English version

THE CHALLENGE OF SMART WORKING AT THE TIME OF COVID-19

THE SMEs GUIDE TO SAVE YOUR BUSINESS PROTECT YOUR DATA AND MAINTAIN CONTROL

ALESSANDRO SCARAFILE

« The incorrect application of information technology
is an extremely exciting way of complicating things »

Alessandro Scarafile

former Operations Manager
Hacking Team

SUMMARY

INTRODUCTION

When Vadim Comanescu (CEO of Syneto) called me with the idea of creating a white paper on the security implications related to Smart Working, I was immediately interested, considering the period.

It was March 18, 2020 and the entire world had just woken up in the **COVID-19 pandemic**.

So I started drafting some thoughts and to elaborate them inside a more structured guide, addressed to companies, managers and all those who want to react to the current situation in an organized way.

For the past 10 years I worked in the field of government interceptions, dealing with offensive hacking techniques and traveling in 50+ countries around the world: a sort of adventurous way of working and living, you may say. Yes, something like that, but... all this was about to change.

The uncertain health situation that is occurring during the writing of this document and the inevitable changes in social interaction that will result from it on global scale, force all organizations to act quickly in order to modify internal procedures, safeguard their business and increase their chances of survival.

Most exposed subjects to this new situation are undoubtedly the small and medium-sized enterprises, which still seem to be uninterested in the topic.

This white paper aims to deal with the topic of Smart Working from an **emergency** point of view, that is, how to make an organization reacting quickly, effectively and safely during an emergency time.

And make it work.

1. THE SMART WORK

Academic definition of Smart Working is *a new model of work that uses new technologies and develops the existing ones to improve both the performance and the satisfaction that is obtained from the job*.

It is important to highlight that Smart Working is a concept that concerns organizations and not individual professionals, who have always been used to working on the move, with flexible hours and using applications and tools that allow to carry out freelance professions.

What Smart Working *is not*

Smart Working is not *working one or two days a week* and is not simply *working from home*.

Rethinking the whole organization

The implementation of Smart Working means starting a process of change aimed at enhancing the individual worker, increasing his/her commitment to achieving corporate objectives and guaranteeing right conditions to combine professional life and personal life (work-life balance).

In this way the worker is:

- Satisfied with the activity he/she carries out and the workplace;
- Engaged and motivated to achieve corporate goals.

1.1 KEY ELEMENTS

Smart Working is a new approach to the way we work and collaborate within an organization, in which there are 3 key elements:

1. the review of leadership and the relationship between manager and employee (control —> trust);
2. the use of collaborative technologies to replace rigid communication systems;
3. the reorganization of the layout and work spaces that go beyond the walls of an office.

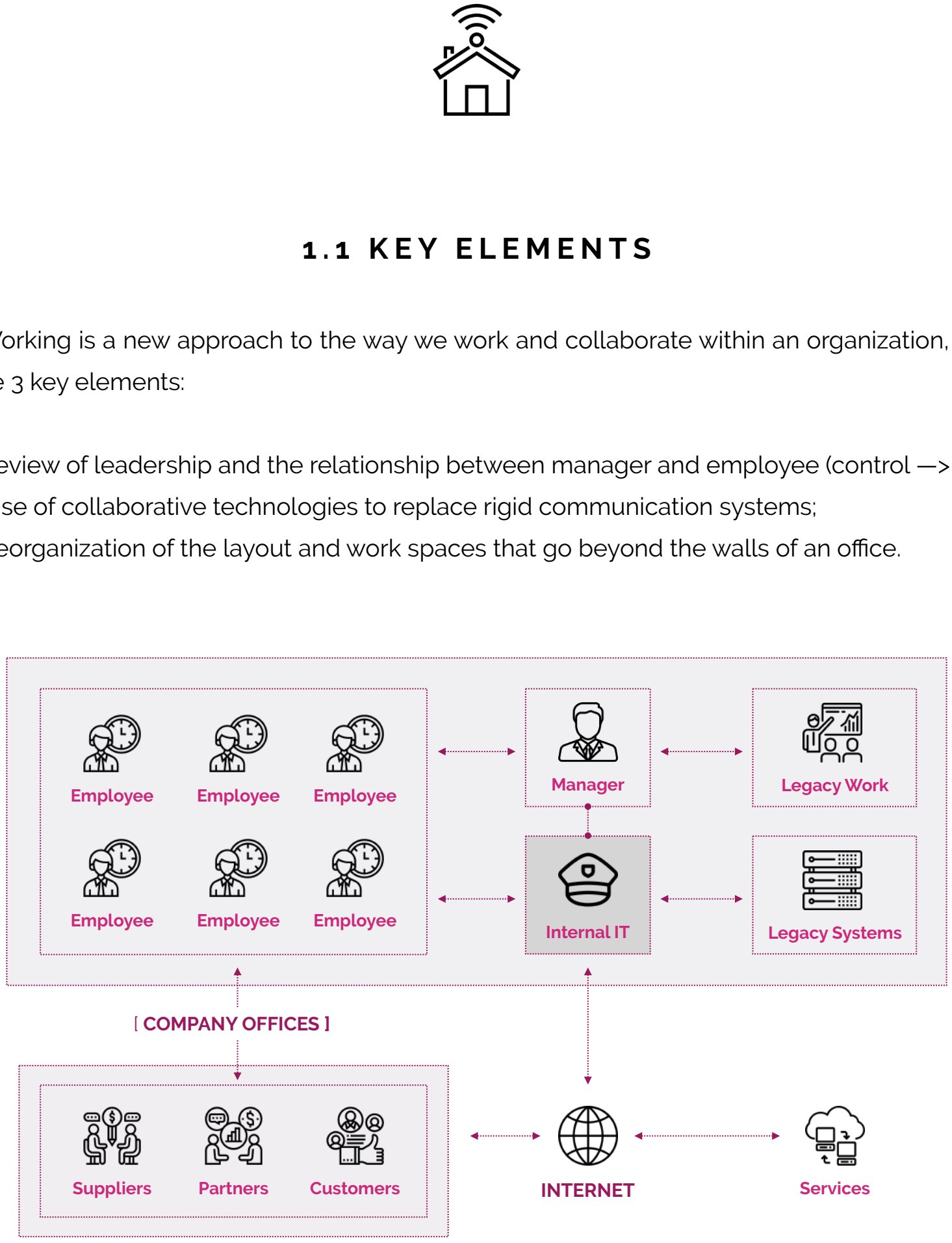


Image 1: Traditional Work

This new approach places **the person** at the center of the organization, making personal and professional objectives converge with corporate ones, in a single mode that guarantees greater corporate productivity.

Therefore the Smart Working tries to empower the individual worker, making him/her **the owner** of the work, aware of the results to be achieved, aware of the team work and autonomous in defining methods and timing of carrying out the activities.

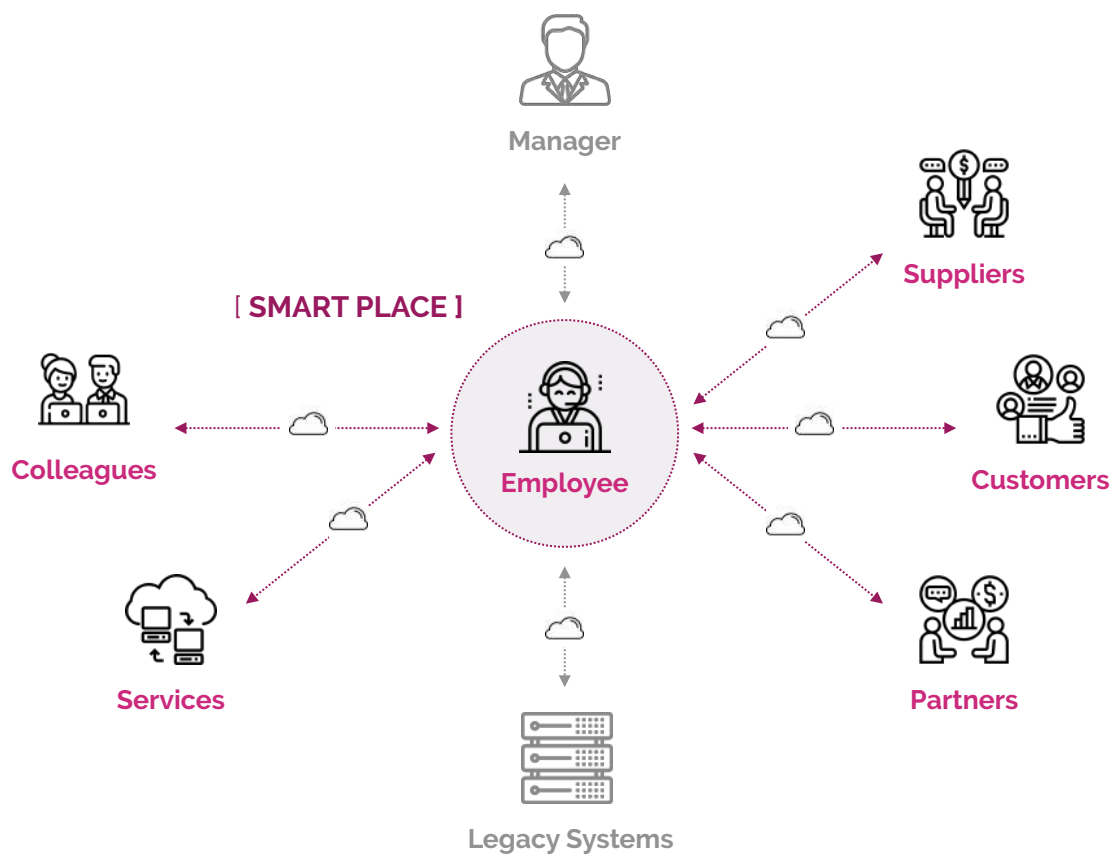


Image 2: **Smart Work**

1.2 WHY SHOULD YOU CARE

Smart Working offers **great advantages**. Beyond the economic data and statistics, the smart work brings about a reduction of worker stress, a reduction in absenteeism, and higher productivity and flexibility; for a company, it thus means being able to employ valid collaborators even at a distance.

Agile work broadens the outlook, cuts business costs and even reduces the environmental impact. The workers are totally **convinced** of this, however most of the companies do not seem aligned yet.

Eight main reasons for introducing the Smart Working in any company:

1. More effective staff selection process

75% of workers would like smart work.

2. Less costs

The average US worker would accept an 8% wage reduction having the opportunity to work from home.

3. More loyal employees

Two out of three employees say they are more loyal to employers who offer smart working methods.

4. More profits

Six out of ten companies worldwide report that smart work policies have increased profits.

5. Keep up with competitors

Almost a third of British workers have flexible hours.

6. More productive workers

Three out of four workers believe they are more productive outside the traditional 9-5 business day.

7. Follow the example of SMEs

Two out of three New Zealand SMEs offer smart working methods.

8. Most motivated employees

According to 65% of managers, smart work helps increase employee motivation.

Sources: PowWowNow, Princeton University, Workplace Insight, Vodafone, Perkbox, Fuze, MYOB Technology, City & Guilds Group

1.3 MANAGING THE TRANSITION

The key to Smart Working is a result-driven culture no longer based on old employment paradigms.

Employers should promote agile working by offering **technological tools** and using internal publicity campaigns, challenging the biggest difficulty: changing the culture around performance evaluations.

Flexible hours, rearranged offices, remote working and a new way of organizing work should be at the basis for a deep internal **corporate renovation**, especially within small and medium-sized enterprises.

Consequently, there is the need to introduce a new corporate figure, the **Smart Working Manager**, who will take care of the whole Smart Working management and - therefore - must have the skills to interact with all the stakeholders within the organization.

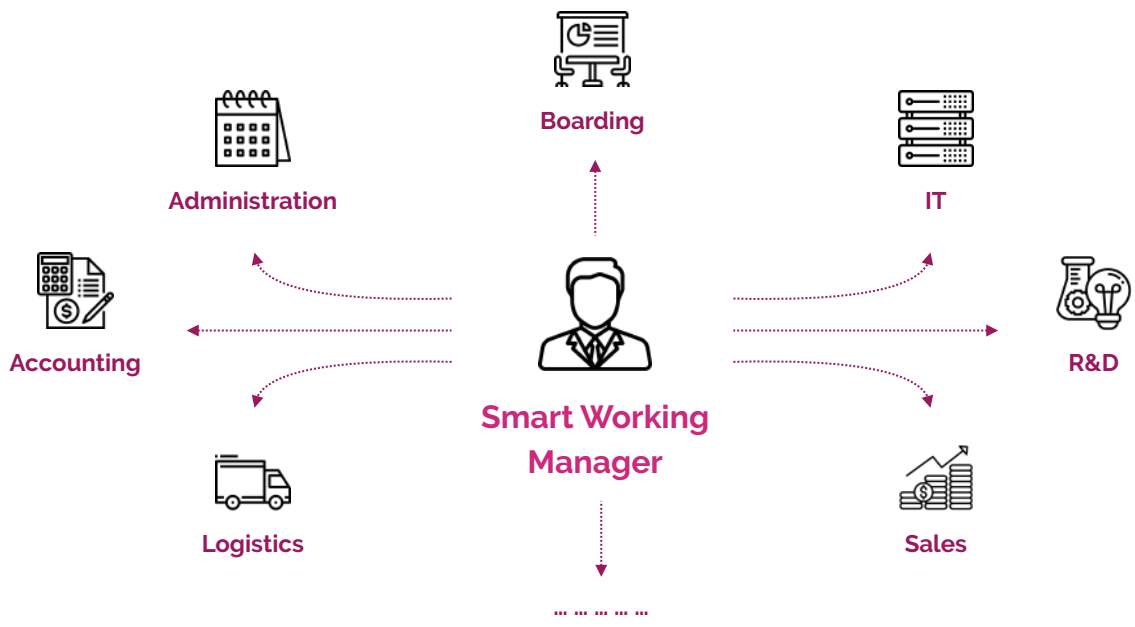


Image 3: A New Management Figure

2. THE ENVIRONMENT

The more comfortable, pleasant and stimulated the working environment for employees will be, the more productivity and quality of work will increase. For all company departments.

