(https://www.fintechfutures.com)

BankingTech

Pandemic forces corporations to balance technology investments on risk and agility

Written by Homaira Akbari and Derek Vadala 12th May 2020

The Coronavirus pandemic has tested the readiness of companies to manage crises and changed the way we work forever. While few corporations around the globe were fully prepared to face this black swan event, the level of readiness has differed significantly across businesses and industries, with those companies with the strongest focus on risk management and agility able to respond with greatest speed and resilience. Many financial services and technology companies are leading the pack.

(https://www.fintechfutures.com/files/2020/02/

In the space of just a few weeks Santander completely transformed the way it works

In the case of financial services, the effectiveness of their response is in part because of years of heavy investment to shore up their business continuity plans against any type of virus attack – physical or cyber. Since the financial crisis in 2008, the importance of anticipating, understanding and mitigating risks has become deeply ingrained in the culture of financial services operations in view of heavy regulations by local and global financial authorities.

At the outset of the COVID-19 crisis, Banco Santander, one of the largest banks in Europe, enabled almost its entire workforce of 26,000 in Spain to work from home, days before the Spanish government ordered a nationwide lockdown. This was possible because the bank had already been expanding its cyber security resilience. Today, the bank has more than 125,000 employees working from home around the world and supports more than three million chat messages and 780,000 video and internet calls a day. In the space of just a few weeks the bank completely transformed the way it works, while continuing to operate effectively and support its clients.

And Santander is not the only example in financial services. Goldman Sachs, for example, had 98% of its 38,000 employees working remotely soon after the World Health Organisation (WHO) declared COVID-19 a pandemic.

Technology is the other sector that has stepped up to the challenge. Being "born in the cloud" has given new technology companies a huge advantage, creating greater agility in their technology platform, processes and workforce. The untethered environments that were already well embedded in the operations allowed them to have a resilient and rapidly scalable response rapidly.

Zoom, for example, seamlessly scaled up its video conferencing application to accommodate the twenty-fold surge in usage in less than four weeks. Very few companies would have been able to respond to such a steep increase in demand in such a short time. Zoom, however, has had some widely reported issues, falling short in its investment in cybersecurity and privacy even though it was warned by security advocates last year. In response, some governments and companies have banned the use of its software, while Zoom has committed to move quickly to address these security and privacy concerns. Agility is paramount to a firm commitment to cyber and privacy defense.

An important ingredient to a resilient response has been companies' investment in information infrastructure, digitisation, and cybersecurity, all at the same time. Having a combined culture of agility and risk is the key to success in dealing with any business disruption. Financial services and technology sectors have led both in global IT investments and in building new capabilities and business innovation. According to Deloitte, banking and technology sectors spent an average of 7.9% and 6.5%, respectively, as percentage of revenues on IT investments, as compared to all industries which average 3.6%.

Now that large corporations have re-organised themselves to work in this new environment in the short-term, CEOs and boards of directors should focus on investments they need to make until such time that the pandemic is broadly contained through an effective vaccine and robust testing capabilities. While reducing IT budgets, as part of larger cost-cutting initiatives, is difficult to avoid, it is important that corporations fully subscribe to and invest in three strategic IT areas:

- First, companies should continue to invest in building agility through the use of technologies such as cloud that enable business continuity, a remote workforce and innovation.
- Second, companies should protect both existing cybersecurity defenses and future investments as new, expanding and perimeter-less networks will pose unknown cyber risks.

- Third, and more than ever before, companies should link investments in cyber, IT infrastructure and digital transformation. This will ensure that as new technologies are brought into the enterprise, the leadership of each of these areas is accountable for the continuity of secure business operations under one enterprise risk management umbrella.

By taking these actions now, companies can better ensure that when the unforeseen occurs, they are ready to respond with resilience and agility. While this may not necessarily lessen the massive cost of the COVID-19 pandemic, an ounce of prevention is worth a pound of cure and can certainly help to mitigate the impact of future crises.

About the authors

(https://www.fintechfutures.com/files/2020/05/Homaira-Akbari.jpg)Homaira Akbari is president and CEO of AKnowledge Partners, a global strategy advisory firm providing services to leading private equity funds and large corporations in the sectors of internet of things (IoT), artificial intelligence (AI) and cybersecurity.

She serves on the board of directors of Banco Santander SA, Temenos AG, and Landstar System, Inc. She is also chairperson of WorkFusion, Inc.

(https://www.fintechfutures.com/files/2020/05/Derek-Vadala.jpg)Derek Vadala is CEO of Cyber Assessments, a joint venture between global credit rating agency Moody's Corporation and Team8, a company-building venture group.

Prior to leading this venture, Vadala was the global head of cyber risk for Moody's Investors Service, and the chief information security officer (CISO) for Moody's Corporation.
