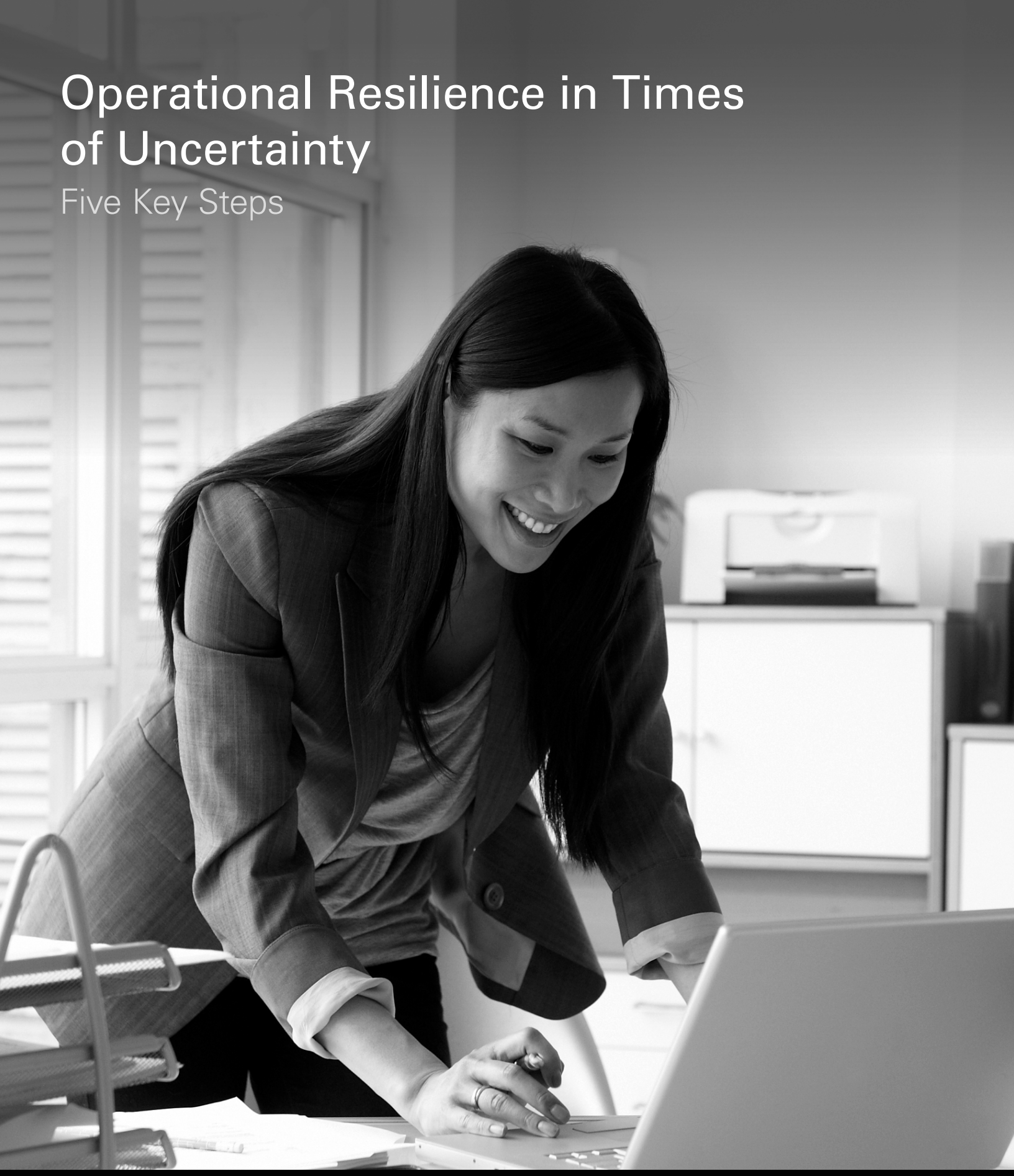
# Operational Resilience in Times of Uncertainty

## Five Key Steps



financial services @ the speed of life®

fiserv.

# Operational Resilience in Times of Uncertainty: Five Key Steps

While the COVID-19 pandemic may have caused a significant decline in economic activity, the need for a robust instant payment system and seamless customer experience remains – if anything, the need is even more acute. This throws up a range of business continuity challenges for financial institutions. Suresh Chandrasekaran, Vice President, Product Solutions at Fiserv examines five key areas to help address these challenges effectively.