Allowing employees to work a few days from **home** is certainly a valid solution, as well as starting a partial or total **office spaces** reorganization, introducing smart work tools and **relaxation areas**, increasing the desire to spend more time at work.

This chapter provides useful insights on the main technological tools that can be quickly implemented within any organization and focused on 2 main topics: **Data Access** and **Collaboration**.

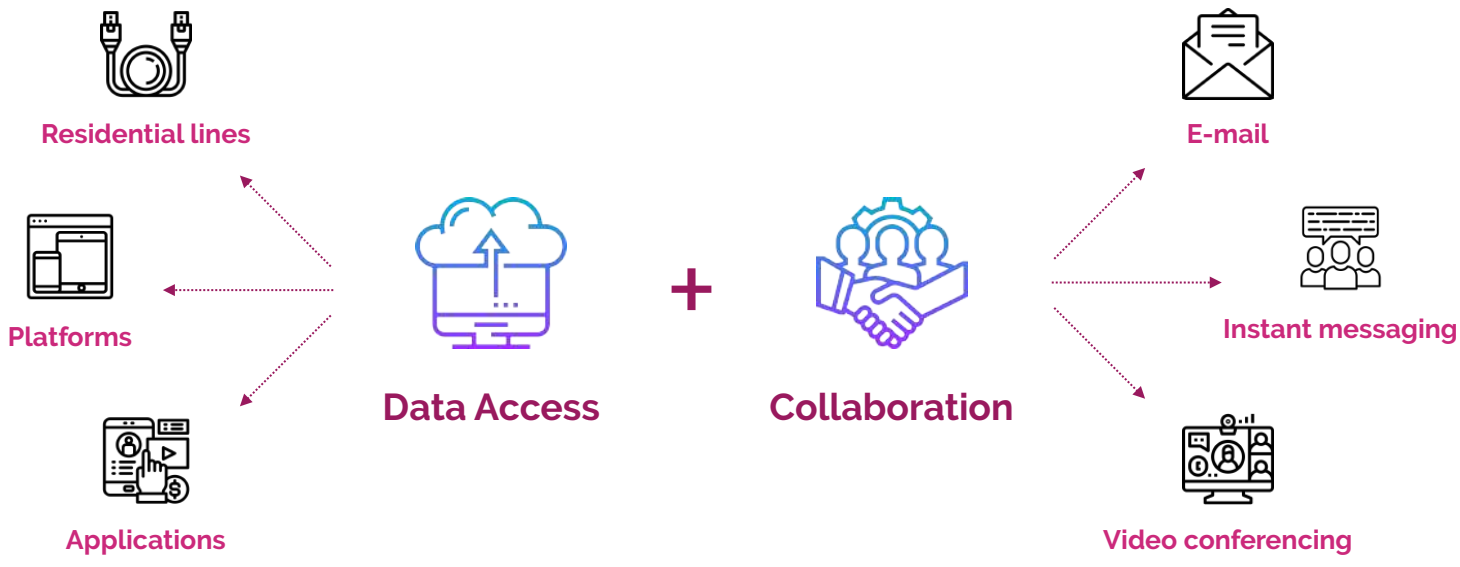


Image 4: **Renovated Work Environment**

2.1 DATA ACCESS

Access to data must be **fast**, **simple** and **reliable**, to take full advantage of modern technologies and allow the best Smart Working experience for remote employees.

The 3 main factors to leverage the best transmission and management of corporate data are: **lines**, **platforms** and **applications**.

All these factors must be chosen considering the company **budget**, the technical **skills** present and the **size** of the staff who will operate in Smart Working mode.

Image 5: Data Access Factors

2.1.1 RESIDENTIAL LINES

Smart Working operated from home requires **broadband** lines, fast enough to guarantee a stable connection to all the necessary resources.

The cost and installation of these lines could be offered to staff directly by the employer, thus increasing employees' loyalty and encouraging their use for work and not just for personal reasons.

For those who live in large cities, the best choice is certainly the **optical fiber**, while for those who live in very small towns - often not covered by fast wired lines - many **satellite** solutions are available.

The monthly cost for a fast Internet line can now be easily absorbed by any company, which can expand its list of benefits with this type of solution.

Image 6: **Residential Lines Maximum Download Speed**

2.1.2 PLATFORMS

The choice of business platforms should meet several requirements, including **business productivity** and **information security**, also considering specific aspects of the organization, such as geolocation, number of employees and the need to work on the go.

In the last decade, mobile operating systems have definitely reached an important market share, therefore requiring **careful evaluation and use**, to allow any company to operate at the right speed.

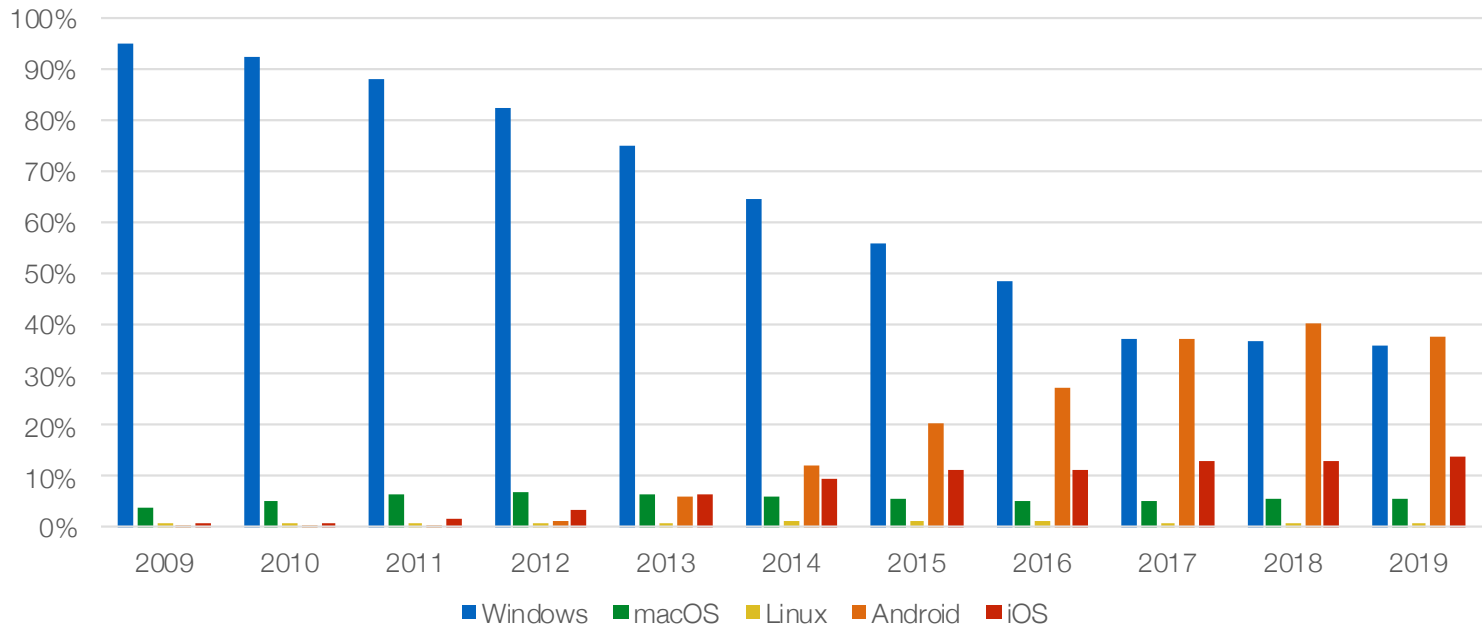


Image 7: **OS Worldwide Market Share**

Source: StatCounter (December 2019)

In order to select or renew company platforms in the best way, the Smart Working Manager will have to work closely with the IT Manager and find the best compromise between reliability, productivity and security, taking into account the **company's internal skills**.

In the context of small and medium-sized enterprises, the operating systems used by employees can be organized into 2 main categories: **Desktop** and **Mobile**.

Generally, in the Desktop area, operating systems such as **Windows** and **macOS** are preferable to increase productivity, while **Linux** is intended for system administrators and low-level IT activities.

The Mobile sector today includes only 2 main operating systems on the market, Android and iOS, both reliable and modern platforms, with strengths and weaknesses.

Android is a so-called "open" platform, owned by Google and available on millions of devices, with a global mobile market share of almost 75% (data of December 2019). Among the strengths of Android there is certainly the low cost and a large community for the development of ad-hoc applications.

iOS, owned by Apple, is a proprietary platform and among its strengths there is certainly a perfect integration between software and hardware (produced by the same company) and a very high ease of use. However, the costs are less cheaper.

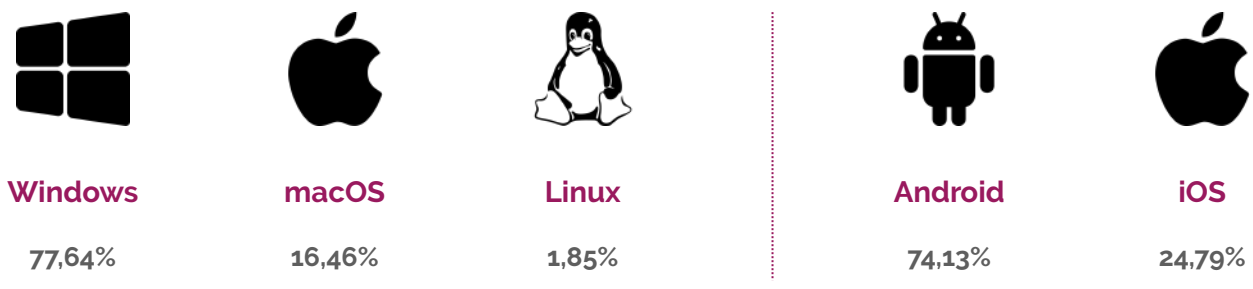


Image 8: **Desktop and Mobile OS Worldwide Market Share**

Source: StatCounter (December 2019)

2.1.3 APPLICATIONS

Software applications are a crucial component for any modern company and a mandatory choice for the **implementation of Smart Working**.

Choosing the right applications means equipping your organization with useful working tools, speeding up production, facilitating collaboration and - consequently - **increasing productivity**.

Applications must be carefully selected, interacting with all company departments and taking into account 3 main aspects: **licensing costs**, **ease of use** and **IT maintenance**.

Image 9: **Applications Choice Variables**

There are hundreds of areas of applications, such as accounting, communication, office automation, each of which allows the acceleration of business productivity.

Regardless of the choice of business applications, there is a critical factor that must be considered within any organization: **data storage** and its security.

The Data Economy

We live in a data economy, where every company accumulates data without erasing it anymore.

Storage applications are responsible for data retention and allow to store and access all company information, such as files, documents, databases, virtual machines, which can be stored at the company headquarters (local network) or using third-party services (cloud services).

Choosing the right storage applications has now become critical and even SMEs should consider opting for **enterprise solutions** in order to protect their data.

Among the most important factors to consider: end-to-end data **integrity**, advanced data **self-healing** mechanisms, **compression** technology and immutable **snapshots**.

End-To-End Data Integrity

Advanced Data Self-Healing

Compression Technology

Immutable Snaphots

Image 10: **Enterprise Storage Features**

2.2 COLLABORATION

Collaboration is essential to allow all Smart Workers to operate as **comfortably** and **efficiently** as possible, but it's also a powerful tool for amplifying the perception of belonging to the company and to share objectives and results.

Among the countless collaboration tools available today on the market, there are 3 types that cannot be missing within any modern organization who wants to take full advantage of Smart Working: **E-mail**, **Instant messaging** and **Video conferencing**.

Image 11: Collaboration Tools

2.2.1 E-MAIL

E-mail is a widely used tool for communication, both inside and outside the company.

With an estimate of almost **250 billion messages** transmitted every day, over the last 5 years has been recorded an overall increase of 20%, with a constant average increase of 5% on an annual basis.

