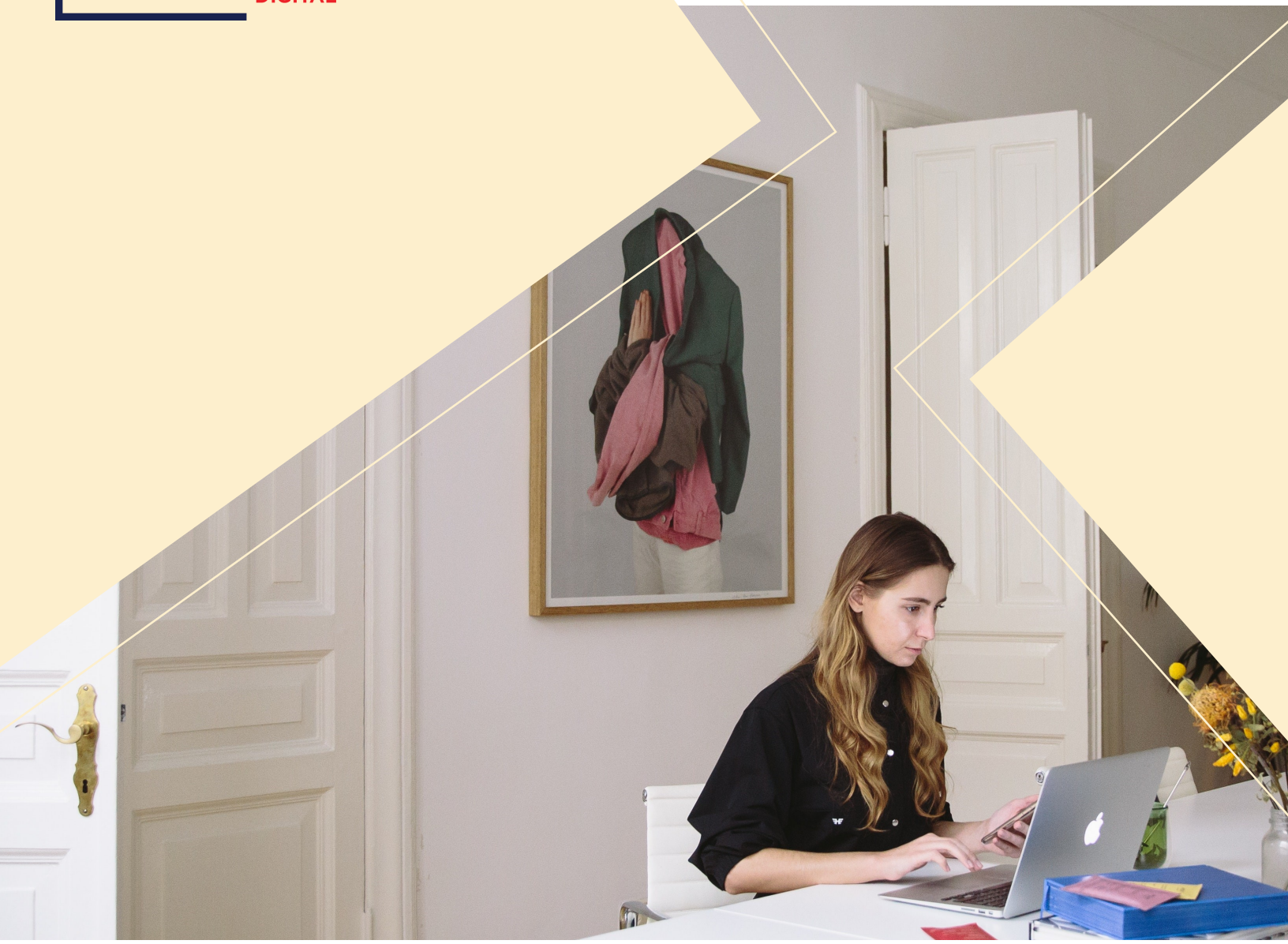
CCW CUSTOMER CONTACT WEEK DIGITAL

2020 SPECIAL REPORT SERIES



Securing & Elevating The Remote Agent Experience

WRITTEN BY: AMANDA CAPARELLI

This report is provided by yubico

Featuring Insights From:

