CYBERSECURITY CHALLENGES AND STRATEGIES FOR ITALIAN SMEs: AN ANALYSIS OF CURRENT PRACTICES AND FUTURE OUTLOOK

ANTONIO RUSSO
MATRICOLA:000107672

INDEX

ABSTRACT

Cybersecurity is one of the most crucial challenge for Italian small and medium-sized enterprises (SMEs), especially in a context of increasing digitalization and complexity of cyber threats. This essay examines the current situation of cybersecurity in Italian SMEs, examining the main issues, current practices and challenges in adopting cybersecurity frameworks. Through a detailed analysis of the main risks and Italian regulations, the essay examines how SMEs often struggle with inefficiencies due to limited resources and poor security awareness. The research also explores future perspectives, discussing how digitalization will affect security strategies and what measures might be adopted to improve protection. The conclusions show practical advices for SMEs, underlining the importance of investing in training and resources to address emerging challenges and strengthen cyber resilience.

INTRODUCTION

Today, as technology changes rapidly and everything becomes more connected, online security has become a major concern for all businesses. Small and medium-sized businesses in Italy, which play a crucial role in the economy, are facing the same challenges. Despite their importance, many of these businesses are at risk because they don't have enough resources or the right knowledge to defend themselves against cyberattacks. This essay explores how Italian small and medium-sized enterprises (SMEs) are handling cybersecurity, starting with a broad overview and then diving into the specific problems they face.

We will discuss the current situation, highlighting the main issues and gaps that leave these businesses vulnerable to online threats. Many SMEs struggle to keep up with the fast pace of technological changes and often lack the necessary tools or expertise to protect their data and systems effectively. We will also look at how these businesses are seeking to implement security measures and the challenges they encounter in doing so, such as limited budgets, lack of training, and the complexity of cybersecurity solutions.

Additionally, we will discuss about the main risks and threats these businesses face online, like hacking, phishing, and data breaches, and we will delve into the Italian laws and regulations designed to help them stay protected. These laws provide a framework for businesses to follow, but understanding and applying them can be difficult for smaller companies with fewer resources.

Finally, we will explore how the increasing move towards digitalization is changing the landscape for these businesses, while going digital offers new opportunities for growth and efficiency, it also brings new risks that need to be managed. We will consider what the future might hold for these businesses in terms of both challenges and opportunities in cybersecurity.

The aim is to provide a clear and straightforward overview of how small and medium-sized businesses in Italy can strengthen their cyber security and better protect themselves against the growing number of digital threats.

1. OVERVIEW OF CYBERSECURITY AND ITALIAN SMEs

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. It seems that everything relies on computers and the internet now, communication (email, smartphones, tablets), entertainment (interactive video games, social media, apps), transportation (navigation systems), shopping (online shopping, credit cards), medicine (medical equipment, medical records), and the list goes on.

There are many risks of having a poor cybersecurity network, among these dangers are malware erasing your entire system, an attacker breaking into your system and altering files, an attacker using your computer to attack others, or an attacker stealing your credit card information and making unauthorized purchases. There is no guarantee that even with the best precautions some of these things won't happen to you, but there are steps you can take to minimize the chances.

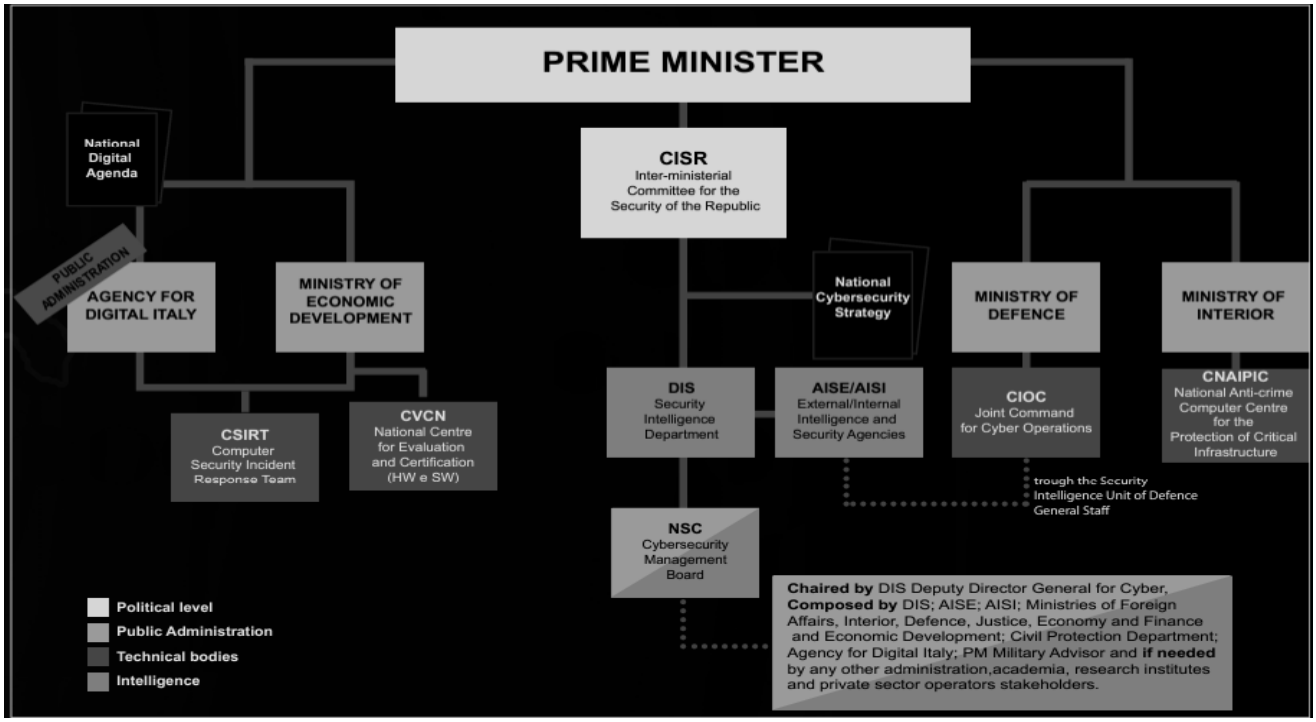
In Italy, over 99% of companies are micro, small or medium-sized, and almost all of them manage one or more IT services internally. In 2022, over a quarter of them suffered cyber-attacks. In the majority of cases (over 80% on a European basis, according to an ENISA study) the primary channel through which the attack on SMEs is conveyed is social engineering and has the human factor at its core. It is therefore essential to accelerate awareness of the key role that cybersecurity plays in the digital transition, through initiatives that allow the countermeasures to be identified and prioritized. In 2023, cyber-attacks against Italian companies increased by 625% compared to 2022. A growing trend also in the current year. These are the numbers released by the National Agency for National Cybersecurity (ACN) which, at the beginning of July, also published for the first time the data relating to cyber-attacks that occurred in our country in May alone. There were 283 total episodes. Compared to the previous month, the increase is 148%. In 175 cases, the final target was national subjects or public bodies, while the remaining ones hit citizens and businesses.

