The Smart Society

Towards smart, secure and future-proof infrastructure

eurofiber

The smart society: towards smart, secure and future-proof infrastructure

We live in a world that is going digital at an accelerating pace. What will our digital infrastructure look like in 2030? What security risks will we have to deal with then? And... how can your organization prepare for the future ahead?

Technological developments are emerging one after another, faster and faster. These emergent trends have a huge impact on the digital infrastructure of our country. We are currently experiencing a huge surge in connectivity and more and more devices are connected to each other; just consider the Internet of Things and Machine-to-Machine solutions. This requires a huge expansion in the capacity of our networks –especially fiber optic connections that will need to carry most of that growth. Companies and government institutions also need to work in closer collaboration to provide a basis for as many smart applications as possible.

In this eBook, we will start by taking you to 2030. We will share our vision for the ICT infrastructure of the future. You will also read about which security risks are likely to occur and how you can configure your future-proof infrastructure for 2030 to achieve a secure and reliable ICT landscape.

Contents

Smart infrastructure for a better future

The ability to rely on a secure ICT infrastructure is crucial for the future of organizations. More and more devices are connected to each other and employees want to have access to the company network anytime, anywhere. What will our infrastructure look like in 2030? Bart Oskam, Eurofiber COO, presents his vision.

One thing is clear: by 2030, using the internet will be as normal as breathing. Internet use will have increased enormously, and the same also holds true for the standard capacity of the underlying network. That does raise the question, of course, of what kind of network we are talking about: will all communication be completely wireless soon, and will land lines become redundant? The answer is no.

Will all communication be completely wireless in 2030 and will land lines become redundant? The answer is no.

In 2030, we will still use a combination of the two, simply because it is impossible to make everything wireless. There will always be a need for super-fast lines to send data from one transmitter mast to the next.

The signal is everywhere

What the future will bring is a fiber optic network connected to a great number of wireless antennas. At certain locations, the antennas will be clustered in very dense proximity, for instance along major motorways. After all, when we're talking about applications such as self-driving cars, it would be disastrous if the signal were to fail even for a second: the network will have to be 100% reliable. Creating such an infallible network is no small challenge for the telecom sector.

Fiber will also be the foundation for mobile communication through new types of networks. In networks, independent transmitters will create connections with each other automatically, ensuring that we communicate with each other directly without any need for a transmitter mast. This aligns with the trend in society to do more and more things locally.

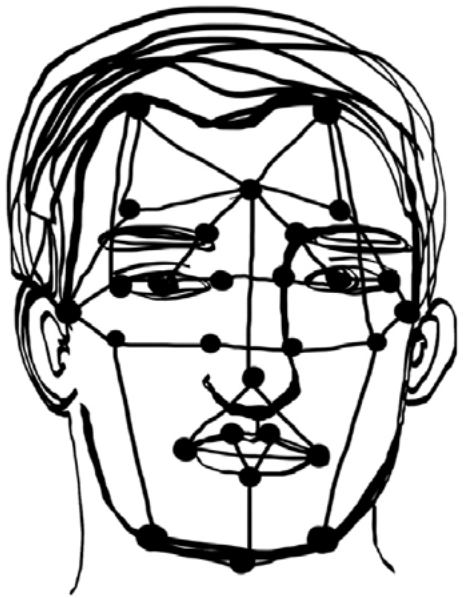
Huge gains in speed

Fiber is also the technology of the future in terms of bandwidth: there is still huge room for progress there. At the moment, our labs are working on 'hollow fiber', which will make it possible to transport even more data at much greater speeds. However, the biggest improvements will not even be in the fibers themselves, but in the devices that we use to light them. Currently, we already have 108 channels providing 10 Gb/s at our disposal over just one fiber. In more tangible terms: it is possible to send two weeks of non-stop HD video from Amsterdam to Paris in a fraction of a second. That would have been inconceivable five years ago. By 2030, bandwidth will have increased exponentially again: in essence, the capacity is limitless.

It will be possible to send two weeks of non-stop HD video from Amsterdam to Paris in a fraction of a second. That would have been inconceivable five years ago.

Self-learning networks

We can also expect much smarter networks. More and more fields are using artificial intelligence or self-learning computers. Examples include online translation services and search engines, or Tesla's smart car. The same trend can also be observed in public infrastructure.
For example, if you are taking a high-speed train from Amsterdam to New York and want to send a video at 16 Kb/s, then the network will automatically ensure that you have the bandwidth you need for that. This does demand public debate: who would be in control of a network that configures itself so automatically? There should be no room for any error in differentiating between data traffic, applications or users.