Rahul Vijay

Head of Global Connectivity, Supply Chain & Operations

Uber

Gordon Schleffer

VP of Customer Care

Magellan Health

Stina Ehrensvärd

CEO and Co-Founder

Yubico

Jerrod Chong

Chief Solutions Officer

Yubico

Abby Guha

Senior Director, Enterprise Product Marketing

Yubico

Guido Appenzeller

Chief Product Officer

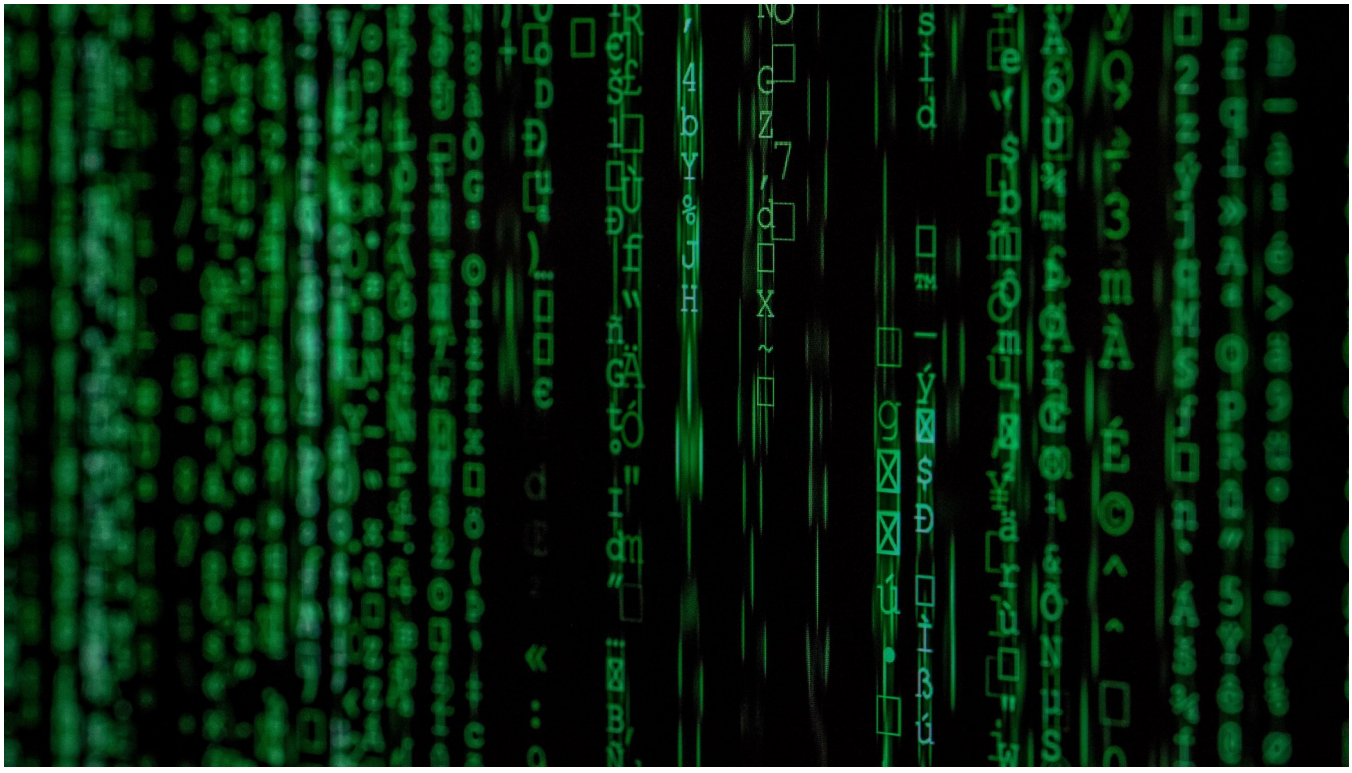
Yubico

Introduction

Ready or not, organizations around the world are asking traditional office-based agents and employees to work from home in response to the COVID-19 pandemic. Beyond questions about workflow and engagement, such an accelerated shift to remote work raises questions about the security of sensitive customer data and confidential information in remote agent environments.

