects. It is not uncommon for an individual to be carrying a number of physical access passes such as tags, tokens and identification cards and having over 10 digital personas to gain access to different online activities. While the limitation and vulnerability of using passwords are already well known, it remains the most frequently used channel today.

As people link their physical self to their digital self, it opens up new ways and a wider variety to serve the same person in different settings. While the digital self opens the possibility of hiding one's true identity, no two identities are ever the same. Authentication technologies trace the unchanging physical attributes of an individual. Digital identity derived from physical identity provides an extra layer of protection through biometric authentication. Not only does it reduce fraud, it enhances the experience, which increases loyalty over the customers' life cycle. While digital identity applies largely to people, it can also apply to ubiquitous objects in an environment. As people and objects become more connected, security and authentication are taken to a new level.

Scenario

AIRPORT



The use of digital identity will enable airports to evolve from being efficient operators to becoming hubs of multiple activities using innovative and new business models

International passenger volume has been on a steady rise. The Airport Council International reported that global passenger volume increased year-on-year by 6.2% in May 2017. It is anticipating passenger traffic to double to 14.6 billion per annum by 2029 and to 23.6 billion by 2040. The data is consistent with the report by the International Air Transport Authority (IATA) that indicated an annual increase of 7.4% in international passenger volume in terms of revenue passenger kilometers. Growth in passenger traffic was the highest in the Middle East followed by Asia-Pacific in 2016 at 11.3% and 10.9% respectively.

While this is good news for airport operators from a revenue point of view, massive growth in passenger traffic also brings greater security threats, resulting in the need for additional layers of checking and screening. The threats are genuine. In 2016, terrorists launched a physical attack on Brussels' Zaventem Airport killing 11 people and injuring hundreds more. Attacks are not just happening at the physical level, as airports are increasingly vulnerable to cyberattacks. There are loopholes in a modern airport infrastructure that provides cyber hackers with a backdoor to gain access to a variety of operating systems.

In mid-2017, a major ransom attack was launched on an international airport in Ukraine. The airport was paralysed by the attack as hackers encrypted files coupled with malicious software that shut down their computer system demanding a large sum of money to fix the problem. A year before that, hackers launched cyber-attacks on Vietnam's two largest airports. The hackers managed to hijack the flight information screen and sound system inside the airports. All Internet systems had to be shut down and documentation had to be done manually. In June 2015, the carriers' IT systems at Poland's Warsaw Chopin Airport were jammed by a major distributed denial of service attack. The airport took five hours to resolve the issue, resulting in 10 flights delayed with 1,400 passengers grounded.

Although no cyberattack has resulted in physical harm up to this point, there is mounting fear among all stake-holders that it will be a matter of time that one day, cyber hackers can take over an aircraft steering wheel and cause planes to crash from their mobile phones.

As airport operators get their heads around security, there is a need to balance other aspects especially from the commercial side of things. Globalisation and economic affluence are bringing about more international travels. To tap into growth opportunities, governments emphasise the desire to see the continuation of frictionless borders to support the transience of mobility as an indication of a transport and transit hub.
To get more people to use their airports, operators have expanded their roles beyond the traditional provision of passenger gates to include multiple activities within an airport environment such as dining, shopping, entertainment and relaxation that bring passengers' experiences to a higher level so that they can be better in attracting passengers and bring about more revenue.

Passengers' experiences start from the moment that they book their plane tickets and check-in online from their own premises. And as they make their way to the airside, they take on a different persona from one place to another carrying out different activities. A passenger can take on the persona of a commuter, a diner, or a passenger in transit seeking entertainment and relaxation before boarding the plane. While there can be many things that passengers can enjoy within an airport, their experiences throughout can be affected by the amount of time needed and the hassle that they go through to reach the airside.

Passengers spend a lot of time complying with security screening, which is one of the things that give them a great amount of stress although it is no doubt necessary. The current approach in dealing with security risk is to pile on more security checks. The battle against identity fraud and terrorism has resulted in longer queues, waiting time and delays in flight schedules.

