Digital Transformation and Cyber Security Strategy in Lebanon: A Practical Guide.

Moustafa Noureddine, Ph.D.

CEO, Micro Tech Solutions S.A.L.

Introduction:

Digital transformation is probably Lebanon's best hope for economic development. This underutilized resource has been idle for over 20 years, living in government strategies and ministerial power point slides. This economic potential will mobilize intelligent labor force, and it will require collaboration among private and public sector, creating a massive need for educated labor. It is probably the best hope for activating economic growth potential, reducing deficit, and attracting intelligent talents that will be lost abroad otherwise.

In recent years, the government efforts to activate this digital economy potential of Lebanon have not been a secret, they have been bundled mostly under the implementation of reforms required under CEDRE program and the hopes of improving the electricity economy and investment in oil and gas opportunities. These three programs, 1) digital transformation, 2) improving electricity economy, and 3) oil and gas revenue are probably the most opportunistic options for rescuing a struggling economy at the edge of collapse. This paper discusses the opportunities in digital transformation in Lebanon, and guidelines for implementation strategy. In the last section of the paper, we look at a use case for implementation to illustrate how an organization can undergo digital transition.

The cybersecurity challenge:

One of the biggest challenges of digital transformation is the exposure of cybersecurity infrastructure. When files are stored in cabinets, and servers are located in locked rooms with no access outside the premises, it is easier to feel safe and worry less about cyber-attacks. However, as soon the larger

internet is at play, cyber strategy becomes a core requirement before any digital transition can take place.

The Lebanese government has been aware of these challenges and has combined both cyber security strategy and digital transformation hand in hand. "We have done something special by advancing from a state of zero strategy to having a national cybersecurity strategy after six months," Lina Oueidat, the head of the ICT committee at the Presidency of the Council of Ministers, tells Executive in September on the sidelines of a cybersecurity conference.

Confidence in the governments' cybersecurity measures and transparency in the use of personal information are vital for gaining citizen's trust and for attracting more people to do business online. Such trust between citizens and governments is critical prior to implementation of digital transformation. There shall be laws in place to ensure citizen data is kept safe and laws to protect citizens in case of data breach.

The international view:

The combined strategy of digital transformation and cybersecurity is certainly paid well attention for at the global community. In 2019, 27 United Nations member countries committed to a statement on "responsible state behavior in cyberspace" at a UN General Assembly session. Based on the notion that digital lifestyle has become ubiquitous to drive productivity, the member states emphasized the criticality of irresponsible cyber behavior by any actor being it a state or individual cyber-criminal. The member states pledged to "hold states accountable and called for voluntary collaboration with other states to uphold an international rules-based order in cyberspace" (1)

Lebanon has proven not long ago that it is not a total stranger to the importance of cybersecurity and digital transition issues for nations' emerging economic fortunes. At the end of last year, the Lebanese government was one of the first 51 countries to join an initiative of French President Emmanuel Macron, the "Paris Call for Trust and Security in Cyberspace." Signatories affirmed their commitment to international legal frameworks and their applicability to digital environments, among other things, reaffirming their support of "an open, secure, stable, accessible and peaceful cyberspace, which has become an integral component of life in all its social, economic, cultural and political aspects." The group also condemned "malicious cyber actions in peace time" and also vowed to "welcome collaboration among government, the private sector and civil society to create new cybersecurity standards that enable infrastructures and organizations to improve cyber protections. (2)

However, as of today, Lebanon is stacking at the bottom in terms of digital transformation and cybersecurity strategy. According to the International Telecommunication Union's (ITU) cybersecurity index of 2018, Lebanon was ranked 17th among 22 Arab member countries and 124th in global terms (2). This low ranking reflected the absence of a national CERT, a computer emergency response team (CERT)—a vital entity in national cybersecurity considerations. CERT will provide benchmark advice and assistance focusing on cyber incident prevention, handling and reporting. CERT will also collect and share cyber-threat intelligence within the country and partner sates. Therefore, Lebanon must undergo

serious infrastructure investment in order to enhance its cybersecurity stance and then move forward with digital transformation implementation.

Implementation Strategy:

Implementations of a digital transformation strategy requires the confidence of clients or citizens in case of government agencies. What prevents people to use digital services is attributed to many factors, examples include:

1. Current services rely on digitizing pre-Internet paper-based business processes that are not best suited to the digital era.
2. Most services do not offer end-to-end transactions, instead they offer part of the service and the require the client to go through face to face in order to fulfil the whole transaction
3. Lack of digital signature implementation. This is a blocker to adopt digital transaction at any organization.
4. Services that has been independently designed with its unique user interface and set of assumptions. This leads to inconsistency in the user experience and causes unnecessary confusion.

In order to implement a digital transformation strategy, the following are list of principles that should be followed:

1. Create a central portal, a single-entry point to navigate various needs that serve the customers or citizens, in case of government agency.

Such implementation makes it easier to locate information needed, being it in government ministry or agency, or simply a commercial store serving their client needs. Today, for example, there are hundreds of government web addresses, where information is organized according to the internal management structure of the ministry rather than the service needed by citizens.

Another important issue to address is the reliability of the information and the services provided. Having stagnant information that are not up to date or outdated reduces confidence and pushes the clients to visit physically or call by phone. Therefore, portal information must be up to date, reliable and written to address the day to day needs of the clients.