Data on your wearable

Increasing bandwidth on the network has eliminated the need to store data in a central location. Data will be saved for the most part on all the various connected devices, from mobile phones and other wearables to all kinds of objects. It is also conceivable that people will share storage capacity on their devices: when they have spare capacity, they can automatically make that available to others.

More secure due to fragmentation

In response to these trends, the role of data centers will change in the next fifteen years. They will turn into something more like central checkpoints, with intelligent applications to manage data remotely. Together, all that geographically fragmented data forms virtual data bases that can be accessed centrally. In contrast to what you might expect, this actually improves security: hackers can only do something with the data once they have access to all the saved fragments. The only thing they should not get their hands on is the key to read all the fragmented data as a whole.

Hackers can only do something with the data once they have access to all the saved fragments. The only thing they should not get their hands on is the key to read all the fragmented data as a whole.

Quantum mechanics

In general, networks and data centers will increasingly fuse into a single entity by 2030, which will make it harder to identify how things have been fragmented. We could also have completely different storage media by that time, unlike anything we can think of right now. A countertop loaded with electrodes, say.

Another exciting development is quantum mechanics. By applying this technology to data processing, we can achieve much higher speeds, especially when combined with optical switches. Right now, electronic switches are still used in computer chips. It is key that we make higher speeds possible in every way, including data transport as well as data storage and processing.

Resolving the major challenges of society

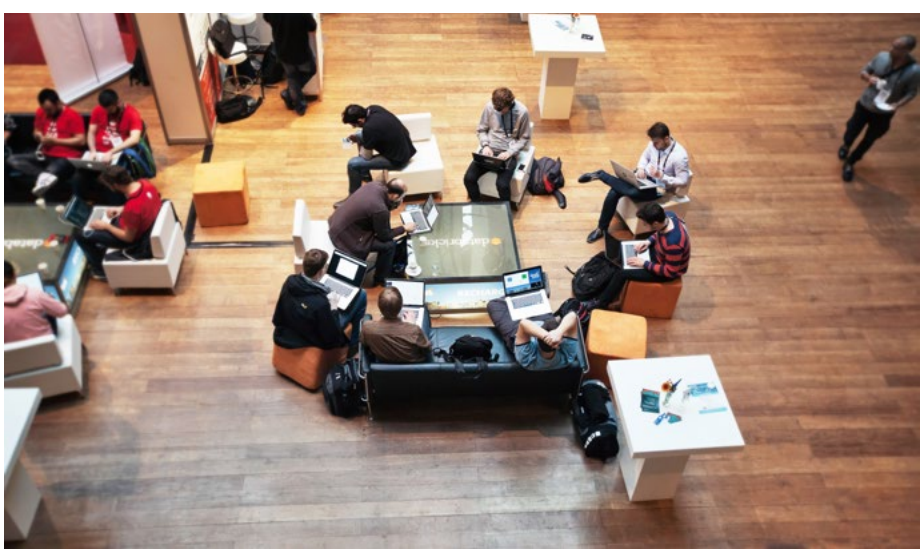
So how will we use this new digital infrastructure in the future? It will in any case be focused on facilitating our lives and improving the way we work in every respect.

Along the way, we should not forget that a stringent regulatory framework is needed to guarantee that our digital infrastructure will comply with the very highest standards .

Future security risks at a glance

More and more devices will be connected over the next years. This means that we will be able to communicate and work faster, anywhere and anytime. This trend will make it increasingly easier for us to live and work.

To make the most of that smart society and its benefits, you should not underestimate the risks that are inherent to this smart society. Since all the devices in your organization will soon be connected to each other, and your employees will be working from many locations, it is vital to ensure that your business-critical information is properly protected. Cybercriminals are already a danger to organizations, and this risk will only increase in the future. All those many, many connected devices will give cybercriminals more and more opportunities to carry out their attacks. So what can we expect from the future of cybercrime?



Cybercrime Europe

Every year the Cyber Security Centre publishes the Cyber Security Assessment. Its purpose is to provide insights into developments, interests, threats and vulnerabilities in the field of cybersecurity. Recent research has revealed a number of serious risks, which should not be underestimated in the private or public sector. McAfee's Threat Predictions Report also addresses key future risks. In the following sections, we will discuss three key future security risks that emerged from these risk assessments.