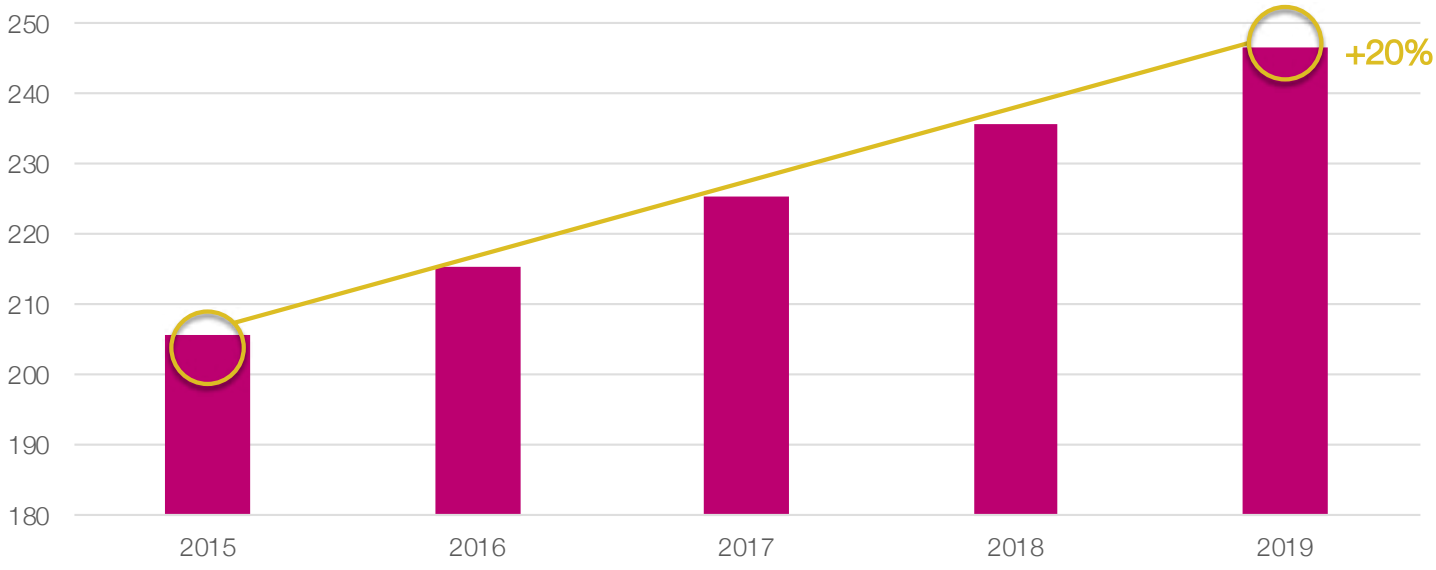


Image 12: **Worldwide E-mail Statistics (billions)**

Source: The Radicati Group | Palo Alto (CA), USA

In 2019 a transmission per day of **128,8 billion business** emails and **117,7 billion consumer** emails was estimated, with a constant annual growth (between 2015 and 2019) of 3% and 6%, respectively for business and consumer.

SPAM messages (which bypassed anti-spam and security filters) are estimated to be **around 20%** of total business messages sent worldwide in 2019.

Based on collected statistics, it is therefore important to use e-mail messages in the right way, by **limiting the sending** to useful communications only, both internally and externally to the company.

Today, dozens of professional email clients are available on the market and some of them also in **multi-platform** mode. The choice of the corporate e-mail client should be made taking into account the three main aspects for choosing the best application solution (see paragraph 2.1.3).

Corporate E-mail

Regarding the management of professional email addresses connected to a corporate Internet domain, small and medium-sized enterprises can evaluate both **home-managed** solutions and third-party **cloud services**.

To completely manage e-mail within the company, **low-level IT skills** will be required, in addition to the presence of dedicated personnel for maintenance; in case of third-party services, instead, additional variables must be taken into consideration, such as the management of remote **backups** and the **privacy** of information stored on servers external to the company.

In both cases, it is important to **protect corporate devices** from receiving SPAM messages, which - on a large scale - could also risk compromising the correct functioning of the corporate network and e-mail clients, saturating the bandwidth and flooding e-mail applications.

2.2.2 INSTANT MESSAGING

Instant messaging (also referred to as “chat”) is an extremely modern and versatile tool that enables companies to increase their **efficiency** and improve **customer relationship**, through valuable features such as speed, multimedia and widespread use.

Recent statistics show how the adoption of IM continues to growth also among business users, offering **real-time communication** between two or more users.

IM solutions, today, are increasingly feature rich and blend with unified communication suites to include group chat, conferencing, voice, video, and much more.

In 2019, the number of worldwide IM accounts total **over 7 billion**. This figure is expected to grow at an average annual rate of about 6% over the next 4 years, and reach over 8,9 billion by the end of 2023.

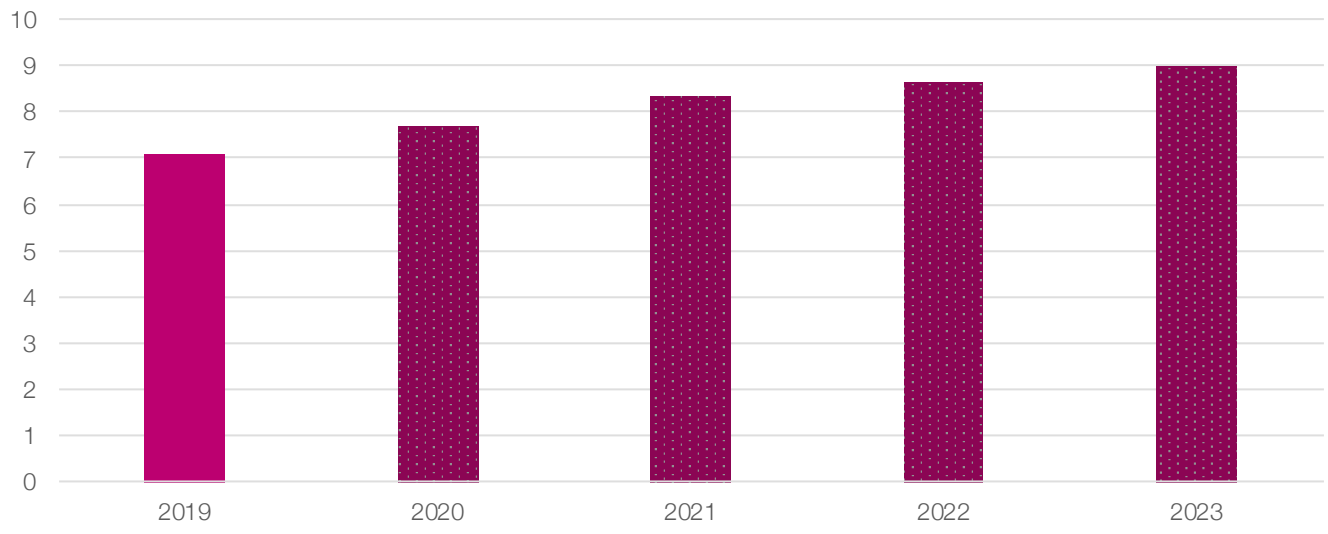


Image 13: **Worldwide IM Accounts Forecast (billions)**

Source: The Radicati Group | Palo Alto (CA), USA

2.2.3 VIDEO CONFERENCING

Video conferences are modern tools particularly suitable for organizing company **internal meetings** or for **direct contact** with suppliers, business partners and customers.

There's more to video conferencing than just serving as a convenient way to communicate; it has become an integral part of the way businesses operate, especially in the era of Smart Working.

Choosing the right video conferencing application should also have security in mind, making sure to activate password-protected accesses (or other authentication mechanisms) and to be able to count on a **fully encrypted** work environment, for example for screen or file sharing.

Where people use video conferencing is changing. It allows employees to work from **wherever** they are, meaning their work, success and happiness is no longer limited to the office or the meeting room.

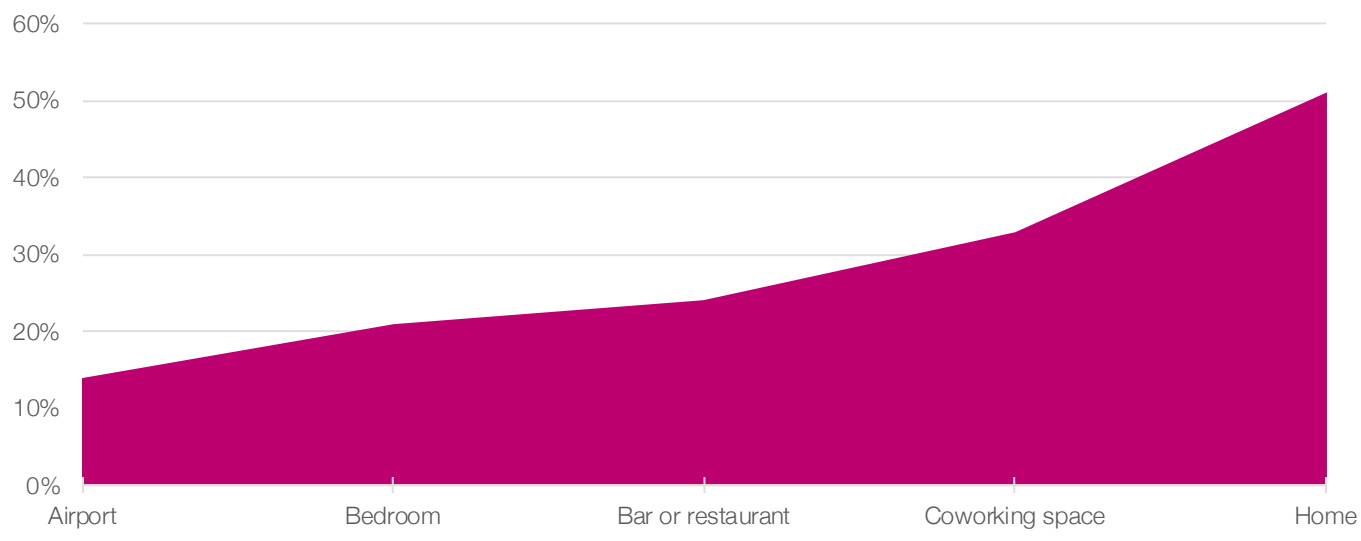


Image 14: Video Conferencing Smart Places

Source: Lifesize, Inc. | Austin (TX), USA

3. THE SECURITY

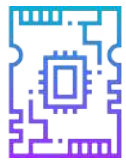
Many companies convince themselves they have nothing of value to hackers. Totally wrong. All data has a value and all companies have something which interest cybercriminals. **Even just for fun**.

Without cyber security measures, any business can face huge loss caused by a vast array of cyber attacks. These attacks can harm personal and business sensitive information.

Computer security is an essential feature, at the basis of any computer tool in the modern era and must take care of protecting from 3 different types of attacks: **Software**, **Hardware**, **Social**.

Software

Data Protection



Hardware

Physical Defenses

Social

Human Factor

Image 15: **Types of Attacks**

There is no way to protect anyone 100% from these attacks, as technological evolution occurs on a daily basis. And exactly for this reason it is vital for every company to manage this topic in the long term and to assign **dedicated internal staff**.

3.1 DATA PROTECTION

Data are radically transforming our society and economy. In a context increasingly focused on the Internet, the use of mobile devices and objects that communicate with each other (IoT), we are witnessing the production of an **unprecedented amount of data**.

Data protection allows to activate security countermeasures against **software attacks** and protect all information transmitted, received or simply stored within company devices, ensuring the protection of business assets.

For all employees or consultants employed in smart working mode, regular sessions should be scheduled in order to share updated information about all possible threats that may risk compromising the security of the entire company and its data.

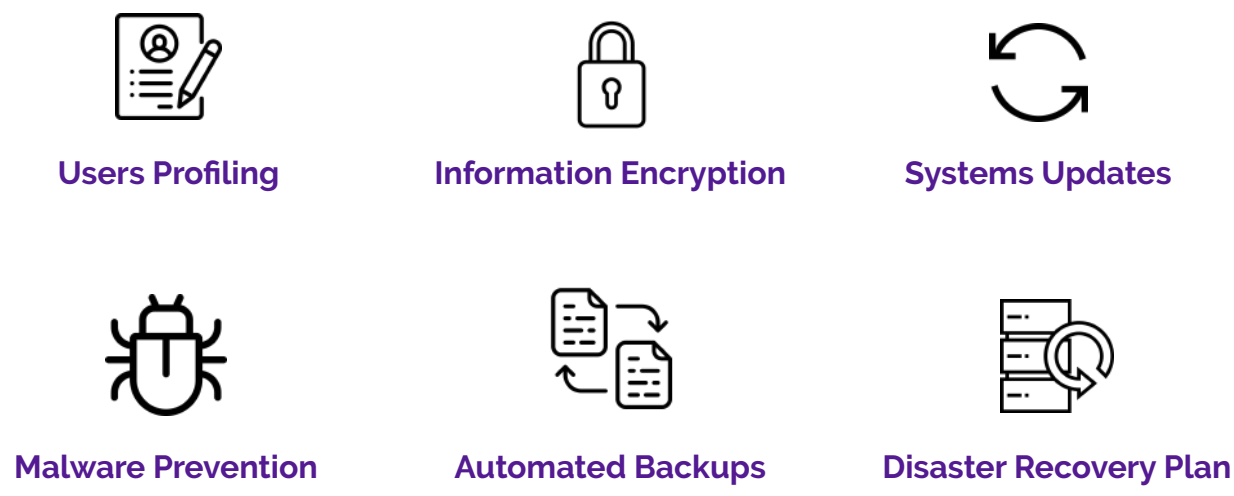


Image 16: Protections from Software Attacks

3.1.1 USERS PROFILING

To minimize unauthorized access attempts to company servers, it's becoming crucial also for SMEs to embrace the **Zero Trust** philosophy: never trust and always check.

