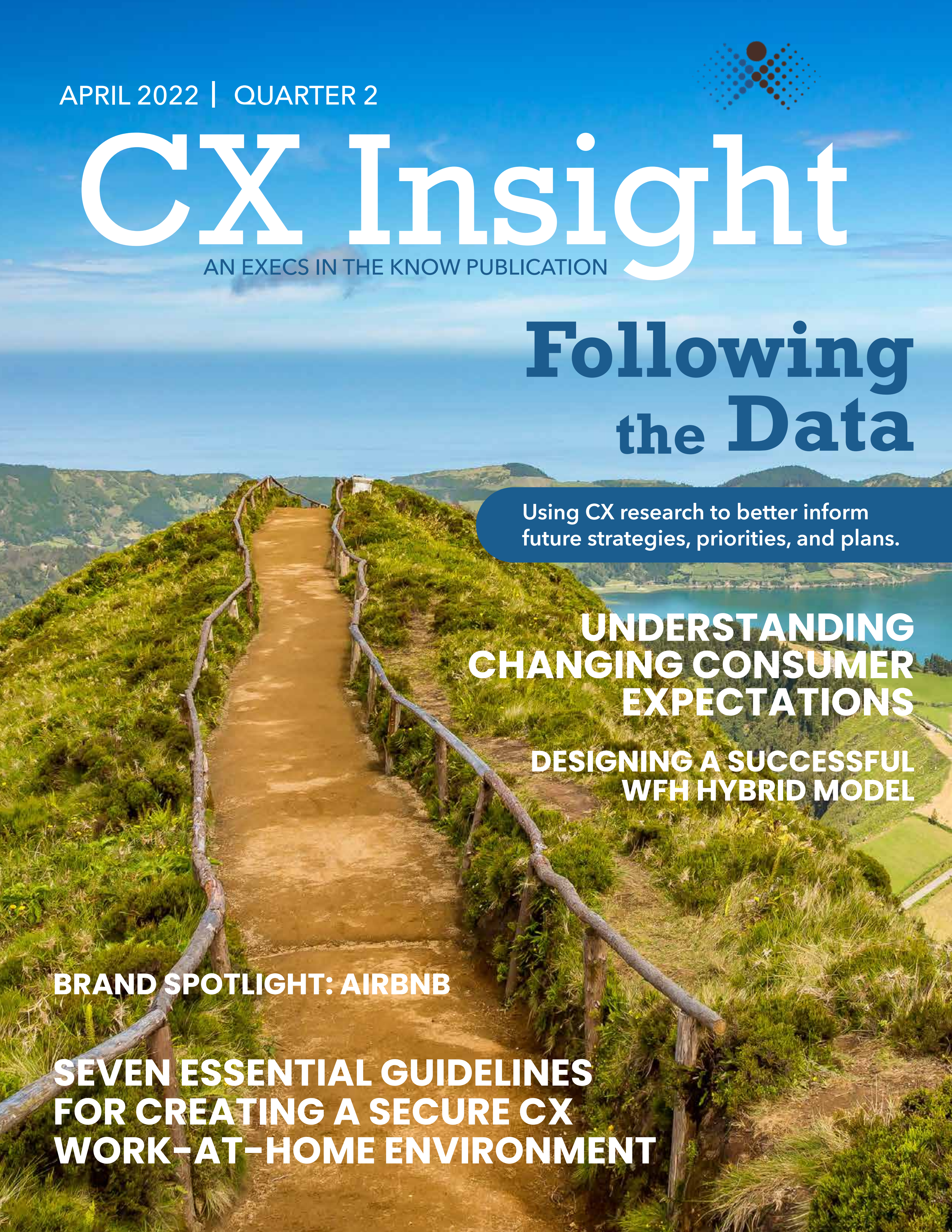
APRIL 2022 | QUARTER 2

CX Insight

AN EXECS IN THE KNOW PUBLICATION



Following the Data

Using CX research to better inform future strategies, priorities, and plans.

UNDERSTANDING CHANGING CONSUMER EXPECTATIONS

DESIGNING A SUCCESSFUL WFH HYBRID MODEL

BRAND SPOTLIGHT: AIRBNB

SEVEN ESSENTIAL GUIDELINES FOR CREATING A SECURE CX WORK-AT-HOME ENVIRONMENT

Making security the first consideration when building your technology stack is the key to successful scaling and shifting.

