Microsoft VERITAS

How to build lasting cyber resiliency in the cloud

to protect your FS institution's most critical assets

PART 1—BUILD YOUR FOUNDATION

Considerations to make and pitfalls to avoid, to build cyber resiliency

By Nirvana Farhadi Smith | January 2023

The cloud is one of the most misused and vaguely understood terms in modern society. We have all heard of it, everyone talks about it, why are they talking about it? What are they getting out of it? Why do they blindly join the masses and follow like sheep? Do people really know why?

Other than those who make it their business to know, not many know what it does and how to best utilize it. Frankly, most organizations are minutes away from making their 'next bad Cloud decision'. They are nowhere near, nor have an iota of a clue as to where they need to be to 'build lasting cyber resiliency' in it!

Cloud adoption

Nowadays we are seeing more and more businesses adopt the cloud to improve efficiency and reduce the cost of software management, although this hasn't always been the case. It wasn't long ago that both regulators and firms were very dubious of the cloud and storing any data off premise. The adoption of cloud technology has been an uphill battle, especially in the financial services industry. As you know, Financial Services organizations require exceptional security to protect customer data, and the financial management process itself is fickle and prone to error.

And when you look at some of the biggest cloud security breaches in recent years, it doesn't instill confidence for those that are still on the fence about adopting it.

2 years of transformation in 2 months

It also worth bearing in mind the legacy of COVID-19. As Microsoft's Setaya Nedalla famously says, "because of COVID we have had 2 years' worth of transformation in 2 months."

When faced with the reality of everything being remote—from work, entertainment, and education to connecting with friends and more—technologies like the cloud have offered solutions to continue some semblance of normality in both business and life. As a result, we've seen decades worth of digital transformation taking place, out of sheer necessity, and with technologies such as Cloud, AI, and ML being a main enabler.

And when you look at some of the biggest cloud security breaches in recent years, it doesn't instill confidence for those that are still on the fence about adopting it.

The impact of these technologies on our lives has been tremendous, but they can and have been manipulated. The global pandemic exposed widespread vulnerabilities everywhere. We saw this in Financial Services, as compliance teams scramble to manage and monitor remote employees spread across the world; regulators and governments tightened restrictions; and the technology had to run at breakneck speed to keep pace with the increasingly sophisticated cyber criminals.

What keeps me up at night

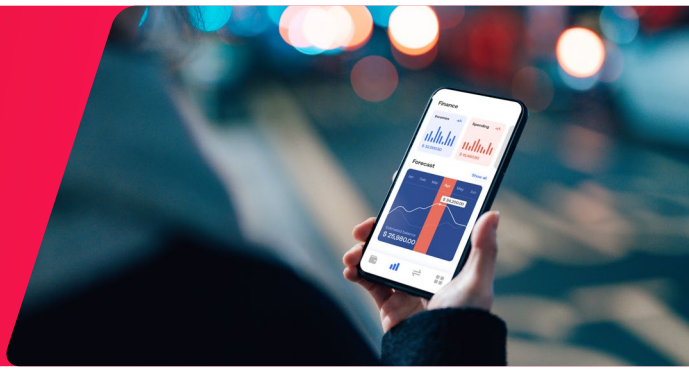
As a regulatory advisor, and professional, there are many things that keep me up at night in our deeply 'clouded' world. We are seeing cyber criminals become more sophisticated, and the current environment is proving an extremely advantageous breeding ground for criminal scams and laundering opportunities associated with the pandemic.

Operational resilience has always been a pain point for firms and regulators alike, and this has been further expounded due to the impact of the recent global pandemic. It's a time of uncertainty, and Financial Services CEOs and senior management have had to accelerate their timeline of digital transformation at breakneck speed just so that their businesses can survive.

Operational resilience has **always** been a pain point for firms and regulators alike

Although we are seeing a lot of proactive thought leadership in organizations, who are anticipating impacts on their businesses, business continuity plans are continuously being revised. Unfortunately, cybercrime has also become more sophisticated and is on the rise—especially in the Financial Services sector. We are seeing deliberate attempts to bypass customer due diligence measures by criminal gangs and alarmingly there is an increase in the misuse of online financial services and virtual assets to move and conceal illicit funds. The misuse and misappropriation of domestic and international financial aid and emergency funding is another example of these criminal activities as well as the increased use of the unregulated financial sector, which is creating additional opportunities for criminals to launder illicit funds.

It's fair to say that no firm is immune to disruptions. No one could have predicted the devastation that the pandemic has caused already, its more common to have outages in the financial services industry in comparison to governments, regulators, and other sectors.



Avoiding those pitfalls

With all this in mind, we now face the insidious invasion of our rights, privacy, political narratives, money flows, storylines, and social cohesion. The challenges facing compliance, CIOs and Operations professionals are both external—from the criminal world—and internal, from within their organizations. So, what does this all mean in relation to choosing the right cloud provider, and what are the pitfalls you should avoid?

In a recent fireside chat, I had the privilege of discussing this topic with Jose Thomas, General Manager of Cloud Enterprise at Microsoft Financial Services, and Rob Thompson, VP of Sales at Veritas Technologies, to glean their thoughts on the topic and to see how they were working together to better serve their clients' needs.

You can read my findings in part two of this report:

Put strategy into practice
Questions to ask yourself (and vendors) to protect your organization

ABOUT NIRVANA FARHADI SMITH

Over the past 25 years, Nirvana has worked extensively as an advisor, regulator, and has advised lawmakers and decision makers on writing regulations, particularly in Financial Services and Technology. She has co-authored 4 books to date as well as numerous industry whitepapers and thought pieces.

Along the way, she's benefited from an invaluable view of the Cloud evolution and met a wide variety of stakeholders. Much of her work has involved helping them understand how regulatory oversight can serve as a filter—to protect, enhance, support the lives, privacy, and well-being of the consumer, without stifling creativity.

She says, "A large part of what I do is to work with industry stakeholders to leverage the maximum efficacy of tech's impact, yet ensure a fair playing field. Who writes the test and establishes the rules is so vital. My job is to design and create that 'filter' through which tech must pass: 'Regulatory Technology' (or RegTech)."

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

Microsoft

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact