LIFELINE

The winning formula for a secure ICT infrastructure

Everything an ICT manager should know

eurofiber

The winning formula for a secure ICT infrastructure

In today's society, we continue to connect more and more devices to each other and to the internet. In our personal lives as well as in our businesses, we are creating networks that can communicate with each other without any human intervention. Consider the emergence of self-driving cars and refrigerators connected to the internet that can automatically order groceries for you.

In business, the internet is also used in more and more ways. Employees increasingly work from home or on the road. And innovative applications make it easier to access all our company information through our smartphones and tablets.

These developments are happening at an incredibly fast pace. Companies need to anticipate their next steps, designing a proper response so they don't fall behind – primarily to leverage all the benefits and new opportunities offered by the internet and by innovative applications, but also to mitigate the new risks emerging as a result of these trends. Cyber-criminals have more and more opportunities to penetrate business networks. That's because more and more devices are connected to the internet – and that means more places where your security can be compromised by vulnerabilities. These vulnerabilities need to be minimized as much as possible, or better yet prevented entirely. So how do you configure your IT infrastructure to ensure that your organization stays as safe as possible, achieving the best possible protection against cyber-attacks?

This e-book contains the winning formula to make your infrastructure even more secure. We will look at why a new, suitable infrastructure is needed, how to achieve maximum security for your network and data, how you can make your data management safer and more secure, why monitoring is absolutely necessary, and the other non-technical requirements you need to take into consideration.

Contents

Choosing your physical infrastructure

This eBook will take a closer look at the winning formula for a secure ICT infrastructure. First, we need to figure out why an ICT infrastructure is so important for your organization. And what types of infrastructure are available to choose from? You will read all about it in this chapter.

A solid digital network infrastructure is the foundation of every company – And connectivity is priceless, especially now that data and applications are increasingly placed outside company premises. If a connection becomes unavailable, the company could quickly run into issues with loss of revenue or damage to its reputation. What the network is used for largely determines the choice of infrastructure. Does your organization frequently handle privacy-sensitive information and interact with business-critical systems? In that case, it is crucial to optimize your availability and reliability. If you rely on twin data centers that run synchronized real-time backups of all data, you will need a different infrastructure than if your company just needs internet access and VOIP telephone services.

The right choice for your organization

When security is a high priority, the best choice is a managed dark fiber connection. Of course the most secure option is a conduit that is completely yours. However, it is crucial in such situations to ensure that your organization has sufficient knowledge and expertise to light the fiber. If that knowledge is not available, then DWDM is a good choice. If you opt for DWDM, a telecom provider will provide an unlit fiber as well as the lighting equipment, but in both cases the network provider will take care of management and maintenance.

The difference between various physical infrastructures

There is no such thing as one single ICT infrastructure; the possibilities are endless. We explain a number of options in the following text, so you can get an impression of what type of connection might be suitable for you.

- **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.

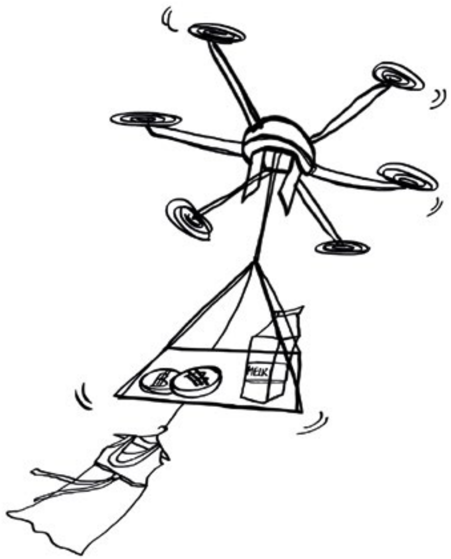
- **Coax**, also known as 'cable' (as in 'cable TV'), is mainly used for internet, television and radio and for consumer telephone services. In general, choices available to organizations are limited.

- **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.

Debating whether to choose DWDM or ethernet? Then check how much bandwidth your organization needs. If you need high bandwidth, you'll want to choose DWDM. If you have a centralized ICT landscape and therefore need a connection to give users access to the ICT environment, then an ethernet connection is what you need.

In conclusion

Privacy-sensitive data should preferably not be transmitted via public internet, since it offers hackers many opportunities to intercept data. The best choice for your organization therefore depends on how you plan to use the connection.



Maximum security for your network and data

Once your new infrastructure has been selected and implemented, it's time to look at how you can improve security. Secure infrastructure requires encryption. But ensuring the security of your ICT infrastructure is not the only reason to use encryption; it also keeps your data secure. In this chapter, we will explain how to achieve effective encryption of your network as well as your data.

