SmartCitiesWorld
White paper

Keeping the lights on

How to ensure connected lighting systems are and remain secure throughout their lifecycle

In association with

signify

Written by

Sue Weekes
News editor,
SmartCitiesWorld

***SmartCitiesWorld* White paper reports examine an emerging or growing trend in smart cities, highlighting progress so far and future potential, as well as spotlighting case studies from cities around the world.**

In this report, we examine how to ensure robust, end-to-end cybersecurity in connected lighting deployments.

www.smartcitiesworld.net

Securing connected lighting

Cybersecurity frequently hits the headlines but usually when it is too late, following a high-profile attack which has cost an organisation dearly. In 2020, the FBI said that the number of cyberattacks being reported to its cyber division was as many as 4,000 daily. It is a global problem: the European Union Agency for Cybersecurity (ENISA) says cyberattacks are becoming more “sophisticated, targeted, widespread and undetected”. In its 8th annual Threat Landscape report, published in October 2020, malware ranks as the number one threat, while the number of potential vulnerabilities in the virtual and physical environment continues to expand as a new phase of digital transformation arises.

The connected world brings a raft of opportunities but also a myriad of threats from the point of view of ensuring systems always remain secure. This report focuses on connected lighting and aims to highlight the importance of having robust end-to-end security measures in place. It contends that a model of shared responsibility is the best approach and highlights why cloud-based systems rather than an on-premise IT infrastructure is better suited to the demands and rigours of today’s connected world. It also aims to explode a number of myths that can cloud an organisation’s decision-making in this area and seeks to share best practice, based on Signify’s experience with customers around the world.

Cybersecurity: who takes responsibility?

The impact that a cybersecurity attack can have on IT systems is well understood, but organisations also need to understand how quickly their operational technology can be impacted. To illustrate this, consider the following worst-case scenario, which could happen if the right security measures are not in place.

An employee in a tunnel control centre in the south of Germany is tricked into opening an email attachment, unwittingly triggering a crippling ransomware attack. The centre controls crucial tunnels for traffic to France and Austria and a malware trojan horse is able to travel from the office IT system into the wider network.

The cybercriminals behind the attack are able to encrypt files and manipulate programmable logic controllers, blocking access to tunnel monitoring and controlling overall systems. Striking at rush hour, the ransomware attack succeeds in shutting down the lighting in all of the connected tunnels, which leads to vehicle accidents. This also creates difficulties for emergency services trying to rescue people. Due to loss of operations and control, 44 tunnels have to be shut down manually.

The incident creates congestion and further accidents on alternative routes to neighbouring countries. The transportation of goods is obstructed and emergency services become overwhelmed.

A message informs the tunnel control system administrator that data had been encrypted and would only be decrypted after the payment of one bitcoin (valued at €7000). Despite the ransom being paid, the attackers do not provide a decrypting key. This means the operator has to bring in an external specialist to help deal with the situation at significant cost. The recovery period lasts six weeks.

The trojan had been able to leap from the IT to the operating technology (OT) because the systems were not physically or virtually separated or protected from each other, creating a vulnerability. While the employee was innocent in their actions, resulting press coverage would have a negative impact on the public's relationship with, and trust in, the road authority and the government.
A broader platform for attack

As ENISA points out, as digital transformation gathers pace in public and private sector organisations around the world, the potential for vulnerabilities is also expanding. In particular, connected environments and Internet of Things (IoT) networks are broadening the attack platform for cybercriminals. Organisations must therefore understand the risks and have the right safeguards in place to mitigate them.

> *“The best defence to any cybersecurity attack is to build in end-to-end security by design”*

The root causes of attacks are many and varied but can be as basic as poor password management. In 2020, the lighting on a bridge in the Netherlands was reportedly publicly accessible and it was now possible for unauthorised personnel to adjust it. The news channel tested it by colouring the bridge pink and then in the colours of the rainbow.

Recent research carried out by Signify reveals that cybersecurity is a major concern for connected lighting clients, with their main categories of risk around the disruption of operations and unauthorised access to data.. There is recognition that the lighting system is a possible entry point for the attack, and that the light itself can come under attack, but these vulnerabilities can be overlooked due to the pressure of everyday operations.

A cybersecurity manager at a major global port said that his biggest concerns around lighting and IoT systems are keeping up with the latest developments in security, most notably in identity access management and software updates. Additionally, he raised concerns about how such solutions are maintained by third-party providers.

