Towards cyber-safe electrification

In the era of digital transformation, **cyber security** is taking on a key role in ensuring business operations.
Typical cyber-attack types have changed radically in recent years: the number has grown exponentially, as has their level of sophistication and impact, making it is increasingly challenging to identify the source in a timely manner. Sector studies confirm that the perception of cyber risk is continuously growing. As compared to previous years, the causes for increased cyberattacks also include geopolitical tensions. In fact the conflict between Russia and Ukraine has increased attention about this issue. In particular, all state security agencies have warned public and private institutions about potential IT threads against critical infrastructures.
In 2022, many of the world's major attacks were carried out by leveraging the supply chain and through compromised third parties, which allowed attackers to target the primary target's customers, partners, and suppliers. This caused a sharp rise in the number of victims and attacks went increasingly undetected (the so-called "scale effect"). It is also interesting to observe that the majority of the attacks in the energy sector include ransomware, an increasingly used method that causes the exfiltration (unauthorized copy, transfer or recovery) of the victim's data and its encryption, which gives the people responsible for the attack an additional lever for receiving payment of ransom.
It is also seen how the vulnerabilities detected in commonly used software products are continuously increasing and how they are taken advantage of with greater speed by cyber criminals. In particular, the zero-day type vulnerabilities represent a large risk because they are discovered before software developers become aware of them and before they can release a patch.
In a similar context of cyberwarfare, the only possible defense is given by processes and technologies, which have been developed and evolved over time to mitigate the IT risk. On top of constantly applying the cyber security strategy, we have set out special measures, also in order to reinforce the "cyber security posture",[5] aware of the fact that overall, cyber risks can become a risk of ecosystemic proportions within the broader context of the complex and interconnected electricity industry. For example, a large-scale blackout in this scenario would have socio-economic ramifications throughout the population, companies and key institutions.
The key elements are therefore sharing and cooperation on cyber security issues with participation among all stakeholders including companies, legal institutions, supervisory bodies, suppliers, customers, and employees.

Policies and management models

In line with the needs of the energy industrial sector and with the Open Power strategic approach that characterizes it, we have adopted a systemic vision of cyber security issues, as well as a global strategy of analysis, prevention and management of cyber security events. The cyber security path to support the Group's digital transformation is based on creating, enhancing and adopting a security governance model, infrastructure and services in order to make full use of opportunities – including with the help of cutting-edge technologies – to boost the cyber resilience of our infrastructure and applications.
Since September 2016, the **Cyber Security** unit has been operating within Global Digital Solutions Function, reporting directly to the Chief Information Officer (CIO) who works under the Group Chief Information Security Officer (CISO). The unit is committed to ensuring the governance, direction and control of cyber security issues, establishing strategy, policies and guidelines in compliance with national and international regulations, engineering support for the protection of the Group's environments, monitoring of the risk posture through checks based on processes and technology, as well as monitoring and implementing compliance requirements tied to cyber security regulations, and adopting technical solutions and procedures to mitigate any weaknesses detected. The unit works synergically with the Business Lines and with the technical units responsible for systems design and management, thanks to the Cyber Security Risk Managers and Cyber Security Response Managers. CISO and the Cyber Security Risk Managers also make up the Cyber Security Operating Committee, which aims to evaluate cyber risks across the business and determine the risk acceptance criteria based on the Group's risk posture. The Cyber Security Committee, chaired by the Group's CEO and made up of his/her front lines, approves the cyber security strategy and periodically checks its progress. As determined at the meeting of April 2021, the Committee meets every six months. Two meetings were held in 2022 (May and October).
In 2022, the Control and Risk Committee held 3 meetings with the objective of addressing in more depth the aspects related to organizational procedures (on a technical and governance level), the crisis management process,

(5) "Cyber Security Posture" refers to the state of society's adoption of cyber security principles.

the CERT operating model and the relative processes that characterize them.
All areas actively participate in implementing the cyber security strategy by way of an integrated operating plan in line with the Group's objectives. Moreover, cyber security strategy and initiatives are a key focus area for the principal executive and control bodies (e.g. Board of Directors, Supervisory Bodies, etc.) for all the legal entities and Countries where the Group is present.