Furthermore, since the beginning of 2024, 18% of attacks have involved companies in the transport sector, while 16% in manufacturing. The least affected are companies in the energy, telecommunications and communication sectors, where there has been greater investment in digital infrastructure and staff training to combat cyberattacks. The numbers, however, could be higher. Often, in fact, it is the companies themselves that avoid reporting cyber-attacks they have suffered, fearful of the impact that the spread of such news could have on the company's reputation.

Among the tools used by hackers, there is above all malware with which they manage to launch attacks classified as serious or very serious, while those with a critical impact are 24%. Critical attacks are those that then have a significant impact in economic, legal and reputational terms for the victims. On average, manufacturing is the most affected sector, where attacks have gone from 5% to 16%, followed by the professional/scientific/technical sector, ICT, healthcare and financial/insurance. The most used techniques for cyber-attacks are malware, which has reached 70% of the total attacks, following the use of unknown vulnerabilities and techniques. Almost a quarter of the attacks had critical impacts, while 67% had serious impacts. This indicates a significant increase in attacks with catastrophic economic, legal or reputational consequences for the victims.

The Italian SMEs show up certain strengths but also reveal some weaknesses. These SMEs appear to be aware of critical information's value. In addition, SMEs detected threats from both inside and outside the organization. Decision-makers are concerned with day-to-day activities; consequently, their long-term planning is limited. Their lack of a cybersecurity budget also confirms this. This lack of a dedicated cybersecurity budget prevents SMEs from taking the required proactive steps to prevent cyber-attacks, which could be due to a lack of awareness and a tendency to focus on corporate activities' more operational aspects. As previously observed, small businesses are less likely to consider themselves targets of cybercriminals. In terms of their weakness, while SMEs apply mandatory regulations (e.g., General Data Protection Regulation (GDPR), their poor application of the regulations, standards, and frameworks related to the cybersecurity domain seems to be their most crucial vulnerability.

Regarding the Italian Cybersecurity Architecture, in 2017 and 2018, Italy streamlined and strengthened its cybersecurity structure in order to boost its cyber capabilities. an interagency and intergovernmental operational body within the DIS tasked with cyber crisis prevention, preparation and management. The Security Intelligence Department (DIS) is at the center of the Italian cybersecurity ecosystem's governance, acting as: supporting body for the Prime Minister and the Inter-Ministerial Committee for the Security of the Republic (CISR) on cyber issues, Chair of the Cybersecurity Management Board (NSC), European Point of Contact under the Network and Information Security (NIS) directive. The NSC is responsible for promoting Italy's participation in cyber activities (such as Cyber Europe organized by ENISA, the European Network and Information Security Agency) and other initiatives aimed at increasing national cybersecurity.



(Cybersecurity in Italy, New opportunity for businesses, Presidency of the Council of Ministers)

2. CURRENT STATE OF CYBERSECURITY IN ITALIAN SMEs

In 2022, the cybersecurity market was valued at $2.1 billion, 18% more than the previous year. Italy continues to rank fourth in the world and first in Europe for the number of cyberattacks. With the growth in remote work, attacks on PCs doubled, as cyber criminals shifted their focus to the weakest link in the chain: the endpoint and the employee's PC. Ransomware threats have the greatest impact, increasingly targeting the manufacturing sector, the public administration, and healthcare facilities. According to the Italian Cybersecurity Association (CLUSIT), in 2022, the Postal and Communications Police (CNAIPIC) managed nearly 13,000 significant cyberattacks, more than twice the number in the previous year. CNAIPIC mostly engages when malware attacks, especially ransomware attacks, phishing, distributed denial-of-service (DDos) attacks, and advanced persistent threat (APT) campaigns are involved. There were over 113,000 security alerts involving IT services of institutions, critical IT infrastructures of national interest, sensitive infrastructure of regional interest, banks, and large companies operating in strategic sectors such as communications and defense. Russia's war against Ukraine and the ensuing financial and energy crisis generated an unprecedented surge in cyberattacks, particularly DDoS attacks, which increased exponentially last year. Many attacks are traceable to Chinese and Russian hacking groups that operate transnationally.