Enabling unnecessary permissions is one of the most risky elements that can allow access, damage and/or destruction of corporate information through unauthorized accesses or human errors.

Each individual must be authorized to access **only the specific resources** with which he/she needs to interact to carry out his/her work. This technique is also known as the *Segregation of Duties*.

Passwords are likely to disappear in the near future, therefore all remote users should be equipped with strong personal authentication mechanisms such as **fingerprint**, **biometric** and **2FA**.

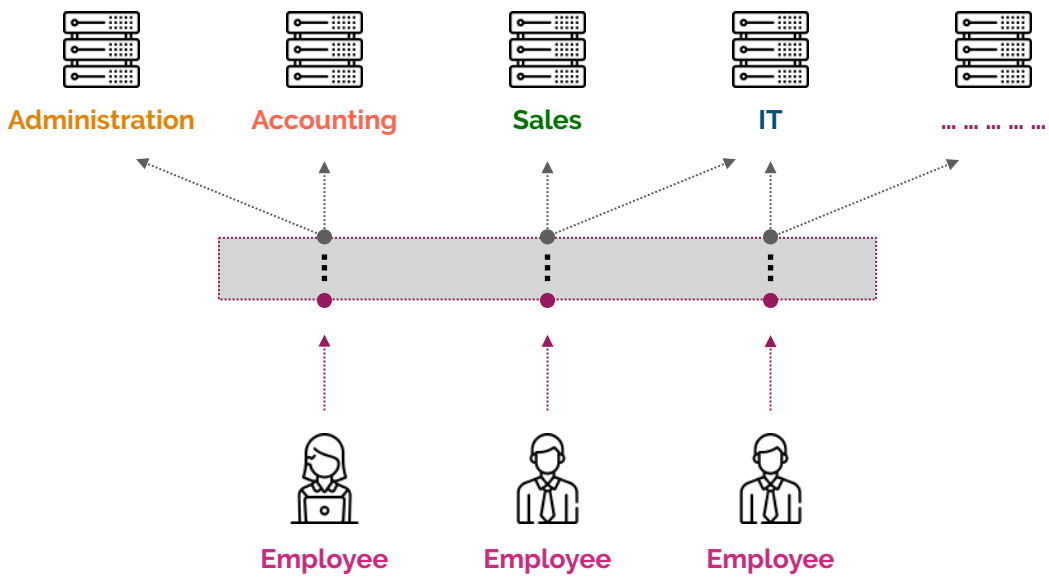


Image 17: **Segregation of Duties**

3.1.2 INFORMATION ENCRYPTION

The encryption allows to transfer data to and from the company infrastructure in a safe way.

Although today it is not possible to avoid 100% the interception of a communication, the adoption of encryption guarantees the protection of the transmitted data, since - even if intercepted by malicious people - they would not be intelligible.

More in detail, the encryption is the process of encoding data so that only a computer with the right decoder will be able to read and use it. Encryption can be used to protect any kind of communication, like files stored on employees systems, e-mails send to colleagues or visited websites.

An encryption key tells the computer what computations to perform on data, to encrypt or decrypt it.

The most common forms of encryption are **symmetric-key** encryption or **public-key** encryption:

- In **symmetric-key encryption**, all computers (or users) share the same key used to both encrypt and decrypt a message.

- In **public-key encryption**, each computer (or user) has a public-private key pair. One computer uses its private key to encrypt a message, and another computer uses the corresponding public key to decrypt that message.

Through the use of algorithms, data is made into meaningless cipher text, that requires the use of a key to transform the data back into its original form. Although there are several encryption algorithms, the most secure are **AES-256** and **RSA-4096**, where 256 and 4096 are the ciphers keys' lengths.

AES (Advanced Encryption Standard)

AES features three different key sizes, 128 bit, 192 bit and 256 bit. The key size determines whether there will be 10, 12 or 14 rounds of the encryption steps. The AES algorithm is used to secure a big number of common applications and protocols, like: WinZip, VeraCrypt, Signal, WhatsApp, TLS, SSH.

AES is also approved by the U.S. Government for encrypting classified information:

- SECRET data can be encrypted with 128 bit keys;
- TOP SECRET data can be encrypted with either 192 bit or 256 bit keys.

There are a number of known side-channel attacks that affect various implementations of AES, but the algorithm itself is considered secure.

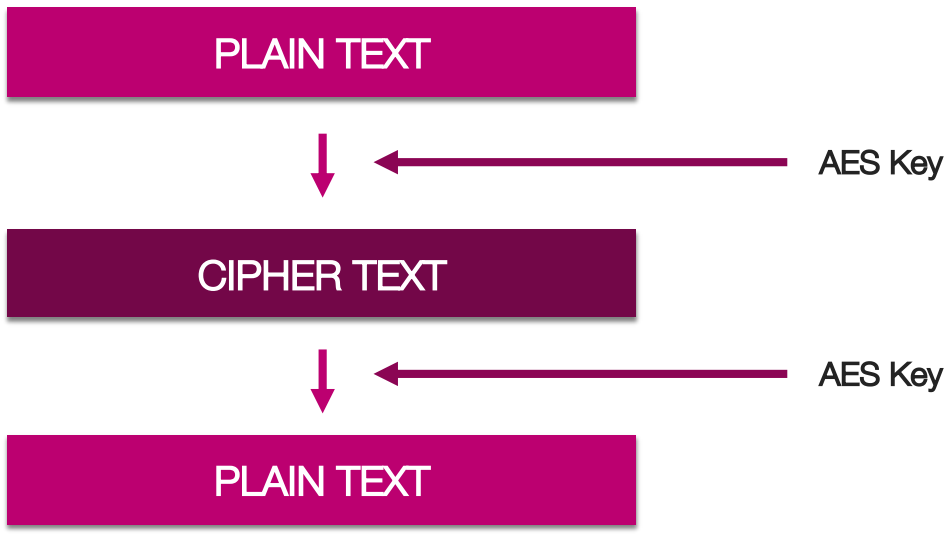


Image 18: AES Encryption Algorithm

RSA (Rivest–Shamir–Adleman)

RSA was the first asymmetric encryption algorithm widely available to the public. Since it's a public-key encryption scheme, its users encrypt data with the public key of their intended recipient, which can only be decrypted with the recipient's private key.

RSA is often used in TLS (Transport Layer Security) and is often the first algorithm that someone turns to when they need public-key encryption. Many VPNs rely on RSA to negotiate secure handshakes and set up encrypted tunnels between servers and clients. RSA is also used to create digital signatures, which verify the authenticity and integrity of data.

A number of vulnerabilities have been discovered in various implementations of RSA, but the algorithm itself is considered safe as long as 2048 bit or larger keys are used.

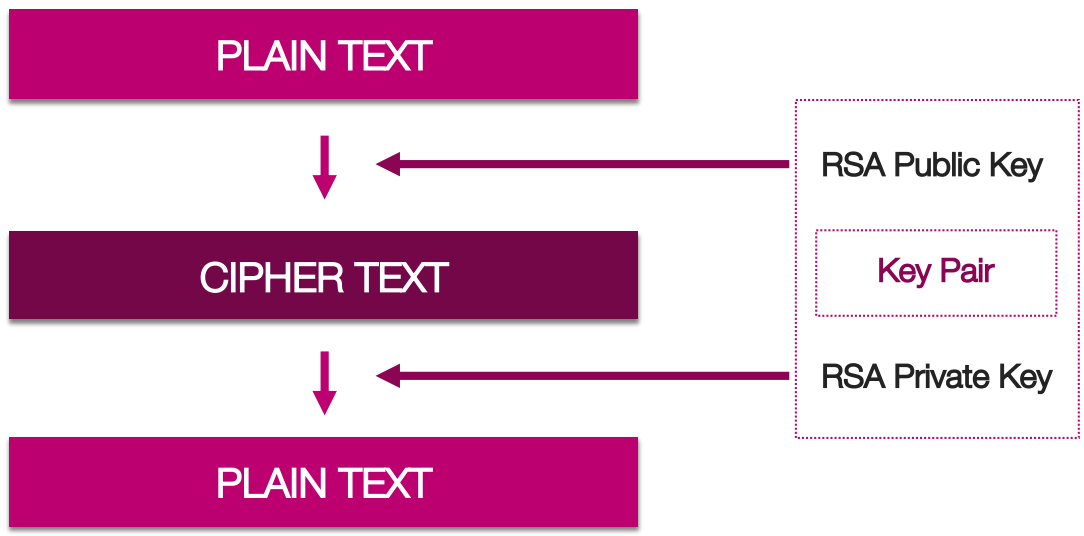


Image 19: **RSA Encryption Algorithm**

An efficient and safe Smart Working environment should consider 5 areas to be protected with encryptions measures: **Drives**, **Connections**, **E-mail**, **Instant messaging** and **Web navigation**.

Drives encryption

The hard drives of all corporate devices (desktop and mobile) should be encrypted, in order to ensure the security of information and its transfer, regardless of whether they remain on the local network or are used by remote users in Smart Working. All modern operating systems provide embedded encryption tools for the rapid encoding and decoding of information.

Connections encryption

VPN stands for Virtual Private Network and consists of creating a virtual tunnel between a client and a server. All information is encrypted before being transferred and the transmission takes place on a dedicated virtual network that cannot be accessed by other devices. Any connection should also be protected with strong password and multi factor authentication.

E-mail encryption

Every day a company sends and receives a large number of emails, to allow communication with its employees, partners and customers. The most used encryption software is called PGP (Pretty Good Privacy) and allows direct encryption of all outgoing email messages. PGP is Open Source and also provides features for the encryption of files, directories and disk partitions.

Instant messaging encryption

When choosing an enterprise messaging application, it is important to identify a software that supports end-to-end encryption. This type of encryption allows to prevent data being read or modified, other than by the true sender and recipient(s). All messages are encrypted by the sender and the service provider does not have a means to decrypt them, storing them encrypted.

Web navigation encryption

Web browsing exposes users to a large number of dangerous threats, some of which are able to intercept the transmitted data, by recording or altering them. To prevent the use of unsafe websites and applications, it is important that all employees check the presence of the security certificate (SSL) every time the connection to a web resource is established.

3.1.3 SYSTEMS UPDATES

Constant updating of **operating systems** is essential to prevent threats and allow immediate application of security patches.

The Smart Working Manager must therefore guarantee the **correct execution of the updates** as soon as they are released by the software houses.

In addition to operating systems, it is essential to monitor the presence of updates and security patches also for **applications** used for business productivity (e.g. office automation programs, messaging applications, mail clients, etc.).

Typically, any software has internal auto-update mechanisms, which must be correctly configured and allowed both at the application and at the network level.

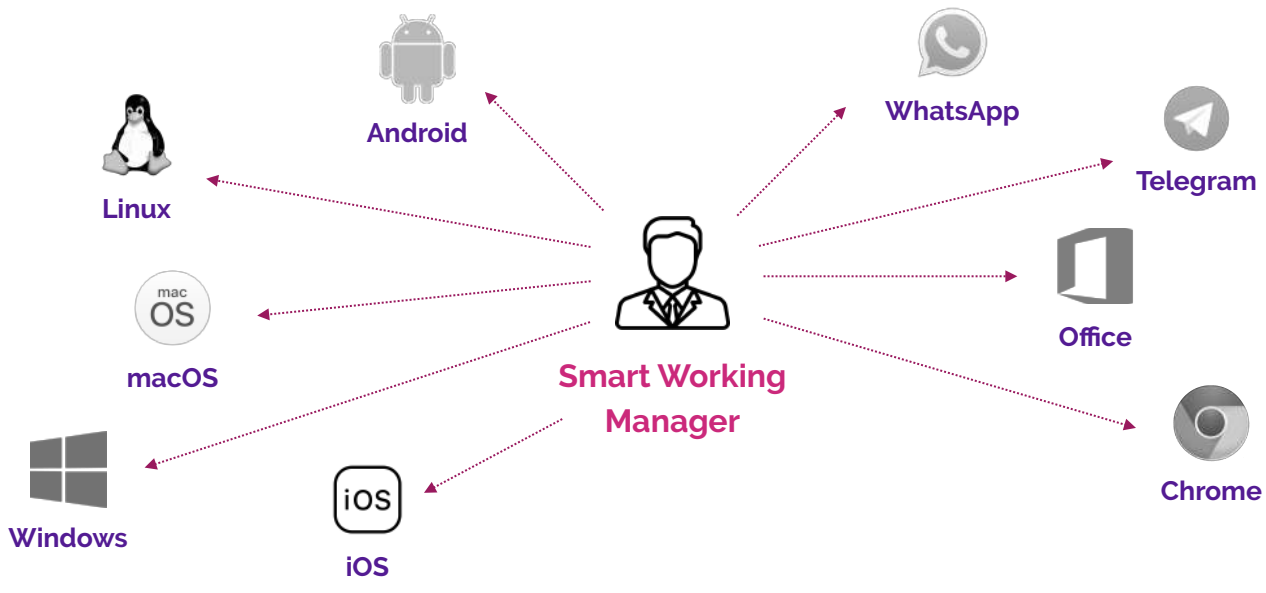


Image 20: **Example of Systems Updates**

3.1.4 MALWARE PREVENTION

Malware and its derivatives are a serious threat in today's communications and must be treated with the highest attention, in order to protect corporate data assets.