Data security breaches put entire organizations – inclusive of customer and employee safety, brand reputability, and stakeholder sentiment – at risk. According to the 2019 Cost of Data Breach Report conducted by Ponemon Institute, the average total cost of a data breach is $3.92 million, with the United States specifically suffering the most expensive average at $8.19 million per data breach.

The current state of today's contact center security is particularly vulnerable. Even under an already fairly controlled environment, physical contact centers are innately susceptible to breaches. Imagine how much riskier the collection and usage of such highly sensitive data is from remote settings around the world.



The Uncontrollable Rise of Remote Work

In recent months, the world has witnessed a truly unprecedented rise in remote work due to COVID-19. Although there are numerous benefits associated with remote work capabilities – from increased productivity and skill-based hiring to overhead cost-reductions – some organizations were simply ill-prepared for such a rapid shift. Within the contact center space specifically, many companies still fall behind the curve of evolving from the conventional call center into a modern, adaptable customer contact service.

Contact center leaders across the world are currently working through this scramble to enable remote work capabilities. From upholding productivity, motivation and KPIs, to implementing automated systems and even investing in AI or self-service in an effort to manage surges in call volume, some aspects may have been overlooked through such whirlwinds. However, there are some serious risks associated with the remote work experience that must be addressed and prioritized by organizations, especially when it comes to sensitive information and customer data.

Fully remote contact centers present a unique – and unprecedented – challenge to the future of data security, as remote environments do not typically possess the same digital and physical safeguards that the traditional office or contact center site provides. As any given agent is sitting at their desk in a traditional contact center, they are also being protected by layers of preventive and approved security controls. It is by no means a foolproof system, but it is much more difficult for an agent to make a mistake – digitally or physically – when all workstations are in a single location being directly controlled by the company. Placing agents in entirely new work environments, without the proper training and secured systems in place, could very well put any company and its data security at high risk.

"It just takes one bad actor to spoil the reputation of a contact center provider and their customer. These challenges escalate as agents are using their home networks to login to client systems. If home networks are compromised, there is a chance for customer data to be impacted." — **Rahul Vijay**

Maintaining Both a Secure and Seamless User Experience

"It seems that data breaches are all too common and accepted these days...until it happens to you! Consumers are craving more connection when they do business and strong customer experience matters. Organizations must realize that loyalty goes both ways and if consumers are willing to trust us with their business, they need to also trust us with their data. The best examples of this can be in on-line purchasing, when reading consumer comments. These comments are focused on both the customer experience, as well as the company's integrity, not merely the product or service itself." — **Gordon Schleffer**

Organizations are continually competing to build deeper, more personalized connections with customers. Building these more personalized experiences means collecting and leveraging more customer data, to which agents will have direct access. This increased access inherently makes data more vulnerable, especially as companies continue to expand digital channels and remote communication capabilities.

In fast-paced environments like the contact center, every second counts – regardless of external factors and uncertainties. As agents today are working remote and using mobile phones, personal laptops, desktops, or tablets, this heightens both productivity concerns and security risks along with their use. How is your organization ensuring a consistently secured user experience is being provided and balanced by a seamless experience on a daily basis?

Customary security practices like multiple layers of authentication, passwords, codes, security questions and red-tape approval processes tend to make things more cumbersome, leading to fragmented and inefficient experiences for agents and customers. Organizations could traditionally only have a consistently secured experience or an efficient one, but new technology has resolved this dilemma.