As the volume of activities and traffic increase, the level of risk faced by an airport operator increases as well. From an airport operator's point of view, a major concern is security as well as the need to get passengers to their airside on time. Safety and security remain the priority and responsibility for all airport stakeholders. Ironically, long queues waiting to go through rigorous security checks make airports highly attractive as soft targets. At the same time, the increase in automated self-service installations that allow check-ins, baggage drops, and identity scans with limited human intervention present cyber security risk that threaten to disrupt operations from flowing smoothly.

Despite extensive measures in place, airport operators today are grappling with legacy and silo systems, a lack of real-time security data, getting passengers to airside areas on time, detecting suspects from leaving their borders and safeguarding access control with different access rights.

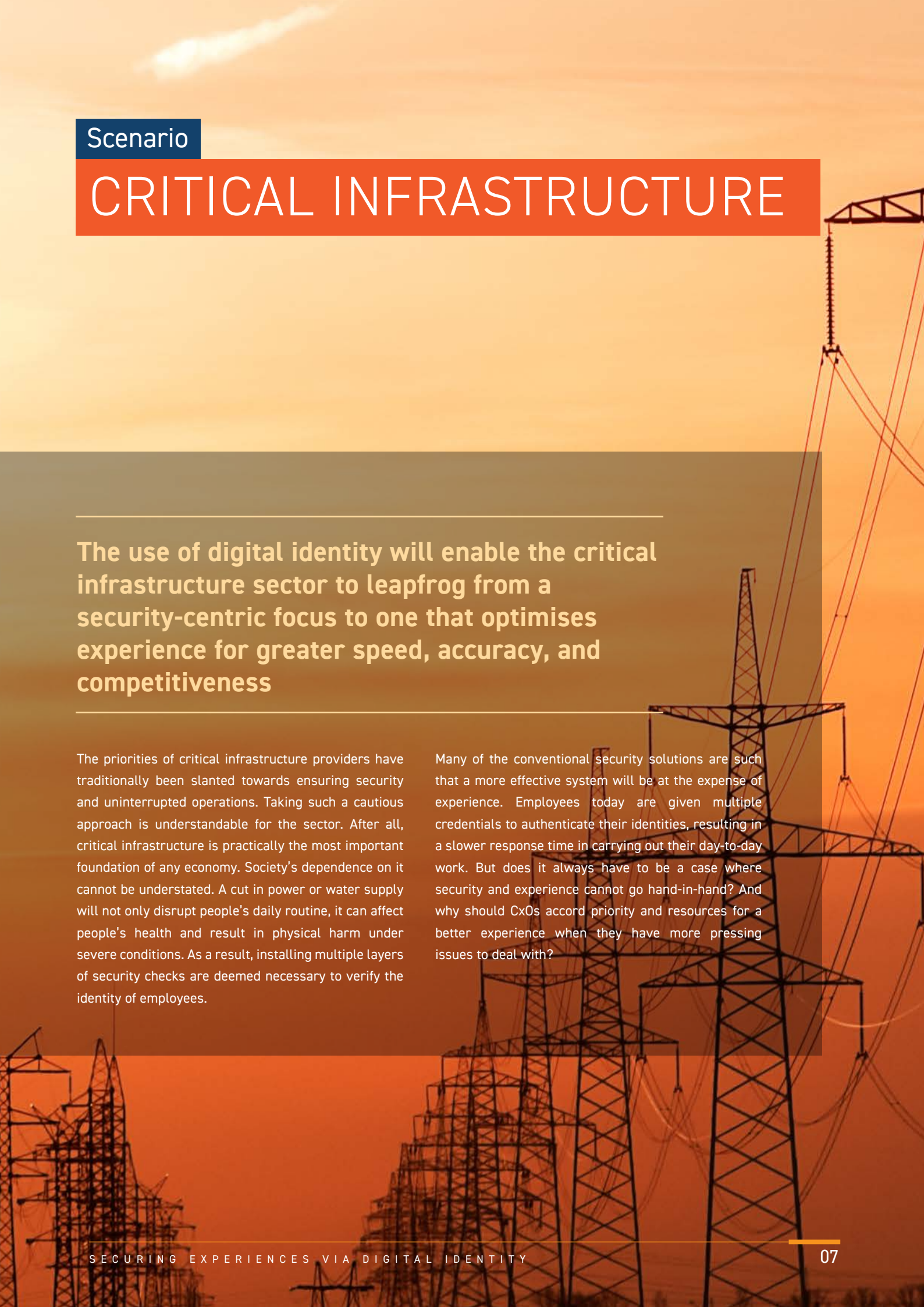
There is a need for airports to adopt a more effective screening process while improving the traveling experience. Having a digital identity provides the ability to quickly verify who the individual is. It supports passengers' experience from check-in, bag drop, dwell time and their way to the airside. It facilitates the management of airport participants and balances a rigorous safety environment while pursuing higher levels of passenger satisfaction.