1. Ransomware: the new business model of cybercriminals
2. The danger of wearables connected to smartphones
3. Vulnerabilities in software negate digital security

Ransomware: the new business model of cybercriminals

Cybercriminals are increasingly using ransomware, like cryptoware, to achieve their goal. This type of malware works on this simple premise: hackers can use ransomware to lock the computer of their victims – 'taking it hostage''. As soon as the victim wants access to their computer and tries to access their files, they get a message that this is only possible if they pay a ransom. Since organizations do not want to lose their valuable business information, many are willing to pay the ransom.

Over the past years, we have seen a spike in the number of ransomware incidents. These attacks have mainly affected organizations. According to the CSAN report, office automation environments were targeted most often last year.

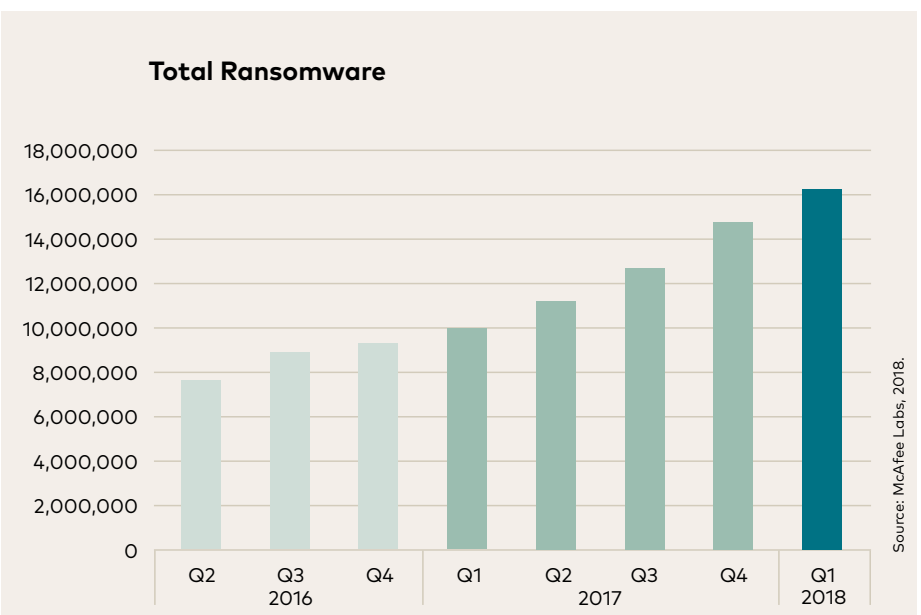
A frequent cause of ransomware infection is reading personal emails at work. This is because the ransomware is often hidden in emails.

Ransomware is already a major threat to organizations. Even though this malware does not immediately destroy your sensitive business information or make it public, a ransomware infection can be very expensive. New ransomware versions continue to flood the market; the total number in the first quarter of 2018 was already 150 percent higher than the year before. You can see this sharp increase in the following graph from the McAfee Labs Threats Report 2018. As you can see, cybercriminals have not been idle. They are currently already looking for ways to infect other media, for instance SD cards and USB drives.

The danger of wearables connected to smartphones

The number of wearable device is increasing rapidly. In the Threat Predictions Report, McAfee indicates that one in ten people in the world has a wearable device. This includes such devices as the Apple Watch. A hacker does not get immediate benefits from hacking a wearable. However, that becomes a different story when the wearable is connected to the smartphone of the person wearing it. The danger of wearables connected to smartphones The number of wearable device is increasing rapidly. In the Threat Predictions Report, McAfee indicates that one in ten people in the world has a wearable device. This includes such devices as the Apple Watch. A hacker does not get immediate benefits from hacking a wearable. However, that becomes a different story when the wearable is connected to the smartphone of the person wearing it.

Bluetooth has a large number of security errors. When sending wearable data to smartphones and tablets, Bluetooth is the weakest link and absolutely not secure at all.



Wearables are a nice addition to society and to business. They encourage and facilitate easy communication and interconnectedness. Unfortunately, they add an additional security risk and a new attack opportunity for hackers, precisely because of their increasing popularity.