Security by design

The best defence to any cybersecurity attack is to build in end-to-end security by design. “We often use the terminology ‘built-in’ versus ‘bolt-on’,” says Fabio Vignoli, head product security lead, Digital Solutions Division, Signify. “So this means built-in from the requirements of the system, through to the design, implementation and testing of the system. Any company that provides such solutions needs to have a proper security development lifecycle.”

Cybersecurity is a highly complex area and the rise of networks which connect an array of different devices adds to this. As Eng Yong Liang, global cities segment director, Signify, points out, there are misconceptions that hacking only happens via the internet or networks which are exposed to the internet. “Security vulnerabilities in the physical devices such as gateways, end-devices and user ID management are often overlooked,” he says.

Data and cybersecurity are typically not a customer's areas of expertise, so choice of partner and approach is crucial. If a customer chooses a cloud-based approach rather than an on-premise one, it will have a “lighter share” of the responsibility for managing security systems, explains Vignoli. “The cloud provider will take care of a large part of the responsibility and the lighting vendor would take care of pretty much everything else such as encryption and back-up. This leaves the customer with the responsibility for safeguarding passwords, user identities and other account management issues. Vignoli adds: “This is why it is so important that the city chooses a true partner who is able to manage and monitor security for both the IT and OT systems.”

The tunnel cyberattack scenario shows what could happen if ransomware is able to leap from IT systems to the network handling day-to-day operations. It is critical, therefore, that an organisation's cybersecurity partner operates to the highest security standards in both areas.

Exploding the myths around cybersecurity for IoT and operational technology

Cybersecurity is a highly complex area, and a lack of knowledge and proper understanding of it can lead to both confusion and misconception. This, in turn, can result in poorly informed decision-making when it comes to buying and implementing systems and services. Here we explode three common myths when it comes to the security surrounding connected technology and how it is implemented.

Myth 1: A product that is developed securely will be installed in a secure way
Reputable connected lighting manufacturers are committed to designing their systems from the ground up in a secure way. Security should be a key consideration throughout the systems development lifecycle when it comes to both hardware and software.

Processes built into the system will include encryption according to industry accepted standards, external penetration testing, automated code analysis and security testing, and hardening of operating systems.

This means that at the point of installation, the system is as secure as it can be, but it is what happens after this point that determines its future security. Systems integrators may tweak elements of the system or make shortcuts that introduce vulnerabilities, especially in the case of an on-premise system. And it may not necessarily be in the installer's interest to go back and make it secure, because that takes more time and effort.

Robust credential management is also key to ensuring that a system developed securely is installed and run securely. This may be put in place at the point of installation, but if those credentials are shared or if there is a complacent approach taken to security – usernames and passwords put on a Post-It note on the wall, to give an egregious example – the system is no longer secure and is accessible by anyone. "This is the most outrageous way of installing a system in a non-secure way but it is one that repeatedly happens," says Vignoli.

Vulnerabilities can also be introduced if the system is connected to a shared database or a legacy system that isn't secure or password protected. Hackers can then access the system through one of these points. Similarly, the communication protocols used to integrate software and devices in a connected lighting installation may not be secure and may again introduce weak points. "A fragmented system put together with components from different vendors may not have the same rigorous system security design," says Yong Liang. "And security is only as strong as the weakest link in the chain."

> *"Security is only as strong as the weakest link in the chain"*

> *"Everything is interconnected, and you can't look at IT and OT as if they are separate anymore"*

These problems are far more likely to arise in an on-premise system than a cloud-based one. The advantage of the cloud-based approach is that the technology vendor will take care of security in the cloud. The cloud service provider looks after security of the cloud on a 24/7 basis, so any weak points that appear in the system will be detected and dealt with.

Myth 2: A securely installed system will stay secure
Even if a systems integrator takes every effort to ensure a system is securely installed, there are a host of reasons why it may not necessarily remain that way. An on-premise system is once again more vulnerable to this happening.

Threats include the impact of changes of personnel not being handled properly at system level. If credentials are not removed immediately, the system can become vulnerable to use by non-authorised personnel. There are many instances of people leaving companies but who still have access to a system.

Another potential weak spot is when a company has a securely installed system but decides to integrate it with a legacy one. This often involves opening a port to get the systems talking to each other, which automatically and inevitably creates a potential threat. "Every time there is a change in the firewall rules, every time there is a change in the IT structure, every time a database is updated, there is a risk that security will not be maintained," says Vignoli.

Even if everything is locked down on the on-premise system, there are external challenges that impact the IT environment, such as the emergence of new viruses. In such cases, systems need to be patched to protect them. This is not a one-off threat, though, and during its lifecycle a system is likely to require a number of software patches to ensure security is maintained.