Maintaining business as close to usual during the height of the COVID-19 pandemic was obviously important for financial institutions, but also clearly not easy. Some may have found a significant proportion of their workforce off sick, or only able to work from home, while in other cases offices or data centres were closed by government order. Others may have lacked the geographical diversity to maintain continuity or the digital capabilities to compensate for closed branches. While this situation may be easing somewhat in certain countries, business as usual, has definitely not yet returned and there are still concerns over occasional COVID-19 reoccurrences and the possibility of second waves.

Nevertheless, the various hurdles faced in this continuing uncertainty can be surmounted if a financial institution can cover five key areas: digital capability, infrastructure, people, cybercrime and process. Few global organisations may have the capacity to cover all these bases in-house, but many others will be looking for external support, which makes the correct choice of external partner utterly critical. One that has the capacity to deliver to a high standard on any or all of the five key areas could do much more than preserve the status quo: it could actually facilitate longtime franchise growth in these most demanding of times.

## Digital: Needed Now, More Than Ever

Many APAC countries implemented split operations or restricted business hours, while in markets such as India, the Philippines and Singapore there were stay-at-home orders or partial lockdowns in cities. While these have in some cases been eased, restrictions are still impacting channels such as branch networks and call centres across APAC, so customer-facing digital capabilities that are robust and fully-featured are vital requirements for financial institutions. While many organisations have invested in these, they all have differing levels of maturity and capability. The more recent digital challenger banks are clearly well-placed here, but others often much less so.

Many customers, staying at home, were forced to adapt to the new norm and embrace digital means to manage their banking needs. According to our data, in April 2020, there was a 30 percent increase in new user registration for mobile platforms, with growth coming from older and younger demographics. Mobile banking logins have also grown 34 percent year-on-year as a result of COVID-19. While there will always be some customers for whom digital is anathema, for many others, digital is already (or is rapidly becoming) the preferred channel because of its convenience and efficiency. However, that is only true if it is well-designed, fully-featured and sufficiently scalable. The first two characteristics are essential now because without them, customer traffic will typically divert to the call centre, further exacerbating existing capacity issues. The latter is critical because if the call centre is overloaded, more digital traffic is likely and there must be sufficient technology resources to handle the additional load.

It is worth noting that given the financial stress that many customers will have been under (furlough/redundancy and so on), this is not just an immediate issue. It is one that could have

a major long-term impact on brand and customer numbers. In many countries, bank customers often show high levels of inertia when it comes to changing banks. However, if a bank is seen to have failed customers at a time when they most needed it, this could easily cause large-scale customer desertion and persistent brand damage.

This is also not a scenario that will necessarily play out quickly; at present, the signs are that economic activity may be materially depressed for six to nine months or possibly longer. An important factor for banks serving clients during this period is their digital maturity, which can vary considerably. Banks that have historically relied on a physical network will have to scale up their digital capabilities swiftly if they are to maintain their transaction volumes and global distribution. This may be easier for larger banks, but some smaller banks will have to adapt quickly to outsourcing their technology, processing and services.

This means that a partner that can step in quickly with the right digital solutions to increase capacity and/or functionality could fundamentally improve the institution's position, not just defensively, but also in terms of competitive edge. During this period, many financial institutions are suspending or restricting the onboarding of new customers, but if other institutions are perceived to be failing and a digital partner can provide onboarding capabilities, then the organisation could actually grow its franchise.

## Infrastructure: Resilience First and Foremost

An institution may have a digital platform, but if its infrastructure is overly concentrated in a location that is shut down or unable to operate at full capacity, then a major issue arises. Now more than ever, geographically distributed resilience is critical to delivering a business as usual experience. Cloud computing obviously has a role to play here in terms of the tools embedded within it that enable the rapid switching and distribution of large transaction processing workloads across multiple locations.

The resilience this can deliver in normal conditions is important enough, but in the current environment it is critical. With countries such as Australia implementing major unemployment benefit programs and stimulus packages and Hong Kong issuing cash payout to all of its permanent residents who have registered through their banks, many consumers are hugely dependent on critical remittances arriving through reliable banking systems.

However, there is an important distinction here between providers who can simply offer generic additional capacity and those who can do this but also provide additional financial technology and expertise. In the case of the latter, the timeline to a successful deployment will be markedly faster and less stressful and the customer experience better. This is particularly true of situations where an institution may have to move all its processing to a single location due to lockdowns in others.

## People: Right Place and Right Skills

Despite all the recent advances in digitisation and technology for financial services, people still matter, which makes an organisation's 'people architecture' as critical as its infrastructure resilience and distribution. This obviously applies to call centres, but also to roles such as technology maintenance.

