Digitalization & Cybersecurity

Adapting to a Rapidly Evolving Digital Landscape

In an increasingly interconnected world, we at One Meralco recognize that embracing and undertaking digital transformation is essential to delivering an efficient and convenient service to continue satisfying our customers. Building on the initial 4Ds Digital Transformation Strategy Meralco executed from 2019 to 2023, our new 7Ds Digital Transformation Framework serves as the foundation of this journey through to the end of the decade, positioning us as a digital leader in the energy industry.

Due to the critical nature of our infrastructure as a utility, we face significantly heightened exposure to cyber risks compared to other businesses, making robust cybersecurity all the more crucial to safeguard our operations and ensure business continuity. Recognizing its strategic importance, Meralco established the CSG in 2020 as a dedicated function—separate from Information, Communications, Technology, and Transformation ("ICT")—to protect our digital infrastructure and shield our stakeholders from potential cyber threats. Complacency is not an option in our industry, and the CSG operates with an "assume breach" mindset that anticipates and prepares for inevitable cyberattacks. This proactive approach not only helps mitigate financial, reputational, legal, and regulatory risks but also reinforces the trust placed in us by our stakeholders.

A. Transforming Our Business Through Digitalization

In 2024, we commenced our revitalized five-year digital transformation journey, using our 7Ds Digital Transformation Framework as our compass. Anchored on seven key pillars—Digital Customer, Digital Grid, Digital Employee, Digital Enterprise, Data Platforms & Artificial Intelligence ("AI"), Digital Infrastructure, and Digital Communications—this framework enables us to strengthen Meralco's position as a digital leader in the Philippine energy sector by focusing on the adoption of emerging technologies and data-driven insights for operational excellence, customer centricity, and business development.

FACILITATING EFFICIENT DATA MANAGEMENT

The Meralco Data Platform ("MDP") acts as the Company's digital backbone, serving as a centralized hub for data archiving and business intelligence. Designed to manage vast volumes of data from diverse sources, including billing systems and online channels, the MDP automates critical tasks and facilitates the creation of data management dashboards to enable informed decision-making, particularly in customer service applications, leading to quicker response times and heightened customer satisfaction.

Harnessing the power of large language models, the MDP conducts real-time customer sentiment analysis, enabling our customer care representatives to address feedback efficiently. Simultaneously, MDP's machine learning models help our staff identify overloaded distribution transformers in advance, enhancing operational efficiency and minimizing the risk of unplanned outages.

The MDP serves as a unified platform for analytics and machine learning, supporting data processing and dashboard creation for insights across various domains, including grid operations and monitoring of sustainability metrics of the company. A self-service analytics program empowers business users, fostering a data-driven culture within Meralco.

The implementation of MDP has led to a 9% reduction in Meralco's average service application processing time. Customers can get their services completed 14 and 0.5 days earlier for project-covered application and ordinary service application, respectively.

Additionally, leveraging MDP, Meralco can now proactively identify distribution transformers requiring rehabilitation, thereby averting unplanned power interruptions for at least 500,000 customers annually.

In 2024, the MDP enabled our customer care representatives to address customer feedback promptly with the help of real-time customer sentiment analysis enabled by large language models ("LLM"). This LLM-powered solution transformed a tedious process into a swift, accurate, and insightful operation.

These customer centric and data-driven digital transformation achievements were recognized at the Cloudera 2024 Data Impact Awards under the Leadership and Transformation category, besting six other international nominees from various industries across Asia Pacific.

As a unified, self-service platform for advanced analytics and machine learning, the MDP supports comprehensive data processing and dashboard creation across various domains, including grid operations and monitoring of sustainability KPIs, fostering a data-driven culture across the Company. By enabling a 50% faster dashboard and analytics generation, the MDP has streamlined data-driven decision-making in our organization.

Looking ahead, we will continue to enhance the MDP, aligned with our evolving business needs as well as technological advancements in the industry, to ensure more efficient service delivery.

ENABLING INTELLIGENT EMPLOYEE AND CUSTOMER SUPPORT

A key priority in our digital transformation journey is the adoption of emerging technologies like AI, with a focus on LLMs, to drive transformative business outcomes. To this end, we have developed the Meralco Interactive Data Assistant ("MIDAS"), an intelligent digital platform akin to ChatGPT. MIDAS will allow users to interact with data through voice and chat, making data more accessible and easier to understand for both tactical and strategic functions.

The AI-based platform will also allow for automatic categorization and analysis of customer feedback as well as generation of actionable recommendations, effectively reducing manual workloads and enhancing customer service.

Moving forward, we aim to expand our self-service data analytics environment and further democratize data access to strengthen our culture of data-driven decision making.

