2022

A guide to security in your hybrid-working contact centre

MaxContact

Introduction

Contact centres are a target for cyberattacks. The sheer weight of customer data stored in contact centre servers makes them attractive to bad actors on the internet. The need for continual communication between agents and customers, and agents and other areas of the business, opens other potential backdoors to customer data and core applications.

In reality, digital transformation is all That's been shown in the real world again and again.

According to a recent study in CIO magazine, a whopping 73% of organisations have experienced a jump of 25% or more in cyber threats and alerts since the start of the pandemic.

These headlines are the tip of the iceberg. Smaller data breaches can also do significant damage, in terms of lost business, fines from regulators and plummeting reputations.

Case in point
Examples like the TalkTalk attack in 2015, which led to the theft of personal data of 157,000 customers, make headline news. Since then the introduction of measures like GDPR has focused minds on security. Ticketmaster was fined almost $2 million last year for contravening GDPR regulations and failing to ensure the security of customer data.

The impact of Covid.

For contact centre managers, Covid has added another level of complexity to the quest for data security. The 'new normal' has seen more customers interacting virtually with companies and organisations.

Online shopping, banking and service provision were already popular, and are now the norm.

The AFR revealed that **Australians spent a record $62 billion online, with figure expected to double in the next five years. More than 80% of Australians shopped online last year.**

Contact centres are dealing with this deluge of new interactions with a remote or semi-remote workforce. This is likely to be the case indefinitely. Workers have become accustomed to the new way of working and the clamour for 'hybrid working' (working some of the week in the office and some at home) is likely to be as loud in the contact centre as it is in other areas of your organisation.

Remote working increases cyberthreats in a number of ways, and cybercriminals have sensed an opportunity.

47% of IT and cybersecurity professionals say the number of genuine cybersecurity threats has increased 'greatly' or 'somewhat' since the start of the pandemic.[1]

As the transition to home working happened, organisations had to adapt and evolve their cybersecurity approach, solutions, and policies to enable remote employees to work productively, access company resources securely, and ensure business continuity.

The impact of Covid.

Many threats have increased because of the mass adoption of remote working:

BYOD and unapproved applications. In one report, organisations admitted that they are struggling to manage remote workers' use of phones and other mobile devices. Remote employees may also adopt apps and services that haven't been approved or security checked by IT, whether that's a note taking app or a password manager.

Home internet and WiFi. Agents are accessing your network via domestic internet connections and their own routers, both of which are likely to be less secure than corporate equivalents. Home WiFi is likely to have weaker protocols too. In a survey of IT and cybersecurity leaders for Computing, poorly protected home networks were called out as the number two threat to data security.

Phishing scams. There was a huge spike in phishing emails at the start of the pandemic, as cybercriminals sensed an opportunity. At the same time, security training for staff is harder to organise away from the office, and information on the latest scams more difficult to disseminate. It's easier for an employee to click on an unsafe link when the IT department isn't on their case all day. In the Computing survey mentioned above, employee behaviour was considered the number one cybersecurity threat.

New apps. When companies transitioned to remote working almost overnight in March 2020, many equipped new remote workforces in an ad hoc way. New solutions (video conferencing, for example) were bolted on to legacy infrastructure. The Computing survey makes plain that remote meeting software, in particular, is considered a serious security threat.

"Home based workers, remote from their usual support and information sources, are potentially vulnerable to fraudsters. In addition, many customers are being faced with personal and financial challenges, so some organisations are presented with an increased level of demanding and emotional contacts, which criminals will emulate and use to gain leverage."
Call Centre Management Association

Securing your contact centre for 2022 and beyond.

So far we've focused on what many of you will already know. Firstly, that contact centres are a magnet for cybercrime, because the potential rewards of a successful hack are so great. Secondly, that the situation has been exacerbated by the pandemic, which forced a mass transition to inherently less secure home working.

So what can businesses do to protect themselves from cybercrime in 2021 and beyond? The answer is to tighten security in two complementary ways.

Employee behaviour

This is perhaps the most pressing concern. As home working (at least for some staff, some of the time) switches from a short-term fix to a long-term solution, now is exactly the right time to draw up a new set of easily understood security standards. A security refresh will also benefit workers returning to the office full time.

What these standards include will depend partly on what your business does, but some features will be universal. The standards should cover BYOD and permitted applications, email and password best practice, and use of two-factor authentication. They should be accompanied by cybersecurity training, which can be delivered remotely if necessary and cover the specific challenges of remote working.

Digial transformation

Contact centres are most secure when alert and mindful agents are equipped with advanced software solutions.

Ideally, your contact centre software will provide full end-to-end encryption, remove the need for the use of personal devices and unregulated online applications, and give managers real-time data on who is using the company's tools and from where. It should allow for easy and secure scaling, and let businesses set stringent criteria for permissions so that nobody has access to data they don't actively need. Your software solution should be tested and tested again to take into account new and developing threats.

Security and the cloud-based contact centre

If there's one area where there is still some resistance to cloud, it's around cybersecurity. The uptake of cloud-based contact centre software has surged since the start of the pandemic, but some managers are still loath to give up the perception of tighter security that an on-premise solution provides.