If personnel are overly concentrated in a location that is shut down or limited, then an organisation will be looking for a partner that can swiftly respond with personnel who are sufficiently well distributed to take up the load with the minimum of disruption. However, as with technological resilience, this isn't just about generic capacity, but also the ability to provide personnel with the right skills (for example, appropriate languages and financial institution experience) in sufficient volume.

# Cybercrime: Stopping the Bad Guys

Unfortunately, cybercriminals are already seeking to exploit the current situation in various ways. APAC has already seen a range of nefarious activity, such as the recent surge in EMI moratorium frauds in India.[1] Some recent research has also highlighted how cyberattacks might even delay the process of digitalisation in APAC.[2]

This increased threat applies in various guises. Customers are increasingly being bombarded with COVID-19 phishing emails, with one email security vendor reporting a 37 fold increase in just two months.[3] At the same time, a far larger number of employees are working from home, in some cases outside the permanent protection of the institution's firewall, so this opens up an additional attack vector. This last point was highlighted as a particular concern by banks participating in a major pandemic simulation exercise in Hong Kong in late 2019.[4]

One of the fastest ways of minimising cybercrime risks is to engage a partner that can provide a 'wraparound' network solution that sits outside the institution's existing digital interfaces and screens inbound and outbound traffic. A crucial consideration here is how much experience and expertise the provider also has in optimising usability. It is possible to achieve 100 percent security by applying over aggressive methods, but these will also deliver an atrocious customer experience that inflicts brand damage.

The current turmoil is also an opportunity for organised crime to increase the volume and ingenuity of its money laundering activities. A recent popular example has been the rise in working from home recruitment for AML schemes.[5] Other related issues are the rise in fake identities in order to make spurious stimulus package claims and the growth in stimulus checking scams.[6] Yet again, any prospective provider of cybercrime support also needs to be able to deliver on these points, as well as generic network security.

---

[1] indianexpress.com/article/technology/tech-news-technology/emi-moratorium-scam-fraudster-trick-people-trying-to-postpone-emi-loan-payments-6392132/

[2] vmware.com/au/company/news/releases/2020/Fear_of_cyberattacks_delaying_digitalization_in_Asia_Pacific.html

[3] mimecast.com/blog/2020/03/coronavirus-phishing-attacks-speed-up-globally/

[4] uk.reuters.com/article/uk-china-health-hongkong-finance/hong-kong-banks-compare-pandemic-stress-test-with-epidemic-reality-idUKKBN2070NL

[5] hotforsecurity.bitdefender.com/blog/coronavirus-job-listings-and-money-laundering-schemes-22705.html

[6] newsweek.com/coronavirus-covid19-financial-stimulus-online-scams-fraud-how-stay-protected-1495297

## Processes: Joining the Dots

The preceding four areas are individually important, but the fifth is perhaps the most critical. Ultimately, all the other areas have to be assembled in a coherent manner that will optimise performance and resilience. Achieving that requires having the right processes and that only comes with decades of corporate experience and memory.

For financial institutions trying to deliver the best possible experience to clients under the most stressful conditions, a partner that can provide the right combination of digital capability, infrastructure, personnel and security is invaluable. This holistic experience is an important consideration for financial institutions looking for where they might need support and choosing the partner best capable of providing it. Their needs might range from business process outsourcing, to additional technology for resilience/throughput, to process migration – or a combination of several of these resources/services. This underlines the value of a partner that cannot only cover all of these bases, but also bind them together into a cohesive high-performing whole.

## Conclusion

It is entirely understandable that at this time financial institutions might be first and foremost thinking defensively: how best to support existing clients and maintain as robust a service as possible? This is obviously essential, but if the right external partner is engaged, an attractive opportunity also becomes available: extending the franchise. This opportunity arises partly because the organisation will stand out favourably in comparison with others who do not respond with the necessary measures. But engaging with the right partner now will also provide the opportunity to future proof the enterprise by making it easier to rapidly roll out new competitive functionality going forward.

**Connect With Us**

For more information,
email **Marketing.ASPAC@fiserv.com** or
visit **fiserv.com**.

## About Fiserv

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today. Visit fiserv.com to learn more.

fiserv.

Fiserv, Inc.
12 Marina Boulevard
#26-04, Marina Bay
Financial Centre Tower 3
Singapore 018982
www.fiserv.com

As each business is unique, you should consider the suitability of the matters above before applying them. As such, the Fiserv group is not responsible for your reliance on the contents of this white paper.



667779 07/20