Every day, **more than 350.000** new malicious programs and potentially unwanted applications are detected over the network, which can cause serious risks if not immediately blocked.

Over the past 9 years, the proliferation of malware has globally increased by **more than 1.400%**.

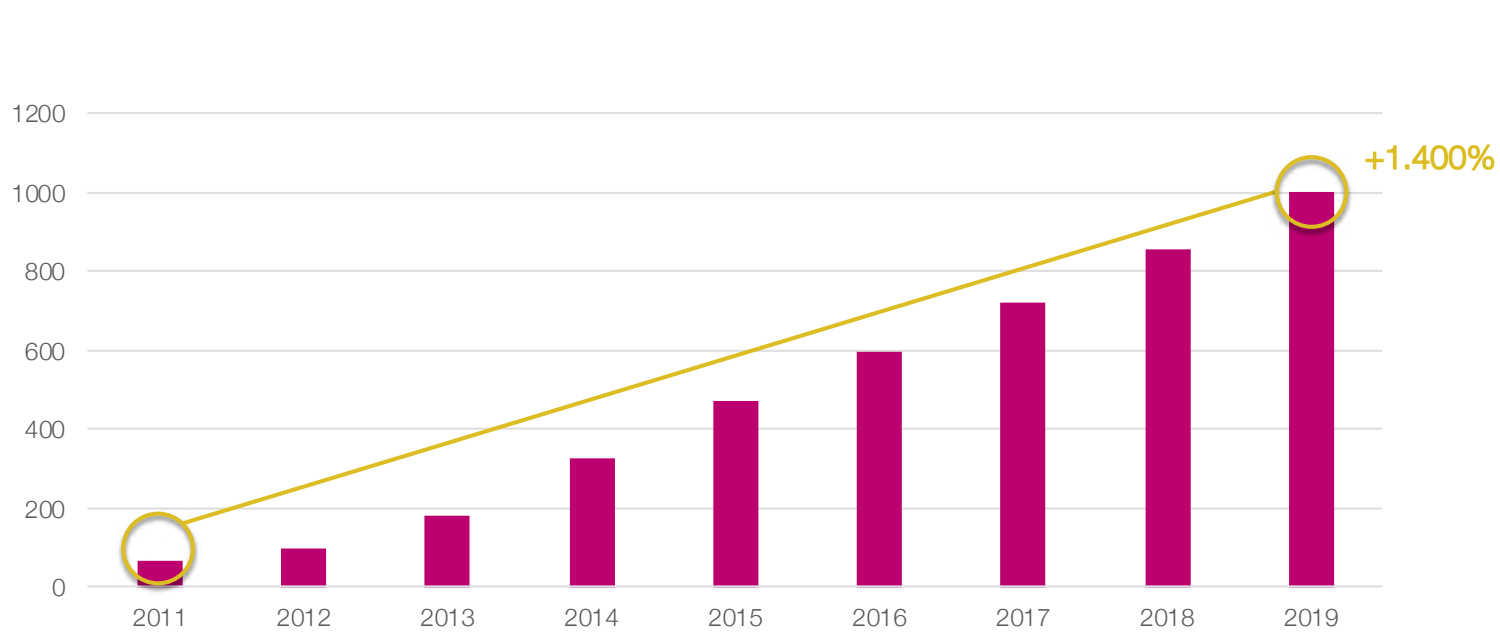


Image 21: Malware Statistics (millions)

Source: AV-TEST Institute (AV-TEST GmbH) | Magdeburg, Germany

Each organization should consider a **careful selection and installation** of protection software for all company devices, whether they are used on the corporate local network or used in Smart Working.

Nowadays several protection applications are available on the market, but it's important to understand that malware protection is **not enough** to fully defend an IT infrastructure.

Hackers evolve along with security, adapting their attacks to **bypass** antivirus security engines and thus be able to install their scripts within the target systems.

In addition, malware protections are completely **useless** in the event of attacks with 0-day exploits.

Hence the need to combine antivirus protection with backups and disaster recovery plans (see paragraphs 3.1.5 and 3.1.6), in order to make the infrastructure **immune** even in the event of an attack.

Below are listed the main software threats most widespread today (in alphabetical order):

Image 22: **Software Threats**

Adware

Adware derives from advertising. Its main function is to show the user advertising. They are usually not dangerous, but disturb the user with annoying warnings and can compromise the stability of the overall system and the availability of resources.

Backdoor

A backdoor is usually used by another program that installs and starts itself to gain malicious access to a target system. Backdoors are very often run by Trojans, so anyone who attacks a system with a backdoor can easily get in. Infected systems are called *bots* and are part of a *botnet*.

Exploit

An exploit is used to take advantage of a specific system vulnerability, within the operating system or inside an application. There are different types of exploits (0-day, private, public, social) and - in general - anyone launching an attack with an exploit will be able to take full or partial control of the target computer.

Key Logger

A key logger records everything is typed from the keyboard. In this way it can steal passwords and other important data, like credentials, banking accounts and other sensitive information.

Ransomware

A ransomware (*blackmail*) is designed to encrypt user's data and/or block the entire system. Once an amount of money has been paid to an anonymous service, system files may be decrypted and the system may be usable again.

Rogue / Scareware

Also known as *Rogue Anti-Spyware* or as *Rogue Anti-Virus*, rogues present themselves as security solutions, but they are fake programs. Most often they show fake warnings that encourage the user to buy programs, created for the sole purpose of stealing money.

Rootkit

A rootkit guarantees free access to an attacker; for example, it will hide other processes and make attacks more invisible to the user. Rootkits are generally installed by Exploits or Trojans.

Spyware

A spyware is used to spy on a target device, for example to collect information that passes through the system without getting noticed by the user.

Trojan

A Trojan is a specific type of malware disguised as benevolent software. When a user installs a Trojan, it takes full control of the computer and do whatever it wants with local resources. Generally, a Trojan is capable of installing other malware such as viruses, backdoors or key loggers.

Virus

A virus is a software that spreads itself by modifying other applications. Its name is an analogy to its biological namesake. A virus start spreading as soon as it can and when the host is not capable to keep it spreading anymore, it starts performing malicious processes.

Worm

A Worm is a malicious software that tries to spread itself as soon as it infects a system. Unlike a virus, it doesn't need other programs to inject, since they generally spread via USB, email messages or vulnerabilities within operating system. The propagation slows down the resources of the infected computer and the network connection. It can also insert malicious code into the system.

3.1.5 AUTOMATED BACKUPS

Choosing the right backup solution plays a crucial role for every small and medium-sized business and must be positioned next to a correct antivirus solution and a disaster recovery plan.

Most commercial and low-cost backup applications are often **vulnerable** to several attacks (like ransomware), since - by making a simple copy of the data - they would duplicate them together with the malware. Thus, it is advisable to equip with an "enterprise automated data protection" solution, capable of performing **distributed backup** of data, also relying on cloud technologies.

Furthermore, albeit at a higher cost, it is highly recommended to choose an automated backup solution with low **RPO** (Recovery Point Objective) and **RTO** (Recovery Time Objective) parameters, which respectively represent the time elapsed between the production of data and its safety (RPO) and the time required for full recovery of the data (RTO).

Image 23: **RPO & RTO Parameters**

Source: ICT&Strategy S.r.l. | Milan, Italy

3.1.6 DISASTER RECOVERY PLAN

By Disaster Recovery we mean the set of technological, logistical and organizational measures aimed at **restoring systems, data and infrastructures** necessary for the provision of business services, in the event of serious emergencies that affect its regular activity.

At first glance, disaster recovery planning may seem as simple as creating a basic summary of how to restore systems following a disaster. In reality, however, effective disaster recovery planning requires much more than this, creating detailed and **step-by-step procedures**.

The Ponemon Institute's *"2019 Global State of Cybersecurity in Small and Medium-Sized Businesses"* study found that **39% don't have a recovery plan** in place. This is in spite of the fact that of the same study participants, **60% had experienced a loss** or theft of sensitive data in the previous 12 months.

The below breakdown provides an insight into the factors causing downtimes:

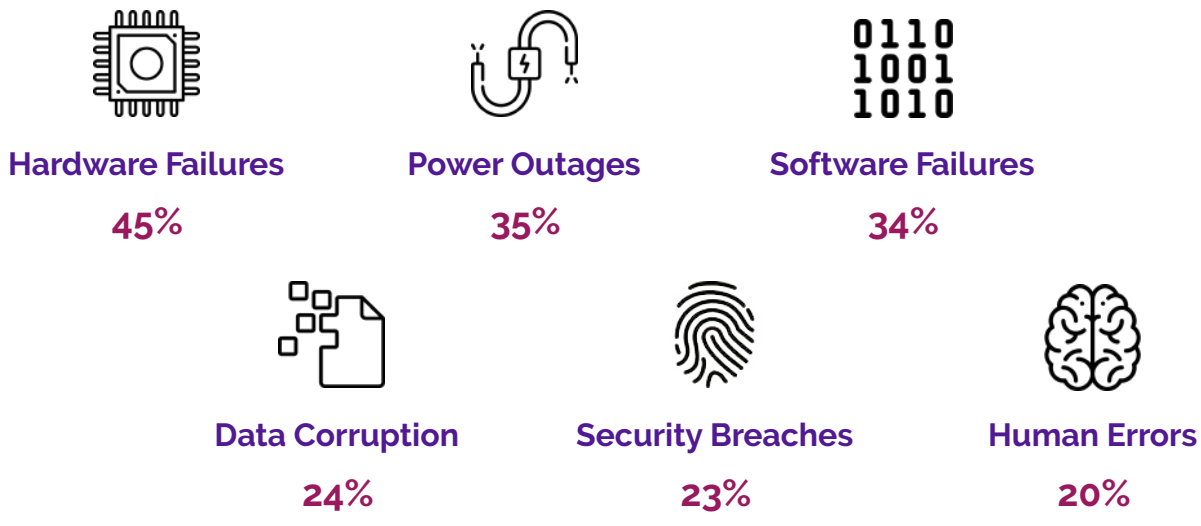


Image 24: **Business Downtime Causes**

Source: Veritis Group, Inc. | Irving (TX), USA

Hardware failures account for 45% of the downtimes globally and are normally linked to the lack of care in choosing consumable components, such as disks. It is therefore necessary to choose modern file system technologies that include concepts such as **software defined RAIDs**, **erasure coding** and **distributed filesystem**.

A careful evaluation between the costs and benefits of the RPO and RTO parameters (see paragraph 3.1.5) is therefore highly suggested, adapting them to the specific company situation.

Data corruption and security breaches also contribute significantly to business downtime, reaching 47% of the total: on these topics, a lack of preparedness could be extremely costly as businesses are required to scramble to return their systems to normal, after a problem or attack.

Even if SMEs might not have the budget for a full disaster recovery plan - or they might choose not to pay for it - the good news is that disaster recovery is **becoming cheaper**, simpler and more effective, through the growth of cloud-based services.

Companies no longer need to invest in dedicated hardware, remote data-centers and skilled staff to maintain them. **Cloud** or **Hybrid cloud** technologies allow smaller companies to outsource much of the technical side of disaster recovery provision and to move to an on-demand model.

Image 25: **Cloud Technologies**

Public cloud

SMEs can usually opt for the public cloud, that means contacting a service provider that will completely manage the servers on which the company data will be stored, without having to worry about anything, neither of maintenance, nor of ordinary management.

The only drawback here concerns data privacy. Even if service providers today guarantee maximum data protection, it is still true that files and documents are stored in a space outside the company.

Private cloud

The second option is the private cloud, which is usually adopted by larger companies that wish to have a greater degree of protection of their internal data. In this case, the virtual server that manages the cloud is internal to the company; costs are therefore fixed and higher than in the public cloud.

Here there is the need to manage everything internally, with dedicated skilled technicians. Furthermore, it is crucial to choose both the appropriate servers and the virtualization system.

Hybrid cloud

The third possibility is a hybrid solution that combines private space with the use of the public cloud.

Costs are variable, because there is a fixed base generated by the private component and another that changes according to the use made of the public cloud. The hybrid cloud is the most difficult system to manage, but - at the same time - it is the **most versatile**, because it offers many more possibilities.

3.2 PHYSICAL DEFENSES

Physical security is often a second thought when it comes to information security. Since physical security has technical and administrative elements, it is often **overlooked** because most organizations focus on "technology-oriented security countermeasures" to prevent hacking attacks.

Hacking into network systems is not the only way that sensitive information can be stolen or used against an organization. Physical security must be implemented to prevent attackers from gaining physical access; firewalls and other security measures would be useless if that were to occur.

The challenges of implementing physical security are much more problematic now than in previous decades. Laptops, USB drives, tablets, flash drives and smartphones all have the ability to store sensitive data that can be lost or stolen.

The objective of physical security is to safeguard facilities, personnel, IT infrastructure, equipment and all other company assets, also in order to avoid facing **civil or criminal penalties** for negligence.

The strategies used to protect the organization's assets need to have a **layered approach**: it's harder for an attacker to reach their objective when multiple layers have to be bypassed to access a resource.