Significantly more malware families were detected in 2022 (208) than in 2021 (163). Infection penetration has also become relevant in mobile, with the FluBot malware infecting mainly Android devices. The primary sectors targeted include finance, insurance, and public administration. Larger companies turned to tools such as firewalls or virtual private networks (VPN) to raise protection levels, providing employees with remote access to corporate VPNs while augmenting perimeter protection.

Large-company investments drive the Italian market for cybersecurity. According to the Cisco Readiness Index, 87% of Italian companies are expected to increase their IT security budgets by 10% in 2024. The financial/banking and utility sectors are the main end-users of IT security, followed by the defense, public (national and local), manufacturing, transportation, and telecommunication sectors.

The current scenario sees small and medium-sized Italian companies in a very challenging position, particularly exposed to IT risks capable of causing serious damage to the production structure up to and including the closure of the business. Data from the most recent studies carried out in the sector say that 80% of Italian companies affected by cyber-attacks are small or medium. If we look at the overall number of attacks, we discover that in the first 6 months of 2023, successful ones grew by over 40% compared to the same period in 2022, with an increase rate that in Italy was four times higher than the global one, transforming Italy into a central target for cyber pirates: today our country alone collects 9,6% of the global total of successful attacks

More than 50% of SMEs are unprepared to face increasing threats and 83% of Italian SMEs believe they are immune from cyber-attacks. One in five companies lack a specific investment plan for IT security or only allocate resources as needed. Small firm managers perceive security as a cost rather than an investment and tend to show resistance in approving IT security expenditures. As this mindset slowly changes, sector analysts expect increased SME investments. Medium-sized companies and (to

a lesser extent) small companies are increasingly choosing to invest in cybersecurity, often opting for advanced cloud security solutions.

Not by chance, according to a study conducted by Grenke Italia, a staggering 72.7% of Italian companies have never undertaken any Cyber Security training activities. Furthermore, 73.3% are unfamiliar with ransomware attacks, 43% lack a designated cybersecurity officer, 26% are almost devoid of protective systems and only one in four companies (22%) maintains a segmented network for enhanced security. These figures underscore the pressing need for raising awareness on the critical issue of cybersecurity. They also emphasize the urgency of guiding companies through the process of developing a robust security strategy. In today's landscape, cybersecurity for SMEs should not be viewed as an "optional" expense but rather as a key investment with tangible returns over time.

3. ADOPTION AND CHALLENGES OF CYBERSECURITY FRAMEWORK

In 2015, the National Framework for Cybersecurity was created, which provides an operational tool useful for organizing the cybersecurity processes of companies, inspired by the NIST Cybersecurity Framework seen in the previous paragraph.
The main objective of the "National Framework for Cybersecurity and Data Protection" is to provide companies with a tool to support the cyber risk management process. However, in the case in which some companies have already had cybersecurity programs and standards for data protection in place for some time, the Framework is not an alternative, but an additional tool in order to:

- Improve or define a cybersecurity and data protection program based on risk management
- Determine the level of maturity of cybersecurity and data protection activities and identify any improvements for a redistribution of resources.
- Carry out benchmarking between companies with similar characteristics to improve the levels of security in the same.
- Facilitate communication with top management and external interlocutors such as suppliers and partners to allow the company greater clarity on the levels of risk to which it may be exposed.

It is possible that for some categories of companies, such as SMEs, there is greater difficulty in implementing cyber risk management based on the National Framework, which may be too complex and costly.

Cyber Index for SMEs

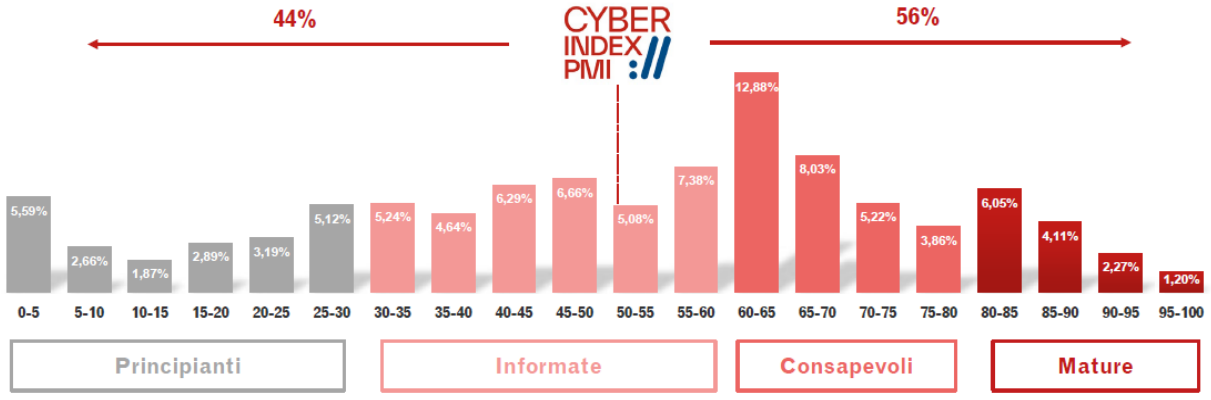
In order to understand and analyze the exposure of SMEs to cybersecurity risk and how they should behave to avoid possible attacks, the "Cyber Index Report" for Smes was introduced in 2023 by a collaboration between Generali and Confindustria, with the scientific support of the Cybersecurity & Data Protection Observatory of the School of Management of the Milan Polytechnic and with the participation of the National Cybersecurity Agency.