Digital identities support passenger experience in many ways. When combined with mobile, beacons and other technologies, customer experience can be taken to a higher level with personalised offering. Passengers can be notified of nearby food and shopping outlets with concessionaires based on their current location and past transaction histories. More control can be given to passengers by updating them about their flight time, boarding gate and things they could do as they make their way to the airside. However, there is also risk involved as more personal data is at risk of being exposed in the face of cyber threats.

Digital identities can also support airport management and control with integrated security solutions that enable automated processes and walk-through screening checks that bring about shorter waiting times and better utilisation of staff. While there are many ways to bring about digital identity, biometrics provides a proven link between people's digital credentials and their physical attributes. As airports increase their investment in innovations, existing systems will be replaced with the biometrics scanners that ensure accurate identity match. Information captured by cutting-edge scanners will enable security personnel to assess passenger risk with speed and accuracy. As physical and cyber security measures become more intertwined, the need for real-time data, alerts, predictive analysis, and a central command center will become critical to anticipate threats and reduce the occurrence of human error.

Scenario

CRITICAL INFRASTRUCTURE



The use of digital identity will enable the critical infrastructure sector to leapfrog from a security-centric focus to one that optimises experience for greater speed, accuracy, and competitiveness

The priorities of critical infrastructure providers have traditionally been slanted towards ensuring security and uninterrupted operations. Taking such a cautious approach is understandable for the sector. After all, critical infrastructure is practically the most important foundation of any economy. Society's dependence on it cannot be understated. A cut in power or water supply will not only disrupt people's daily routine, it can affect people's health and result in physical harm under severe conditions. As a result, installing multiple layers of security checks are deemed necessary to verify the identity of employees.

Many of the conventional security solutions are such that a more effective system will be at the expense of experience. Employees today are given multiple credentials to authenticate their identities, resulting in a slower response time in carrying out their day-to-day work. But does it always have to be a case where security and experience cannot go hand-in-hand? And why should CxOs accord priority and resources for a better experience when they have more pressing issues to deal with?

Perhaps the concept of experience may be perceived to be overrated in light of the threats that the sector is facing. CxOs have more problems to grapple with than before. Nevertheless, to stay ahead and remain competitive, security should not be the only consideration factor of CxOs. Instead, decision makers should explore whether or not they are neglecting other aspects that are critical in driving productivity. Is their existing security system compromising and complicating employees' ability to safeguard their facilities?

Having said that, CxOs are well aware that critical infrastructure in future will eventually be fully automated in operating devices and systems. Whether or not significant gains can be further derived from employees' daily productivity will be debatable until the time comes. However, in the case of a crisis, the ability to authenticate identity and regulate the seamless movement of manpower within the vicinity will be critical.