What is encryption?

Encryption locks data up using algorithms, ensuring that it is useless to malicious parties if it is unexpectedly stolen or lost. After all, without the key, they cannot decipher the data. Encryption is not just a necessary precaution to protect your data, either; it is also required by law. The latest Personal Data Protection Act requires organizations to provide optimal protection for their data. You must be able to prove that your data was properly protected at the time of its loss or theft. Encryption tools make that possible.

Encryption on the network

Network encryption means that all data that is transported across the network is encrypted before transmission. Even if malicious parties discover a vulnerability in the connection or manage to dig up the cable somewhere, the data will be useless to them without the key.

Data encryption

Data encryption means that the data is encrypted and then stored on a hard drive. If any malicious party runs off with the hard drive, it will be useless to them without the encryption key.

Encryption on the network

If you opt for network encryption, you first need to come up with an encryption key, or a code word. It is crucial to define a good encryption key that is changed regularly and has various bICT lengths. The longer the bICT lengths, the harder it is to hack. The code word is entered into an algorithm, such as AES (Advanced Encryption Standard) based on the American FIPS (Federal Information Processing Standard) (see text box). The algorithm ensures that the data is scrambled in a specific way. Once it has been scrambled, it is nearly impossible to decipher stolen data. Then the encryption key is exchanged with the equipment on the connection. A time limit is also set when the key needs to be changed, usually once a minute. Even if a malicious party manages to retrieve the key itself, it resets a minute later, so the data is scrambled in a different way again.

Hardware-based versus software-based encryption

There are various ways to encrypt a network. The best choice for your organization depends on how the connection is being used. For instance, it is possible to implement hardware-based encryption by placing encryptors in the equipment used to light the fiber. Hardware-based encryption ensures that all data transferred through the connection is encrypted. If the connection is used to transfer large quantities of privacy-sensitive and confidential information, we recommend encryption at the hardware level.

Hardware-based encryption requires specific hardware that provides the encryption key. This encryption method is extremely secure. If a hacker tries to access the hardware to identify exactly how the encryption words, and removes so much as a single tiny screw, then the key is immediately erased.

There also various options for software-based encryption. The benefit is that it is possible to differentiate between data that needs to be encrypted and data that can be left unencrypted. A drawback of software-based encryption is that it adds more and more latency, which could slow down the connection.

Advances in network encryption standards

The Advanced Encryption Standard (AES) replaced the original FIPS for data encryption: **the Data Encryption Standard** (DES). By the late 1990s, DES was no longer considered fit for purpose, so a global competition was organized to design a new standard. The Rijndael block cipher algorithm won due to its combination of security, performance, efficiency, simplicity and flexibility.

RSA (an acronym for the names of its inventors: Rivest, Shamir and Adleman) is an asymmetric cryptographic algorithm that was designed in 1977. The security of RSA is based on the fact that it is hard to factorize very large composite integers. The encryption strength of RSA is based on the key size, which is still considered unbreakable; the risk is that new developments in this field could render the algorithm useless.