The report stress that, despite the progressive awareness of the importance of the matter, the cyber index highlights a general picture of delay in Italian SMEs. The average value of the index is 51 out of a maximum score of 100.
The SMEs CYBER INDEX is divided into three levels of aggregation:

1. a synthetic index on a scale of 1 to 100 that offers an overall picture of the maturity of SMEs
2. 3 dimensions - strategic approach, identification, implementation - which aggregate the areas of analysis
3. 18 areas of analysis that group the individual questions of the questionnaire. The following pages illustrate in detail the analysis methodology and the relationship between the 3 levels that make up the index.

Starting from the distribution, through an aggregation of companies that have obtained similar scores it is possible to identify 4 levels of maturity. Grouping companies into four classes - called beginners, informed, aware and mature - contributes not only to a better understanding of the general state of health of Italian SMEs, but also to outline recurring company profiles. From this activity it is possible to undertake a multi-year monitoring process, with the aim of detecting the evolution of the maturity of Italian SMEs in the cybersecurity field. The hope is that in the coming years we can witness a general growth of all companies, both those that are approaching security and those whose maturity journey has already been started. It is important to underline that even mature companies will continually find themselves facing new security challenges and threats, which are transformed with the evolution of technologies and the context.

The graphic below shows the distribution of digital security awareness among Italian SMEs.



(Cyber Index PMI Report 2023)

To sum up, the main outcomes show that Italian SMEs struggle to approach cybersecurity in a strategic manner. Further, Small organizations have great difficulty in identifying and understanding cyber risk, due to both the slow cultural transformation and the limited digital skills present. Finally, data processing shows that small and medium-sized enterprises have already undertaken mitigation activities for cyber risks, but often with little awareness of the correct use of levers. This message confirms that cyber security is too often seen as the exclusive responsibility of IT Managers and systems engineers, despite the fact that cyber risk also has a strong impact on business.

Having established a framework for understanding the maturity levels of SMEs, it is crucial to delve into the specific factors that increase their exposure to cyber risks. The “Risk Exposure Analysis”

section of the report provides a detailed mapping of these factors, which include the technological tools used, the involvement in critical supply chains, foreign activities, and previous cybersecurity breaches.

Digital Devices

The introduction of hardware and software, as well as the increase in the user base that uses them, contribute to defining the attack surface. The digitalization process supports the business in generating value, but at the same time it is important to monitor the vulnerabilities generated by new technologies, implementing appropriate protection measures. The analysis of the technological endowment allows to define the share of companies equipped with basic technologies, such as ERP and CRM systems, or advanced ones, such as IoT and Cloud.

83% of Italian Smes use digital tools to support their business processes, not by chance companies are investing heavily in digital tools to take advantage of the opportunities emerging from technological evolution. Introducing new technologies means expanding the potential attack surface, so if these are not correctly accompanied by security solutions, they can introduce new latent vulnerabilities in the company perimeter, increasing the probability of a violation. The survey conducted shows that 35% of SMEs have introduced advanced digital tools, i.e. Cloud solutions or IoT devices. In particular, this last technology, particularly widespread in the industrial sector to the point of constituting a security area in its own right (OT Security), requires a high level of attention. Following this, 48% of SMEs say they have already introduced essential digital tools with the aim of supporting business processes, such as software for the management and operational planning of resources and applications to support management that digitize the front-end and back-end parts of the company. The view is completed by 17% of companies that instead declare they have not yet introduced digital tools.

Belonging to a critical supply chain

Sharing information systems with third parties, suppliers or partners of a company, implies points of contact between two external perimeters. This situation is an opportunity for cyber criminals, who can exploit the vulnerabilities of one company to violate another, triggering a cascade mechanism. Operating in supply chains that involve critical infrastructures, multinationals or Public Administration exposes SMEs to greater risks, since they could be the weak link to penetrate a more strategic target.

Companies rely on a wide range of partners, both as suppliers of production inputs and to outsource processes to specialized companies. This often involves a relationship between the parties, with a consequent exchange of data or the granting of access privileges to resources, which requires the utmost attention. A cybercriminal who manages to violate a company's systems could in fact easily gain access to the systems of its partners as well. The CYBER INDEX 2023 REPORT shows that 52% of Italian SMEs operate within a potentially critical supply chain. Among the most common situations, there is the supply of products and/or services to multinational companies and operations in politically unstable countries (30% of SMEs). The data presented shows a strong exposure to supply chain risks, which requires careful analysis both with a view to defending information systems and protecting the participation of small and medium-sized organizations in strategic value chains.

