

Contact Center Resilience

5 things we've learned
from COVID-19



Eckoh[•]

How ready are you - and what about next time?

Coronavirus posed huge questions for every customer service operation.

For years, organizations have created and honed their business continuity plans for natural disasters, cyber attacks and terrorist incidents.

But it's only when emergencies occur, that we see what really works — and where the gaps appear.

Some previous decisions may be shown to be folly while others are revealed as far-sighted.

So, as the world's economies recover slowly from the coronavirus pandemic, it's time to pause for thought.

This guide examines the five lessons learned for contact centers.

It'll prove useful if you're a CEO, CIO or CFO — or if you hold a senior position in customer service, customer experience, contact center management, HR or compliance.

COVID-19: The ultimate stress test for contact center resilience

The global pandemic has challenged contact centers like never before.

With news seemingly changing by the hour and different advice issued in different regions, organizations were left wondering how to mobilise their operations — and when they'd ever manage to get 'back to the office.'

Even small decisions took on a strategic significance, potentially impacting company profitability and survival, employee safety and productivity, and customer service and confidence.

As the dust settles, it's clear that some organizations have coped better than others. But why?

Through talking with leading contact center professionals, five lessons have stood out.



Let's look at each of them...

Lesson #1

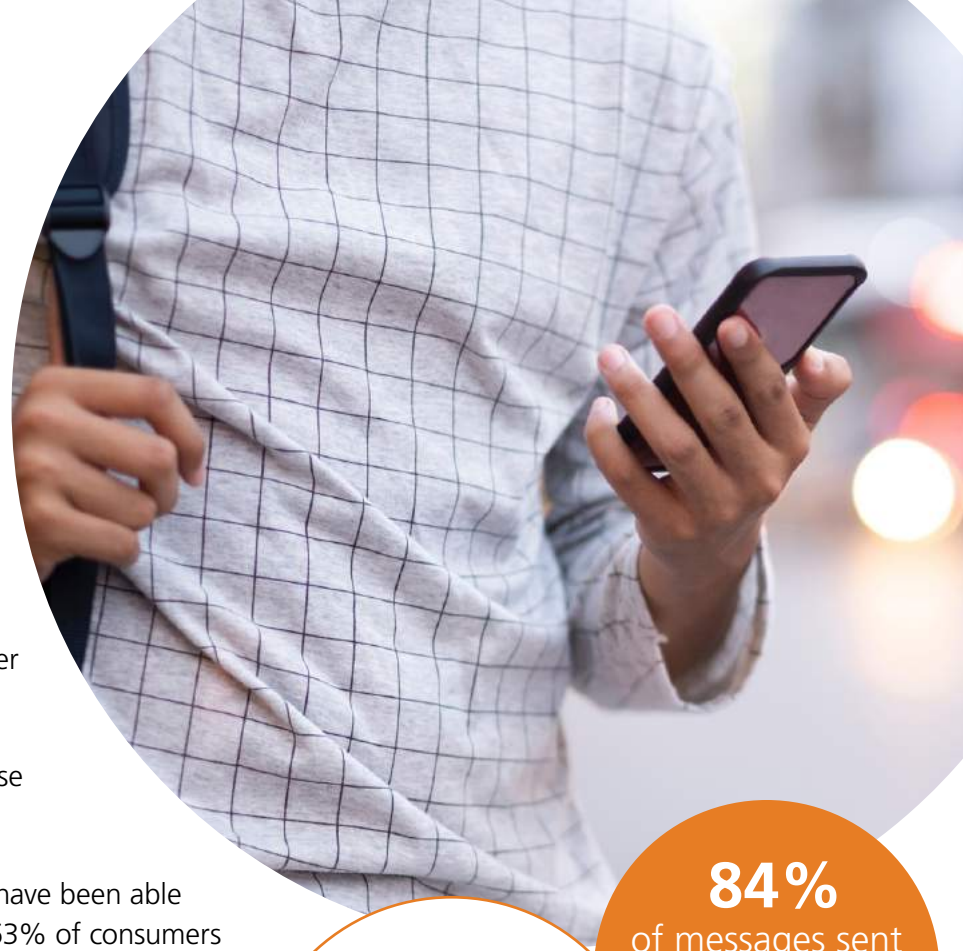
Good customer communication is essential — and tech can make the difference, especially if half your team is suddenly unavailable.