Moreover, the Group policy adopted in 2017 (the "**Cyber Security Framework**") addresses the principles and operational processes that support a global strategy of risk analysis, prevention and management.
This Framework, based on a 'systemic' vision applies across the more traditional Information Technology (**IT**) sector, as well as to Operational Technology (**OT**) environments tied to the industrial world and the Internet of Things (**IoT**). In applying this Framework, the Cyber Security Risk Management method was established in 2017. The method is applicable to all IT, OT and IoT environments and includes all of the phases required to carry out a risk analysis and define the related mitigation plan, in line with the stated cyber security goals. To balance the advantages obtained by the operation and use of IT/OT/IoT systems with the risk that can potentially derive from them, well-informed, risk-based decisions are of fundamental importance.
Enel has also created a "**Cyber Emergency Readiness Team**" (CERT) to ensure proactive management and responses to cyber incidents, while also encouraging collaboration and exchanges of information within a network of accredited international partners. Having entered into an agreement with the US national CERT, there are now 9 accreditations with: Romania, Italy, Chile, Argentina, Peru, Colombia, Brazil, Spain, and the US. Enel's CERT is also part of Trusted Introducer – a service that includes 464 CERTs in 72 countries. In September 2018 Enel also joined FIRST (Forum of Incident Response and Security Teams), which is the largest and most widespread community in the sector, with 602 members spread across 99 countries. Furthermore, in 2022 the CERT operating model was strengthened with the creation of an internal team of security analysts. The new operating model has exceeded the previous one, implementing the internalization of the incident monitoring and management activities and therefore, strengthening the activities 24x7.

Definition of the IT security strategy

The cyber security strategy covers setting objectives and priorities to direct and coordinate investment initiatives for the Group as a whole, and to ensure adherence to cyber security policies, setting targets, management reporting, and constant monitoring of ongoing security activities.
This process is guided by CISO and uses close integration and synergy with the various business areas, which communicate their needs, analyze opportunities, manage any criticalities, and make proposals for initiatives.
Devising strategies is an iterative activity based on sharing and consolidation of the Group's risk posture target. The various actors involved analyze the options and potential initiatives within their respective business areas in order to assess the feasibility, guarantee consensus, and the necessary funds. The Cyber Security unit guides the process and, together with the other key players, gradually consolidates aspects such as future scenario, objectives, and possible strategic initiatives in a cyber security strategy proposal document, with a high-level budget estimate and prioritization.

Cyber security incident management

The multiplicity and complexity of the areas in which we operate (data, industry, and people) and of the technological components (e.g. business critical systems such as SCADA – Supervisory Control and Data Acquisition, smart grids and smart meters) increasingly integrated in the Group's digital life, have made it necessary to configure a structured cyber security system. This leads to the need for a cyber defense model based on a systemic vision that integrates the IT sector (starting from the cloud down to the data center and mobile phone), the OT (everything concerning industrial sector, such as generation plant remote control) and the IoT (extension of communication and artificial intelligence to the world of things).
Through the monitoring systems, CERT collects 3 billion events every day relating to the company's assets from 7 thousand data sources, correlates them through automatic analysis, and produces a hundred "incidents" on average. The incidents are classified based on the Enel Cyber Impact Matrix (on a scale of 0 to 4), making use of the best events correlation capabilities thanks to the adoption of highly advanced services.
The vast majority of "incidents" are classified as **0/1**; these have no significant impact on Group systems and are automatically or semi-automatically intercepted and/or managed by the existing company defenses; this way they are able to prevent and/or mitigate the impact of potential cyber-attacks.
Incidents classified as **2/3/4** have a potential impact on the Group and are managed by CERT analysts, involving any affected stakeholders. Thanks to the protection services, every day, in 2022 **CERT intercepted on average 1.2 million at risk e-mails, 57 viruses, 172 web portal attacks, and 1.3 million connections to harmful websites every day**.

In 2022 Enel CERT responded to: **175 cyber security incidents with impact level 2; 16 incidents with impact level 3; and 0 incidents with the highest impact level of 4**.
In the cases detected, to ensure an efficient and rapid response and minimize the impact on people, services and assets, all the relevant management procedures have been put in place.
Specifically, when a cyber security incident translates into a potential data breach, the necessary actions are taken immediately, in line with the Enel Group "**Personal Data Breach Management**" policy. Should a crisis situation arise that threatens the Enel Group's business continuity, assets, reputation and/or profitability, the appropriate actions are taken immediately, in line with the specific Group policy on "Critical events management".
Moreover, the "**IT Service Continuity Management**" policy formalizes a process to bring the risk affecting the availability of IT infrastructure down to an acceptable level, support business continuity requirements, and restore IT services based on the results deriving from a Business Impact Analysis when a severe interruption occurs, including when caused by an accident.