Many companies simply do not have the resources to stay on top of this. Indeed, the need for ongoing monitoring and the ability to respond to new threats is one of the biggest points in favour of taking a cloud-based versus an on-premise approach, largely because it becomes the responsibility of a vendor with the expertise of dealing with these threats.

> *"You need to have the right balance and make sure that the triad of confidentiality, integrity and availability is satisfied"*

On-premise IT means that the customer has responsibility for owning, building and running its end-to-end IT infrastructure. While the IT department will shoulder the responsibility for set-up, maintenance, security and back-up, the day-to-day running of systems and processes will often be decentralised. And IT will often take a server-centric approach with a major focus on the physical assets rather than what might impact the security of the system on an ongoing basis.

The on-premise approach also means that organisations must continually invest in IT security expertise to keep pace with emerging threats. And, in the event of an attack, the organisation bears responsibility and the cost of identifying where and what has happened and recovering from it.

By contrast, cloud computing shifts a large part of the ownership, responsibility and day-to-day running to the vendor and cloud provider. Continuous updates are automatic, and the partner companies also have the capacity and resources to continuously monitor the system to ensure it remains secure and compliant. This will also involve testing on any third-party systems or devices that are part of the installation. Indeed, their whole focus is on protecting the customer's day-to-day operations, data and systems.

Technology vendors and cloud providers also have robust incident reporting and recovery processes in place so if there is an attack, the recovery time will be far quicker than in an on-premise situation. Such companies also benefit from having learned the lessons of other customers' experiences, which help to inform procedures and activities.

Myth 3: Operational technology and information technology are two separate activities

Technology has become increasingly connected, especially in the era of wireless connectivity and the IoT. According to the analyst IDC, there will be 41.6 billion IoT devices in operation in the field by 2025.

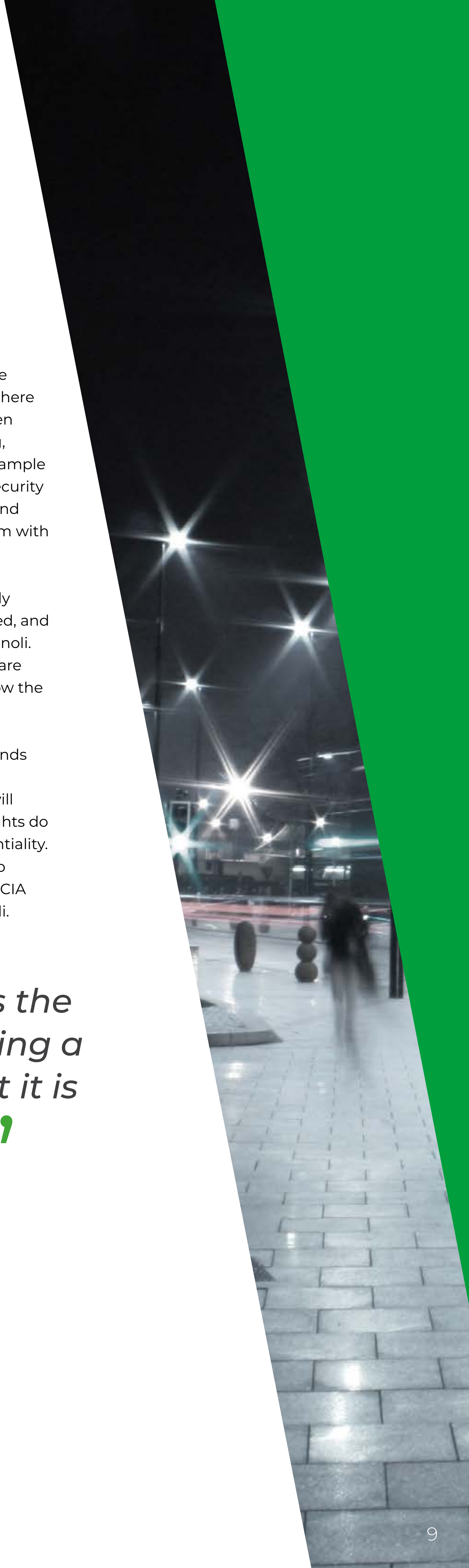
It used to be that information technology (IT) and operational technology (OT) existed as separate entities, but that has changed. In the connected world in which we all live, organisations need to understand that anything that happens to their OT can have a serious impact on the IT infrastructure and vice versa. The attack on the German tunnel showed how quickly a piece of ransomware can disrupt an entire system.

