RAAS

RECOVERY AS A SERVICE

# EVERYTHING YOU NEED TO KNOW

## TO PROTECT YOUR INFORMATION

# CONTENTS

# INTRODUCTION

Data security is very important for business success as more and more consumers and other stakeholders are concerned about the privacy of the information they provide to businesses. Ensuring the confidentiality of business data is a daily struggle of managers and employees need to be aware of the importance of information security.

Computer attacks are becoming more and more sophisticated, so that those responsible for information security are always alert and have a proactive attitude to security. When data security fails, the consequences for a company can be disastrous, and can even lead to bankruptcy.

In such a digital world, it isn't always easy to protect the confidential information that companies store. Due to mobility, the devices used in companies are increasing in number, which makes it necessary to create security policies not only for static equipment, but also for mobile equipment such as laptops and smartphones. And this means that threats also exist in greater numbers.

In this e-book, we'll cover a number of data security issues in business so you can start protecting your most valuable asset right now: your information!

# THE 7 CAPITAL SINS OF SECURITY IN BUSINESS

## 1.Negligence

Despite growing awareness of the importance of protecting data, there are still many companies that fail in this area and are negligent with regard to the use of an antivirus, for example. Even the most basic rules of security must be applied and made known, because this is the only way to motivate employees to work to protect all confidential information.

## 2. Curiosity

"Curiosity killed the cat" is a very old proverb that must be taken very seriously! However tempting it is to click on a link, we shouldn't do it if we don't have full trust in the sender. Many of the viruses installed on computers entering through hacking emails present seemingly relevant subjects that are more than schemes designed to get people's data, get them to subscribe to fraudulent services or install spyware on their equipment. A warned user should never access a link from an unknown sender even though it appears to be trusted.

## 3. Opportunism

Related to previous sin, opportunism is one of the greatest dangers of the digital world. Tempting raffles, free travel and very easy credit are ways that hackers can find to attack the most innocent users. The probability of a trap to steal data in these cases is more than 98%. Make sure that all employees of the company adopt a very precautionary behavior.

# THE 7 CAPITAL SINS OF SECURITY IN BUSINESS

### 4. Leisure

In a work environment, the Internet must be used objectively and with a purpose. It is true that at some point all employees use the Internet for personal purposes, but you have to be very careful not to get carried away by idleness. Downloading e-mail attachments or entering unreliable sites to buy something is quite risky and can compromise the entire security of the organization.

### 5. Innocence

There are people who are not suspicious of receiving too many identical emails or receiving too generous offers. One must be careful not to be too innocent in the digital world. Be wary of all the strange emails and all the senders you don't know - in doubt it's a fraudulent message that should be discarded.

### 6. Indiscrimination

Don't trust your passwords with anyone and be very careful when setting your passwords. Use a password manager with strong encryption to store all your private information and never leave passwords exposed in post-its.

### 7. Waste

There can be no vacation in care about private data, so information security is an area you should always be working on and looking for better ways to ensure your privacy.

# THE 7 CAPITAL SINS OF SECURITY IN BUSINESS

**78%** of companies around the world suffered at least one computer attack in the last two years

**92%** of attacks suffered due to internal security flaws

**35%** of attacks suffered due to information loss on mobile devices

**57%** companies doesn't protect your information with data protection solutions

**61%** is the average loss of productivity in every computer attack

**42%** is the average loss of revenue resulting from a every computer attack

RAAS
RECOVERY AS A SERVICE

# MOBILE SECURITY: THE MAIN TIPS FOR PROTECTING INFORMATION

### Create a mobile security policy

Having a security policy for mobile devices is critical to ensure compliance by employees. Also develop awareness programs for the team so they realize the importance of protecting business data. This security policy should contain explicit penalties for violators, to awaken employees' sense of responsibility.

### Use encryption

Mobile devices are often connected to public Wi-Fi networks and this is quite dangerous if there is no encryption when transferring important information such as usernames, passwords, keys to APIs, and other sensitive information.

### Cloud Solutions

It is difficult to find a business these days that has a fixed schedule from 9am to 5pm. Nowadays, companies are more flexible regarding schedules and due to the use of Cloud and mobile technology it is possible to work from any location and at any time. Cloud storage synchronizes information between different devices, so everyone can work on the most up-to-date version of a particular document, regardless of which device they are using and where they are. Cloud, if correctly configured, guarantees high level security and maximum privacy.