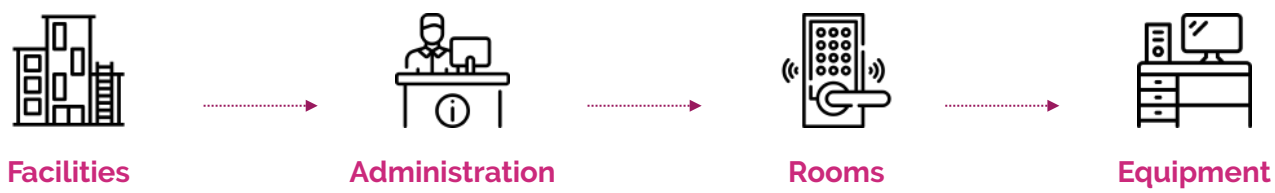


Image 26: **Physical Protection Layered Approach**

3.2.1 COMPANY FACILITIES

All facilities should have **automated controls** in place to protect the physical environment.

The first line of defense must be physical, technical and administrative controls; the last line of defense should always be employees, in order to reduce the risk of injury.

Server rooms or any place that houses IT or communications equipment must be off-limits to unauthorized individuals. These rooms have to be **locked down** to prevent attacks and should be protected with limited access to those employees that require access for job duties.

The more **human-incompatible** these rooms are, the less likely attacks are executed.

As stated in the *"Physical Security and Why It Is Important"* report of the SANS Institute, many mechanisms exist to discourage and detect access from unauthorized individuals and can be summarized in 4 main categories:

Image 27: **Facilities Protection Mechanisms**

Perimeter

Gates and fences are used outside of the facility to create an additional layer of security before accessing the building. Gates should be limited in number, to consolidate resources needed to secure them, and monitored by surveillance cameras when personnel is not present.

Badges

Proof of identity is necessary for verifying if a person is an employee or a visitor. These cards come in the forms of name tags, badges and identification (ID) cards. Badges can also be smart cards that integrate with access control systems.

Detectors

Motion detectors are used as intrusion detection devices and work in combination with alarm systems. There are different types of motion detectors that can be installed, according to the characteristics of the facility: infrared, heat-based, wave-based, capacity-based, photoelectric and passive-audio.

Alarms

Alarms monitor various sensors and detectors. Notification alarms send alarm signals through GSM (cellular) or Internet access. The siren output may be silenced or audible depending on if the organization is trying to catch criminals in the act.

3.2.2 EMPLOYEES EQUIPMENT

Companies that adopt Smart Working need to have a solid devices security plan in place. Without the proper tools and strategies, any remote device can become a **major security risk**.

Also, any company has the **right** and **obligation** to detail its security requirements. If an organization doesn't discuss this with employees, then they may not know the risks their devices pose.

Below are the 5 most used advises that help any small and medium-sized enterprise to use remote solutions while keeping enterprise safe.

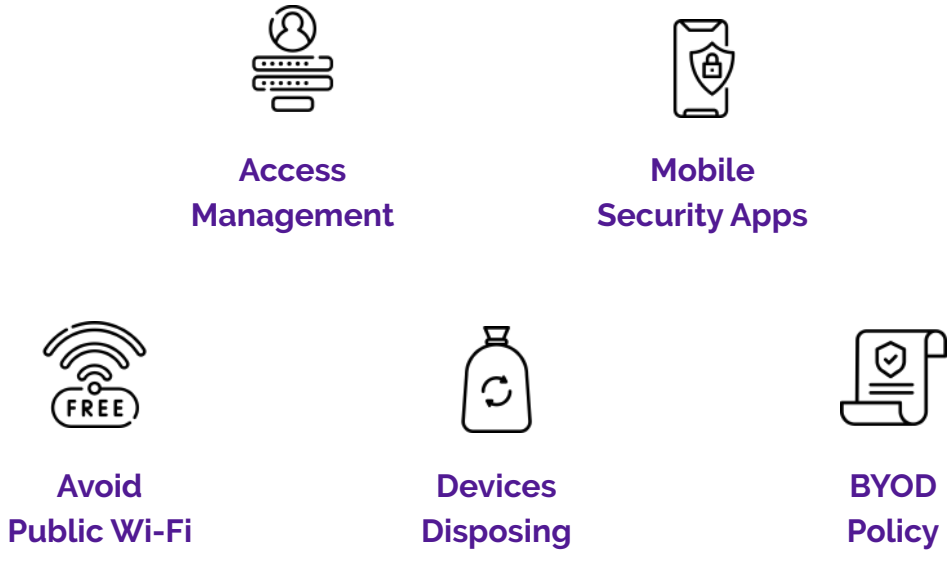


Image 28: Employees Equipment Security Tips

Access management

Security strategies need to account for the person that uses the device. If an enterprise assigns devices to employees, it should also make sure that only that employee can access that device, through security practices like passwords, 2FA and biometrics.

Mobile security apps

When designing a mobile device security strategy, any company need to consider how to secure the mobile device itself. One way to do this is by installing mobile security apps. These apps usually run in the background and constantly check for suspicious files or data transmissions.

Avoid public Wi-Fi

Although it's tempting for employees to do so, an enterprise device should never connect to public Wi-Fi networks, since are often much less secure and a frequent target for hackers. If employees take devices out of office, the employer needs to enforce keeping devices off from unprotected networks.

Devices disposing

Enterprises might decide to remove a device from their infrastructures. This could be because of the need to upgrade the hardware, to switch to a different model or when a device is lost. Whatever the reason, performing a full factory reset (local or remote) of device is strictly advised.

BYOD policy

BYOD (Bring-Your-Own-Device) is the practice of allowing employees to use their own computers and smartphones to connect to company network. Although personal devices provide employers with a constantly connected workforce and the ability to work remotely provides employees with flexibility, it can also put at risk business data and the status as a compliant company.

Creating an effective BYOD policy and monitoring employee security, helps protecting information transmitted and - consequently - the entire organization and its customers.

To ensure security over personal devices, any company should determine which of the following wants to apply to its organization:

- Password protecting devices according to the device's abilities;
- Requiring a strong password for device if it accesses the network;
- Automatic device lock requirements;
- Number of failed login attempts before the device locks itself;
- Forbidding use of devices that bypass manufacturer settings (i.e. jailbroken or rooted devices);
- Preventing downloading or installing applications not on the "allowed" list;
- Preventing devices not listed in the policy from accessing the network;
- Preventing employee-owned "personal use only" devices from connecting to the company network;
- Restricting employee access to company data based on user profiles (see paragraph 3.1.1).

3.3 HUMAN FACTOR

One of the threats still driving the lowest level of concern is the human factor.

Computer security is not just about technology and systems. It is also about the **people** that use those systems and how their vulnerable behaviors can lead to exploitation.

There are 3 main types of “errors” that employees can make - involuntarily or voluntarily - within any organization: **Unintentional errors**, **Unfaithful activities** and **Social Engineering**.

According to a study from CompTIA, human factor accounts for **52%** of the root causes of damages.

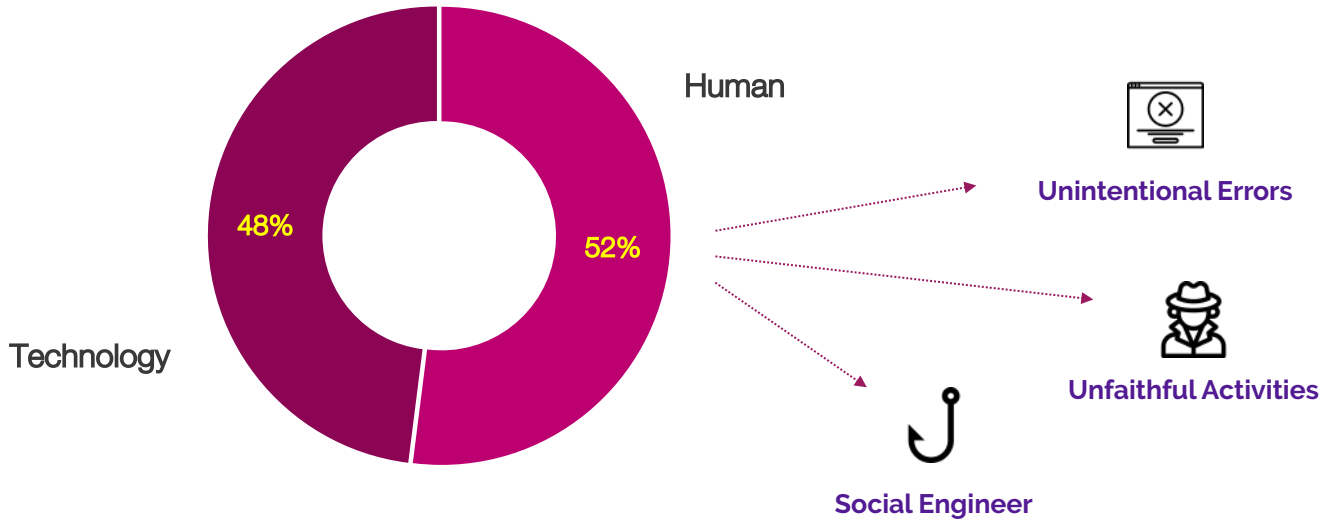


Image 29: **Security Breaches Root Causes**

Source: CompTIA, Inc. | Downers Grove (IL), USA

3.3.1 UNINTENTIONAL ERRORS

Sometimes employee take cybersecurity requirements too lightly, leading to dramatic consequences for the organizations they work for, whether that error comes from general staff or from IT staff.

Among the main causes that lead staff to make involuntary mistakes are:

- **26%** IT staff failure to follow policies and procedures;
- **29%** lack of expertise with websites/applications;
- **31%** failure to get up to speed on new threats;
- **42%** personnel general carelessness;
- **42%** end users failure to follow policies and procedures.

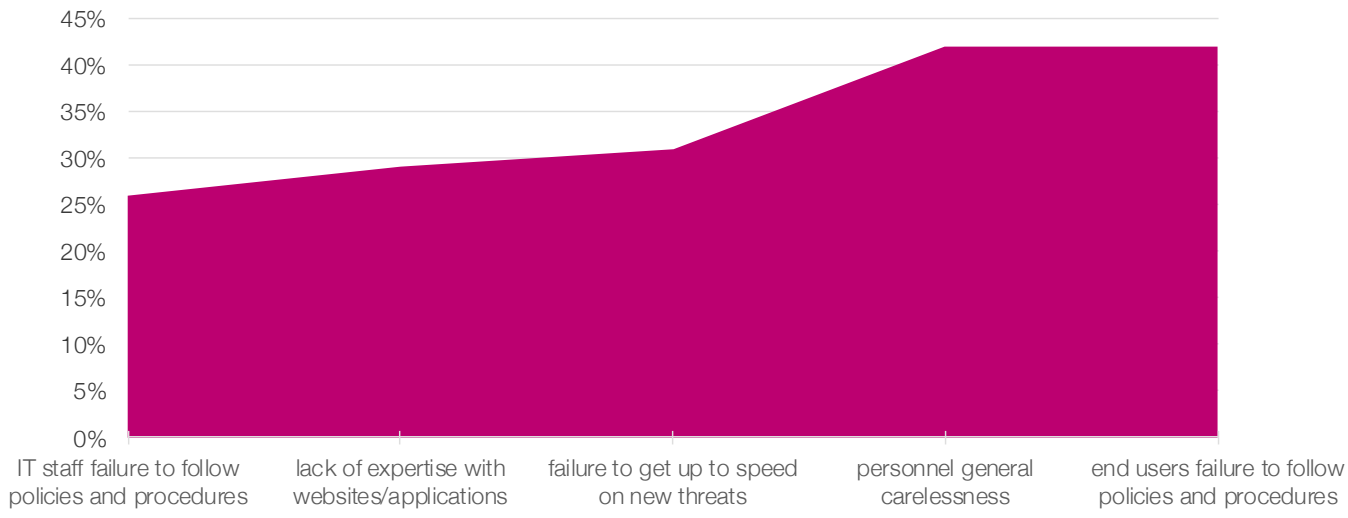


Image 30: Top Unintentional Human Errors Sources

Source: CompTIA, Inc. | Downers Grove (IL), USA

Internal training

A high level of concern over malware or hacking can be addressed with an investment in technology. A high level of concern about employee errors can possibly be addressed with an investment in training, but there are complications involved.

Most businesses struggle with the thought of providing education. It is not their *forte* and the effects are very difficult to measure. Some trainings offer direct correlation to business results, but this is especially complicated for an area like security, since the desired effect is the absence of any incident.

Still, most businesses have some notion of providing foundational training, whether that is job-related, compliance-driven, or HR-mandated. Security training is one of the most common offerings and several available programs should be seriously considered by SMEs as well.