There are many other examples that show how attacks can occur on one part of a system and have a devastating effect elsewhere. For instance, there have been instances where customer credit card details have been stolen after a cybercriminal was able to enter the network through the heating, ventilation and air conditioning system. Similarly, there is a notorious example of cybercriminals using a fish tank as a means of bypassing a casino's security system. Criminals stole a wi-fi connected thermometer from the tank, and because the thermometer was not password-protected, it provided them with an easy back door to open.

Connected lighting installations are vulnerable to similar risks, and it only takes one insecure device to let a hacker in. "Everything is interconnected, and you can't look at IT and OT as if they are separate anymore," explains Vignoli. "Organisations need to be far more aware of this and understand there are implications in the way devices on a network are managed as well as how the information that is received by them is handled."

Customers need to look for a technology partner that not only understands this but whose system has been developed to make sure the IT and OT components conform to the highest security standards. OT standards will typically focus on availability – so, in the case of lighting, ensuring the lights do not go out – but they will not necessarily focus on integrity and confidentiality. There tends to be a much stronger focus on the latter in IT, in addition to availability. "You need to have the right balance and make sure that the CIA triad [of confidentiality, integrity and availability] is satisfied," says Vignoli.

> *"Poor password management is the most outrageous way of installing a system in a non-secure way but it is one that repeatedly happens"*



The Signify approach to secured connected lighting

To avoid the dangers highlighted in this report, customers must look for a technology partner that can ensure the connected lighting system is not only securely developed and installed but remains so throughout its lifecycle.

Signify is the global leader in lighting, with its systems managing more than 71 million connected light points around the world. There are more than 2,500 of its Interact connected street lighting systems in use across 58 countries. Interact offers a flexible, cost-efficient, scalable lighting system for many professional applications, from smart cities to smart buildings, warehousing and manufacturing, retail, sports facilities, highways, and hotels. With connected luminaires and two-way data communications, Interact uses the lighting infrastructure as a foundation for distributing a wide range of IoT capabilities throughout the lit environment.

Interact collects and analyses data from connected luminaires, sensors and other devices to provide actionable insight. It can also integrate with other IoT services and solutions, such as smart building and smart city platforms. Given the tasks it performs, Interact has been designed with the highest cybersecurity standards from the ground up.

Signify encourages customers to run Interact from the cloud, rather than on-premise, and the company partners with global cloud service providers to offer a resilient end-to-end platform on which to build.

When cloud computing first appeared, there was concern and considerable debate about how secure it is compared to the on-premise approach. After all, it involved entrusting a third party to host systems and data outside of the organisation. But the idea that on-premise IT is more secure than the cloud is fast becoming an outmoded view. Moreover, the workload and responsibility it brings compared to the cloud approach from a cybersecurity perspective means the cloud-based options are becoming the preferred route for many applications.

Signify's aim is to exceed market and customer expectations when it comes to security. Significantly, it is the only connected lighting provider that has certification for OT (IEC62443) as well as IT (ISO27001). It helps customers achieve their security goals through strong governance, ensuring end-to-end security by design, operation and maintenance activities and robust incident management processes.

> *"Anything added to the system must be developed using secure design principles to minimise vulnerabilities"*

Three-tiered approach to security

Viewing security as a shared responsibility, Signify puts forward a three-tiered model for cloud-based implementations, which sees the customer taking responsibility for ensuring security in their processes; Signify making sure that everything happens securely in the cloud; and the cloud service providers having responsibility for the security of the cloud itself.

"This shared responsibility with manufacturers is a key part of the customer's defence-in-depth security strategy," explains Vignoli.

Under the three-tiered shared model for the cloud, the areas of responsibility break down as follows

Customer	
Security of operations	
Credentials	
Identity management	Installation of field devices