Vulnerabilities in software negate digital security

The Cyber Security Assessment shows that vulnerabilities in software are also major threats to organizations. The report states that software is a crucial part of our digital infrastructure.
Consider the Heartbleed Bug, for instance. The vulnerability in OpenSSL made it possible for cybercriminals to remotely read out the internal memory of systems. Another example is a POODLE attack, which takes advantage of a vulnerability. POODLE was an exploit that allowed attackers to hack into secure connections using SSLv3.
Providers have been trying to solve these vulnerabilities by releasing updates. However, many organizations do not see the need for frequent updates, or are concerned that the updates will conflict with other programs, they often avoid installing updates at all – so the vulnerabilities remain a risk. Research shows that 39 percent of the computers investigated

were still running older, non-secure versions of Java, Adobe Flash or Adobe Reader. Hackers use identified leaks in these software programs to get in. As long as the updates have not been installed, your company network remains vulnerable. Now that organizations need software more and more often, such as all the applications and solutions involving the Internet of Things, you need to have a stricter policy that all updates need to be implemented consistently.

Software updates are just as important to protecting computers as virus scanners.

5 steps to a secure, future-proof infrastructure

As the previous chapter explained, the main risks to our smart society are caused by the major increase in cybercrime. The three threats we discussed in this chapter are just the tip of the iceberg. Cybercriminals can strike in many other ways. How do you make sure that your organization is set up as securely as possible, while still reaping all the benefits of our smart society?

In this chapter, you will learn in five steps how to make your infrastructure secure and future-proof.

Step 1:

Choosing the physical infrastructure

Is your infrastructure obsolete? Should security be improved? And do you want to configure your environment more efficiently, so you get more out of your current IT hardware? Then it is time to explore the possibilities for a new IT infrastructure that meets your needs. But how can you tell which network will be the best and safest choice for your organization?

Dark fiber

When security is a high priority, the best choice is a managed dark fiber connection. A fully dedicated conduit is the most secure option, but this is neither feasible nor affordable for most organizations. An organization needs to have substantial knowledge and expertise within its workforce in order to light the fiber. Don't have that knowledge in your organization? Then a lit fiber optic connection would be a good choice. In that case, a telecom provider not only delivers an unlit fiber, but also provides the lighting equipment.

DWDM of Ethernet

The choice between DWDM or Ethernet depends on the bandwidth required. If your organization needs high bandwidth, often in combination with a storage solution, you'll want to opt for DWDM. If a transport connection is needed to connect users to the data center, Ethernet is often the preferred choice. Privacy-sensitive data should preferably not be transmitted via public internet, since such a public channel offers hackers many opportunities to intercept data.

You can choose from a range of options for your infrastructure:

- **Dark fiber** is an unlit fiber optic connection. With dark fiber, organizations install their own equipment to light the fiber. This type of connection is often used to transport massive volumes of data, up to 100 GB/s or more, in which organizations can make their own decisions regarding bandwidth.
- **DWDM** stands for Dense Wavelength Division Multiplexing. DWDM can be used for all data communication protocols, including Ethernet, Fiber Channel, SDH and non-compressed video. Each service has its own light path, which makes WDM extremely secure. The combination of WDM technology and fiber optics makes it possible to achieve speeds up to 1.6 Tb/s, which will provide organizations with sufficient data transport capacity for even the most demanding applications.
- **Ethernet** technology that has been used for years to provide secure connections between connect offices, employees and data centers. Based on the ethernet protocol, a virtual private network can be configured for secure transport ICT services such as internet, telephone and video. Combined with fiber optics, it is possible to achieve speeds up to 5 Gb/s.
- **Coax**, also known as 'cable' (as in 'cable TV'), is mainly used for internet, television and radio and for consumer telephone services. In general, there is usually only one cable service provider in each region, which limits the choices available to organizations.
- **DSL** stands for Digital Subscriber Line. Unlike fiber optics, DSL does not have symmetrical bandwidths by default and can achieve maximum speeds up to 50 Mb/s (VDSL). DSL is mostly used by small and medium-sized organizations.

Step 2:

Protecting your data

The European General Data Protection Regulation (GDPR) has entered into force. The GDPR requires the best possible protection for personal data and other sensitive information of individual citizens in the European Union. That places certain demands on organizations that work with that type of data. IT in general and network connectivity specifically are crucial in that context. According to the GDPR, organizations are required to protect sensitive data, for instance by means of encryption. The European legislator has also decided that said information should be sent from A to B in a secure manner. Encryption is an absolute necessity here.