Seven Essential Guidelines for Creating a Secure CX Work-at-Home Environment

by Wayne White, Chief Information Officer and Art Burt, Chief Information Security Officer

In early 2020, conventional wisdom across the BPO industry predicted that CX was going digital. As a result, companies would largely return to in-house customer support thanks to a sweeping decrease in the need for customer contact requiring human interaction. However, when COVID hit, we all learned differently. Not only did it become impossible to staff internal CX operations in a timely manner, but even as the customer experience went digital in a big way, much more guidance and personal interaction were needed. Many outsourcing brands which already had at-home footprints found it challenging to ramp up to meet demand. However, clients did expect their CX partners to do so – and quickly.

Focus on People, Process, and Technology

Those first few months of the pandemic were a sprint to get agents up and running at home. Some organizations, especially those with significant at-home operations, made the decision to scale existing solutions to accommodate the growth in capacity. Others like ResultsCX built a new platform from scratch, benefiting from the ability to incorporate far stronger security measures in a brand-new system. That's when many organizations learned that there are three make-or-break components of home-based support, and security is a big part of all of them: people, process, and technology. To start, you need people who understand how to work in a virtual environment. Then, operating processes must be completely shifted and adapted to match a virtual environment; security considerations must apply to every altered process, as well as to every change in the technology involved which, in many cases, needed to be completely re-architected.

Think about the former contact center environment, where managing core security practices was systematized until it was practically effortless; everything, from a clean desktop to what showed up on agent PCs, was constantly monitored on the production floor. In the new world, every PC sitting in a home is in essence a contact center, with its own network that must be kept secure. Now, every function needs to feed into a single secure platform. Systems for training, coaching, and monitoring have had to be reimagined and scaled in ways that had never been done before. Those who skipped this necessary step opened themselves up to security risks, as well as network penetration and hacking.

Managing all these networks also requires managing the increased risks, whether data leaks, privacy breaches, increased credit card fraud, or other serious threats. In many cases, clients used third parties as technology partners for going to work-at-home, which means BPO companies had to integrate with many more partners. In essence, the security threat quintupled overnight.

Helping Clients Handle Security

Having established a strong security stance involves the commitment to security measures at the highest level. It also means that you apply strict controls to your systems and processes and limit access whenever and wherever necessary. A beneficial effect is that you become a resource for your clients. Several times a week, ResultsCX holds security reviews with our clients where we examine their security configurations and offer expert guidance on implementing additional security and compliance best practices. Many clients realize that our daily diligence with managing security across multiple industries makes us a source of knowledge on new or unexpected threats, as well as trustworthy advisors on steps to take and tools to implement. Recently, a client reached out to our Information Security team with questions about adopting a new cloud

> ResultsCX has successfully created a secure virtual CX environment, earning a near-perfect 800 score from BitSight and the number 1 ranking among our competitors for more than 20 months running.

ACD platform. Five years ago, such outreach by our clients was almost unheard of. Typically in the past, a client led the charge when it came to security requirements. Now, they have seen our success at maintaining a secure environment and want our advice on how to always be prepared for the inevitable attacks of hackers, phishing, and other attempts to breach system protections.

Web Log-In Access and VPN — What Can Go Wrong

One way organizations accommodated their new remote workforces was to simply allow agents to access applications with web passwords and logins from home, without taking into consideration that this could now involve thousands of agents across multiple vendors. In many instances, there was no way to monitor access, which opened up clients to epic levels of fraud. In a situation like this, one to five percent of agents are likely to do something inappropriate or potentially even break client, industry, state, or federal regulations. Once system access was opened up on the web, hackers across the globe were eager to take advantage of limited ability to block their access.

Many organizations entered the work-at-home era with VPN systems that supported standard general and administrative staff, but these VPNs are not designed for working with customers and in patient accounts. Many of the CRMs and primary software tools weren't even reconfigured for work-at-home. This meant an employee could work on a VPN for a while, then log off to spend personal time on the internet. If the employee accidentally downloaded a virus, it now had an infection path straight into the company network the next time that employee used the VPN for system access.