Foreign activity

The sale of products and services in foreign territories and/or the geographical relocation of some offices imply a logical and technological extension of the corporate domain. This situation generates an expansion of the scope of action and consequently increases the organization's exposure to new risks. This risk is exacerbated if the production activity is conducted within geopolitically unstable countries, since the company may be the target of targeted attacks by parastatal criminal groups.

Italian Smes are prone to operate on international markets: 53% sold products and/or services abroad in 2021.

Cybersecurity and data protection are important elements to consider for companies that operate internationally and sell their products abroad. When considering the international dimension, further complexity is added, linked to the regulations on privacy and data security in the countries in which they operate. The European Union has introduced the General Data Protection Regulation (GDPR), non-EU countries have adopted similar regulations, but they often require companies to adapt to heterogeneous regulatory requirements. To sell their products abroad safely, it is important for companies to familiarize themselves with the cybersecurity regulations of foreign countries.

Violations suffered in the last four years

A company that has already been a victim of cyber-attacks is at greater risk, as information about its information system and vulnerabilities may have been shared and publicly exposed, making them easily available to cybercriminals. It is therefore important for these companies to implement constantly updated cyber risk protection strategies and tools. The analysis aims to estimate the share of companies that have suffered a breach, although this percentage (based on self-declared data) may be underestimated compared to reality.

Cyber breaches* can cause negative repercussions on various fronts: from data theft to business interruption, through sanctions in the event that the compliance measures required by current regulations are not respected. Even organizations that do not consider themselves particularly exposed to risk can be hit by malicious actions and the probability increases if the factors seen previously occur: in the event that they operate within a strategic supply chain, have international relations or security vulnerabilities linked to technologies that are not appropriately mitigated. Furthermore, an often underestimated consequence is linked to the possibility that a first attack can help cyber criminals in identifying vulnerable points of the system, exposing the company to potential new security incidents 40. This scenario is particularly common and requires immediate intervention to secure the information system. The message that emerges, in relation to the analysis of risk exposure, is that small and medium-sized enterprises are a particularly attractive target for cyber criminals. The survey shows that 13% of SMEs have suffered at least one breach of company information systems. In support of what has been stated in this section, it emerges that the companies within this portion of the sample have on average a greater exposure to risk. In fact, the percentages of companies that operate within a critical supply chain and/or in international contexts are growing.

4. RISK MANAGEMENT AND MAIN CYBER THREATS

In an increasingly interconnected and technologically advanced world, SMEs must exploit the benefits of digital transformation in order to grow and flourish their businesses. However, new technologies also present new risks and difficulties to address. One of the greatest dangers comes from the possible compromise of confidential information systems and company data by malicious actors. In order to best protect company information systems, the concepts of so-called Information Security must be implemented.

“Information Security” refers to the set of measures and tools aimed at guaranteeing and preserving the confidentiality, integrity and availability of information. Information Security is a broad concept that encompasses the security of information assets as a whole, including organizational and physical security aspects.

- Offering confidentiality means ensuring that data and resources are preserved from possible use or access by unauthorized parties. Confidentiality must be ensured throughout all phases of the data's life: from storage to the phases of use and transit along a connection network.
- Integrity is the ability to maintain the veracity of data and resources and to ensure that they are not modified or deleted in any way, except by authorized parties.
- Availability refers to the ability for authorized entities to be able to access resources for a set time and in an uninterrupted manner. This means preventing service interruptions and ensuring that infrastructure resources are ready for the correct provision of what is requested.

Information Security therefore aims to mitigate CYBER RISK, that is, any risk of financial loss, interruption of business or damage to the reputation of an organization resulting from breaches of data or corporate IT systems. Corporate information systems are typically compromised using common attack tools and techniques, such as malware, ransomware, DoS/DDoS, or phishing attacks.

Corporate information systems are typically compromised using common attack tools and techniques, such as malware, ransomware, DDoS attack or phishing attacks.

Malware

Malware, a contraction of the English words malicious and software, is malicious software capable of intruding into a computer, mobile device, or corporate network without the user's authorization with the aim of stealing confidential data, spying on victims, or causing more or less serious damage to the computer system in which it is running.

Ransomware

Ransomware is one of the most common forms of malicious software, and ransomware attacks can cost affected organizations millions of dollars. Ransomware is a type of malware that holds a victim’s

sensitive data or device hostage, threatening to keep it locked—or worse—unless the victim pays a ransom to the attacker.

Phishing

This is maybe, the most common cyberattack toward Italian SMEs. Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

Ddos

Distributed Network Attacks are often referred to as Distributed Denial of Service (DDoS) attacks. This type of attack takes advantage of the specific capacity limits that apply to any network resources – such as the infrastructure that enables a company's website. The DDoS attack will send multiple requests to the attacked web resource – with the aim of exceeding the website's capacity to handle multiple requests… and prevent the website from functioning correctly.