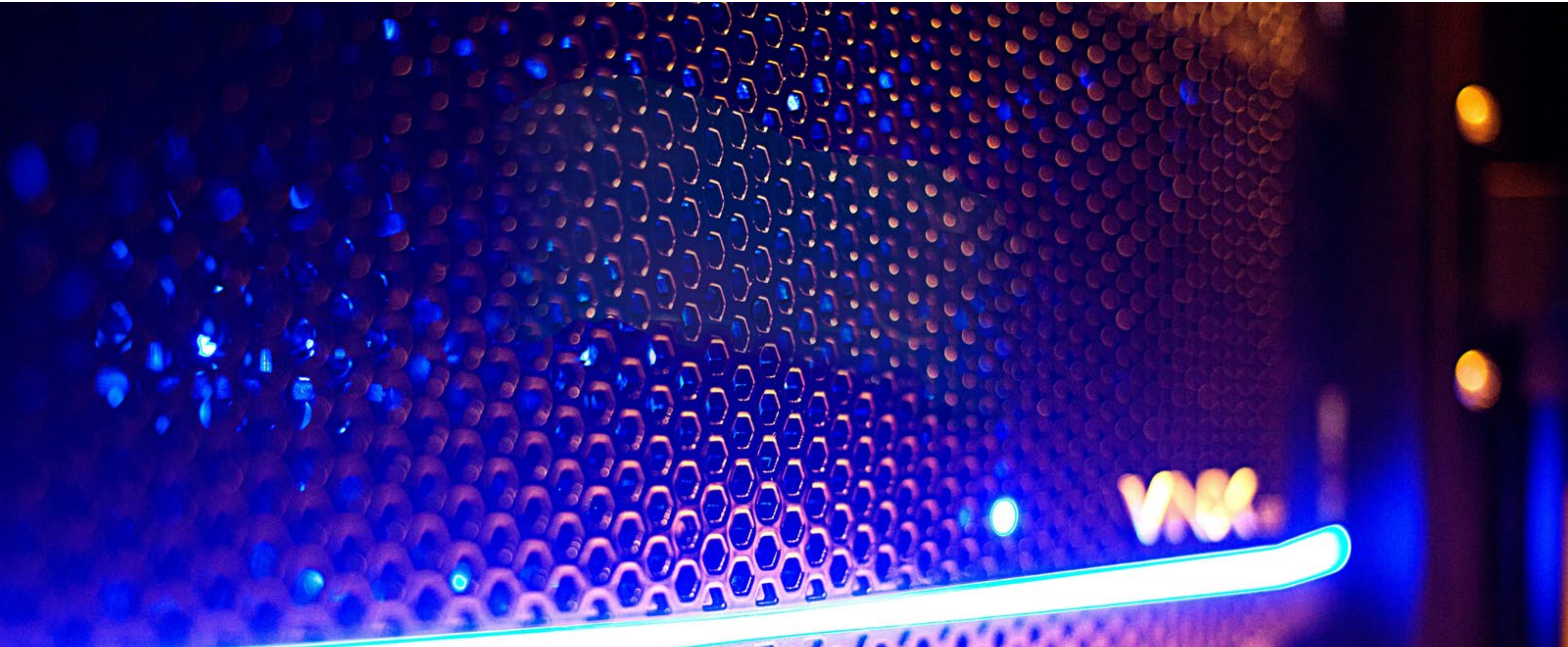
The **Federal Information Processing Standard** (FIPS) is an American encryption standard. The Federal Information Processing Standards (FIPS) are issued by the US federal government and specify how certain information needs to be stored in information systems. Intended for use by non-military government agencies and government contractors, these standards include DES (FIPS 46) and AES (FIPS 197), see below.

Data encryption

Encryption at the network level means that the data is only protected if it is transferred across the connection. However, data can also be encrypted on an organization's internal and external file storage systems.

In general, the server is equipped with a separate chip where the encryption key is stored, so the key is always physically separated from the hard drive. A hacker would only be able to decipher the key if he had the hard drive and could also access the chip on the server. Even if a laptop, smartphone or portable storage device were lost or stolen, then the information on the hard drive would still be secure.

Encrypting as much of your data as possible is recommended in order to ensure optimal data protection. This is especially important when the data is stored outside the organization's own facilities, such as with a hosting or storage provider or in an external data center. In such situations, the data passes through various external providers. Full data encryption is the only way to make sure your data stays safe every step of the way.



Managing your ICT environment within your organization or in a data center

Today's society involves interacting with massive volumes of data. Your business information is generally confidential, so it may seem obvious to manage it yourself. However, an external data center often proves far more secure. Why? This chapter takes a closer look.

The benefits of a data center

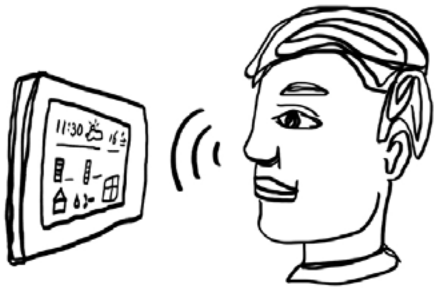
Obviously, you are absolutely certain that you are protecting your data properly. However, an external data center is completely configured for the express purpose of managing ICT environments. Since its entire focus is that one thing, an external data center is often much more secure.

How do you choose the right data center for you?

No two data centers are the same, and some are very different indeed. So what do you need to keep in mind to make the right choice? The most important factor to consider is security. A data center should have high standards for safety and security. After all, you also invest considerable time and money in your ICT infrastructure to ensure secure transport of data between the data center and your organization. All your security efforts will be completely negated if security measures at the data center are insufficient. For instance, physical security of the building is very important. It is essential 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.

The benefits at a glance:

- Complete focus on managing your ICT environment, by specialized professionals.
- Solid security measures, such as a big fence around the building and security cameras. And nobody can just walk in off the street. The only time anyone will be near your ICT environment is during maintenance. When you do your own data management, it is often possible for employees to just walk in unexpectedly, getting very close to business-critical data.
- Highly efficient use of cooling technology and energy. Since multiple ICT environments are managed here, this leverages capacity to maximum effect.