EDR (Endpoint Detection and Response) technology blocks violations by using innovative features and advanced paradigms not only to identify viruses and malware on endpoints, but also to detect suspicious sequences of technical events that could prove to be part of an attempted attack.

Detailed below is the number of cyber security events recorded in 2022.

	2022
Total number of cyber security breaches or other cyber security incidents[1]	0
Total amount of fines/sanctions paid related to cyber security breaches or other cyber security incidents	0
Total number of customers and employees impacted by data breaches affecting the Group	0
Total number of data breaches[2]	0

(1) The value reported for the KPI "Total number of cyber security breaches or other cyber security incidents" refers to Level 4 incidents.
(2) The KPI "Total number of data breaches" refers to the number of events that occurred as a result of a cyber security incident (i.e. the number reported does not include any disclosures occurring as a result of non-digital incidents).

Furthermore, in order to boost our capacity to prevent, react to and manage incidents, some **cyber exercises** simulating a real attack were carried out, involving staff working in the production environments. At the end of each exercise, reports were produced containing details of the actions taken during the simulation, to assess – with a view to continuous improvement – the quality and completeness of the materials provided to help with decision-making, the execution times for each phase, and how well the procedures had been followed. In 2022, in particular, 50 cyber exercises were carried out in industrial environments in 11 Countries where the Group is present.

Main projects and initiatives

All cyber security projects, programs, and initiatives are designed to avoid, mitigate or remediate cyber security risks for the entire Group. As a result, all activities are managed with a risk-based approach following the security by design principle to ensure a continuous due diligence process that also includes self-assurance activities.

CERT – RISK MONITORING EXTENSION

"**CERT – Risk Monitoring extension**". CERT uses emergency technologies such as SOAR (Security Orchestration, Automation and Response) and machine learning to support Big Data, which make it possible to automate and streamline incident management activities and make use of improved visibility of cyber threats, increasing efficiency in managing new ones and the related investigations. In particular, thanks to the SOAR system, through the definition of operating flows it is possible to automate repetitive tasks, whereas through machine learning, a branch of artificial intelligence, it is possible to learn or improve detection capacities based on available data.
These technologies make it possible to consistently accelerate, enrich and trace the necessary activities during the analysis and management phase of an incident, providing considerable support to the analyst who can therefore parallelize and concentrate on more complex tasks that require human intervention.

MULTI-FACTOR AUTHENTICATION (MFA)

"**Multi Factor Authentication (MFA)**" is a cloud solution used to enforce the identification method for users during the authentication procedure. Adopting MFA enables a person accessing a system to identify himself/herself through a second authentication factor via SMS or an app installed on his/her smartphone. The MFA solution is in line with the regulatory framework and is strongly recommended to counter emerging threats of theft of credentials, including those using social engineering techniques (e.g., phishing or potential user behavior not in line with policy). The adoption of the solution is operational for all users.

ASSURANCE CHECKS

Assurance checks (Ethical Hacking, Vulnerability Assessment). These activities are carried out on an ongoing basis both using automated tools and manually, to assess and quantify any weaknesses in IT, OT and IoT environments (applications, systems, IoT devices, architectures and/or infrastructures). 1,587 checks were performed in 2022. Following these checks, we can identify the best measures to eliminate or mitigate the detected vulnerabilities or threats and, in turn, any associated harmful exploits.

DMARC "E-MAIL FRAUD DEFENSE"

DMARC "E-mail Fraud Defense". This solution completes the application map covering threats of spam, phishing and fraud attempts. Thanks to this, all of Enel's e-mail domains are configured to permit blocking e-mails with an incorrect sender address that exploits the Group brand. Deployment took place across the entire perimeter, thereby providing complete coverage of the domains.