Malicious actors have various and diverse motives for carrying out their criminal actions against companies. Let's try to summarize some of the most common risk factors below:

- **Possession of customer, supplier and employee data:** Confidential data stored by the company can be an attractive target for criminals, who can steal it and then resell it to other criminals or encrypt it and ask for a subsequent ransom to make it accessible again.
- **Patent/Trade secret ownership:** Similar to confidential data, patents and industrial production secrets can also be an attractive target for malicious people. In these cases, malicious actors very often carry out these actions on behalf of national states, for espionage purposes.
- **Participation in a strategic supply chain:** Being a member of a strategic supply chain increases the possibility of being a victim of attacks, as malicious actors try to exploit the weak links in the supply chain to gain access to the connected information systems to attack well-defended and prestigious victims from the inside.
- **Exposure in the geopolitical context**: In conflict situations, there is an increase in the probability of suffering an attack, or targeted attack campaigns: in these cases, the malicious actor mainly aims to damage and compromise a specific business, putting the extortion purpose in the background**.**

Unfortunately, cyber-attacks by malicious actors can sometimes be successful and overcome corporate defenses by violating the company's information and computer systems. Let's examine the most common consequences that Italian SMEs have to face following a successful hacker attack:

- **Service disruption or delays in business operations:** A hacker attack can lead to the shutdown of production machines or the blocking of information systems used in the company, causing significant monetary damage related to the interruption of activities.
- **Data breach or alteration:** A company's confidential data can be encrypted by ransomware, making it unusable without proper backup. Another possibility is that the data is stolen and then spread across the web or sold for profit.

- **Extortion**: The main goal of many criminals who use ransomware is to demand a ransom, pushing victims to pay a sum of money to obtain the keys to regain possession of confidential data that has been encrypted. It is good to specify that, when dealing with criminal organizations, paying the ransom does not imply the guarantee of obtaining the keys to unlock the data in exchange.
- **Recovery costs and compensation:** Following a hacker attack, companies must spend huge amounts of money to restore and re-secure their information systems. Sometimes, the companies themselves can also be subject to sanctions by the authorities for not having protected their customers' personal data with the measures required by current regulations.
- **Image/Reputational Damage**: In the post-attack phases, the company must also restore its public image, damaged by the inability to successfully defend its customers' or partners' data and/or by inadequate management of the incident.

5. REGULATIONS AND NORMS ON CYBERSECURITY IN ITALY

As in many other areas, legislation helps define standards and obligations for companies to guide operational and strategic choices related to cyber risk management. Legislation can be issued either by a national government or by a supranational institution, such as the European Union. For example, the EU approved the General Data Protection Regulation, also known as GDPR, in 2016 and since 2018 it has been fully applicable in all Member States. Regardless of the executive body, regulations can address specific organizations or sectors, promoting or imposing a certain behavior, including:

1. The implementation of adequate security measures to protect information considered sensitive. Measures include the implementation of strengthened authentication systems, access control, data encryption and potentially also the designation of an information security officer.
2. The notification of security breaches to the competent authorities or the individuals concerned. This means that if an organization suffers a data breach or its security is compromised, it may be obliged to inform the interested parties and adopt corrective measures.
3. The adaptation to specific standards, such as the ISO/IEC 27001 standard, which provides a framework for the implementation of an information security management system.

Finally, regulations may provide for criminal or administrative sanctions in the event that they are not implemented promptly, especially in the event that cybersecurity violations occur. Regulations therefore play a fundamental role in directing the actions of companies and ensuring an adequate level of cybersecurity, even within small and medium-sized enterprises; the following sections therefore examine in depth the GDPR regulation and the NIS 2 directive, both applicable to Italian SMEs.

GDPR

Among the various regulatory provisions that may affect Italian SMEs, the most relevant is certainly that contained in the General Data Protection Regulation (GDPR). The GDPR is a regulation issued

by the European Union (EU) that establishes a legal framework for the protection of personal data and the rights of natural persons with regard to the processing of such data.

The General Regulation came into force on 24 May 2016 and became mandatorily applicable starting from 25 May 2018, after a two-year transition period, which allowed the recipients to implement what was necessary to comply. The GDPR pursues two fundamental objectives: on the one hand, to adapt the regulation, now dating back to 1995, to new technologies, on the other to harmonize and standardize the regulation itself at European level, creating a common regulatory framework. These intentions are met through the imposition of a series of fundamental obligations and principles to ensure the protection of personal data. These include the principle of lawfulness, fairness and transparency, which requires that data processing has a legal basis, is transparent for the data subjects and is carried out lawfully.

Furthermore, the principle of purpose limitation requires that personal data be collected for specific, explicit and legitimate purposes and not be processed in a way that is incompatible with those purposes. The GDPR also imposes data security obligations. Organizations must adopt adequate technical and organizational measures to ensure a level of security appropriate to the risk, including those of unauthorized access, loss, alteration or disclosure of personal data. The Regulation also provides for the obligation to notify the competent authorities within 72 hours in the event of a personal data breach.

In the event of failure to comply with the provisions, the Regulation provides for sanctions of varying degrees. Supervisory authorities can impose administrative fines proportionate to the extent of the violation: for example, in 2021 Amazon was fined 746 million euros for failing to comply with profiling consent for online advertising.

NIS2

The new European Directive NIS 2 (Network and Information Security), which came into force on 17 January 2023, is a regulation on cybersecurity that concerns companies operating in the European common market. It is a revision of the previous NIS Directive of 2016, which introduced cybersecurity obligations for operators of essential services (OSEs) and digital service providers. The NIS Directive 2 must be implemented within 21 months of its entry into force and for the first time it will also concern medium-sized companies, not only those with over 250 employees.

The purpose of the directive is to ensure a high level of security of networks and information systems, prevent and counter cyberattacks, and improve cooperation between the competent authorities. The Directive therefore broadens the scope of the previous NIS, including new sectors and activities that are considered critical for the functioning of the economy and society, such as public administrations, financial services, health services, postal and courier services, waste management services, social services, chemical industries, food services and industrial manufacturing.

