BIZCOMMUNITY

Cybersecurity is key during digital transformation in the financial services sector

By Sarthak Rohal

31 Mar 2021

The financial services landscape is changing quickly as banks face increasing competition from technology-based financial services. Innovation is key to growing the customer base, and this requires digital transformation.

Sarthak Rohal, VP - IT services at AlphaCodes | image supplied

While cloud is a major part of the IT strategy of most large financial service enterprises, its adoption was accelerated as a result of the Covid-19 pandemic. This has highlighted the need to address security as a matter of priority, not only to safeguard IT systems but also to ensure customer data is protected in line with relevant legislation such as the Protection of Personal Information Act (PoPIA).

The future is cloud

Digital disruptors and new market entrants rely entirely on technology - cloud-enabled ecosystems, saas-based digital financial platforms, virtual platforms to support customer services to high-end technical support, etc. Cloud computing is the fundamental enabler of digital transformation, providing the scale and speed required for modern applications, and the foundation required to deliver the business value of agility.

Agility underpins the ability to innovate and deliver products fast enough to respond to market demand and the needs of customers. In addition, the cloud enables artificial intelligence (AI) and machine learning (ML).

Chat holds the key to future innovation in insurance

31 Mar 2021

The move to the cloud became imperative during the pandemic-related shutdown in 2020, as the majority of financial

services workforces needed to work remotely. Even after the lockdowns eased, many organisations are maintaining a majority remote workforce on a permanent basis.

The challenge is that, as enterprises fast-tracked initiatives like agile and DevOps to improve speed to market, security has typically been a secondary consideration. The result has been a number of high-profile security lapses, which are likely to be the result of the inability of security teams to manage digital risk.

Increased cloud adoption means increased risk

As more data enters the cloud, cloud computing providers are bigger targets for security breaches. Organisations making use of cloud services are therefore exposed to increased risk. This means that digital transformation, cloud computing and security need to go hand-in-hand to ensure financial services organisations can leverage the benefits of transformation while minimising exposure and mitigating risk.

Data protection and the impact on business performance raise the risk quotient exponentially. A global IDC web-based survey shows that 53% of US financial services providers rate complexity as a top concern, while 46% rate impacts business performance as a top concern.

The push for digital transformation and increased adoption of cloud has made data protection more complex because of establishing encryption, tokenisation and management policies for applications deployed across the board includes public, private or hybrid datacentres.

Security complexities are daunting enough even in single datacenter deployment, but it is only compounded for the financial sector as it continues to roll out multiple clouds involved in applications.

This makes it critical to know who has access to the data, what is being done with it, which devices are being used for access, and where the data ends up.

Planning for security

When developing and implementing a transformation strategy, security cannot be an afterthought. Vulnerabilities need to be accounted for from the start, and when IT infrastructure is rebuilt, security must be rewired simultaneously. This includes everything from legacy data centre IT to multi-cloud ecosystems. The ultimate goal is to provide security for all aspects of business operations.

Cloud security begins with a change in mindset around what the perimeter is – from a static frontier guarded by a firewall to a dynamic edge that includes remote workers, mobile devices, and applications hosted outside the organisation.

The unfortunate cybersecurity risks quantum computers pose to SA businesses

Riaan de Villiers 25 Mar 2021

In order to establish this new edge, enterprises need a variety of technologies, from identity as a service to a cloud access security broke, cloud security posture management, security information and event management, zero-day endpoint protection, a secure web gateway, and more.

IDaaS and CASB technologies work together to ensure only authorised users can access cloud applications and data. These technologies also ensure that data is secured and policies are enforced, while CSPM protects resources from accidental exposure.

SIEM helps organisations aggregate data from the new perimeter and zero-day endpoint protection enhances security on all endpoints, from the traditional office infrastructure to remote workers and connected devices.

Managing the risks of a hyperconnected world

As digital transformation continues, the speed and impact of risks in a hyperconnected world will become more difficult to manage, requiring rapid decision and response.

Many challenger banks will face risks stemming from heavy reliance on third parties, and from the enormous effort required to institute anti-money laundering and anti-fraud capabilities, fair lending practices, payment processing and other digitally-enabled processes.

Integrated risk management is critical to success. Effective risk management requires collaboration, integration, transparency and measurements that cross organisational boundaries.

The future success of financial services organisations rests on banks' ability to embrace digital transformation and the cloud to deliver the speed and agility customers require while balancing the risks and ensuring security remains a top priority.

ABOUT THE AUTHOR

Rohal is VP of IT services at AlphaCodes.