When an unexpected event occurs, a non-operational security staff is the among first to receive an alert notification. In response to the alarm, he proceeds to investigate the cause of it. With conventional security systems, the employee has to stop at various checkpoints to validate his identity using his physical pass to enter restricted areas to see if any of the security systems such as cameras and locks have been breached.

Ideally, instead of relying on multiple credentials to verify authorised personnel, the use of digital identity will allow for a split-second verification that allows employees to cover the premises in a shorter time span. Operators of critical infrastructure will benefit from shaving off precious seconds of unnecessary identity processing.

Even so, this is possible only if the security personnel are within the premises of the critical infrastructure. But natural and man-made disasters can happen any time. During off-operation hours where there is nobody in the vicinity, employees have no visibility of the place unless the security system can authenticate their identities remotely using biometrics authenticated via the touch screen and/or a facial scan from the camera of their devices.

This is where digital identity will enable employees to gain access into the security system to see who has entered the building and their movements within the place. Conventional security systems such as the use of physical access tags will result in the need to make a trip to the site to investigate and generate a report. Time is wasted when ideally, emergency help should be called for without delay.

Even as the emergency response unit is called upon for assistance, gatekeepers face the challenge in verifying the identities of these people as they arrive to address the situation.

Ideally, the team should jump straight to action in a critical emergency setting. But a security staff will not grant entry to the premises of any critical infrastructure site unless he is certain of their identities and credentials. So time is lost in the verification process of identifying the emergency respondents and other third party contractors arriving at the scene, resulting in unnecessary delay and hassle. The process can be even more time-consuming for disperse facilities located across distant places.

There is a need for a security staff to respond to critical situations in a more effective and efficient manner. Conventional security systems using passwords, identify tags and cards are no longer effective in a mission-critical situation that requires prompt responses from multiple stakeholders. The use of digital identity empowers a security staff to access the system of restricted premises remotely upon getting an alert notification. So an immediate investigation can be launched without delay. Similarly, the use of digital identity for emergency respondents comprising their credentials, expertise, organisation and what they are authorised to do will enable the security staff to grant clearance with greater certainty and speed.

Hence, using digital identity will simplify worksite management where personnel coming from various sites can be mobilised and managed in a flexible and secure manner, leading towards greater cost savings.

Nevertheless, justifying the replacement of legacy infrastructure will inevitably face resistance in any organisation. An attempt in quantifying the return on investment using conventional financial metrics may not provide the best decision-making tool in the case of preventive measures because the idea is similar to measuring the ROI of an insurance policy. They will realise the value only when they need to make a claim. Instead, decision-makers should assess the value of the assets that they need to safeguard. They can quantify the potential cost of damages to machines and control systems, increase in insurance premium, loss in revenue, loss in data and downtime. There will also be an impact on intangibles such as their public image, consumers' loyalty, employees' productivity and time wasted. It is obvious that the critical infrastructure sector cannot afford the risk and impact of such consequences.

Decision-makers have to come to terms that preventive and proactive measures need to be taken to safeguard the assets that are critical to their business. Digital identity provides the essential means to optimise their resources that will sharpen their competitive edge.

Technologies Driving Digital ID

Leveraging on Technologies to Ensure the Rule of Three

Emerging technological tools are creating safer outcomes for critical infrastructure and airports. Increasing digitisation has been the key backbone for the growth of biometrics. In addition, the proliferation of biometrics is rapidly changing the public safety landscape.

Biometrics enables authorities and security personnel to address incidents in a near real-time manner for applications such as border control and facilities surveillance. While fingerprint scanning is the most popular technology, contactless technologies are rapidly gaining user acceptance. The pinnacle of contactless biometrics is in facial recognition, allowing solutions to be implemented with minimal friction for places with a high throughput of people.

While passwords and identification tags remain highly used to protect restricted areas, there is one thing they cannot offer which biometrics is able to provide. That is a proven link between people's digital credentials and their physical attributes. Advancements in biometrics technology such as deep learning for video analytics have made these technologies highly accurate, allowing authorities to pinpoint security threats to address some of the biggest challenges in public safety.