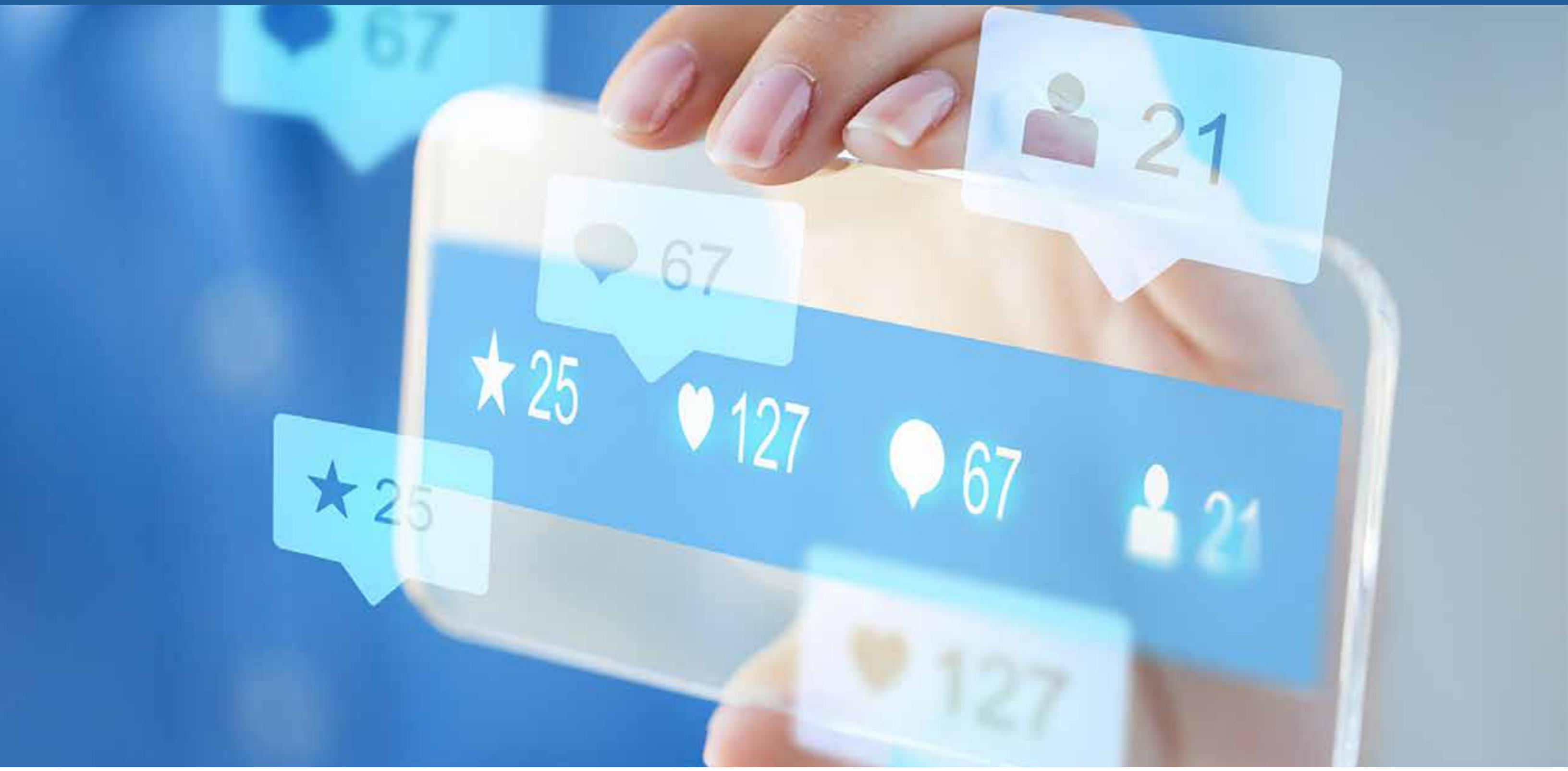
During the transition to widespread working from home, large BPO providers have been hit by ransomware and brought down by malware left and right. Almost without exception, these attacks entered through technology the business already used and assumed would scale effectively. What had been thought to be a secure, stable platform really was a stable, but not universally secure platform. The vulnerability posed by VPN on home PCs was not recognized; bad actors caught on early and quickly seized on the opportunity.

