VIRTUAL ASSISTANTS ENTER THE OFFICE

Trending Topics summarizes news, information and perspective on matters affecting businesses and business leaders today. This insight is being provided to keep you up to date on the latest developments and trends influencing these topics. These views do not necessarily represent the views and opinions of PNC. For additional research on these topics, please consult the sources cited in this article.

The number of Amazon Alexa devices being used in homes is predicted to reach 128 million by 2020.[1] Researchers estimate Amazon could gain more than $10 billion in revenues from voice-activated internet sales over that same time period.

The popularity of virtual assistants (VAs) in the home has spurred technology companies to create voice-activated devices for workplace environments. These devices ease interactions with physical workspaces, technology tools and company applications to handle a wide range of office tasks such as managing meeting rooms, starting video conferences and merging calendars.[2]

Although workplace applications are still relatively new, at least 19% of global organizations are already using VAs and 46% expect to have them in the office by 2022.[3] The field of office VA candidates includes Amazon's Alexa for Business, Alphabet's Google, Apple's Siri and Microsoft's Cortana. Even Staples has the Digital Easy Button with voice interface for ordering office supplies and managing business accounts on the Staples Easy System.[4]

While the popularity of VA devices is spurring their adoption in the workplace, many IT executives are concerned about the security and privacy risks they create for companies.

Werner Vogels, Amazon's chief technology officer, believes voice interface was the game-changer for VA devices, both at home and in the workplace. Using one's voice to make requests is the most natural way to interact with technology. It is instinctive, spontaneous and requires no knowledge of complex interface systems.[5] Users appreciate the ease, convenience and value of using VA devices.

Office VAs are Internet of Things (IoT) devices with voice activation. They can interact with many corporate network applications such as conferencing and phone systems, customer relationship management (CRM) software, and travel and expense reporting and systems. As more IoT applications and custom corporate programs using voice interface are created, office VAs will be at the hub of linking employees and customers to new workplace technology.

SECURITY CONCERNS

While the popularity of VA devices is spurring their adoption in the workplace, many IT executives are concerned about the security and privacy risks they create for companies. Voice activation adds another layer of concern for cybersecurity risks.

Like any IoT device with a microphone, VA devices are always on and listening. Audio recordings of private or sensitive information can be transmitted through them, either inadvertently or for malicious intent. VAs can record conversations as long as the power source is on and even if the microphone is turned off.[6] Developers are working to create security protocols to overcome these concerns.

PNC

These smart devices can make life easier and more efficient, but employees must be vigilant to protect personal, corporate and customer data when using VA devices in the workplace.

Many companies are developing their own security standards and protocols for office VA use.[7] Companies with existing security policies for IoT devices are adding controls and protocols specifically for VA devices. For example, VA devices should not be located in areas where sensitive conversations are held or private information is verbally shared.

As VAs become more commonplace and personalized to the user, some employees may bring their own VAs to work. When employees began bringing their smartphones to work, companies had to develop "BYOD" smartphone policies, and so "BYOD" VA policies will likely follow suit.

Raising employee awareness of the potential privacy and security risks that VA devices present will be an important part of corporate VA security policies and training. These smart devices can make life easier and more efficient, but employees must be vigilant to protect personal, corporate and customer data when using VA devices in the workplace.

To discuss these topics in more detail, please contact your PNC Relationship Manager.

1 "Amazon Plans to Send Alexa to the Office," by Jay Greene and Laura Stevens, *The Wall Street Journal*, Nov. 29, 2017. Available at: https://www.wsj.com/articles/amazon-plans-to-send-alexa-to-the-office-1512008730

2 "Unlocking Enterprise systems using voice," by Werner Vogels, All Things Distributed blog, March 12, 2018. Available at: https://www.allthingsdistributed.com/2018/03/unlocking-enterprise-systems-using-voice.html

3 "5 ways to keep virtual assistants from sharing your company's secrets," by James A. Martin, CIO blog, April 19, 2017. Available at: https://www.cio.com/article/3190912/security/5-ways-to-keep-virtual-assistants-from-sharing-your-companys-secrets.html

4 "Staples Easy Button gets IoT makeover," by Dave Michels, Network World, Aug, 28. 2017. Available at: https://www.networkworld.com/article/3219711/internet-of-things/staples-easy-button-gets-iot-makeover.html

5 "Unlocking Enterprise systems using voice," by Werner Vogels, All Things Distributed blog, March 12, 2018. Available at: https://www.allthingsdistributed.com/2018/03/unlocking-enterprise-systems-using-voice.html

6 "5 ways to keep virtual assistants from sharing your company's secrets," by James A. Martin, CIO blog, April 19, 2017. Available at: https://www.cio.com/article/3190912/security/5-ways-to-keep-virtual-assistants-from-sharing-your-companys-secrets.html

7 "5 ways to keep virtual assistants from sharing your company's secrets," by James A. Martin, CIO blog, April 19, 2017. Available at: https://www.cio.com/article/3190912/security/5-ways-to-keep-virtual-assistants-from-sharing-your-companys-secrets.html

PNC is a registered mark of The PNC Financial Services Group, Inc. ("PNC").

The article you read was prepared for general information purposes only and is not intended as legal, tax or accounting advice or as recommendations to engage in any specific transaction, including with respect to any securities of PNC, and do not purport to be comprehensive. Under no circumstances should any information contained in this article be used or considered as an offer or commitment, or a solicitation of an offer or commitment, to participate in any particular transaction or strategy. Any reliance upon any such information is solely and exclusively at your own risk. Please consult your own counsel, accountant or other advisor regarding your specific situation. Neither PNC Bank nor any other subsidiary of The PNC Financial Services Group, Inc. will be responsible for any consequences of reliance upon any opinion or statement contained here, or any omission. The opinions expressed in this article are not necessarily the opinions of PNC Bank or any of its affiliates, directors, officers or employees.

©2018 The PNC Financial Services Group, Inc. All rights reserved.

CIB ENT PDF 0318-0253-777403