## Use VPN

A virtual private network (VPN) is a type of private connection that uses a public network to access your company data. It contains a connection encryption that prevents data interception and IP tracing. This is the safest way to access company data through public networks, such as hotels and airports, and it must be the only way a user can connect to the corporate network.

## Limit access to resources

When using your smartphone, you may have to install several applications. Each application needs access to certain device features to function properly. However, in many cases the applications ask for access to resources that are not essential for its correct functioning. Therefore, it is advised that you do not allow applications to have access to features that are not absolutely essential to your use.

# HOW TO CREATE AN INFORMATION SECURITY POLICY AT YOUR COMPANY

The protection of company information is the theme of the moment, due to the arrival of the new General Regulation of Data Protection of the European Union (GDPR). Companies are increasingly digital and without adequate prevention measures, data security is seriously compromised. Corporate security policy is an essential tool to ensure that your data remains secure.

## What is a security policy?

The security policy is a document developed by the company that records the principles of security that the company adopts and that must be followed by the employees. Security policy should be applied across all information systems, and cover the entire infrastructure. For policy to be respected, it's essential that top managers actively participate in its implementation.

## How to create a good information security policy

- Define the responsibility of the employees: establish penalties for the misuse of the company's IT resources. There should also be clear and well-understood rules on access to websites and recommendations on the use of the electronic devices provided.
- Training: there must be practical training in the presentation of the information security policy. The company must collect individual statements from employees, where they undertake to comply with the rules contained in the document. This manual should be easily accessible to employees and should be reviewed frequently so that it is kept up-to-date.

# HOW TO CREATE AN INFORMATION SECURITY POLICY AT YOUR COMPANY

- Name a person in charge: the company must appoint a responsible person to monitor compliance with the information security policy. This employee should be responsible for detecting breaches of rules.
- Make the security policy known: the document must be approved by the human resources department of the company. The rules in this document must be in accordance with the laws of the workplace and the internal staff manual. After approval by the human resources, top managers should also do their approval. There follows a wide dissemination of the security policy, which should be easily accessible to all employees.
- Adopt a disaster recovery plan: disaster recovery plans are essential for planning actions that ensure that a disaster that doesn't interfere with the company's performance. In addition to this proactive action, disaster recovery plans also have a reactive action, through the action of executing emergency actions, previously planned, that guarantee immediate resolution of problems. Disaster recovery is still defined as the set of procedures to be performed in crisis situations. The ultimate goal is to save your business data so your information stays safe and sound.

# DISASTROUS CONSEQUENCES OF LACK OF DATA SECURITY

Computer attacks are becoming more and more sophisticated, so that those responsible for information security are always alert and have a proactive attitude to security. When data security fails, the consequences for a company can be disastrous.

## Exposure of data

When the company doesn't have an effective data security policy, one of the worst consequences is the exposure of data. If a company doesn't adopt encryption or masking rules and if it doesn't protect its devices through passwords, the likelihood of confidential data being exposed is much higher. And when this data leak occurs, the company loses credibility, and may even fail.

## Heavy fines

With the entry into force of the GDPR, companies need to be very careful about how they manage the most sensitive data. The new GDPR focuses heavily on enforcement and penalties, through the application of high fines for offenders. In cases of minor infringements, it may reach 10 million euros or 2% of the global turnover of the group in which the company operates, and in the most serious cases it may reach 20 million euros or 4% of world turnover.

# DISASTROUS CONSEQUENCES OF LACK OF DATA SECURITY

## Damage to the company image

When a company leaves their confidential data exposed, their credibility with customers and suppliers is compromised. No company and no customer likes to deal with an organization that is not able to guarantee the privacy of your information. These image damages can compromise the survival of the business.

## Repetition of work

When there is no guarantee of information protection, IT teams are very likely to be forced to do the same tasks over and over again to recover data that has been lost. It is essential that the company has well defined processes for the management and processing of confidential data. The constant repetition of tasks can lead to the demotivation of the employees and the consequent increase of the turnover rate in the company.