BRIGHT SPARKS

Promoting Responsibility in the Use of AI in *Our Business*

Our Responsible Use of AI Policy sets out appropriate guardrails around the use of AI while we explore this innovative technology within Meralco. As the proliferation and use of AI continue to expand, setting clear policies and governance measures is necessary to prevent these tools from being abused. Applying to all our officers, employees, and third-party partners, the policy includes the following guiding principles:

- **Accountability** – All individuals representing Meralco shall be accountable for the proper selection, use, deployment, integration, and retirement of AI technology;
- **Fairness and Bias Detection** – Any AI tool adopted and used in Meralco must be regularly tested to prevent discrimination and reduce biases, in line with the Company's Code of Business Conduct and Ethics as well as the Diversity and Inclusion Policy;
- **Inclusive Growth, Sustainable Development, and Well-Being** Meralco's pursuit of trustworthy AI should promote inclusive growth, well-being, and reduced environmental impact;
- **Privacy** – Individual privacy must be respected, following Meralco's data privacy obligations;
- **Robustness, Security, and Safety** – Meralco's AI systems must be robust, secure, and safe throughout their lifecycle, ensuring they do not pose unreasonable safety and security risks; and
- **Transparency and Explainability** – AI usage in content development must be explained and shall be transparent to relevant stakeholders. Employees shall be informed and trained on the strengths, limitations, and responsible use of AI.

B. Securing Our Critical Cyber Infrastructure

Meralco's increasing reliance on digital technologies, combined with the accelerating convergence of information technology ("IT") and operational technology ("OT"), has significantly broadened our attack surface, introducing complex security challenges that demand heightened vigilance and protection. As traditional air-gap cybersecurity architectures erode, safeguarding our digital infrastructure requires a more robust and versatile cybersecurity approach.

The evolving cyber threat landscape is further compounded by tightening legal requirements in the Philippines, including the Data Privacy Act, the National Cybersecurity Plan ("NCSP") 2025–2028, and the proposed Energy Sector Cybersecurity and Cyber Resilience Framework by the DOE. These regulations mandate stringent security measures, data protection protocols, and incident reporting. At Meralco, we aim to not only meet but also exceed these regulatory demands by investing in advanced technologies and personnel training as well as adopting a proactive approach to threat detection and response. By ensuring that our cybersecurity measures remain agile, resilient, and future-ready, we successfully blocked and prevented a total of 414 million cyberattacks in 2024 alone.

BUILDING AN ARSENAL AGAINST CYBER THREATS

Our long-term vision for cybersecurity is embodied in ARSENAL, a strategic program designed to elevate Meralco's cybersecurity maturity by 2028, in alignment with the NCSP. Our mission is clear: to defend the Company from current and emerging cyber threats by securing our digital assets, protecting our stakeholders from these threats, and minimizing our exposure to financial, reputational, legal, and regulatory risks stemming from cybersecurity incidents.

ARSENAL lays the foundation for our proactive defense strategy, supported by the following pillars:

- **Asset Visibility** – maintaining a comprehensive inventory of all digital assets, ensuring that we can protect what we can identify;
- **Access Management** – adopting the zero-trust principle ("never trust, always verify") to mitigate risks from internal and external threats;
- **Risk Quantification** – centralizing and automating vulnerability assessments to enable faster, data-driven security investments;
- **Resilience** – building resilience into our architecture and operations to prepare for unpredictable cyber events, with specialized teams focused on early threat detection, dark web monitoring, and brand protection;
- **Response Orchestration and Automation** – enhancing incident response capabilities through automation for rapid and precise threat mitigation;
- **Security by Design** – embedding cybersecurity considerations into every phase of the system and service lifecycle;
- **Supply Chain Ecosystem** – managing third-party cyber risks through dedicated oversight, ensuring the resilience of our digital supply chain;
- **Employee Engagement and Enablement** – cultivating a strong cybersecurity culture through continuous awareness programs, empowering employees as our first line of defense;
- **Employee Workforce Development** – investing in the growth of our cybersecurity talent to manage and mitigate industry-specific threats effectively;
- **Exposure Management** – continuously identifying and addressing vulnerabilities through proactive threat exposure assessments;
- **Executive Cybersecurity Awareness** – facilitating leadership collaboration and providing executives with timely insights into emerging threats;
- **Next-Generation Technologies** – deploying advanced defense systems, intelligent automation, and robust security controls to enhance threat detection and response;
- **Adoption of Global Standards** – reinforcing stakeholder trust by adhering to global cybersecurity best practices; and
- **Legal and Regulatory Compliance** – ensuring compliance with national regulations to effectively manage legal and regulatory risks.

Through ARSENAL, we fortify our cyber infrastructure to withstand the challenges of an increasingly digitalized energy landscape. Given that Meralco powers a significant portion of the Philippines, any disruption caused by a cyberattack could have far-reaching consequences for our 8 million customers, posing a serious national security risk. As such, our proactive, collaborative, and innovative approach to cybersecurity maintains Meralco's resilience as a utility while safeguarding the trust of our stakeholders.

FOSTERING A CULTURE OF CYBER VIGILANCE AND RESPONSIBILITY

Meralco's operational risk framework focuses on identification, assessment, mitigation, and continuous improvement. At the heart of this framework is the commitment to cultivate a culture of cybersecurity awareness that transcends technical jargon and resonates with all audiences. Believing that cybersecurity is a shared responsibility, we empower our workforce to be our strongest line of defense and foster a cybersecurity culture that extends beyond our organization and into the broader community.