"In an environment where success is largely driven by the number of customer queries solved in a day, it can be easy for even the most well-intentioned agents to cut corners. Unfortunately, in today's digital era, and now with the growth of remote work, this often equates to poor security practices that affect the business. If an organization's defense mechanisms are cumbersome and reduce an agent's productivity, it will impact the end customer experience, impede overall job satisfaction, and ultimately a successful profitable-run contact center." — **Jerrod Chong**

The Rise of Account Takeovers and Social Engineering

"Hackers thrive on crisis and both the US and UK governments have recently issued COVID-19 cyber threat related security advisories warning against online attacks, especially targeting VPNs and remote workers…as agents work remotely it is imperative not only to offer a seamless and productive work experience, but doing so with top security approaches in place is of paramount importance." — **Abby Guha**

Customer data concerns are on the rise, and for good reason. As broadcasts of high-profile company data breaches have been put on center stage over the years, innovative and efficient measures are being taken to better secure customer data. However, consumer trust is still fading year after year. What does this mean for assumed protected information customers are willingly providing to healthcare providers, businesses, and financial services from remote settings around the world?

Account takeover fraud in particular is growing at scale in the contact center. According to a recent Forbes study, 51% of financial services companies identify the contact center as the primary access point for account takeover attacks. This number becomes particularly alarming when considering current remote work environments, and how securely – or insecurely – agents may be accessing systems holding sensitive customer data.

Data fraudsters are likely already capitalizing on the current global crisis, predominantly due to these fluid and sudden shifts in work environments, both digitally and physically. To make matters even worse, contact center agents oftentimes utilize knowledge-based authentication when accessing a given caller's personal information, a process that is highly susceptible to social engineering.

A scam used to manipulate individuals into divulging sensitive or personal data, social engineering is something that remote agents may now be particularly defenseless against.

According to Verizon's 2019 Data Breach Investigations Report, one-third of all data breaches include social attacks, and this percentage of human-related security attacks has been on the rise in recent years. This method of manipulation poses a serious risk to any organization's security-preparedness, as agents without the proper security training and awareness are now all the more vulnerable from remote settings.

Today's top security challenges are centered around data integrity & security. Whether it's PHI in Healthcare or financial information in other industries, protecting both the company and customers' information is an ongoing security focus. Increasing the work-from-home (WFH) footprint only makes this more complicated. Not only must companies ensure security on site, but now must guard against intrusion at home. These potential threats can come from employees themselves (cell-phones with cameras, company information "open" at home), as well from outside (unsecure connections and unrestricted access)."

— **Gordon Schleffer**

Agent Training and Security Awareness

Today's remote agents are using new tools, working from new environments, and connecting with customers under wildly different circumstances. This unforeseen reality inherently leads to increased frustrations and misunderstandings without the proper agent training and strategy in place.

Customer contact channels and service operations are more complex than ever before. Contact center agents must be able to rapidly resolve complicated customer issues and answer questions, all while seamlessly transitioning between multiple channels and platforms. These oftentimes convoluted processes may unfortunately leave remote agents particularly susceptible to online attacks and social engineering scams. Security awareness becomes even more crucial when considering data-sensitive industries like financial services and healthcare organizations, whose agents have access to highly confidential information and must continue to meet regulatory compliance standards.

More than ever before, agents around the world are accessing internal systems and sensitive customer data from remote settings on a daily basis. Training is time-consuming, costly and particularly difficult to conduct from a remote setting. When considering the high attrition and turnover rates typically seen in contact centers, the challenge here lies in effectively monitoring and training each remote agent to be exceptionally attentive.

Investments in Securing the Remote Agent Environment

Data security has increasingly become more important as organizations continue to expand their digital service offerings, and more customer data points are being collected and analyzed. Because of this, properly investing in secured access to company and customer data is critical to upholding brand reputation, customer trust, and agent confidence in accessing such sensitive information. However, as this massive shift to remote work has occurred at such an accelerated pace, security solutions may have taken a backseat to other investments in remote agent experience, cloud and self-service systems, and AI capabilities.