Customers will make allowances when they see your 'bear patiently with us' notice at the top of your home page. But they'll get anxious if that's where communication stops. Fortunately, smart tools and automation can help.

An emergency might lead to you losing a significant amount of agents. They could be furloughed, made redundant, on sick leave or unable to work from home. So, with fewer 'human' contact points, how can an organization maintain customer service levels?

Amid the coronavirus pandemic, some contact centers have risen to the challenge in these ways:

- **Using messaging tools to reach thousands of customers at once:** Companies have been able to tailor messages to suit the recipients, sharing links to more detailed information. 63% of consumers believe businesses should be available on messaging apps. ^[1]
- **Turning their IVR into a front desk:** Companies have used IVRs to give out accurate, consistent, up-to-date information relevant to customers at any moment. This automation has saved agents from having to handle a high volume of calls that required the same response.
- **Handling vast numbers of basic, repetitive enquiries via a chatbot:** Many customers — especially younger consumers — prefer chat to calling up. The better chatbots let customers use their own words to ask for what they want. Also, many chatbots learn as they go, absorbing information and query terms from the questions asked.
- **Enabling greater customer self-service:** Customers of some companies were able to log into their accounts, check balances and pay bills without having to speak to an agent.



81%
of consumers
already interact
with voice
assistants via
smartphone ^[2]

84%
of messages sent
through a chatbot
are read by
its user ^[3]



Lesson #2

Remote working isn't a 'nice to have' any more. Contact center agents also need the full stack of functionality at home — at the press of a button.

When emergencies happen, most consumers are extremely patient. But customer service can't shut down completely without long-term consequences for your brand. You need to get operational, quickly.

When the pandemic hit, contact centers faced different challenges, depending on their geographical location and infrastructure. Some had to reduce on-site operations while others needed to shut down their premises completely and work almost entirely remotely.

Companies that handled remote working in the best way ensured that customers couldn't tell that agents were dispersed across different locations. They maintained a great customer experience. This was because their cloud platforms enabled:

Call routing: Some companies could easily re-route calls to agents wherever they were. Contact center managers could stay in control, overseeing incoming calls, assigning them to the right agents and managing traffic. Some used dial-back so that when it's the agents' turn to take a call, the contact center platform rings them and then on answering the customer is connected from the contact center platform's telephone lines.

The full suite of agent tools: Some companies already had universal (virtual) desktop technology in place in the contact center, bringing together multiple business systems within a single interface. When agents worked remotely, they could log in and access everything needed to resolve customer issues first time around. They could handle calls, emails, web chats, social media and other contact channels as part of an omnichannel experience for customers. And they did this from home.

Remote secure payments: Because these companies were using smart tech anyway that kept card details hidden from agents in the contact center, the shift to home-working didn't suddenly present a major securing risk. Agents could take PCI DSS secure payments over the phone and via web chat, maintaining essential cash-flow for the business.

Lesson #3

It's better to have tried and deployed remote working already at some level, rather than grasping for a solution when you're under pressure.

Remote working has its own learning curve. The understandable need to act quickly may have led to some unwise purchasing decisions. Some companies have struggled with unforeseen practical issues too.


A deep assessment of the marketplace for tech solutions for remote working might normally take months and involve multiple departments and discussions. But as soon as the pandemic impacted the industry, contact centers were being targeted by quick-fix remote working solutions. Some companies have had to learn fast about a specific product's strengths and weaknesses.

Key issues that companies have had to consider have included:

- Will the solution integrate seamlessly with other systems?
- Can PCI DSS secure payments be taken across key channels?
- Will agents see, hear or record any sensitive customer information?

Some companies have also found that remote working needs its own 'support system' too. Even when agents and their colleagues are up and running at home, there are other factors to consider. Practical issues can be around:

- Agents working with young children at home or they don't have a dedicated home office.
- Remote agents needing a laptop, smartphone and a strong data connection at home.
- Whether agents have their own devices or use company equipment.
- Maintaining team and individual meets to keep up morale and employee engagement.
- The importance of companies maintaining a record of their IT assets.
- The need for home user policies — and the risks around apps, websites and malicious software.
- How users can be supported by their managers and teams using messaging platforms and videoconferencing.



By 2023, crowdsourcing, home-working, telecommuting and the gig economy will account for 35% of the customer service workforce ^[4]

Lesson #4

As soon as an organization shifts to remote working, it increases the risk of attack from cyber criminals. They may now see you as a softer target.