A Fundamental Focus on Security

Building a new platform from scratch allows you to focus on security at a fundamental level. Even end users become part of the security team, watching for indications that an interaction or transaction isn't legitimate. At ResultsCX, security is at the core of everything we have built. For example, we were almost completely launched on Windows Virtual Desktop (WVD) 1.0. for our at-home agent interface when security considerations gave us pause. Ultimately, our choice was to leapfrog to a higher level of security effectiveness. We instead chose to work directly with Microsoft as a strategic development partner to build out our own platform on WVD 2.0. The collaborative build with WVD, now known as Azure Virtual Desktop, was so robust that it has taken on a life of its own. In this same vein, we've also realized the value in bringing on a certified chief information security officer into decisions that affect processes and technology. Security is always the first consideration now whenever changes are planned.

Seven Essential Guidelines for Creating a Secure CX Work-at-Home Environment

ResultsCX has successfully created a secure virtual CX environment, earning a near-perfect 800 score from BitSight and the number one ranking among our competitors for more than 20 months running. Underpinning this track record are the following guidelines that can help other CX providers who hope to follow in



our footsteps.

1. **Tighten up overall enterprise security and permissions.** Look at the technology layers you've built out and ensure each one is rock solid. Every new tool builds on this foundation, and existing problems will be magnified when you add an at-home workforce to the mix. A crack in the foundation can quickly result in tens or hundreds of thousands of people experiencing the same issue or vulnerability.

2. **Stop trying to balance security against openness and communication.** Communication tools can create significant security risks. Help employees figure out how to connect, but securely.

3. **Make security the very beginning of every conversation.** Discuss security first before you deploy an individual tool, and again with each layer that you build out.

4. **Stop thinking you need to save all that data.** Large amounts of saved data can be a massive source of threat. Lower risks by removing any non-essential data. If you don't save data on a widespread basis, you are a less interesting target for hackers. Conduct an overall review of your data retention and find ways to limit it.

5. **Examine every potential risk point in your service environment.** When it comes to the systems that support your work environment, know which are absolutely required for operations. Everything else needs to be eliminated to make your operations far more secure.

6. **Undergo regular third-party risk assessments.** Find an outside company to regularly assess risk on your actual platform. ResultsCX also performs risk assessments for multiple clients, looking at their technology to find holes in it. Four eyes are always better than two when assessing the security of your base infrastructure,

especially when it comes to at-home infrastructure.

7. **Make security a mandatory employee responsibility.** All employees need to know their obligations when it comes to maintaining security. If you can't get buy-in from the whole company, you're always going to have issues. Backing the commitment to security is a decision that begins in the C-Suite decision and extends all the way to frontline employees.

A common misconception in many organizations is that if they lock everything down, they can't do business. That's not true. You can restrict access, follow stringent security practices, achieve stability, and still operate successfully as a company. But inevitably, companies that try to negotiate on security practices fall prey to the same mistake. They build their solutions and only then try to apply security. Making security the first consideration when building your technology stack is the key to successful scaling and shifting. It's an essential approach that can no longer be treated as optional.

> With the interconnectedness of the world, having a vendor that doesn't take security at least as seriously as you do increases your vulnerability regardless of your practices.

Finally, choose partners who are every bit as security-conscious as you are. If you're dealing with a partner who has a low security rating, ask yourself why you are doing business with them. With the interconnectedness of the world, having a vendor that doesn't take security at least as seriously as you do increases your vulnerability regardless of your practices. We all must operate on the assumption that we will get attacked at some point, and our security systems need to be as strong and prepared and possible.

Wayne White
Chief Information Officer, ResultsCX

Wayne leads all information technology functions for ResultsCX. He brings a broad spectrum of experience from more than 25 years in technology. Wayne's core areas of expertise include the development of new IP and network designs, processes, products, and tools to enhance business solutions and client offerings.

Arthur Burt
Chief Information Security Officer, ResultsCX

Arthur leads Security & Compliance for ResultsCX and is a proven high-level manager of security teams and programs. He has 30 years of BPO experience that includes 20 years in IT leadership as IT Chief of Staff, CISO, and Solutions Architect Team Leader, in support of 50K+ employees and 300+ clients.

ResultsCX

For more information, visit:
Results-CX.com