While these priorities are understandably front-of-mind for contact center leaders shifting teams to entirely new work environments, managing unpredictable surges in call volumes, and training agents on new technologies, protocols, and systems, it is still critical for customers to continually feel comfortable providing their personal information to these remote agents.

Safeguarding personal data throughout all digital experiences relative to the holistic customer journey will provide stronger growth in customer loyalty, advocacy, and spending. As a business, taking the human-centered approach through such unprecedented times is more important now than ever. Proving to customers that your organization is putting both them and the safety of their information first is key to maintaining trust.

"Poor security and data breaches affect customer stock prices, valuation, brand perceptions and customer acquisition and retention. There is a basic level of trust and safety expected from contact center providers. If there is a breach to this, this will impact the business relationship severely." — **Rahul Vijay**

Top 4 Recommendations to Protecting Remote Agents

Contact center agents are continually accessing more customer data, leaving more room for error and higher probabilities in data attacks and social engineering scams. With a rise in remote agent work leading to a lack of direct physical and digital oversight, these security risks are innately heightened.

Against a backdrop of so much uncertainty, assuring customers that their personal information is and will remain protected is something that should not be overlooked. There is no doubt that data fraudsters will be capitalizing on the current crisis, and there are security measures that your organization should be actively working toward to ensure agents are taking proper care of sensitive information, and mitigating the potential for risks.

1. Securing the physical and digital environment

"Fast-paced and mobile-restricted environments, compliance mandates, shared workstations, and global workforces much of which is now remote, all make it challenging for call centers to efficiently and cost-effectively defend against security vulnerabilities. However, it's environments like these that are best suited for the authentication assurances offered by physical security keys.

With one device, call centers can meet the most stringent security requirements, while also allowing agents to move freely and securely between devices, workstations, and systems, and in this global climate, work remotely in a secure way without slowing down effectiveness." — **Guido Appenzeller**

This is likely the first, yet most integral step many organizations should take in safeguarding their remote agent experience. Without a properly secured system and strategy in place, agents will likely feel uncertain about handling and protecting customer data, especially from a remote setting.

Because of the lack of direct oversight, companies dealing with particularly sensitive data or regulations have largely resisted the remote work trend. COVID-19 has taken this choice away from them, heightening the current need to secure the remote environment. Nevertheless, these lessons apply in both remote and on-site locations to ensure the preservation of customer trust and regulatory compliance.

- **Ensure protected connectivity:** Ensure agents are connected to a secure network when accessing internal systems, and prohibit log-in or password sharing with family and friends on any device that holds sensitive company, client or customer data.

- **Stay off personal devices:** Discourage the use of personal laptops, mobile phones or drives whenever possible, as the use of these devices increases the risk of malware and data breaches.

- **Utilize webcam or screen-sharing capabilities:** When agents are dealing with particularly sensitive information, this will allow for a stronger monitoring of the physical environment, ensuring agents are working in a secured room where nobody is monitoring their screens or conversations.

- **Prohibit data sharing and duplicating:** Consider disabling printing capabilities, and prohibit the use of USB drives, so agents are unable to share sensitive customer information in any capacity.

- **Establish a cohesive strategy:** Set clear expectations and strategies around privacy, compliance and the physical remote workstation structure with agents. Employees are working through a wide range of environments and circumstances, from living with roommates, friends, families, and everything in between. Securing a remote agent's physical environment has its inherent limitations, but instilling awareness around the risks behind potential information-sharing is critical.

With these security measures in place, the burden can be taken off of individual agents, as they will feel more comfortable dealing with sensitive customer data from different environments knowing their platform is properly secured.

"[Enabling a secure remote access] involves the business empowering agents with secure access to all the systems they need so that their productivity isn't negatively impacted. Protecting agents from rising online threats so that they are protected, and so is their personal or corporate data, is critical to ensuring optimal agent effort and job satisfaction in these otherwise uncertain times." — **Abby Guha**

2. Empowering agents through training and awareness

The guaranteed security of more controlled digital and physical environments takes away much of the burden for individual agents, but it does not completely immunize customer and company data. Agents will still play a role in preventing fraud, online attacks and other data breaches, and it is important to prepare them for this responsibility.