Checklist – Choose the right data center in 6 steps

Choosing a data center is easy when you follow this checklist.

1. Identify your current and future needs

You will be able to choose the data center that is right for you once you know the current and future needs of your ICT environment.

2. Decide which services and availability you need

Decide which services your organization would like to use in a data center. Do you need a footprint, a rack, a suite, a cage or possibly an entire room?

Map your organization's current ICT landscape by answering the following questions:

- How much power does the ICT environment actually use?
- How much space does the ICT environment take up?
- Is all the equipment connected to a redundant back-up power supply?
- What are the connections to the outside world?
- Does the organization rely on external contractors to maintain the ICT environment?
- Is there a need for a primary and secondary location?
- What is the maximum latency allowed between the locations?

In addition, determine what your future ICT environment will look like. You can use the following questions to help you along the way:

- Will the ICT systems be consolidated or virtualized in the future?
- What is the growth scenario in terms of rack space?
- What is the expected energy use per rack?
- Is the organization planning to outsource and if so, to which provider?
- How is the demand for connectivity expected to develop (in terms of bandwidth)?
- Is there a need for internet access and if so, in what way (access, peering or transit)?
- Does the organization need to be able to connect to public cloud providers?

Which data center service suits your organization?

F Footprint: floor area per m2 with power supply and cooling, where customers can install their own data racks.

R Rack: a 19″ rack with its own power supply and cooling.

S Suite: multiple interconnected racks, closed off by an access door that can only be opened by that customer.

C Cage: a suite, surrounded by a fence that creates an additional layer of security around the ICT equipment.

If you work in a hospital, your systems should probably achieve high availability, at least 'four nines' (99.99%). If temporary downtime does not immediately create a life-threatening crisis or if you have redundant locations, you might consider choosing a slightly lower availability – which obviously comes with a lower price tag.

3. Define the selection criteria

What does your organization consider important in a data center, and which aspects are essential for the ICT environment to work properly? These criteria can be divided into must-haves for crucial ICT and data center processes, should-haves for optimal user convenience in the data center, and nice-to-haves as a bonus.

4. Draw up a long list and a short list

Based on the selection criteria, you can now draw up a long list of data centers that are worth considering as service providers for your organization. Start by looking at the technical requirements and your must-haves. You can use the should-haves and nice-to-haves to shorten the list, narrowing it down to about three data centers that meet as many of your criteria as possible. Then you make an appointment to visit the data centers on your short list.

5. Visit the data centers

When you visit the data centers on your short list, listen closely to what they tell you, but also keep your eyes open. What is your overall impression of the location, the building and the people you see there?

6. Request quotes

Chances are that the data centers on your short list will meet virtually all your criteria. If your impression during the visit does not help you make a final decision, you can compare prices. Request a quote from all the data centers still on the short list, and then decide based on how much it will cost.

Is the data center secure enough?

During your visit, you can immediately test the facility's security protocols. Are you allowed to enter the building unchallenged, because they know you have an appointment, or do you have to show your ID and are you subjected to a security check? Pay close attention to how easy or difficult it is to gain access to various rooms. Can you go anywhere you like once you are inside, or are additional security measures in place? How many barriers did you encounter before you were in the server room?
Is the fence high enough, or could someone get over it with hardly any effort? Are there security cameras everywhere? And is someone actually monitoring those camera feeds?

Other relevant factors

Once you identify the infrastructure that meets your needs, encrypt your data and arrange professional data management, you are well on your way to a secure infrastructure. Of course there are lots more elements that can affect the security of your infrastructure. In this chapter, we will explain two important elements in more detail.

1. Network monitoring

Despite all the security measures, you will still need to continue monitoring your network – Not only to detect failures quickly, but also to keep a close eye on any unauthorized activity, for instance by cybercriminals.

What is monitoring?
Monitoring means that use monitoring software to keep a close eye on all connections and active equipment. If all is well, you won't see anything at all. But as soon as an ethernet switch has issues or equipment starts malfunctioning, the monitoring software will alert you to the problem so you can take action immediately.

Network monitoring often takes place from two sides. If you decide to use a managed connection, the network will be monitored by the organization and by the telecom provider. The provider can see what's happening on their own network, while the organization has a comprehensive overview of their entire ICT infrastructure, including their own network and the equipment in it.

