BUILDING RESILIENCE TO CYBER WEAKNESS DURING DIGITAL TRANSFORMATION

No organization functions in a zero-risk environment but digital transformation is rapidly exposing weaknesses in the cyber security fabric of an organization, prompting risk assessment and continuity planning, explains Yasser Zeineldin, CEO, eHosting DataFort.

For regional businesses, it appears their exposure to risk is continuously moving upwards. In the past, risks were limited to acts of nature, macroeconomic volatility and depending on the geography of the country, possible hostilities with adjacent countries.

Today, there are additional variables that need to be brought into the assessment of risk for businesses. The exposure of an organization to cyber threats and the added vulnerability of an organization due to its embarking on a digital transformation journey, are recent variables whose risk impact needs to be added into the overall equation of resilience.

Booz Allen Hamilton estimates that the annual global losses from exposure to cybersecurity threats is $600 billion, bringing the average loss per cybersecurity breach to an estimated $3.86 million. Moreover, the intensity and frequency of cyberattacks are being amplified by the adoption of digital transformation technologies.

Digital transformation technologies are rapidly removing silos and barriers that used to exist due to legacy technologies and, analog industrial control systems. This is making organizations more interconnected and can contribute to a domino-like cascading effect in the case of significant breaches into regional enterprises.

The rapid adoption of digital technologies is also throwing legislation into a catch-up game and bringing information technology departments, CIOs, CISOs, into the forefront in terms of interpretations and implementations of new guidelines and compliances. All put together, the working environments of both business and information technology are becoming more complex to manage, raising the possibility of costly and unpredictable errors. Booz Allen states that growing complexities stemming from rapid digitalization and changes in legislation are having a dizzying effect on businesses. Organization heads are still grappling with the speed of digital transformation and the impact of growing interconnectivity on their business landscape. They have had even less time to factor in the additional challenge of their vastly exposed cybersecurity landscape, amongst all these numerous other challenges.

Lack of adequate risk management in the face of advanced cyber security threat attacks, growth of interconnected enterprises, and rapid adoption of digital technologies, are eroding 10.2% of annual profits on an average of global organizations, through unplanned events.

So, what is the way forward now?

Organizations adopting digital technologies such as Cloud, analytics and artificial intelligence, mobility, Internet of Things, must adopt a two-pronged approach towards building their future resilience.

No organization can operate in a utopian climate of zero risk and hence as the first step an organization should perform an objective assessment like a SWOT analysis (Strengths-Weaknesses-Opportunity-Threats) or equivalent to identify the organization's strength and weaknesses including a rigorous cyber security related Threat and Vulnerability assessment. The second step is to build a recovery and continuity process through any disruption to keep the organization functioning with minimum of loss and performance".

During the first stage of planning, as a process of risk management, it is important to identify all the risks that can cause disruption in an organization's capability to function. This includes weaknesses in an organization's cyber security framework, and the probability of their exploitation. Following this, is the business impact analysis, to quantify the business loss from the impact of each of these possible cyber security disruptions.

This will lead to a matrix of incidents between most probable and most disruptive to an organization's functioning and performance. Some of the numeric metrics used at this stage are the maximum tolerable period of disruption (MTPD), the recovery time objective (RTO) and recovery point objective (RPO).

The second stage, involves detailed planning on how critical processes within the organization can continue to function and meet the expectations of MTPD, RTO and RPO objectives. However, this planning may not be of much use unless it is practiced and tested and improved, across the organization.

Feedback and open communication across the organization, on improvement of such continuity process planning, are an important part of building resilience during adoption of digital transformation, amongst others.