# LOSS OF BUSINESS DATA: WHAT TO DO TO MINIMIZE THE IMPACT?

As far as data loss is concerned, prevention is always the best solution. It is through the data they have that companies can analyze their audience, define marketing campaigns and guide the whole strategy of the business. However, there are more and more threats to information security, so it is essential to devise strategies to minimize the impact in case of data loss in companies.

**Backup in different environments**

It is essential that the most important information of your company has several copies, so that there is no risk of being lost forever. If you previously saved data to disk or tape was considered sufficient, nowadays it is strongly advised to use the Cloud, because it is the most reliable and secure solutions that simultaneously ensures an offsite copy (off-site). In addition to having your data stored in a secure location, you can access it from anywhere and from any device, as long as you have access to the Internet.

**Promote conditional access**

Often companies do not condition access to certain documents by some employees and this can compromise information security. It is important that each employee has only access to the data that he or she really needs, otherwise, if there is a computer attack, it is difficult to find out where they came from. It is also essential that companies block access to sensitive information over unsafe public networks. In this way, the probability of suffering external attacks is minimized on a large scale.

# LOSS OF BUSINESS DATA: WHAT TO DO TO MINIMIZE THE IMPACT?

## Have a recovery service in the Cloud

It is very important to have a recovery service in the Cloud, so that even in the event of a disaster that affects information systems, there is no total loss of data. RAAS (Recovery as a Service), for example, provides a dedicated recovery infrastructure with the possibility of selective data replication. This service enables near-instant disaster activation on virtual servers in a remote environment. In this way, even in the case of more extreme disasters, the information is easily recovered, not interfering with the usual performance of the company.

## Encryption and data masking

Data encryption transforms information by using an algorithm so that there is no easy and perceivable access by a third party, but only by those who have the correct encryption key, which shows their true content. Data masking creates a version similar to the original data in terms of structure, but without revealing its true information. Its original format remains unchanged, but the data presented is fictitious. Masked data can be used in test and auditing environments without compromising the result of the analysis, but always ensuring the confidentiality of sensitive information. It is essential to use these two mechanisms, so that even if the information is picked up by
can not be deciphered.

# DATA STORAGE: HOW TO REDUCE COSTS AND INCREASE SAFETY?

The volume of data created in companies is increasing and there is great difficulty in managing and storing all the information created daily. Technology helps companies cope with this "data boom," but it isn't always easy to find the balance between cost savings and increased security.

## Adopt a storage

Using storage to consolidate disks and centralize data storage brings immense benefits to businesses. First, it is a scalable service and consumes much less energy than having multiple servers with scattered information, helping to reduce the costs of the business and facilitate the whole process of administration and management of the infrastructure. It is a secure solution, with high redundancy rates against faults, and even allows to use replication, that is, all information can be duplicated in two different devices, reducing to almost zero the probability of information loss. Finally, modern arrays have a high degree of efficiency, both for the performance they afford against reduced energy consumption, and for the data compression and deduplication features, which allow for better disk performance. system.

## Invest in Cloud Storage

A study carried out by KPMG concluded that half of the companies that choose to store in the Cloud refer to low costs as the main motivational factor. Using Cloud will allow physical documents to be deleted, which reduces employee costs and storage. Cloud allows the enterprise to not have to invest in expensive, complex structures such as datacenters. In addition, using Cloud is extremely secure and allows any employee of the company to have access to information from any device with Internet access, which will improve their performance.

# RAAS

RECOVERY AS A SERVICE

**No initial investment**
Recovery and backup provided as a single service with monthly payment

**Guaranteed service**
Fully managed services provided by our specialized team

**Quick recovery**
Recover a virtual server in seconds

**Continuous management**
Managed service 24 hours a day and 7 days a week ensures your applications' availability

**Easier Disaster Activation**
Instantly enable remote virtual servers for fast recovery

**Dedicated Infrastructure**
Guaranteed isolation of your data for a total protection of your information

# RAAS

RECOVERY AS A SERVICE

| | |
|---|---|
| PHONE | +351 220 101 587 |
| OFFICE | Rua Eng. Frederico Ulrich 3210, 1° andar.<br>s. 101, 4470-605 Maia |
| EMAIL | raas.info@itpeers.com |
| WEBSITE | https://raas.itpeers.com/ |