2. Set standards for clients centered information

A number of standards, guides and frameworks focusing on areas of high importance for citizens and clients such as cloud security, use of personal data, digital assurance must be mandated by government agencies in order to ensure confidence and data protection. Without such standards and regulations, data privacy can become a major concern and a blocker for digital adoption in various agencies especially banking. For example, setting a data privacy law will ensure that businesses and government agencies do not collect customer private information. Other examples of standards are data exposure laws that require organizations to inform customers when their data is accessed illegally. This is usually the main driver for organizations to protect data, since any exposure require embarrassing announcement to their customers, organizations tend to protect their customers data to ovoid such

scenarios. In the USA for example, most banks decided to move to the Cloud to avoid embarrassing data exposure scenarios with their customers since the banks are required to inform every customer when their data is accessed illegally or potentially stolen by hackers. The lack of such law in Lebanon drives banks to ignore hacking incidents and focus on fixing the problem that caused it until they hit again, there is no marketing hit due to relaxed cybersecurity platform.

3. Transform transactions to be digital by default.

Proactively transform transactional services to be digital-by-default thriving to make

service's convenience to users the top design priority and to be more responsive to their needs.

Bearing in mind that digital transformation is not about digitizing existing paper-based processes, but it is about inventing the best new "Internet era" way to deliver the service.

To achieve this effectively, it is vital to have a user centered approach with emphasis on customer conveniences. In some digital transactions, the end users end up with duplicating the necessary tasks to complete the job, one that is digital and then duplicated by cumbersome paperwork. Such inconveniences lead to blocking such transformation.

In digitizing services, an organization must adopt the user's perspective and look for innovative ways of improving the experiences of clients and businesses. This involves challenging long-held assumptions and being willing to remake products, processes, and policies. To digitize a business process effectively, it is recommended to digitize the entire chain of activities that make up the process resulting in a valued end-to-end multi-stage transaction. There is a need to streamline inefficient or hard-to-automate business processes before digitizing them.

The digital organization also must recognize that not all members of the community can access digital services equally and that consideration will always need to be given to their particular needs. Therefore, the digital should be the default, but also the non-digital transaction must remain available for those who are not able to obtain it.

4. Plan for cybersecurity from the beginning

To protect its digital assets, any organization must invest the time to know the cyber risks, be clear about what to protect, know the threats to protecting against, train and educate staff and keep up to date with international best practices. Cyber security risks need to be comprehensively addressed and adequately mitigated all the levels: infrastructure, software, systems, people and processes. It is essential to have a growing cross-government cyber security capability to strategically plan and adequately prevent, detect and respond to cyber threats. Digital transformation to the Open World must be secured through:

- Building capability to prevent, detect and respond to cyber-attacks, manage incidents and secure services.

- Pursuing a systematic, collaborative and comprehensive cybersecurity approach that embraces international best practices. This includes continuous security enhancement to network, product, system and application security as well as operating within a strong governance framework.
- Guarding citizen's privacy, providing transparency in the use of personal information and ensuring that security is usable in digital services.
- Raising awareness, increasing knowledge, promoting expertise and strengthening international cooperation
- Improving the technical, legal and cultural means of preventing and combating cybercrime

Case Study:

A good case study to reference here is the digital transformation strategy for Lebanon government agency (the name will not be shared due to confidentiality). The study looked at transitioning the entire agency processes to become digital and the vision is to become paperless. In order to do so, we looked at the following execution strategy:

1. Digitizing internal processes
2. Digitizing transactional processes
3. Implementation of a central portal for information and access to services.

Cybersecurity remained a horizontal item that covered all processes, it is front and central to any digitization process. The following are processes that the agency will consider as they embrace digital transformation:

- **Human Resources Automation:** A full-featured Human Resources Management System that manages employee records, benefits, compensation, leaves, promotions, discipline, recruitment.
- **Payroll Automation:** Fully integrated with the Human Resources Management system as well as other modules, Payroll Automation manages, calculates and reports on employee salaries, benefits, income tax, vacations and leaves.
- **Budget Automation:** A solution that enables businesses and government offices to efficiently plan and manage their yearly budgets and financials covering estimation, formulation, hearings, execution, reporting
- **Assets Management:** A solution for the management of physical assets used to manage all types of assets, perform asset and condition analysis, enhance the efficiency of assets, provide advanced reporting including location, status of repairs and maintenance records.
- **Stock and Warehousing:** A full featured stock management and warehousing system that manages items, shipping, reception, access, control, storage, and reporting.
- **Accounting and Finance:** A solution to manage the accounting and financials of the Government offices covering financial reporting, bookkeeping, regulations, budget heads and control, auditing, and reporting

- **Physical and Digital Archives:** A comprehensive Electronic Document and Records Management System for the management of the entire content lifecycle of the business or government office
- **Correspondence Automation:** Full featured, document-centric Workflow Management System for the automation of Incoming, Outgoing and Internal Correspondences.
- **Meeting Management:** Advanced Meeting Management Solution to manage committee meetings, from the agenda preparation, to attendee invitation, meeting agenda items discussion, commenting, minutes preparation and dispatching.

This plan helped the agency establish a vision for becoming a digital and paperless organization.

In conclusion, the purpose of any digital transformation strategy must guide the digital transition of public services in Lebanon into an inclusive digital society where all citizens, businesses, government departments and organizations can benefit from digital era opportunities offered by digital technologies. The strategy must radically improve way of life for typical Lebanese citizens to enjoy speedy processing of typical day to day transactions such as opening a bank account, obtaining government records, signing a sales agreement, or depositing a check in the bank. Such transactions have been ubiquitous in many parts of the world. The last time I personally deposited a check in my bank account by physically going to the bank was at least 5 years ago.

References:

1. https://www.un.org/disarmament/wp-content/uploads/2018/04/Civil-Society-2017.pdf

2. McKinsey Global Institute (MGI). A future that works: Automation, employment, and productivity / 2017 https://www.mckinsey.com/mgi/overview

3. LEBANON DIGITAL TRANSFORMATION STRATEGY, 2018. https://drive.google.com/file/d/1Xxcae5moWkdyBktLCfQ_OPxbr8Iejjd7/view