The NIS 2 Directive also sets more stringent requirements for the cybersecurity risk management measures that covered entities must take, as well as for the reporting of cybersecurity incidents to the competent authorities. In addition, the NIS 2 Directive provides for increased cooperation between Member States and EU institutions to address common cybersecurity challenges, through the NIS Cooperation Group, the Cybersecurity Incident Response Teams (CSIRTs) and the European Centre for Industrial, Technology and Research Cybersecurity (ECCC).

These two regulatory instruments, although with specific objectives, complement each other in promoting a safe and compliant digital ecosystem. It is in this context of strengthening data security and protection that Law no. 90 of 2024 fits in, representing a further step forward in national regulation, aligning Italy with European directives and introducing new measures for the management and mitigation of cyber risks.

LAW NO.90 OF 2024

This new act aims to strengthen the cyber resilience of our country, by increasing penalties for cyber-crimes on the one hand and by strengthening prevention and counteraction tools on the other.

Law 90/2024 primarily introduces significant changes in the regulation of computer crimes, including increased penalties, new aggravating factors, and stricter conditions for mitigating circumstances. It specifically targets companies and organizations that fail to comply with GDPR and NIS2 directives, imposing higher financial sanctions and legal consequences. The law emphasizes the critical need for robust cybersecurity and data protection measures, holding entities accountable for breaches or data loss, even when they are victims of cyber-attacks due to insufficient safeguards.

Finally, the new paragraph 1-bis has been introduced, which punishes the new type of extortion through computer crimes with a pecuniary sanction of between three hundred and eight hundred quotas and with interdictory sanctions for a period of no less than two years.

6. FUTURE OF CYBERSECURITY FOR ITALIAN SMEs: THE ROLE OF DIGITALIZATION

As Italian SMEs increasingly embrace digitalization, they face new and growing cybersecurity challenges. Digital transformation, characterized by the adoption of technologies such as IoT, big data and AI, significantly improves business operations, but also expands the potential attack surface for cyber threats.

The interconnected nature of digital systems means that every device, network or application can become a possible access point for attacks, making essential cybersecurity measures robust. Therefore, digitalization and cybersecurity are two sides of the same coin, where the advancement of one requires the strengthening of the other. The future of cybersecurity in Italian SMEs will increasingly see the integration of cybersecurity with digital transformation. It will be essential that security measures are integrated into every phase of digital adoption, from IoT implementation to cloud computing, this requires a change in mindset, where cybersecurity is seen as a fundamental element of the business strategy, essential to protect digital assets and maintain customer trust.

One emerging area of particular importance will be the adoption of Zero Trust architectures, a paradigm that requires “never trust, always verify.” This model goes beyond the traditional approach, which assumed that everything within the network was trustworthy. Instead, Zero Trust requires that every access and data request be authenticated and verified, regardless of its origin. A salient aspect

of Zero Trust Architecture is the application of an algorithm that does not simply consider static information such as username/password, trusted IP or MAC addresses to allow access to a particular resource, but that uses as much contextual information as possible to make the decision for each access. The merit of Zero Trust Architecture is that of introducing a conceptual framework within which to carve out one's own declination of the architecture.

For SMEs, implementing a Zero Trust architecture will mean greater protection against internal and external threats, ensuring that only authorized users and devices can access critical resources.

In addition to adopting recognized cybersecurity standards, such as the ISO 27000 series or Cyber Essentials, SMEs will need to strengthen cybersecurity awareness and training. The human factor remains one of the most significant vulnerabilities, and for SMEs, which often lack IT security teams, dedicated, awareness-raising and regular training of employees will be critical.

Additionally, SMEs will benefit from collaborative approaches to cybersecurity, participating in industry groups, sharing threat intelligence, and using managed security services to access otherwise inaccessible expertise and tools. Regulatory compliance and resilience will also be key. As the regulatory landscape evolves, SMEs will need to proactively adapt to new laws and regulations, such as those introduced by Law No. 90/2024. Future cybersecurity strategies for SMEs will need to emphasize resilience, preparing for, responding to, and recovering from cyber incidents.

This involves not only preventative measures, but also incident response plans and business continuity strategies to minimize downtime and mitigate damage in the event of a breach. In summary, as Italian SMEs navigate the complexities of digital transformation, integrating comprehensive cybersecurity measures, including Zero Trust architectures, will be paramount. By addressing these emerging challenges and proactively adapting to evolving threats, SMEs can secure their future in an increasingly digital world.

7. CONCLUSIONS

In summary, cybersecurity represents a growing and complex challenge for Italian small and medium-sized enterprises (SMEs), an essential sector for the national economy. The overview of the current cybersecurity context has showed that, regardless the importance of protecting corporate data and infrastructure, many SMEs struggle to implement adequate security measures due to limited resources and insufficient awareness. Challenges in adopting cybersecurity frameworks, combined with prevailing risks and threats, highlight the immediate need for change. Italian regulations offer valuable system, but their practical application in SMEs often remains fragmented and insufficient. To effectively address these challenges, it is imperative that SMEs invest significantly in training and resources dedicated to cybersecurity.