Monitoring by the provider

A managed fiber optic connection often comes with an RFTS (Remote Fiber Test System) installed by the provider. This software detects malfunctions in the fiber optic cables, with the additional advantage of being able to identify unauthorized taps. An example. Occasionally, especially in smaller organizations, the cleaners enter the building around 17:00 and unplug something so they can use the vacuum cleaner. The provider immediately gets a notification that the device has switched off, and can investigate what is happening. Has there been a power outage? Is planned work being done on the system?

situation, targeted steps can be taken to resolve the problem. When a cleaner accidentally unplugs something, emergency measures aren't required… but if the problem is caused by something that broke, a technician can be dispatched to the location post-haste.

Monitoring by your own organization

Of course your own ICT department should also keep a close eye on the network and the active equipment. Network equipment is often provided with monitoring tools that can measure latency, retransmissions and bit errors. We recommend that you actively monitor your network components and network ports, configuring your monitoring system to alert you in case of any latency changes and signal interruptions. Those are indications that unauthorized devices may have been connected to the network.

2. Non-technical requirements: the human factor is the weakest link

In addition to all the options offered by technology, it is also important for your organization to draw up clear policies on handling sensitive data. In practice, the human factor is still the weakest link when it comes to the security of your business-critical information.

The human factor is often the weakest link where security is concerned.
To reduce the risks that your confidential business information will be leaked, it is key to:
- Configure access rights that effectively determine which employees are allowed and able to access and use specific data.
- Promote employee awareness of the potential risks.

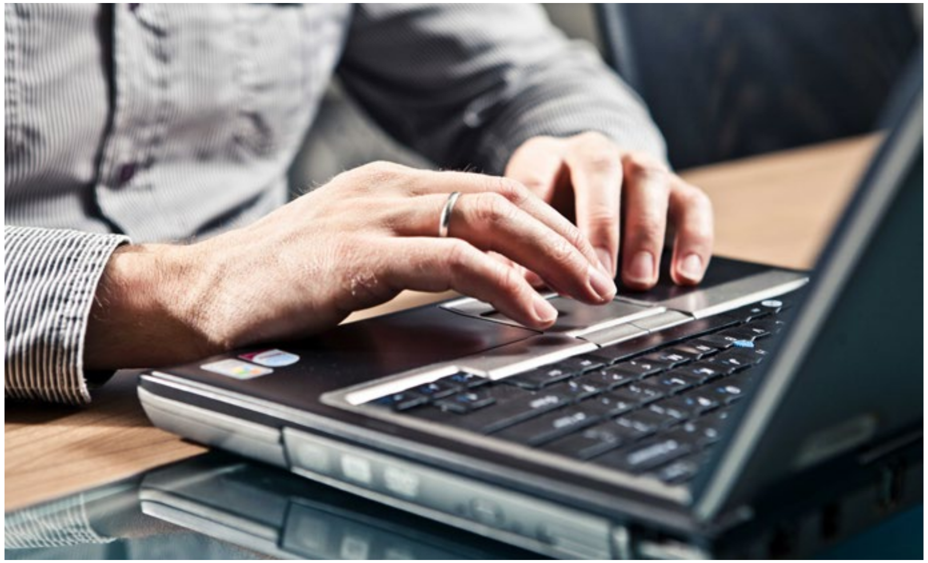
The importance of Identity & Access Management

Identity & Access Management means that you manage access to your business information in a structured way and that you can identify and verify the users of your data. Some examples of what should be included in an Identity & Access Management policy:

- Departure clean-up: When employees leave the company, their login codes and accounts should be blocked immediately
- An annual check to eliminate any 'ghost accounts'
- Mandatory screening of employees
- Checks on moving certain amounts of data
- Ban on using external storage (like USB sticks)
- Provide a guest network for your visitors and be aware of who is logged into the guest network at any given moment

Promoting employee awareness

Awareness is an ongoing process in any organization, which will constantly help your employees be more aware of how to handle sensitive data securely. They need to become aware of the risks of careless data use, realize that today's cybercriminals have more and more ways to get their hands on business information. For instance, we are connecting more and more devices to the internet.



Improved employee awareness could be achieved by providing regular awareness sessions. A few examples of what these sessions could be about:

- Show how cybercriminals operate, e.g. explain how a phishing e-mail works.
- Explain what can happen when people log in on unsecured Wi-Fi connections.
- Make employees aware that writing down passwords is very dangerous, and give them tips on how to use and remember strong passwords.

In conclusion

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 data policy for your organization, you might not be able to prevent an attack entirely, but you will have the right measures in place if it happens, and will be able to respond appropriately. These measures will minimize the risk of losing your business-critical information.

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