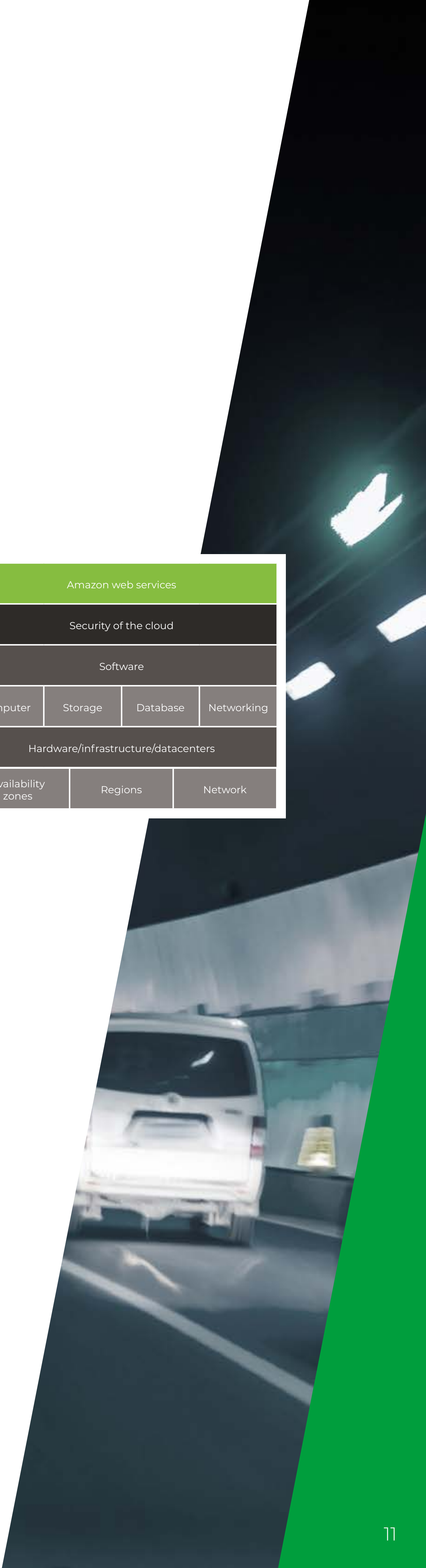
Signify and interact			
Security in the cloud			
Customer data			
Platform	Application	Identity	Access management
Operating systems			
Encryption at rest, in transit	Data integrity, backup	Network protection	

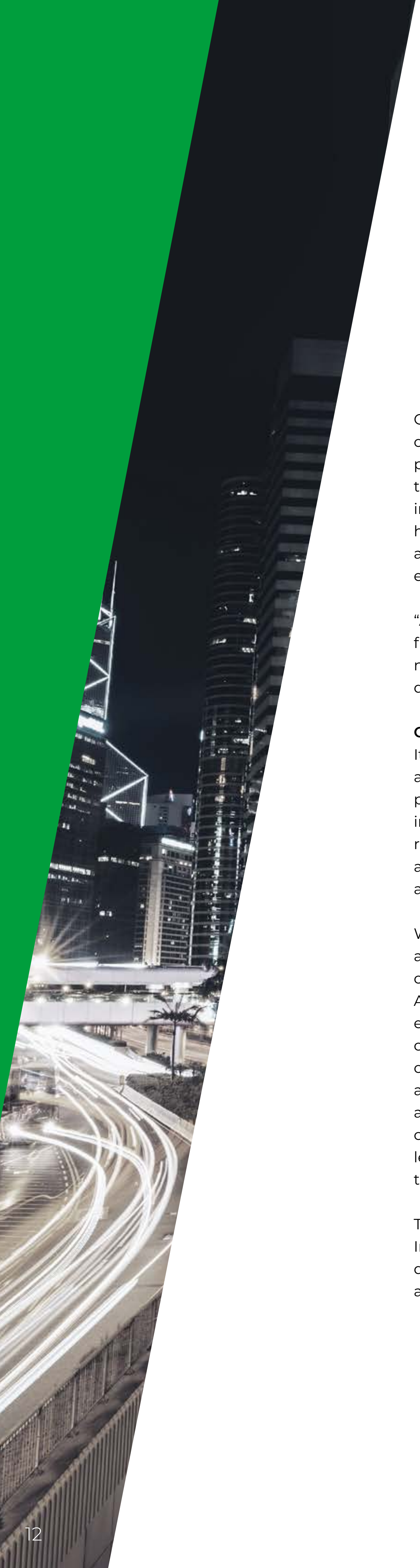
Amazon web services			
Security of the cloud			
Software			
Computer	Storage	Database	Networking
Hardware/infrastructure/datacenters			
Availability zones	Regions	Network	

Signify ensures security in the cloud via a number of measures, including:

- applying continuous security updates
- regularly updating the system against security vulnerabilities
- analysing vulnerabilities and assessing what could happen if they were exploited
- assessing the likelihood of exploitation and making an overall risk calculation
- conducting third party penetration tests periodically to ensure security resilience and static code analysis from an independent third party when required
- compiling a prioritised list of threats and recommended mitigations for final security requirements

In an on-premise installation, the vast majority of the duties carried out by Signify would shift to the customer. Taking the cloud-based approach, Vignoli recommends that in addition to the above advanced security capabilities, customers should also demand help to secure installations and to ensure the system remains secure. "Anything added to the system must be developed using secure design principles to minimise vulnerabilities," he adds.