Remote agents are working under much more independent circumstances. The luxury of simply walking over to a supervisor's desk and asking for help whenever something seems suspicious is no longer available for agents working from home. According to CCW Digital's New Standards in Customer Contact Performance Market Study, respondents noted that remote training limitations have negatively impacted work-from-home initiative success by 29%. Furthermore, a lack of real-time supervision and support has prevented 32% of respondents from achieving a more successful remote agent experience.

With more secured platforms, formalized training models can be much more impactful and scalable across both insourced contact centers and outsourced partners alike. Providing agents with training and instilling awareness around security protocols will help to optimize agent experience and boost confidence around handling sensitive information.

- **Provide remote agent training:** Offering security awareness training and certifications wherever necessary will continue to empower and motivate agents. Training doesn't have to be especially costly or time-consuming, and will go a long way in protecting customer data and brand loyalty.

- **Build a fundamental security awareness:** Guarantee all remote agents are operating with caution when opening external emails, websites, and links, or downloading content onto both personal and professional devices.

- **Succeed under continued support:** Assure remote agents that contact center leaders are available as a resource to ask questions and monitor calls to ensure that security protocols and regulations are understood and being followed.

3. Streamlining Agent Experience

With a secured network and environment, along with a properly trained workforce, the next step lies in ensuring your agents can seamlessly connect to customer data, both on-site and from a remote setting. Today's customers expect the brands they interact with to meet their needs and deliver on – or exceed – expectations.

Streamlining contact center systems and processes is the most efficient way to optimize agent time and deliver on these quality customer experiences. Below are a few ways to start implementing these processes:

- **Stay compliant:** Migrate to a universal agent platform that meets regulations and prevents the transfer of sensitive information from the digital platform environment onto other devices. This will provide a 360-degree view of the customer on a single screen, enhancing agent experience, transparency and productivity.

- **Set a clear data governance framework:** This is all about how your organization is handling the customer data being collected and, more specifically, managed within the contact center. Effective data governance will make it easier to monitor what is happening across the database, clarify what data is accessible to which agents, and therefore make more apparent any areas that pose a risk to contact center security.

- **Mitigate repetitive tasks:** Automating time-consuming and oftentimes tedious tasks will certainly help to optimize agent time, performance and productivity. CCW Digital's New Standards market study found that 39% of companies say their agents lack an integrated desktop for performing tasks across channels, negatively impacting overall customer contact performance. As a result of these inadequacies, over 34% of respondents are more heavily leveraging process automation in response to COVID-19 and the rise in remote work.

- **Leverage a continuously updated knowledge base:** Beyond agent training and awareness, implementing a contact center knowledge base will help to streamline agent efficiencies, acting as a continuous source for remote and on-site agents alike.

Taking these steps will effectively eliminate wasted time, helping to ensure that a better agent and customer experience will be delivered across the board.

"Typically, many agents are not the most sophisticated users of technology, especially the temporary seasonal workers. In these cases, the experience really matters, which then translates to productivity. Easy and fast ways to verify the agent before delivering them secure access to important systems is key to saving them time, which then translates to overall contact center productivity and customer retention." — **Abby Guha**

4. Adopting physical security keys: balance security with usability

Today's customers expect frictionless experiences and secured services, but a more secure experience doesn't necessarily mean a more time-consuming one. Assuring that remote agents are addressing customer needs and sentiment accordingly while still operating from a fully secured environment is truly a balancing act. Investing in the best-suited security solution for your remote agent workforce will guarantee stability in security and ease of use for agents and customers alike.

Providers like Yubico offer low-cost physical security keys, allowing organizations to achieve these benefits of implementing a secured environment, effectively training an agent workforce, and achieving a streamlined experience at scale. These solutions help to create a more seamless end-to-end agent experience, without compromising security.