In the rush towards home-working, some companies have put themselves at greater risk. Cyber criminals and fraudsters don't let up during a crisis. Payment card details will likely be their No.1 target.

An emergency may make a company more vulnerable. But it's not an 'excuse' for compliance failures. Regulations don't ease off. PCI DSS, GDPR, CCPA, FCA, HIPAA, ISO, among others, remain intact and relevant to ensure that standards are maintained to protect customers and organizations from the risks.

It's important to have a well embedded security culture and awareness in your organization as well as clear policies and processes. These must guard against data leakage, unsupported solution providers and to protect against the malicious phishing attacks.

Taking payments without compromising PCI DSS compliance

Contact centers are often seen by criminals as a weak link because card and personal data is collected by an agent over the phone or by web chat.

Some methods to secure payments just won't work outside the contact center and so you could become more exposed to fraud and data breaches. Only time will tell whether the coronavirus emergency has led to some major security incidents.

The most effective approach is to de-scope as much of your contact center as possible from PCI DSS. It's essential that agents cannot see, hear, store or record any sensitive data — whether they work within a contact center building or at home.



81%
of contact center
employees are now
working remotely^[5]

41%
of remote working
contact center agents
expect to do so in the
'new normal' ^[5]

Lesson #5

It's essential that knowledge gained during an emergency is embedded within a company's everyday processes as well as its business continuity strategy.

Many people are talking about the 'new normal' and how business will have changed forever because of the COVID-19 pandemic. Certainly, it will have exposed uncomfortable truths about a company's resilience. But it might also lead to better ways of working in some areas.

It's important to capture and continue with any improvements to your operations.

- You may wish to start with a mini audit that considers:
- How well your agents and managers performed in a home working environment?
- How much remote working should become business-as-usual?
- In which areas did you lack resilience — and how could this be strengthened?
- How did any changes impact the customers experience?
- Would customer self-service tools have reduced the pressure on your team?
- If you used stop-gap technology to handle an emergency, is it now time to consider a more robust, long-term solution?
- Should automation — such as advanced IVRs, natural language speech recognition, knowledge bases and chatbots — now form a greater part of your customer service strategy?

The answers to these will be different for every company. **But it's important to embed your learning within business practices — and emerge as a stronger, more adaptable and resilient organization.**



Conclusion

Resilience must represent more than a continuity plan that's refreshed once in a while and then filed away. It must be foundational for every organization — if they are to survive and thrive.

Perhaps in future, companies will even appoint a CRO (Chief Resilience Officer) to ensure their future is protected? If not, then resilience must be a focus for the entire C-suite.

When any emergency strikes, there will always be two challenges — managing the 'today' and preparing for the 'tomorrow'. Both require careful but decisive thinking and efficient implementation.

Rushing at a solution to provide a short-term fix can lead to more problems than it solves. Many organizations may have been tempted to jump at the cheapest and quickest solution, only to find that it misses the mark and, as a result, they could be exposed to increased risk. This is usually a sign that their resilience was low.

Resilience — 'the ability to recover readily from a crisis' — is the key to coping and should be built into your operation, your tools and your workforce. To build such resilience requires imaginative thinking, understanding of risk and opportunities as well as the willingness to harness technology to help.

Cloud services, internet channels, apps, collaboration, self-service, security and a whole host of other tools exist to make organizations more productive, agile and responsive to change. Now is the time to invest in IT rather than cut back.

Some countries will emerge from the pandemic at different speeds — and at different strengths. The same will be true of different companies. The ones with greater resilience will succeed.

Market analysts, investors and consumers will judge each company on its ability to respond to a crisis. So, now's the time to get prepared.

The new normal is not clear yet, but we need to start moving towards it ^[6]

Eckoh is a global provider of **Secure Payment** products and **Customer Engagement** technology. Our Secure Payments products help businesses take payments securely through all engagement channels by removing sensitive personal and payment data from contact centers and IT environments. The technology offers a simple yet effective way to reduce the risk of fraud, secure sensitive data and become compliant with the Payment Card Industry Data Security Standards (PCI DSS) and wider data security regulations. **Eckoh has been PCI DSS Level One Accredited since 2010.**

[Agent Payments](#) | [Automated Payments](#) | [Web Chat Payments](#) | [Customer Engagement](#)

Eckoh^o

Start a conversation about how to achieve contact center resiliency...

t: **866 258 9297** e: tellmemoreus@eckoh.com www.eckoh.com