One of the challenges to remaining secure after installation is the evolution of the system. For example, connected lighting systems are often the starting point for a smart city, which means other vertical applications can be added to the connected infrastructure. It is important that the technology vendor and installer understand the security implications of this. As Yong Liang has already highlighted, any security is only as strong as the weakest link and not all device and application vendors have the same rigorous system security design. For example, Signify has built security into its luminaires.

“An end-to-end offering from a system vendor in which the vendor has full ownership of all the components of the system from end-devices to networking to application security and database ensures the complete system design is secure,” explains Yong Liang.

Operations and incident management
It is important that customers understand that a cyberattack and breach is always a possibility but can be reassured that Signify has a set of established procedures to respond to any suspect attacks. In the unlikely event of an incident, a strict recovery process is in place. Access to systems will be restricted immediately and systems are isolated. Data can be easily restored, as back-up is performed on a continuous basis . Application infrastructure can also be easily restored.

While robust cybersecurity is about having the right processes, procedures and policies in place, it is also about trust and confidence between the customer, vendor and other third parties such as a cloud services provider. A cybersecurity professional from an international airport said that they have experienced companies over-promising on security and compliance, which can seriously erode trust. When asked about the security requirements for connected/IoT systems in the organisation, they said that they “suggest and request” suppliers comply to certification or standards such as IEC62443 and ISO27001. They also invest in a broad range of security services, including consulting and design implementation, describing them as part of the legacy and governance structure. “They are not a choice; this is a must-have,” they added.

The customer survey undertaken by Signify showed that more than half of Interact customers have a chief information security officer (CISO) and/or a dedicated cybersecurity team. Typically, they are part of the IT department, and those that are separate collaborate closely with IT. Security requirements and approvals are decided by the CISO or IT director in these cases. At the other end of the scale, though, some customers define themselves as immature when it comes to cybersecurity requirements and will need to rely on technology providers to ensure systems remain secure.

The majority of organisations are taking the lead from their IT departments and applying the same extensive security requirements as defined by the CISO and are also alert to issues surrounding personal data.

An example is a security manager at a grid operator who stressed that its biggest concern is including personal data and system data. They don’t want third parties to access and use or even sell that data for their own benefit.

The connected lighting and IoT security services landscape is still evolving. Customers largely expect security services to be part of, not separate from, the system vendor’s offering, but some opt to buy from companies that are independent of the vendors. Going forward there is also likely to be more demand for extended services such as training and security certification and integration with IT networks. Who provides these services will vary, but it is important that organisations continue to see security as a shared responsibility and exercise due diligence when choosing providers. The goal should always be robust and continuous end-to-end security throughout the system’s lifecycle.

> *“Robust cybersecurity also requires trust and confidence between the customer, vendor and other third parties”*

Conclusions

Securing a smart and connected future

Digital transformation is taking place in cities and public and private sector organisations around the world. Connected lighting, whether for functional or aesthetic reasons, is factored into many strategies because it brings energy cost savings and makes a major contribution towards reducing a city or organisation's carbon footprint. As highlighted in this report, though, without the right security measures in place, it can also be an entry point for a crippling and costly cyberattack.

As the technology gets smarter and more sophisticated, then so will cybercriminals and the approaches they take. The majority of customers surveyed by Signify accepted that security requirements will only become more strict, more international and more standardised. While it is difficult to predict the shape of the attacks to come and how security vulnerabilities might be exploited in the future, there are a number of best practices that can be put in place to mitigate the risks. These include ensuring security is designed and built in rather than bolted on at every stage of a connected lighting system's evolution.

Defences can be further bolstered by all parties involved buying into a model of shared responsibility and understanding where the demarcation lines begin and end. This will ultimately be easier for the customer if they make the shift in thinking away from on-premise models to a cloud-based approach, where security of systems, data and servers is the responsibility and core competency of the technology partners.

About Signify
Signify is the world leader in lighting for professionals, consumers and lighting for the Internet of Things. Its energy efficient lighting products, systems and services enable customers to enjoy a superior quality of light, and make people's lives safer and more comfortable, businesses more productive and cities more liveable. With approximately 36,000 employees and a presence in over 70 countries, the company aims to unlock the extraordinary potential of light for brighter lives and a better world.