- **Provide secure access every time:** Solutions like physical security keys deliver an easy and efficient way to ensure agent verification before allowing secured access to company systems and customer data. This will lead to an enhanced agent experience, and will increase customer loyalty, advocacy and retention.

- **Deliver a seamless experience every time:** Providing agents with the ability to safely access sensitive data without the hassle of remembering usernames, passwords, or security questions, all while eliminating the susceptibility of stolen passwords, will directly lead to increased productivity. This will ultimately optimize agent effort and experience, helping agents feel more empowered and in control from any location.

- **Deploy rapid security solutions at scale:** Remote work is here to stay. With remote and on-site agents accessing the same information from different locations, an effective and secure solution should be easily deployed at low cost and without reduction in agent productivity. Physical security keys provide this kind of convenience to the contact center.

"The future of modern authentication standards like WebAuthn is just beginning. With full support from all major browsers and platforms, now is the time for services and applications to adopt these technologies. Imagine call centers run without passwords, identities proven with just the touch of a finger, and the elimination of account takeovers. These are the types of experiences that can transform the customer service industry at scale, and are now available to the world." — **Stina Ehrensvärd**

About the Author

Amanda Caparelli, Research Development Analyst and Digital Writer, Customer Management Practice

Amanda Caparelli is a research development analyst, digital writer and content producer for CCW Digital and D&I Global, the global online communities and research hubs for Customer Contact and Design & Innovation professionals, respectively. In her current role, Amanda writes articles and reports, produces and speaks on webinars and online events, and contributes to event content creation. She is responsible for the production of meaningful content within the customer experience, consumer behavior, service design, UI/UX, brand strategy, and human-centered design spaces to help bring customer insights to life through cutting-edge market research and content development.

Meet Our Analysts

Brian Cantor

Principal Analyst &
CCW Digital Director

Max Ribitzky

Principal Analyst,
Go-to-market Research

Sandy Ko

Senior Analyst &
Conference Director,
CCW Series

Michael DeJager

Principal Analyst & Divisional Director
Experience Design Series

Nadia Chaity

Senior Analyst, CCO Series

Amanda Caparelli

Research Development
Analyst, D&I Series

Get Involved

Ben McClymont

Business Development Director

E: Ben.McClymont@customermanagementpractice.com

P: 212 885 2662

Simon Copcutt

Head of Strategic Accounts

E: Simon.Copcutt@customermanagementpractice.com

P: 212 885 2771

Upcoming Events

MAY

CCW Virtual Executive Exchange
May 13-15, 2020

New Standards for Contact Center Performance

May 19-22, 2020

https://www.customercontactweekdigital.com/events-new-standards-for-customer-contact-performance

JUNE

CCW Virtual Executive Exchange
June 23-25, 2020

JULY

Chief Experience Officer Exchange Denver
July 27-29, 2020
Denver, CO
https://www.customercontactweekdigital.com/events-cxoexchange/?mac=CMIQ_Events_Title_Listing

AUGUST

CCW Executive Exchange St. Louis
August 16-18, 2020
St. Louis, MO

https://www.customercontactweekdigital.com/events-ccwexecutiveexchange/?mac=CMIQ_Events_Title_Listing

CCW Vegas
August 24-28, 2020
Caesar's Forum, Las Vegas

https://www.customercontactweekdigital.com/events-customercontactweek/srspricing?mac=CMIQ_Events_Register_Listing#/

SEPTEMBER

Design Thinking
September 8-11, 2020
Hilton Austin, TX

https://www.designinnovationglobal.com/events-design-thinking/srspricing#/

CX Trends, Challenges,& Innovation
September 22-24, 2020

https://www.customercontactweekdigital.com/events-customer-experience-trends-challenges-innovations/

OCTOBER

CCW Executive Exchange
October 6-8, 2020
Bonaventure Resort & Spa, Miami Metro, FL

https://www.customercontactweekdigital.com/events-ccwexchangeusa