But it is perception, rather than reality. In fact, modern cloud contact centre software is generally more secure than on-premise alternatives, for the following reasons:

Big company security. It doesn't matter the size of your organisation, if your solution is hosted by public cloud giants like Microsoft Azure or AWS, you're benefiting from a huge and ongoing investment in cybersecurity. Expect the highest standards of encryption, network monitoring and firewalls - far more stringent security, in fact, than the majority of the world's private data centres or colocation sites can provide.

Automatic updating. A good provider will update your software as soon as a new patch or security feature is released, so you're always using the most up-to-date version. That's important, because we know cybercriminals often prey on legacy systems and unsupported or unpatched services. As soon as AWS or Azure role out new security protocols, contact centres benefit.

Strict permissions. Cloud software lets you set and revoke permissions in seconds, giving employees access to the data they need, when they need it, and nothing more.

CISOs and security experts aren't required. Vendors that specialise in delivering cloud-based solutions have invested in the type of technical expertise needed to maintain data integrity and security, so you don't have to.

Safer BYOD. A good cloud solution will provide a secure softphone that can be used on company and personal devices, and a full omnichannel communications service that stops remote workers filling in gaps with unverified applications.

Reporting and data. Good cloud-based solutions will provide managers with real time data on who is using what, where and why. Detailed insight into your dispersed IT estate can help managers spot unusual behaviour or guideline breaches.

OpEx investment. Many businesses are feeling the squeeze right now, and might not be able to afford the heavy CapEx investment of replacing an insecure legacy system. Cloud solutions don't need on-premise equipment, and offer per-user-per-month payment models, making more secure contact centre software affordable for any business.

Easy scaling. Because good cloud solutions let you add users in a couple of clicks, new or seasonal staff can be added to your secure system straight away, without the need for temporary - and most likely less secure - measures.

With all that said – this is not surprising...

38%
of respondents said their organisations currently use cloud-based security tools.

30%
said they were likely to adopt them in the next 12 months.

The questions you need to ask every cloud contact centre provider.

But not all cloud contact centre software providers are the same. When deciding on who to trust with your data (and, by extension, your business), you should analyse the features and technology a provider offers, and also their overall attitude to security. Is security a tick box exercise, or something that permeates an entire operation? Are they as careful with their own security as you want them to be with your own?

Here are six security questions you should ask your cloud-software provider:

1. Where will my service be hosted?

At a minimum, your service should be hosted by one of the large public cloud providers with a reputation to protect and a significant budget for security innovation.

2. What happens during a major cloud outage?

Cloud providers should back up data regularly and use multiple redundant data centres for automatic failover.

3. What encryption do you use?

Full SSL/TLS encryption for voice and data is essential.

4. What are your accreditations?

Third-party accreditation of the software and the infrastructure it's housed on is essential, so check if the solution is PCI-compliant and certified ISO 27001- at the very least.

5. What security tests do you run?

Providers should regularly test their network and applications for vulnerabilities, and organisations that take security seriously will conduct external penetration testing.

6. How do staff work on the contact centre platform?

Most security issues come from poor configuration, which is human error. Find out how the organisation works to minimise this risk.

How MaxContact goes further.

MaxContact meets all these baseline security standards, and then goes further. For example, all services are hosted on Microsoft Azure, a platform that spends over $1billion a year on security and fends off seven trillion cyberthreats per day. It's no surprise that, in a recent CCS Insight's survey, Azure was rated the most trusted public cloud provider by senior executives.

Not only do we host on Azure, we build on the platform's highest level of enterprise security. All our customers are given their own, entirely segregated enclave on Azure, along with a heavily protected vault for data storage.

We backup all customer data every day, using a rotating schedule to ensure availability. Levaraging Azure's global redundancy, all customer data, storage and backups are encrypted securely and replicated to data centres across the globe. If every Australia data centre went down, customers would still be back up and running in no time.

As far as transmission security goes, we employ full end-to-end encryption for voice and data. With MaxContact you get the highest level of TLS encryption available, which is over and above what many competitors offer.

And of course, we know that your customer data is the most important thing to protect. Along with transmission and database security we also use on-disk encryption, bitlocker and Azure vaults. We ensure any data we log from the application services has anonymised PII, removing any customer details.

But many system compromises come from bad configuration or being left open, rather than technical vulnerability. At MaxContact we guard against this by giving our teams limited, role-based access to production environments that can only be accessed through trusted "jump" servers. These are opened to staff by request, IP whitelisted to our offices and MFA protected.

And at MaxContact, security is never a tick box exercise. We constantly monitor the threat analysis dashboards for bad actors and attacks and provide real time alerting for any issues.

We work to highly regarded industry standards such as CIS baseline images and NIST coding standards. We're accredited by organisations like ISO and Cyber Essentials, and are working towards ever more exacting certificates that further demonstrate our industry-leading cybersecurity credentials.

Finally, we perform rigorous annual third party penetration testing, and regular internal tests. Any vulnerabilities this testing discovers are patched in the quickest possible time.

Security you can trust.

We could go on, but suffice to say that organisations from household names to international banks trust our contact centre software for its sensitive customer communications.

MaxContact go above and beyond baseline security protocols - at every level, from network and application to transmission, our philosophy is "everything questioned, everything tested".

You can learn more about our commitment to security here.

If you'd like to chat security or contact centre solutions simply call us on:
1300 570 703 or email
info@maxcontactaustralia.com.au