BUSINESS CONTINUITY AND CYBER RESILIENCE

Between "Business Continuity" and "Resilience", the former is a more well-understood term. After all, we all – individually and collectively – have been familiar with Business Continuity (BC) Planning since just over a decade (for those of us who still remember the introduction of ISO 22301 in 2012), even more (for those of us who cut our teeth on BS 25999 and the initial versions of the BCI Good Practice Guidelines).

In the GCC, and in Qatar in particular, we noted Business Continuity slowly move to the top of Management radars in the last 7 to 8 years starting around 2016-17 and being very much top of the mind in the run-up to the FIFA World Cup events in 2022.

The intervening years of the pandemic also reinforced in Management minds, the importance as well as urgency of "having a plan to deal with difficult situations, so the organization can continue to function with as little disruption as possible ".

As BC Planning becomes more of a household term – and practice – incorporates and leading organizations, the more mature adherents are already evaluating and exploring about what comes next. Business Resilience is the natural candidate and as we speak, is being vigorously debated and better defined in the industry. Simply put, if Business Continuity Planning has been about anticipating potential risks and being able to not only mitigate those risks but also to continue operational activities and tasks – designed to minimize impact on critical customers and on the organization itself, then Resilience is the capability to withstand those anticipated risks (sometimes the unanticipated or the Black Swans also) and be able to absorb the impacts of the threatening events and about bouncing back to not only business as usual but perhaps to "better than usual". The central quality that potentials this kind of "bounce back" is of course flexibility or the ability to adapt quickly in difficult circumstances.

Business Resilience is of course quite a wide field and has many components such as Business Continuity Management, Disaster Recovery, Enterprise Risk management, Financial Management and Resilience, Operational Resilience, Technology Resilience, Cybersecurity Management etc. all complementing and intersecting with each other in their own ways. Describing all those components however is not the key focus of today's discussion and will be taken up further in our subsequent posts on this topic.

Meantime, as we continue our journey today, let us focus on how significant leveraging technology is for those who seek to improve and enhance resilience and the criticality of keeping an eye on cyber risks as well as cyber resilience. Forrester, for example, postulates that "Organizations that turn resilience into a competitive advantage use a crisis to seek new opportunities." According to Forrester, a "future fit" tech strategy creates an effective foundation for business resilience during a crisis. An important enabler or "pillar" for such a future-fit strategy is of course excelling at automation and prioritizing disruption to create new products or services to gain increased customers or customer satisfaction. This also builds upon our initial premise that technology resilience is one of the critical components of seeking organizational resilience.

As Moore Qatar, we have had the opportunity to work closely with enterprises and large organizations in Qatar to develop their Business Continuity and Resilience plans. We also have worked with organizations of varying level of maturity and technology adoption. Invariably, we find that organizations that have systematic well-defined processes and are moving towards automation of those processes exhibit better characteristics of resilience and are able to face or handle disruptions better. Obviously, technology adoption and automation help improve resilience and are enablers to more effective business continuity plans.

At the same time, increase in technology adoption also understandably increases the cyber threat attack surface and increases exposures to existing and new cyber threats. With conventional cyber threat vectors like malware, denial of service, brute force logins, SQL injections getting more potent due to combination of newer advances in AI and AI-based tools and (relatively) newer vectors and threats including sensitive data exposures, APTs, etc. all becoming more innovative and adaptive, it is incumbent upon these organizations to bolster up their own levels of cyber resilience. Here again we have come a long way since the days of ISO 27001 (BS 7799, anyone?) when the focus of the PDCA is on risk mitigation and prevention of cyber-attacks. Cyber-resilience demands that in addition to defensive cybersecurity, organizations should prepare for response – with the assumption that breaches will materialize (its not a question of "if" but only that of "when"). What happens when that inevitable cyberattack happens – how do I keep my availability of business services going?

Cyber-defenders and Resilience professionals will have to closely look at this question and work with newer standards such as ISO 27001:2022 and frameworks such as the NIST Cybersecurity Framework or the Zero Trust paradigms to enhance and strengthen their cybersecurity throughout the lifecycle. Not only will cyber-risk have to be thoroughly identified, evaluated and managed, key risk indicators (KRI) will have to be continually monitored and cyber-defenders will have to be on alert for the slightest signs of cracks or exposures. Developing and improving Incident Response and integrating with processes for Security Operations (SOC) – ither insourced or outsourced – will have to be consistently and adequately accomplished. Cyber-resilience will have to be continuously enhanced, built upon the foundations of continual improvement with the understanding that resilience is not a destination, but an ongoing journey.

At Moore Qatar, we work with almost all the aspects highlighted above and have had the good fortune of working with organizations at various stages of their cyber-resilience journeys. One thing that we have understood by looking at the diverse set of businesses and organizations – with differing technology adoption and maturity levels – is that there is no "one size fits all". Each organization has its own unique business footprint and risk profile and resilience improvement programs – including cyber-resilience always have take this into consideration and customize controls, practices, procedures to suit each individual environment. Ultimately however, the objective of business resilience is common to all and the journey to move towards enhanced business resilience is something that each organization has to take at its own due time.

ABOUT AUTHOR

Gautam Sarnaik, IT Advisory Director, Moore Qatar, is a 20+ year experienced IT GRC and Cybersecurity professional with deep experience in designing, building and auditing risk-driven controls. Starting his career as an Electronics and Telecom Engineer in 1997, he progressed through various roles as Software Engineer, ITSM and Information Security Consultant, IT Auditor, IT GRC Manager, Cybersecurity Practice Director, and Entrepreneur.

While building knowledge and expertise over the years, he retains a zest for new learning and finding innovative applications for the knowledge gained. He is a CISA and Platinum member of ISACA since 2003. He is also CBCI and TOGAF certified and recently certified to CISSP to reinforce the knowledge gains over last 2 decades and intends to study more about Cloud based systems, Blockchains, IoT and other emerging Technologies in future.

Please reach us at:

Sami Zaitoon
Managing Partner
sami.zaitoon@moore-qatar.com

Gaurav Kakkar
Partner, Head of Advisory
gaurav.kakkar@moore-qatar.com

Jamal Al Naseh
IT & Business Strategic Advisor
Jamal.naseh@moore-qatar.com

Gautam Sarnaik
Director – IT Advisory Services
gautam.sarnaik@moore-qatar.com

For MOORE - CONTACT US

Sharq Plaza, D-Ring Road, Zone 44, Street 250, Bldg 189, 2nd Floor - P.O Box: 17085
Mobile: +974 3045 8222 - Office: +974 444 36156 | +974 444 36105 - Fax: +974 442 79617
info@moore-qatar.com - www.moore-qatar.com