Collaborations with external bodies and agencies

In line with the Open Power approach, we believe that networking with external entities and organizations is a key element in the cyber security strategy, to share best practices and operational models, develop and strengthen information sharing channels, and help establish standards and regulations. In 2022, we provided feedback in public consultations to help draw up cyber security regulations, including by drafting legislations, promoting a harmonization of the current regulatory landscape in this area, and implementing a risk-based approach and the principle of security by design. Collaborations carried out also aim to construct more homogeneous structures for defining the taxonomy of security incidents, more organic criteria for their classification, as well as more harmonious notification procedures in European contexts. These collaborations are also guided by a complex regulatory landscape in the cyber security area, both in terms of an increase in standards produced as well as in terms of complexity, mainly due to the new regulations that are added every year, in addition to the heterogeneity of requirements and the methods of adoption.

In this sense, the process aimed at regulatory compliance can have a strong impact both on company processes ad well as on the technological infrastructure, requiring a major effort in terms of management and monitoring.

Moreover, taking into account the context of regulatory compliance, **no cases of non-compliance with standards or cyber security regulations were detected in 2022**.

In recent years, a solid network has been established and developed by interacting with key stakeholders in the energy sector such as ANEEL (Agência Nacional de Energia Elétrica) and ONS (Operador Nacional do Sistema Elétrico) in Brazil and CNO (Consejo Nacional de Operación) in Colombia. We took part, for example, in the Confindustria Digitale team, which aims to help develop the Italian digital ecosystem, we participated in the working groups of the World Economic Forum, and contributed in recent years to the publication of several reports including "Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain" and "Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors".

Furthermore, Enel X, Gridspertise and Enel Grids have reached an important goal in the area of IT security by obtaining **ISO 27001 certification**. This important result certifies some processes that have an IT security management system – policies, procedures and guidelines for providing customers with trusted products and services.

Training and information

The "**Cyber Security Awareness Program**" has become a constant and ongoing initiative at Group level; it used to disseminate our cyber security culture and raise awareness of threats and attacks that exploit the human vector. This program contributes in fact to digitalization, because it creates a culture of IT security, changes the behavior of people in order to reduce the cyber risk, develops technical IT security skills and makes people the first line of company defense. It also uses various communication channels and dissemination tools, including both communication campaigns as well as dedicated training initiatives for clusters of people. Specifically, 19 knowledge sharing events were held in 2022 on a Global level on the issues of cyber security and various initiatives were held also on a local level. For example, within the scope of these initiatives, Policy no. 1097 "Rules of Behavior for Digital People" was integrated with a quick guide, available in all the main languages adopted in the Group (5 different languages) targeted towards facilitating a quick consultation of topics for directing the correct use of digital resources. Bulletins and news were also created and disseminated through the company intranet and documents were made available to stay always up to date on these issues. All of this was made possible also thanks to the awareness platform "TheRedPill", the Group platform through which training content and modules are delivered in order to strengthen the IT security culture, allowing the continuous improvement of training initiatives and the performance of simulated phishing campaigns. Its objective is to raise awareness of the main cyber security issues, address any upskilling and reskilling needs and teach how to defend against possible attacks. Four global simulated phishing campaigns, a knowledge assessment and an awareness campaign were launched in 2021 – the year the platform was updated. During 2022, additional initiatives were launched on a global level, such as the dissemination of the "Antiphishing Kit" module, or the launch of the "People Cyber Empowerment Journey", or the program that aims to make Enel people the first line of IT defense. Furthermore, 6 simulated phishing campaigns, 3 awareness campaigns related to digital identity protection, data and device protection, and 19 events targeted to disseminating the culture of IT security were designed and launched (so-called "knowledge sharing").

In addition to the dissemination and communication initiatives, during 2022 the simulated phishing campaigns targeted toward the entire Enel population continued, in order to train employees to recognize malicious e-mails. Following the results obtained by the phishing campaigns, specific initiatives were created to increase employee sensitivity and awareness (for example, specific infographics, instructions and guidelines were shared with those who were not able to recognize a phishing e-mail).

The **Open Tech Journey** project also continued to provide access to training courses focused on technological topics, promoting internal skills to spread awareness of strategic topics and manage upskilling and reskilling needs. This was the background to the creation of the **Cyber School**, which delivered seven courses on the main cyber security topics. All the courses were engineered and made available to the entire Enel population in e-learning mode, in order to reach multi-specialistic skills in the various companies of the Group.