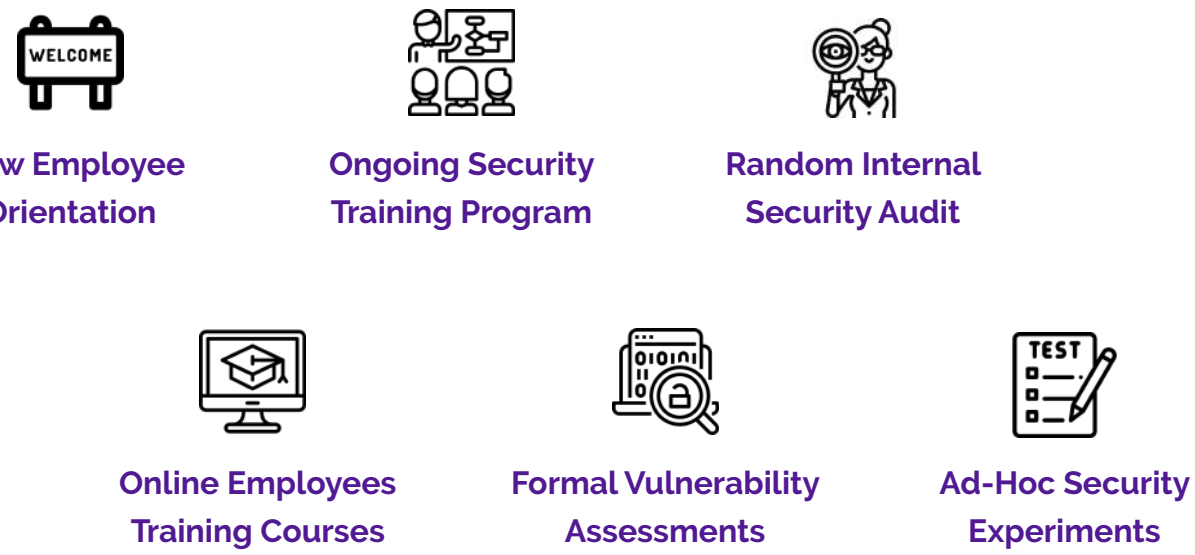


Image 31: Types of Security Training

3.3.2 UNFAITHFUL ACTIVITIES

Every company would like to believe that its employees will always conduct themselves correctly. The desire to implicitly trust the people a company has hired must be balanced with the reality that the risk of being attacked from **the inside** is constantly growing.

Some employees may choose to **intentionally** take advantage of that trust and seek to benefit themselves, producing devastating effects on company operations, reputation and bottom line.

There are 2 main types of employee misconduct. The first is known as **immediate discovery** and usually it's a physical theft, so immediately detectable. The second is called **delayed discovery** and can happen when an employee steals information and theft is not discovered until he resigned.

Therefore it's critical to understand the protection options available.

Image 32: Employees Misconduct Protections

Know your employees

Before hiring any employee make sure adequate due diligence is done. While reference checking is a great start, for executive management positions and those roles that require money management and access to intellectual property, client and financial records, a background check is recommended.

Ensure adequate supervision

While it's not recommend looking over an employee's shoulder every minute, close supervision can help to discourage theft, fraud and crimes of opportunity. It is also sensible to have more than one person responsible for critical management duties like money management and security.

Watch for changes in behavior

There are often signs or red flags that employees exhibit when considering or doing the wrong thing. A sudden change in their attitude towards work, for example, like coming in late, taking longer breaks, having more sick days, erratic behavior and frequent disappearances.

The opposite can also be a red flag, like a sudden commitment to working harder and later, a keen interest in operational procedures, or strong opinions and objections to procedural changes.

Install computer security measures

With a rise in flexible work arrangements, employers are being forced to give employees greater access to confidential information, to improve business efficiency and productivity.

While this can be beneficial for a business, it also increases the risk and opportunity for misconduct with confidential information being able to be accessed remotely.

For this reason, it's important to ensure to have adequate computer security measures in place. These may include implementing secure firewalls at the network perimeter, locking down remote access to users without a secure connection and enforcing 2FA (Two-Factor Authentication) for services.

It may also be a good time to review backup procedures (see paragraph 3.1.5) and perform disaster recovery testing (see paragraph 3.1.6).

Establish clear policies

Policies are crucial to a successful employer and employee relationship and can protect any business in a number of ways. They are also the only documents an organization have the power to update and change unilaterally.

A clear misconduct policy and a comprehensive code of conduct ensure that employees know what is expected from them and have a clear understanding on the consequences they can face.

Be specific in employment contracts

The employment contract is one of the most understated documents in any business, and yet it can be one of the most important when it comes to the employment relationship.

In any employment contracts it's possible to include clauses that protect company's intellectual property, address restraint of trade and the poaching of staff and clients, safeguard against underperformance and misconduct and most importantly address termination of employment.

When an employment contract is ongoing, it is crucial to have termination clauses that outline circumstances when employment can be terminated and how the termination will be carried out. Even though these clauses exist within contracts for company protection, it is recommended to speak to an employment law specialist before it's enforced, as there's a specific process that should be followed when terminating for misconduct which greatly reduces risks and liability for the organization.

3.3.3 SOCIAL ENGINEERING

Social engineering is a security topic of growing interest since it allows the implementation among the most effective and dangerous techniques for **accessing** and **stealing** information.

These techniques circumvent most of the cyber security systems, by exploiting human side and organizational weakness, focusing on **people and their roles** within a company and pushing users to perform specific actions, creating the conditions for the flaw through which to enter.

Attacks are conducted through **email**, **social media**, the **web**, **cloud apps**, or other vectors, whether they are motivated by financial gain or personal interests. Victims click malicious links, download unsafe files, install malware, transfer funds and disclose sensitive information at scale.

How can all this happen? Because hacking humans is **easier** than hacking computers.

A typical social engineering attack is accomplished through 3 distinct phases:

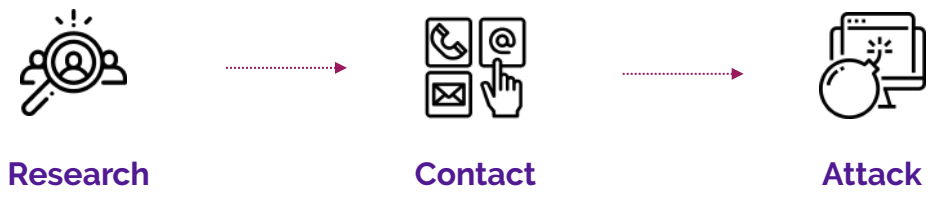


Image 33: **Social Engineering Attack Phases**

Research Phase

The first phase of any social engineering attack is research. During this phase, attackers search for information about a company and/or a specific employee.

The easiest route to find potential information is through the web or social networks. Social security best practices are key, as people often post personal information that attackers can use against them.

Contact Phase

After the research phase has finished, attackers will move on to the contact phase. During this phase, attackers will use researched information to look for other weaknesses and gain the target's trust.

This often includes pretending to be someone the target trusts. Once the victim trusts the attackers, the attackers can then leverage this for more information or access.

Attack Phase

The attack phase builds on the previous two phases. In most cases, this means that attackers have the necessary information and access to a specific person or company's systems.

Basic attacks use this access to steal information from a system, but some hackers go further. Advanced attacks can use this access to aid them in future attacks, for example by leaving a backdoor.

Social engineering is the new preferred tactic among the hacker community, since it's easier to exploit users' flaws than to discover a vulnerability in networks or systems.

Understanding different types of social engineering attacks is an essential aspect of protection.

Phishing

Phishing is one of the most common types of social engineering, especially against users who are not well-versed in browsing the internet or those who are new to using social media and online resources to search for information, content and media.

This technique presents a website, article or online community as authentic and secure, but - instead - uses a URL that is not official, to gain false hope and trust from potential victims and to receive sensitive information such as usernames, email addresses and passwords.

Baiting

Baiting is used in both the digital and physical world and consists of leaving devices in public areas that are packed with malware, spyware or other damaging software, which is then used to steal and collect the information of users who are tempted to see the contents of the device.

Most commonly, flash USB drives are left in areas such as bathrooms, libraries, subway stations, or even on airplanes in hopes to attract the curiosity of individuals. Once the user plugs the device into their computer, malware is downloaded onto the hard drive.

Spear Phishing

Spear Phishing is designed to personally attack an individual or organization to appear more authentic and legitimate, often utilizing a user's personal information or details about an individual to gain the trust and curiosity of the target before stealing information.

Spear Phishing is becoming more popular than traditional Phishing as users become aware of checking URLs and verifying the websites they browse. With a Spear Phishing attack, it becomes increasingly difficult to determine whether or not the URL or information is malicious.

Scareware

Scareware are extremely successful in obtaining user information and financial details and are often presented as popups or programs while prompting users with warnings or threats to receive information such as names, credit card details, and even social security numbers.

In many cases, Scareware are used to prompt individuals to download malicious software due to a threat of spyware or malware already infecting the user's hard drive; once the targets start the download, their computer is compromised and hackers then gain direct access.

Pretexting

Pretexting scams are used to collect personal information from individuals by impersonating police, government officials, bank account managers or even co-workers, targeting unsuspecting individuals who are likely to feel threatened if they do not share information requested.

Pretexting is done over the phone, via email, or in some cases, even with the use of social media messenger applications. Perpetrators who use pretexting often inform individuals that they are in need of highly sensitive information to complete a task or to prevent the individual from legal trouble.

Quid Pro Quo

Quid Pro Quo attack requests information from unsuspecting individuals with the promise of offering something in return. Targets are likely to receive offers of compensation, free vacations, or gifts such as new products that are most relevant to the individual's lifestyle.

Quid Pro Quo attacks occur over the phone, social media, or even through traditional email newsletters that have been hacked, compromised, or impersonated. Users are presented with the promise of something in exchange for login information, credential verification, or other sensitive details.

3.4 HACKER APPROACH

Chapter 3 covered security in all its aspects: software, hardware and human. However, a correct IT security must take into account another variable, the so-called "hacker approach".

Why hacking happens

Hackers can act just for fun, but most business cases are about **profit**. Paid by whom? By anyone who may be interested in stealing information (industrial espionage), or simply to put a company out of business (unfair competition).

Whatever the reason, as long as there are computers, there will still be hackers. And since it is certainly not possible to predict what type of attack a company could be subjected to in the future, it is always better to prepare to face the worst eventualities, even those deemed impossible.

The concept of *impossible*

Erri De Luca, a well-known Italian writer, gave this definition of the word *impossible*:

« Impossible is the definition of an event until the moment before it happens »

If a company intends to protect its data, *really* protect it, it must understand that any gateway must be considered, just like a person would do to protect their home, without neglecting anything.

When it comes to hacking, there are no impossible events: only events not considered.

Types of hackers

Hacking often refers to the unauthorized intrusion into a network or computer; normally carried out by one or more “hackers.” However, a hacker can be anyone. They can be an individual of the next door, they can work solo or be employed by an organization. Often, they look to alter security systems to achieve their goal, which differs from the actual purpose of the system.

BLACK-HAT HACKERS

The term “black hat” originated from Western movies, where the bad guys wore black hats and the good guys wore white hats. A black-hat hacker is an individual who attempts to gain unauthorized entry into a system or network to exploit them for malicious reasons.

The black-hat hacker does not have any permission or authority to compromise their targets. They try to inflict damage by compromising security systems, altering functions of websites and networks, or shutting down systems.

They often do so to steal or gain access to passwords, financial information, and other personal data.

WHITE-HAT HACKERS

White-hat hackers, on the other hand, are deemed to be the good guys, working with organizations to strengthen the security of a system. A white-hat has permission to engage the targets and to compromise them within the prescribed rules of engagement.

White-hat hackers are often referred to as ethical hackers. This individual specializes in ethical hacking tools, techniques, and methodologies to secure an organization's information systems.

Unlike black-hat hackers, ethical hackers exploit security networks and look for backdoors when they are legally permitted to do so. White-hat hackers always disclose every vulnerability they find in the company's security system so that it can be fixed before they are being exploited by malicious actors.

Some Fortune 50 companies like Facebook, Microsoft, and Google also use white-hat hackers.

GREY-HAT HACKERS

Grey-hats exploit networks and computer systems in the way that black hats do, but do so without any malicious intent, disclosing all loopholes and vulnerabilities to law enforcement agencies or intelligence agencies.

Usually, grey-hat hackers surf the net and hack into computer systems to notify the administrator or the owner that their system/network contains one or more vulnerabilities that must be fixed immediately.

Grey-hats may also extort the hacked company, offering to correct the defect for a nominal fee.

Think like a hacker

As masterfully reported by Giovanni Vigna (CTO of Lastline) in an article appeared on Darkreading.com, in the arms race of computer security it's never been more important to develop an **adversarial mindset** that can identify assumptions and determine if and how they can be violated.

Computer security is a very unique field. Unlike other fields in which the challenge is to overcome the scale of a problem or the complexity of an algorithm, in computer security the challenge is the wit of another **human being** who is trying to carry out an attack in order to compromise and disrupt a computing infrastructure.

Because of its **adversarial nature**, computer security is in continuous evolution. As it happens in many game-theoretical models, every move from either an attacker or a defender changes the state of the game and might invalidate current defenses or foil future attacks.

In this “game”, everything evolves, all the time, and anticipating the possible threats becomes of paramount importance. Therefore, security professionals need to always **think as an adversary**, or — essentially — “think like a hacker”.

« The best way to defend a network is by knowing how to attack it »

4. THE CONTROL

Management is required to carefully operate a constant **control at all levels**, to ensure that the benefits deriving from Smart Working do not alter corporate performance and business objectives.

The implementation of performance systems and processes are fundamental to assess the progress, to be able to know **at every moment** how the company is doing and what can be enhanced.

Performance management can be analyzed at 4 levels: **strategic**, **operational**, **team** and **individual**. This chapter focuses on the last two levels (team and individual), most impacted on agile work.