Supplementing the use of biometrics with video analytics improve surveillance and enable dynamic responses based on the output of the videos. Surveillance cameras that leverage on emerging technologies such as artificial intelligence are fast becoming integral in the video analytics space to improve performance, real-time threat detection, and efficiency of the system in border control and safeguarding physical access in critical infrastructure.

Video analytics is already being used for a wide range of applications to improve safety, security, and operational intelligence in perimeter breach, object classification, motion tracking, and people counting. And finally, cyber-security measures become paramount and have to be incorporated with physical security measures. It involves safeguarding systems, critical infrastructure and sensitive data. While cyber security is not a product-driven solution, it emphasises a holistic network monitoring, incident reporting and response at the department level. At the same time, cyber security threats cannot be solved with a unilateral approach. All stakeholders need to be involved to ensure the integrity, confidentiality, and availability of data.

Transforming Experience and Operations with Digital Identity

For people's identity to be the core of their digital experience, a more seamless and convenient authentication method is needed to transform security measures. Biometrics has become the ideal gateway to establishing a digital identity that bridges the gap between our physical and cyber identities. It can transform the experience of customers, employees, and bring a higher level of efficiency by enabling new applications and innovative digital services in public safety.

Together with emerging technologies like video analytics and cyber security solutions, an integrated suite of solutions can bring about the necessary security to combat sophisticated cyber threats in today's complex digital ecosystem. The future of public safety will set the foundation of customer experience transformation using digital identity that sets itself apart with convenience, secure credentials, and customer-centric applications.

Decision-makers and key influencers have many considerations in deploying a holistic security solution. It is important to appoint an established technology partner with a proven track record in public safety and the foresight to anticipate threats that do not exist today. NEC has invested substantially in technological innovations to safeguard against integrated cyber-physical attacks. It has been commissioned by a number of authorities to deploy an integrated suite of solutions that includes biometrics and advanced video analytics that visualise human behaviour, detect wanted individuals, safeguard restricted premises, and translate data into insights in real-time to support informed decisions.

NEC has been a pioneer in multimodal biometrics authentication with staggering advances over the years in terms of its accuracy as its facial recognition solution employs some of the most cutting-edge technologies in the world.

We Accelerate Growth

WWW.FROST.COM

Auckland	Colombo	London	Paris	Singapore
Bahrain	Detroit	Manhattan	Pune	Sophia Antipolis
Bangkok	Dubai	Mexico City	Rockville Centre	Sydney
Beijing	Frankfurt	Miami	San Antonio	Taipei
Bengaluru	Iskandar, Johor Bahru	Milan	Sao Paulo	Tel Aviv
Bogota	Istanbul	Mumbai	Seoul	Tokyo
Buenos Aires	Jakarta	Moscow	Shanghai	Toronto
Cape Town	Kolkata	New Delhi	Shenzhen	Warsaw
Chennai	Kuala Lumpur	Oxford	Silicon Valley	Washington D.C.

ABOUT FROST & SULLIVAN

Frost & Sullivan is a growth partnership company focused on helping our clients achieve transformational growth as they are impacted by an economic environment dominated by accelerating change, driven by disruptive technologies, mega trends, and new business models. The research practice conducts monitoring and analyzing technical, economic, mega trends, competitive, customer, best practices and emerging markets research into one system which supports the entire "growth cycle", which enables clients to have a complete picture of their industry, as well as how all other industries are impacted by these factors.

Contact us: Start the discussion

To join our Growth Partnership, please visit www.frost.com

ABOUT NEC

NEC Corporation is a leader in the integration of IT and network technologies with a presence in 160 countries and $25 billion in revenues. NEC delivers integrated Solutions for Society that are aligned with our customers' priorities to create new value for people, businesses and society, with a special focus on safety, security and efficiency.

For more information, visit NEC at www.nec.com