To raise our employees' awareness of cybersecurity, we run ongoing campaigns that include weekly advisories on cybersecurity best practices as well as alerts on threats like phishing and smishing scams. In 2024, we issued 87 advisories focused on actionable insights and practical measures.

We also measure our employees' level of vigilance through simulations of phishing attacks. During the reporting period, 4,637 Meralco employees received a simulated phishing email, with only less than 7% clicking on the embedded links. All employees who failed the test were required to undergo phishing awareness training to make them resilient against such threats.

In celebration of the Cyber Security Awareness Month in October 2024, we launched the Annual Cyber Mandatory E-Learning in Meralco, achieving a remarkable 99.93% compliance rate and an 88% overall passing rate.
The learning module combined a comprehensive instructional video with a 14-item quiz to assess employees' understanding of cybersecurity fundamentals.

Our celebration culminated in our inaugural Cybersecurity Awareness Forum, which brought together over 1,500 attendees across One Meralco.
The forum explored critical cybersecurity-related topics such as adoption of AI technologies and IT and OT convergence, as well as enhancing cybersecurity awareness across all levels of our organization. Additionally, we launched the CSG internal portal, a centralized hub for Meralco employees to access cybersecurity advisories and information security policies, and other relevant materials. This platform reinforces our commitment to ensuring that cybersecurity awareness resources remain accessible to all our employees.

PROMOTING VISIBILITY AND SYNERGY FOR CYBERSECURITY

Meralco recognizes the importance of demonstrating relevance, transparency, and accountability in our cybersecurity practices. This is achieved through initiatives that enhance visibility and promote knowledge sharing within our organization.

In 2024, we established Cytadel, an interactive cyber operations and risk management dashboard that provides a holistic view of our cybersecurity operational effectiveness, including platform stability, service responsiveness, vulnerability management, and SLA adherence. Cytadel facilitates performance tracking and reporting by consolidating data from diverse sources, promoting transparency and data-driven decision making.

We also launched the Meralco Intelligence Cyber Security Synergy ("MINT Cynergy"), a threat intelligence sharing community to elevate our managers' awareness of emerging cyber threats, empowering them to make informed decisions about cybersecurity strategy and resource allocation. Through MINT Cynergy, we are able to share and circulate: analysis and reports on security breaches, data leaks, and other critical incidents; case studies on recent security incidents affecting Meralco; updates on our brand protection initiatives, including detecting and addressing fake social media platforms and fraudulent websites; as well as detailed briefs on specific threat actors, covering their capabilities, intentions, attack methods, and possible mitigation measures.

Finally, we also actively forge public-private partnerships to strengthen national cybersecurity resilience and further promote knowledge sharing. In 2024, Meralco launched Wavemaker, in partnership with OMF, to equip teachers with essential cybersecurity knowledge that they can share with their students. We also collaborated with the Philippine National Intelligence Coordinating Agency to understand and enhance the national view of the cyber threat landscape, enabling us to better respond to country-level threats.

For more information about Wavemaker, please refer to the Community Engagement section.

BRIGHT SPARKS

Championing *Data Privacy* Within and Beyond One Meralco

At One Meralco, privacy is more than just a policy—it is a responsibility we uphold to protect and maintain the trust of our stakeholders. Through Meralco's Data Privacy Office ("DPO"), we strive to integrate data privacy principles in every aspect of our business, ensuring that privacy is prioritized by design and by default. We raise awareness among our employees through information campaigns and training sessions to foster a culture of privacy across One Meralco.

In 2024, we launched the Data Privacy Roadshow, starting with the Business Centers, to strengthen our customer-facing teams' understanding of our data privacy policies, guidelines, and risk management requirements. Our goal was to empower our employees to uphold the highest data privacy standards and help them better identify and address potential data privacy concerns. As a result of this initiative, compliance with our Privacy Risk Management requirements improved. We also saw an uptick in inquiries regarding potential data privacy concerns.

During the reporting period, we also conducted a refresher course for Meralco's Learning and Development partners, ensuring they remain well-versed in data privacy concepts and the Company's Privacy Risk and Management Program.

We extend our privacy advocacy to our subsidiaries through capacity-building efforts. Our annual Data Privacy Bootcamp, held during our Privacy Awareness Week, gathered the data privacy teams and other key personnel from our subsidiaries to enable them to stay updated on the latest guidelines and requirements from the National Privacy Commission ("NPC") and the evolving landscape of data privacy in the Philippines. Additionally, we supported MIESCOR Infrastructure Development Corporation ("MIDC") in registering its Data Protection Officer and data processing systems with the NPC.

Our commitment to data privacy goes beyond our organization. In 2024, we led the Data Privacy Council Sectoral Training for Utilities in partnership with Maynilad and the Visayan Electric Company. The training was attended by 26 data protection officers from various utility companies across the country. By actively collaborating with industry peers and the NPC, we strengthen our role as a champion of data privacy, helping protect our stakeholders, especially our customers, in an increasingly digital world.