OPERATIONAL RESILIENCY IN FINANCIAL SERVICES IS A CORNERSTONE OF EVENT PREPARATION

Operational resiliency is a non-negotiable component of the financial services industry. In *The FinServ Future*, a new *Forbes Insights* and BMC survey of 300 U.S.-based C-level executives at financial services firms, 65 percent of respondents agreed that their firms are experiencing increased regulatory pressure to deliver seamless, integrated, and secure services without failure.

With the worldwide spread of COVID-19 this spring, the financial markets have hit a level of volatility not seen in over a decade. As companies in the financial services—and really, all—industries look to protect the health and safety of their workforces, it's vital that the services in place driving that always-on connectivity are secure, reliable, and resilient. With the adoption of social distancing and shelter-in-place initiatives, the availability of online services for both your employees and customers is of utmost importance.

A matter of trust

The study cites identity and authorized usage as leading security considerations. Ed Calusinski, Vice President of Enterprise Architecture at Discover Financial Services, has turned to tech to get it done. "We've instituted AI throughout our internal processes…to better enable us to deliver safe and sound products to our customers while running in a heavily-regulated industry that requires a high degree of security," he tells *Forbes Insights*.

A recent Accenture study, *Operational Resiliency is Financial Resiliency*, points out that maintaining and improving enterprise resiliency can help you build trust with your customers, regulators, and the economy you serve. It highlights the importance of tech, recommending that technology assets be

kept up-to-date to retain currency and mitigate against cyber-threats and older, unsupported solutions.

A global issue

Operational resiliency across the finance sector is a concern that's also growing internationally, and recent studies acknowledge the importance of planning ahead. Deloitte's 2019 report, *Time to flourish: A practical guide to enhancing operational resilience in the UK financial services sector*, asserts that disruptions are inevitable and potentially severe, and the onus is on financial organizations to reduce their impact, not just in how they respond, but by how they prevent and prepare for both severe events and routine disruptions.

In late 2019, the Prudential Regulation Authority (PRA), the Bank of England (BoE), and the Financial Conduct Authority (FCA) released *Building operational resilience: impact tolerances for important business services*. In that paper, Andrew Bailey, FCA Chief Executive, asserted, "Disruptive events can have a high impact on consumers and businesses, so firms and FMIs need to know where risks…lie and for any service disruption by testing their planned response."

As Sam Woods, Chief Executive of the PRA and Deputy Governor of Prudential Regulation, put it. "Operational resilience is a vital part of firms' safety and soundness," he says. " firms to be resilient in their adoption of new technologies." Those new technologies may in fact be the make-or-break differentiator between businesses that survive and thrive during the Coronavirus pandemic and those that don't.

Rethinking operational resilience as a business mandate, a 2019 PwC study, highlighted that some of those new technologies can also create new challenges. For example, the growing use of cloud service providers has expanded the security perimeter beyond security controls that were originally designed for in-house data centers.

Overall, the executives surveyed by *Forbes Insights* are still searching for best practices when it comes to resiliency. For now, they're tackling those requirements with:

- Cost and vulnerability management
- Collaboration with industry peers
- Increased audits/assessments
- More clearly-defined ownership of resiliency measures

Considering site reliability engineering

Financial organizations could also benefit from establishing site reliability engineering (SRE) groups to bolster resiliency. According to Ben Treynor Sloss, Vice President of Google Engineering and founder of Google SRE, who, quite literally wrote some of the book on it, SRE is, "what happens when you ask a software engineer to design an operations team belief in and aptitude for developing software systems to solve complex problems."

Robin van Zijll and Janna Brummel, site reliability engineers at ING Bank, first implemented SRE back in 2016, and have given talks on their process. In 2019, they provided an update at QCon. " are DevOps within our team. Basically, anyone can do anything, so there's no real restriction," said Brummel. " see…people from the dev side solve issues in a different way than the ops engineers in our team."

Information sharing is also important. "We facilitate knowledge sharing about SRE topics a meet group, which we call a guild for SREs, where interested engineers from other domains can join and share information…On our intranet, we document ways to improve your operational resilience."

Predictive technologies

As with the above example from Discover Financial Services, AI is a useful solution for getting ahead of problems before they start. Several of the CIOs surveyed by *Forbes Insights* agree. Seventy-eight percent of respondents see AI as transformative technology; machine learning (ML) edges it slightly with 80 percent.

The Commodity Futures Trading Commission (CFTC) looks at AI in its *A Primer of Artificial Intelligence in Financial Markets*, and considers it a useful way to, "use data to develop market models and identify risk factors, conduct ongoing market and risk surveillance, and help identify market manipulation, abusive trading, and fraud."

They point to the predictive nature of AI as particularly beneficial, while also considering its risks. "A strength of AI is its ability to identify correlations in vast data sets, can be helpful in systemic risk monitoring, which depends on predicting when circumstances may require intervention," says the commission. "While AI has the potential to enhance human capabilities and experiences…financial market participants should AI systems are working as intended, safe…do not generate or exacerbate systemic risk, protect privacy."

AI research group Emerj recently issued a compilation on how seven of the top US banks are implementing AI. One key takeaway is that AI is currently more pervasive behind the scenes than in front of customers, with 25 percent of AI product offerings in customer-facing functions like customer service, wealth management, and marketing and sales, and 56 percent in risk-related functions like fraud, cybersecurity, compliance, risk management, and financing and loans.

BMC's solution

BMC can help you meet growing regulatory demands for resiliency with the proper tools and the right technology. BMC Helix Capacity Optimization uses AI/ML insights to help you plan for changes in your business demand, optimize your IT cost and capacity, and balance risk and efficiency.

For more information on resiliency and other issues at the forefront of the financial services industry's digital evolution, check out *The FinServ Future*.