The future of cybersecurity for Italian SMEs is closely linked to their ability to adapt and carefully respond to new emerging threats. Digitalization, while offering numerous opportunities, also brings with it new risks that takes advanced and updated protection strategies. Investing in continuous training programs for staff and in adequate technological solutions is not only a matter of regulatory compliance, but an essential strategy to ensure the resilience and long-term sustainability of SMEs.

In conclusion, to foster cybersecurity and protect their data and operations, Italian SMEs must adopt an integrated approach that includes both staff training, the adoption of advanced technologies and

the securization of digital activities. Only through a serious and coordinated commitment in these areas will SMEs be able to face the challenges of cybersecurity and successfully navigate the ever-changing digital economic process.

BIBLIOGRAPHY

- *What is Cybersecurity? | CISA*. (2021, February 1). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/what-cybersecurity
- Neri, M., Niccolini, F., & Pugliese, R. (2022). Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey. Online Journal of Applied Knowledge Management, 10(2), 1–22. https://doi.org/10.36965/ojakm.2022.10(2)1-22
- Cybersicurezza: campagna contro gli attacchi informatici alle PMI. (n.d.). Dipartimento per L'informazione E L'editoria. https://informazioneeditoria.gov.it/it/notizie/cybersicurezza-campagna-contro-gli-attacchi-informatici-alle-pmi/
- Ore, I. S. 2. (2024, March 22). Si moltiplicano gli attacchi degli hacker, Pmi nel mirino. Il Sole 24 ORE. https://www.ilsole24ore.com/art/si-moltiplicano-attacchi-hacker-pmi-mirino-AFgTqLAD
- Esperti, G. (2024, July 10). Attacchi cyber contro le aziende in aumento in Italia. Wired Italia. https://www.wired.it/article/attacchi-cyber-aumento-aziende-italia/
- SGBox. (2023, December 12). Cyber Security and SMEs: the current state of play. SGBox - Piattaforma SIEM e SOAR. https://www.sgbox.eu/en/cyber-security-and-smes-the-current-state-of-play/
- Italy - Cybersecurity. (2024, January 23). International Trade Administration | Trade.gov. https://www.trade.gov/country-commercial-guides/italy-cybersecurity
- SMEs TOO EXPOSED TO CYBERATTACKS AND AT RISK OF CLOSURE: SUPPORT COMES FROM ITALIAN UNIVERSITIES - UCBM. (2024, April 22). UCBM. https://www.unicampus.it/en/news/SMEs-too-exposed-to-cyber-attacks-and-at-risk-of-closure%2C-support-comes-from-Italian-universities/
- Angelini, M. & Ciccotelli, C. & Franchina, L. & Spaccamela, M. A. & Querzoni, L. (2019). Framework Nazionale per la Cybersecurity e la Data Protection. https://www.cybersecurityframework.it/sites/default/files/framework2/Framework_nazionale_cybersecurity_data_protection.pdf
- Ministry of Foreign Affairs and International Cooperation, Cybersecurity in Italy, New Opportunity for Businesses, September 2019, https://www.esteri.it/mae/resource/doc/2019/09/esteri_cibersecurity_web.pdf
- Presentato a Roma il Cyber Index PMI: una fotografia del rischio cyber delle imprese. (n.d.). ACN. https://www.acn.gov.it/portale/w/presentato-a-roma-il-cyber-index-pmi-una-fotografia-del-rischio-cyber-delle-imprese
- Cyber Index PMI 2023://La cultura digitale protegge la tua impresa, Rapporto 2023, Promoted by Generali, Confindustria, Partner scientifico Politecnico Milano e

Osservatori.Net, Partner Istituzionale Agenzia per la Cybersicurezza Nazionale, https://www.smile-dih.eu/wp-content/uploads/2023/10/Cyber-Index-PMI-2023.pdf
- Tarsitano, P., & Tarsitano, P. (2022, October 25). Malware: cosa sono, come riconoscerli e come rimuoverli. Cyber Security 360. https://www.cybersecurity360.it/nuove-minacce/malware-cosa-sono-come-riconoscerli-e-come-rimuoverli/
- What is ransomware? | IBM. (n.d.). https://www.ibm.com/topics/ransomware
- KnowBe. (n.d.). Phishing | What is phishing? https://www.phishing.org/what-is-phishing
- What is a DDoS Attack | DDoS Meaning. (2019, January 31). /. https://www.kaspersky.com/resource-center/threats/ddos-attacks
- Legge 90/2024 sulla Cybersicurezza e compliance integrata: gli impatti su Modello 231 e privacy. (n.d.). NT+ Diritto. https://ntplusdiritto.ilsole24ore.com/art/legge-902024-cybersicurezza-e-compliance-integrata-impatti-modello-231-e-privacy-AF8FWtuC
- Arroyabe, M. F., Arranz, C. F., De Arroyabe, J. C. F., & Fernandez, I. (2024). Digitalization and Cybersecurity in SMEs: A Bibliometric analysis. Procedia Computer Science, 237, 80–87. https://doi.org/10.1016/j.procs.2024.05.082
- Cisternino, A., & Cisternino, A. (2022, January 5). Zero Trust Architecture: strumenti e consigli per implementarla sui sistemi aziendali. Cyber Security 360. https://www.cybersecurity360.it/soluzioni-aziendali/zero-trust-architecture-strumenti-e-consigli-per-implementarla-sui-sistemi-aziendali/