Encryption locks data up using algorithms, ensuring that it is useless to malicious parties if it is unexpectedly stolen or lost, since they cannot decrypt the data. Encryption can take place on different layers in the OSI model and depends on the application of the connection. The higher the level of the OSI model where the encryption is added, the more latency it adds, which could slow down the connection.

The benefit of encryption on layer 3 (Ethernet) is that it is possible to differentiate between data that needs to be encrypted and data that can be left unencrypted, because all traffic is encrypted on the lowest layer using hardware-based encryption. This means that the most logical place for encryption depends on the application.

A data encryptor scrambles data in such a way that it is nearly impossible to decipher stolen data. It is crucial to define a good encryption key that is changed regularly and has various bICT lengths (the longer it is, the harder it is to hack). In addition, encryption needs to adhere to the most commonly used standards, such as AES (Advanced Encryption Standard) based on the American FIPS (Federal Information Processing Standard.

Step 3:

Choosing a data center and making choices in the data center

A safe infrastructure provides secure data transport between the data center and the organization. That means that the choice of data center is closely tied to the security of the data. All the precautions of a secure infrastructure will be completely negated if security measures at the data center are insufficient.

The physical security of the building is key to ensure that uninvited guests cannot get to the systems. ISO 27001 and NEN 7510 security standards offer guidelines for the desired level of security. A data center also has various options for providing extra protection for vulnerable data, such as building a cage or suite around the equipment.

Step 4:

Monitoring of the network

Disruptions in the network can be detected by means of monitoring. In the event of a dark fiber connection, it is the customer that monitors the active equipment in the network.

When a customer has arranged a lit fiber optic connection, the monitoring is done by the organization as well as by the telecom provider. The provider can see what's happening on their own network, while the customer has a comprehensive overview of everything, including their own network and the equipment in it. If any disruptions occur, it is easy to verify if it is a failure due to (planned) work activities or if something else is wrong, All network equipment is provided with monitoring tools that can measure latency, retransmissions and bit errors. Eurofiber advises their customers to actively monitor their network components and ports, to ensure that they will be alerted in case of any latency changes and signal interruptions; these are indications that unauthorized devices may have been connected to the network.

Step 5:

Other relevant factors

In practice, the human factor is still the weakest link when it comes to the security of privacy-sensitive information. In addition to all the options offered by technology, it is also important to draw up clear policies on handling sensitive data. For instance, it is important to carefully configure which employee is allowed and able to access and use which data (Identity & Access Management). When employees leave the company, their login codes and accounts should be blocked immediately, and the system should be checked every year to eliminate 'ghost accounts'. More stringent measures could include the screening of employees, checks on moving certain amounts of data and a ban on using external storage (like USB sticks).

Awareness is an ongoing process in any organization, which will constantly help employees be more aware of how to handle sensitive data securely.

In conclusion: remain vigilant

No matter how well an organization sets up its security, we know that cybercriminals will always be one step ahead. When dealing with security, trust no one but yourself, and use encryption on as much of your organization's network as possible. Considering the increase in the number of cyberattacks, it is no longer a matter whether hackers will try to get into your systems, but when. If you choose the right infrastructure, encryption and policy for your organization, you might not be able to prevent an attempted hack entirely, but you will have the right measures in place if it happens.

Curious to hear more about what we could achieve for your organization?

Eurofiber has been a fast-growing international provider of industry-leading digital infrastructure since 2000. Relying on our own fiber optic network and data centers, we provide smart, open, future-proof infrastructure to companies, government bodies and non-profit organizations. Customers have complete freedom to choose the services, applications and providers they need, allowing them to tap into the full potential of digital innovation. Eurofiber has an extensive fiber optic network in the Netherlands and Belgium, it unlocks its four data centers of its own and almost all public data centers in the Benelux.

This is a Lifeline eBook brought to you by Eurofiber. The Lifeline platform offers information and inspiration in the field of digital connectivity. Eurofiber.be/lifeline.

Eurofiber. Lifeline for the digital society

Fountain Plaza 504, Belgicastraat 5 bus 7,
1930 Zaventem, t +32 (0)2 307 12 00
info@eurofiber.be, www.eurofiber.be

eurofiber