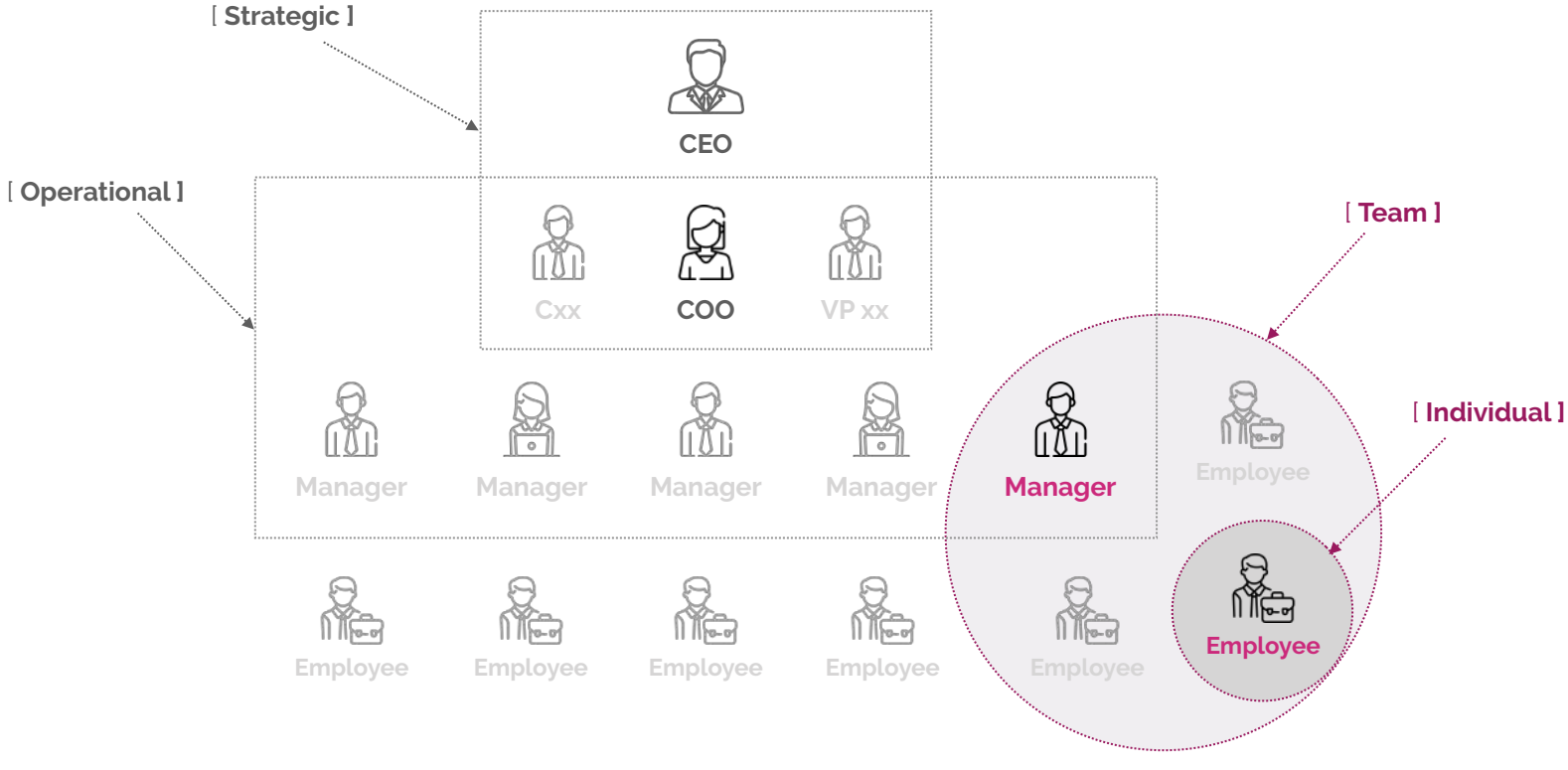


Image 34: **Team & Individual Performance Management**

4.1 PRODUCTIVITY MONITORING

Smart Working changes the concept of human resource management, no longer based on presence, but on real production and **achieved results**. More meritocratic, we could say.

A correct evaluation of results is possible only by applying a correct **information collection**, which should be based on 5 characteristics:

- **Accuracy:** information gathered must be accurate;
- **Timeliness:** information gathered must be in time to allow corrective action to be taken;
- **Economy:** benefits of gathering the information must be greater than the cost of gathering it;
- **Ease of understanding:** information should be understandable by the target audience;
- **Meeting needs:** information must meet the needs of the organization and the individuals involved.

There are 3 main ways to collect information from employees within any small and medium-sized enterprise that applies Smart Working: **Involvement**, **Tracking** and **Support**.

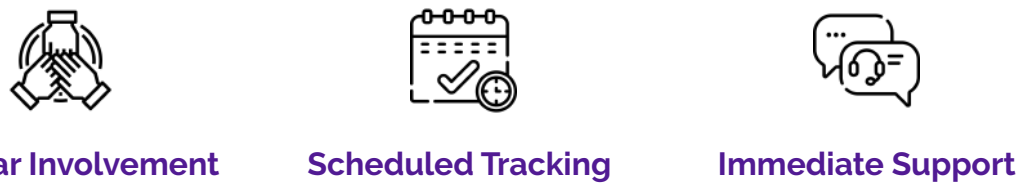


Image 35: **Smart Working Information Collection Techniques**

4.1.1 REGULAR INVOLVEMENT

Successful productivity monitoring starts with establishing a routine of **regular remote meetings**, by group or one-by-one. This one step alone can radically improve any manager's ability to stay on top of the details and hold people accountable.

This very common management technique assumes even more relevance when applied to Smart Working, considering that employees will spend a lot of time outside the company.

Although choosing the right tool and setting a clear agenda to save coworkers' time might be challenging, there are many benefits of remote meetings:

They are focused: good remote meetings are usually organized when there's something to discuss, to update or to solve, so the team can focus and achieve something together.

They are result-oriented: on successful calls, nobody wants to waste time, and — unlike with face-to-face meetings — it's harder to reschedule or walk away without a clear plan or list of action items.

They are well-structured: a remote meeting with a clear format, agenda and expectations allows everyone to prepare, think of the possible scenarios, and — ultimately — make sure voices are heard.

After a remote meeting is always a good idea to send a **follow-up**, to remind participants about the main points of the meeting and to increase its effectiveness and importance.

4.1.2 SCHEDULED TRACKING

Although it can be difficult to admit it, it's important to always have one point clear: in every company there are employees who invest themselves fully, while others only work just enough not to get fired, whether in traditional or smart work.

One way to override this attitude is to distribute tasks with **due dates** and **regular reminders**.

When workers have ownership of their own tasks and can see the progress made at every step, their attitude is likely to change towards completing that task on time. A **transparent team culture** increases employee trust, which is necessary to keep everybody focused on the same goal.

Activity tracking offers a window into how much a team or a single individual is working. In this way, the manager can see if someone is regularly going over their capacity and take some work off their plate before they burn out.

When a team knows that the company is using timesheet data to maintain a healthy work-life balance, they're more likely to see time tracking as something positive and actually do it.

Tracking can be achieved through the adoption of **dedicated software** and applications, which help in the management and scheduling of the company projects and their progress.

4.1.3 IMMEDIATE SUPPORT

Although the application of Smart Working allows companies to improve employee work-life balance, it is equally important that all remote staff are constantly able to perform the required business tasks without difficulty or blockages.

For this reason, it is necessary to have **prompt intervention procedures** in case of technical difficulties, through the use of e-mail, instant messaging or video conferences (see chapter 2.2).

The figure of Smart Working Manager could therefore be the central role to collect all the needs that risk slowing down the normal performance of activities outside the corporate headquarters.

Support tools available today are many, from the simplest ones based on direct and real-time contact, to the more structured ones based on **ticketing systems** or real support platforms.

Each company should make a choice based on factors such as its size, the number of employees in Smart Working and the available budget, as well as providing - in the case of more structured support systems - the allocation of dedicated internal staff.

In any case, every Smart Working employee must perceive the **constant availability** of the company, to be supported in the shortest possible time and avoid a heavy decrease in productivity.

4.2 SECURITY AUDIT

Chapter 3 ("The Security") dealt with security from a prevention point of view, focusing on different types of attacks for which it is necessary to equip a company with defense tools.

However, these important tools must be used in parallel with internal control and audit techniques, without which it would not be possible to realize their **effectiveness** and the **risks avoided**.

The frequency and sophistication of cyber attacks on SMEs are increasing. As per the 2019 Data Breach Investigations Report by Verizon, **43%** of cyber attacks is targeted at small and medium-sized enterprises. To set up a strong defense against cyber threats, every company must be aware of not just the threats but also the **state** of its IT security and vulnerabilities.

There are 2 types of technology security audits: **automated** and **manual**.

Automated audits are done using monitoring softwares that generate audit reports for changes made to files and system settings. Manual audits are done using IT audit checklists that covers 4 different security areas: **Physical**, **Administrative**, **Technical** and **Network**.

Image 36: **Security Audit Areas**

4.2.1 PHYSICAL SECURITY

When we talk about IT security, physical security (see chapter 3.2) doesn't readily come to mind. People generally tend to think about software, virtual infrastructure, and the Internet.

But a simple physical access restriction can mitigate a number of IT security risks.

Examples of audit checks for physical security

- Do you have policies to restrict physical access to servers or electronic information systems?
- Do you have controls such as door locks, access control systems, video monitoring, etc?
- Is access to your office controlled via security or reception desk, sign-in log or access badges?
- Do you escort visitors in and out of controlled areas?
- Do you use a physical lock or cable to secure laptops?

4.2.2 ADMINISTRATIVE SECURITY

It's amazing what can be done with a tiny USB storage device and high-speed Internet connectivity: within minutes company files can be copied, corrupted or hacked.

Therefore, strong administrative security controls must be in place and as a company reviews and updates its IT policies, all employees must also be educated about them.

Human error (see chapter 3.3) is a big challenge for IT security. Regular discussions on IT security threats, preventive measures, and phishing drills go a long way in reducing human error. Most phishing or malware attacks will fail if employees are aware of company policies and follow security protocols.

Examples of audit checks for administrative security

- Do you create a unique user account and username for each individual?
- Are admin accounts used only for performing admin tasks?
- Do you give remote access only to authorized users?
- Do you have a robust password policy to ensure all users have strong passwords?
- Have you implemented 2FA (Two-Factor Authentication) on all supported devices?

4.2.3 TECHNICAL SECURITY

With the adoption of every new technology, the complexities and consequent vulnerabilities increase. A company has to think of not just IT infrastructure, but also the cloud, SaaS platforms, network devices, etc. and their complex interplay.

Therefore, it is advisable to hire **professionals** to help with setting up the IT security.

Even if in-house IT staff is available, it is very likely that they do not have optimum exposure to new devices and security features. External help is also ideal for conducting penetration tests and phishing simulations.

Examples of audit checks for technical security

- Are anti-virus and malware protection installed on all computers and mobile devices?
- Do you maintain a list of all hardware including device name, type and serial number?
- Do you maintain a whitelist of applications that are allowed to be installed on devices?
- Do you maintain a list of accounts (usernames and passwords) that use online services?
- Is the use of USBs and external hard drives from unfamiliar sources restricted?

4.2.4 NETWORK SECURITY

The network infrastructure of small businesses is a **common target** for cyber attackers. This is because network devices such as routers, switches, firewalls, etc. are generally not maintained at the same security level as desktops and mobile devices.

Examples of audit checks for network security

- Do you have a firewall in place to protect your internal network against unauthorized access?
- Do you ensure that all devices on your network are using WPA2 security?
- Are all unnecessary services on routers and switches turned off?
- Are software updates and security patches installed as soon as they are available?
- Is your anti-malware software configured to perform regular scans?

4.2.5 HOW TO CONDUCT A SECURITY AUDIT

Security audits are not one-time projects, but a **living document**. The advances in technology and changes in business models create vulnerabilities in information technology systems and these advances and changes are dynamic. So, to be effective, security audit also has to evolve continuously.

It is clear that SMEs are normally less responsive to this matter, both for a smaller number of employees and for lower budgets to be allocated; in any case, it is important not to underestimate the importance of carrying out a **continuous security audit**, in order to assess company's IT security state.

It is highly recommended to identify a supplier for an IT audit service, able to provide a simple, clear and reliable service, in order to assess the entire **IT security state** of the company.

Based on my experience, I would suggest the adoption of **recurring** and **checklist-based** services, highly used by the vast majority of companies, where each "No" answer to security questions represents a **possible threat**, which must be prioritized by calculating the risk that threat poses.

Risk is the combination of the impact that a threat has and the likelihood of that threat occurring.

Risk = Impact x Likelihood

Each check presents numeric values to be assigned, ranging from 0 for "no impact" to 5 for "very high impact". Similarly, 0 is used for "not likely to occur" and 5 for "very likely to occur".

CONCLUSIONS

This document was written in March 2020, at the height of the COVID-19 virus pandemic.

Although not a virologist and not having the ability to make predictions about the end of this drama, one thing is certain to me: we will get out of it. How do I know? Because we have no other choice.

Among the most important lessons I have learned so far thanks to my work, is that - sometimes - the only way to do something well is to be forced to do it. This situation will end, and when it ends only those who have had the foresight to **adapt to change** will save their company, their business, their life.

In one of my Cyber Security articles published on LinkedIn in the last years,
I reported a well-known quote from Charles Darwin:

« It is not the strongest that survive,
nor the most intelligent,
but the one most responsive to change »

Over 150 years have passed.
And this lesson is more current than ever.